

МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ  
имени М. В. Ломоносова  
Ю р и д и ч е с к и й   ф а к у л ь т е т

В. А. Северин

# КОММЕРЧЕСКАЯ ТАЙНА В РОССИИ



Москва  
Зерцало-М  
2009

Рецензенты:

*Андреаса Любовь Васильевна*, доктор юридических наук, профессор кафедры предпринимательского (хозяйственного) права Московской государственной юридической академии

*Бачило Иллария Лаврентьевна*, заслуженный юрист Российской Федерации, доктор юридических наук, профессор, академик Международной академии информатизации, заведующая сектором информационного права Института государства и права РАН

*Зенин Иван Александрович*, заслуженный профессор Московского университета, доктор юридических наук, профессор кафедры гражданского права юридического факультета МГУ им. М.В. Ломоносова

*Лопатин Владимир Николаевич*, доктор юридических наук, профессор, директор Республиканского НИИ интеллектуальной собственности

## ПРЕДИСЛОВИЕ

Решение задач по углублению и расширению рыночных отношений, реализации стратегии инновационного прорыва в экономике России, повышению конкурентоспособности российских товаропроизводителей требует рационального использования и защиты информации технического, технологического и делового характера, активно влияющей на рост новых технологий и развитие товарного рынка.

Предлагаемая читателю книга представляет собой фундаментальный труд, содержащий комплексное научное учение о коммерчески значимой информации и ее защите. В ней впервые в отечественной практике представлена концепция гражданско-правового регулирования обращения такой информации и охраны ее конфиденциальности в сфере предпринимательской деятельности, отражающая вектор развития государственной политики, направленной на приоритетное развитие информационных технологий в процессе модернизации экономики, создания эффективной правовой основы для защиты интеллектуальной собственности и предотвращения правонарушений, совершаемых в этой сфере. Полученные выводы имеют значение для достижения целей правовой защиты информации информационной сферы бизнеса, и, соответственно, обеспечения одного из ключевых направлений информационной безопасности страны.

Комплексный подход к определению направлений исследования позволил автору предложить обоснованный вариант решения задачи защиты экономических интересов предпринимателей с использованием правового института коммерческой тайны. Результаты исследования по многим аспектам доведены до уровня разработок и рекомендаций и могут быть использованы в правоприменительной и

законодательной деятельности, в учебном процессе по гражданскому, коммерческому и информационному праву, по вопросам обеспечения информационной безопасности фирм и корпоративных образований.

*Ректор МГУ им. М.В. Ломоносова,  
академик РАН*

*В.А. Садовничий*

*Директор Института проблем информационной безопасности  
МГУ им. М.В. Ломоносова,*

*член-корреспондент Академии криптографии РФ*

*В.П. Шерстюк*

*Декан юридического факультета МГУ им. М.В. Ломоносова,*

*доктор юридических наук, профессор*

*А.К. Голицынов*

## СОДЕРЖАНИЕ

Предисловие.....	III
Введение .....	1
Глава 1. Теоретические основы правового института коммерческой тайны в России .....	8
§ 1. Теоретико-методологические и историко-правовые проблемы охраны коммерческой тайны в России .....	8
§ 2. Понятие коммерчески значимой информации и сущность ее обращения в рыночной экономике .....	38
§ 3. Опыт правового регулирования информации с ограниченным доступом в советский период.....	57
§ 4. Современное законодательство о коммерческой тайне .....	76
Глава 2. Использование правовых средств при обращении коммерчески значимой информации .....	106
§ 1. Понятие правовых средств и их применение при обращении коммерчески значимой информации .....	106
§ 2. Роль норм трудового права в регулировании обращения коммерчески значимой информации.....	128
§ 3. Гражданско-правовое регулирование обращения коммерчески значимой информации .....	156
§ 4. Формирование договорных условий об охране конфиденциальности информации .....	180
Глава 3. Организационное обеспечение деятельности по охране конфиденциальности информации .....	218
§ 1. Угрозы интересам коммерческой организации и основные параметры построения системы ее безопасности.....	218

§ 2. Опыт защиты секретной информации в советский период .....	234
§ 3. Осуществление организацией права на установление режима коммерческой тайны.....	250
§ 4. Методология и методика определения степени конфиденциальности коммерчески значимой информации .....	272
§ 5. Система мер по установлению режима коммерческой тайны .....	297
Глава 4. Правовое обеспечение деятельности по охране конфиденциальности информации .....	317
§ 1. Характеристика нарушений режима конфиденциальности информации и каналов ее возможной утечки .....	317
§ 2. Причины и обстоятельства, способствующие нарушениям режима конфиденциальности информации .....	334
§ 3. Характеристика лиц, допускающих нарушения в сфере обращения коммерчески значимой информации .....	354
§ 4. Предупреждение правонарушений в сфере обращения коммерчески значимой информации .....	373
Глава 5. Научно-методическое обеспечение деятельности по охране конфиденциальности информации .....	408
§ 1. Система и методы контроля в сфере обращения коммерчески значимой информации .....	408
§ 2. Организация и методика аналитических исследований в сфере обращения коммерчески значимой информации .....	430

## **ВВЕДЕНИЕ**

В результате произошедших в России в последние два десятилетия фундаментальных изменений в области экономических отношений в полной мере встал вопрос об эффективной защите коммерческими организациями в новой обстановке своих частных интересов в области коммерческой тайны. С упрочением позиций науки частного права, определившей основную часть правовых основ рыночной экономики, все более отчетливо проявляется тенденция усиления внимания ученых к исследованию в качестве самостоятельной проблемы коммерчески значимой информации (КЗИ), разработке ключевых аспектов становления и развития правового института коммерческой тайны и формированию теории правового регулирования обращения КЗИ и охраны ее конфиденциальности.

Длительное отсутствие в стране надлежащего законодательства и недочеты действующего Закона о коммерческой тайне от 29 июля 2004 г. (в редакции федерального закона от 18 декабря 2006 г. № 231-ФЗ) привели к накоплению большого числа нерешенных проблем, возникновение которых объясняется сложным комплексом взаимосвязей государственных и частных интересов, касающихся использования и охраны конфиденциальности информации производственно-технического и коммерческого характера, включая интересы отечественных и иностранных партнеров и конкурентов. Подобная тенденция в определенной мере сохраняется и после введения в действие названного Закона, вступления в силу нового базового Закона об информации, информационных технологиях и о защите информации от 27 июля 2006 г. № 149-ФЗ и части четвертой Гражданского кодекса Российской Федерации (далее — ГК РФ) от 18 декабря 2006 г. № 230-ФЗ, существенно укрепивших правовую базу рыночных отношений, в частности, закрепившую за владельце-

лем исключительное право на секрет производства (ноу-хау) и его защиту с использованием режима коммерческой тайны.

Развитие рыночного хозяйства затрудняет известная острота цивилизации в подходе к выделению отдельных проблем, обладающих высокой актуальностью, что влечет появление публикаций, не выходящих подчас далее комментариев к положениям Закона о коммерческой тайне без научного анализа использования организациями правовых возможностей для защиты КЗИ в процессе ее обращения. Нельзя также не заметить, что принципы обеспечения национальной безопасности сформулированы в Доктрине информационной безопасности Российской Федерации без должного учета частных интересов предпринимателей, которые оказались перед лицом многих вызовов и угроз их бизнесу. Показательно, что среди различных форм недобросовестной конкуренции особое место занимает противоправное завладение производственными и коммерческими секретами в целях последующего несанкционированного их использования при производстве и реализации продукции, выполнении работ и оказании услуг. Правонарушения, совершаемые в сфере обращения КЗИ, реально наносят значительный ущерб экономике. На практике происходит явная недооценка вредных последствий, причиняемых этими правонарушениями экономическим интересам организаций. Упущения и недостатки в борьбе с этими нарушениями связаны с тем, что значительное их число не попадает в поле зрения правоохранительных структур, в том числе в коммерческих организациях. Материальный ущерб, причиняемый такими нарушениями, в должной мере не возмещается.

Одной из наиболее существенных причин такого рода явлений, как представляется, выступает то, что в условиях разгосударствления экономики, расширения внешнеэкономических связей и самостоятельного ведения предпринимательской деятельности малый и средний бизнес в силу объективных и субъективных причин практически оказался неспособным защищать свою КЗИ. Коммерческие организации лишились необходимой поддержки государства после разделение массива секретной информации на государственную и коммерческую тайны.

КЗИ приобрела в рыночной экономике огромную ценность как в прямом, так и переносном смысле. Ее доля потребления значительно выше всех традиционных продуктов интеллектуальной деятельности и иных видов информации с ограниченным доступом. Информация, обрабатываемая в организациях, «овеществляется» во всех факторах

общественного производства и составляет необходимый и обязательный элемент деятельности по производству и реализации товаров (работ, услуг). КЗИ способствует наращиванию объемов товарооборота, развитию товарного рынка и ускорению процессов оборота торгового капитала. Учитывая важность КЗИ для ведения бизнеса, укрепления экономики страны, в ее охране заинтересованы не только субъекты коммерческой деятельности, но и государство в целом. Между тем используемые организациями силы и средства не отвечают возросшим требованиям защиты КЗИ, новым формам промышленного шпионажа, осуществляемого конкурентами как на внутригосударственном, так и международном уровне.

Учитывая высокие темпы развития информатизации, значительно возросшую «цену» ущерба, причиняемого организациям в связи с неправомерным использованием, разглашением (утечкой) КЗИ и невыполнением договорных обязательств по поводу охраны такой информации, сокращение числа нарушений в сфере обращения КЗИ имеет не только серьезное правовое, но и большое экономическое значение, превращаясь, по существу, в общегосударственную проблему развития высокотехнологичной цивилизованной экономики России.

Следует отметить, что определенный опыт теоретического анализа вопросов правового регулирования КЗИ и охраны ее конфиденциальности в стране имеется. Эти проблемы в разное время в той или иной мере исследовались в работах многих ученых. Вопросы коммерческой тайны в основном рассматривались в пределах следующих проблем: формирования теоретико-методических основ защиты информации в информационных и телекоммуникационных системах от несанкционированного доступа (В.С. Анашин, В.А. Васенин, В.А. Герасименко, А.А. Грушо, П.Д. Зегжда, А.А. Малюк, В.Б. Краваченко, В.А. Носов, Э.А. Применко, В.И. Ярочкин, В.В. Ященко и др.), обеспечения экономической безопасности фирм и корпоративных образований (Л.И. Абалкин, Н.П. Ващенко, Э.Я. Вольтнец-Руссет, М.А. Вус, Р.М. Гасанов, М.И. Дзлийев, М.В. Докучаев, М.И. Лугачев, П.С. Никулин, В.К. Сенчагов, М.К. Старовойтов, А.Д. Урсул, В.М. Чаплыгин, А.Г. Шаваев и др.), обеспечения информационной безопасности личности, общества и государства (Г.В. Емельянов, В.Н. Лопатин, В.А. Рубанов, В.А. Садовничий, А.А. Стрельцов, Д.С. Черешкин, В.П. Шерстюк и др.), исследования информации как объекта гражданских прав и гражданско-правовых способов ее защиты (В.М. Богданов, Ф.Н. Богашева, С.Н. Веретенникова, В.В. Зло-

бин, Е.В. Измайлова, А.В. Коломиец, И.И. Салихов, О.Ю. Сидорова, А.А. Снытников и др.), обоснования коммерческой тайны в составе нетрадиционных объектов интеллектуальной собственности (В.А. Дозорцев, А.П. Сергеев и др.) и правового режима защиты ноу-хау (И.А. Зенин, М.С. Зельцер, В.В. Погуляев, И.В. Строганова и др.) либо в рамках информационного права (И.Л. Бачило, Ю.М. Батурин, О.А. Гаврилов, О.А. Городов, В.А. Копылов, В.Н. Лопатин, М.М. Рассолов, М.А. Федоров и др.) и комплексного обеспечения безопасности информации (А.И. Алексенцев, Г.В. Виталиев, И.К. Корнеев, А.А. Левин, А.Ф. Мохов, Э.Я. Соловьев, Е.А. Степанов, А.А. Фатьянов, А.А. Шиверский и др.).

Признавая несомненные заслуги названных авторов в освещении вопросов коммерческой тайны, вместе с тем нельзя не заметить, что комплексных исследований данной проблематики не предпринималось, что обусловило наличие вполне объяснимых пробелов в теории и, как следствие, нерешенность значимой группы вопросов применения правовых средств в сфере обращения КЗИ, организационного, правового и научно-методического обеспечения деятельности по охране конфиденциальности информации. Поэтому разработка теоретических аспектов темы является актуальной в теоретическом плане. Не меньшую значимость она представляет и в практическом отношении. В пользу такого вывода свидетельствует включение проблем конфиденциальности и правовой защиты информации в число приоритетных направлений научных исследований в области информационной безопасности Российской Федерации, одобренных секцией по информационной безопасности Научного совета при Совете Безопасности Российской Федерации.

Предпринятое исследование позволило сформулировать научные положения и принципы, характеризующие особенности формирования и реализации механизмов правового регулирования обращения КЗИ и обеспечения охраны ее конфиденциальности. При исследовании данной проблемы, учитывая уникальный характер организации работы с документами ограниченного пользования в советский период, было признано необходимым изучение советского опыта и его использование применительно к условиям деятельности российских коммерческих организаций, с учетом дальнейшего совершенствования законодательства о коммерческой тайне. Названные обстоятельства предопределили содержательную направленность исследования, результаты которого составили основу настоящей монографии.

*Объектом настоящего исследования* являлся процесс становления и развития правового института коммерческой тайны, его роль и место в обеспечении охраны конфиденциальности информации в сфере частного права России.

В качестве предмета исследования выступали закономерности, определяющие основы теории, методологии, методики и технологии формирования и реализации механизмов правового регулирования коммерчески значимой информации и охраны ее конфиденциальности в гражданском (торговом) обороте.

*Целью исследования* являлась разработка научно обоснованных положений, выводов и рекомендаций, направленных на повышение эффективности механизма правового регулирования КЗИ, принципов и методов организационного, правового и научно-методического обеспечения деятельности по охране конфиденциальности информации, обрабатываемой в частных коммерческих организациях.

*Основными задачами* при этом выступали: разработка содержания правового института коммерческой тайны как составной части наук частного права, регулирующего КЗИ в сфере предпринимательства; определение сущности и форм проявления КЗИ в различных сферах гражданского (торгового) оборота при производстве и реализации товаров (работ, услуг), связанных с эволюцией законодательно-регулирующего КЗИ в России; изучение советского опыта правового регулирования отношений по поводу КЗИ и его использование для развития современного российского законодательства о коммерческой тайне; анализ применения правовых средств в сфере обращения КЗИ в рамках трудовых и гражданско-правовых, в том числе корпоративных, отношений, связанных с использованием информации и охраной ее конфиденциальности; характеристика организационного обеспечения деятельности по установлению режима коммерческой тайны на уровне отдельной организации; обоснование основных направлений, принципов и методов правового и научно-методического обеспечения деятельности по охране конфиденциальности информации.

*Основу методологии работы* составляет материалистическая диалектика, общенаучные методы, комплексный подход к изучаемым явлениям и процессам. Нормативной базой исследования являлись Конституция РФ, гражданское, торговое и информационное законодательство, иные правовые акты, касающиеся вопросов использования информации и обеспечения охраны ее конфиденциальности в сфере предпринимательства. В ходе исследования при-

менялись системный подход к изучению обращения КЗИ, конкретные исторические, сравнительно-правовой и социологические методы. Выводы и положения, содержащиеся в книге, основываются на материалах практики правового регулирования обращения КЗИ в организациях, анализе деятельности по охране конфиденциальности информации.

В теоретико-методологическом плане важную роль в раскрытии объекта и предмета исследования составили научные идеи и положения, содержащиеся в трудах ученых — Л.И. Абалкина, Г.А. Аванесова, С.А. Авакьяна, С.С. Алексеева, А.П. Алексина, Л.В. Андреевой, И.Л. Бачило, М.И. Брагинского, Ю.Е. Булатецкого, В.В. Витрянского, Б.В. Власова, Э.Я. Вольнец-Руссет, Э.П. Гаврилова, В.П. Грибанова, Е.П. Губина, К.Ф. Гуценко, И.К. Дмитриевой, В.А. Дозорцева, Г.В. Емельянова, А.Г. Здравомыслова, И.А. Зенина, В.Д. Камаева, И.И. Карпеца, Т.В. Кашаниной, Н.Г. Кобец, Н.В. Козловой, А.С. Комарова, В.С. Комиссарова, В.А. Копылова, Е.А. Кочерина, В.В. Крылова, В.Н. Кудрянцева, Н.Ф. Кузнецовой, Б.Н. Кузык, А.М. Куренного, В.Н. Лопатина, А.Л. Маковского, А.В. Малько, М.Н. Марченко, С.М. Меньшикова, С.Д. Могилевского, Б.И. Пугинского, В.В. Радаева, М.М. Рассолова, М.П. Ринга, М.Г. Розенберга, В.А. Рубанова, В.А. Садовниченко, М.А. Сажинной, Д.Н. Сафиуллина, В.К. Сенчагова, А.П. Сергеева, В.Н. Смирнова, А.Г. Спиркина, А.А. Стрельцова, Е.А. Суханова, Л.К. Терещенко, Ю.П. Титова, Ю.А. Тихомирова, М.К. Треушников, О.И. Чистякова, Ю.К. Толстого, В.А. Томсинова, А.Е. Шерстобитова, В.П. Шерстока, И.С. Шиткиной, С.А. Хохлова, Ю.В. Яковец, В.И. Ярочкина, В.Б. Ястребова, В.В. Ященко и др.<sup>1</sup>

Наряду с юридической литературой, относящейся к частному праву, в монографии использованы результаты научных разработок в области публичного права (конституционное, административное, уголовное и информационное право, криминология и др.), теории государства и права, истории отечественного государства и права, философии, экономики, управления, социологии, психологии, обеспечения экономической и информационной безопасности.

Исследовательские материалы, положенные в основу монографии, являются итогом многолетней работы автора в области науч-

ной, педагогической и хозяйственной деятельности, связанной с обращением информации и охраной ее конфиденциальности, в качестве исполнителя и руководителя ряда научно-исследовательских работ, начальника подразделения научно-производственного объединения, генерального директора юридической фирмы, преподавателя учебных дисциплин по правоведению, коммерческому праву, правовой и организационной защите информации.

В книге впервые разработан комплекс проблем правового регулирования обращения КЗИ и обеспечения деятельности по охране ее конфиденциальности как самостоятельное направление в науке частного права. Обобщение отечественного опыта позволило выявить сущность обращения КЗИ в рыночной экономике и правовые средства, которые используются в этом процессе, разработать научные и практические принципы и методы охраны конфиденциальности информации в современный период. Отличительной чертой исследования является его направленность на рассмотрение проблем правового регулирования обращения КЗИ и охраны ее конфиденциальности как единого, взаимосвязанного комплекса вопросов, характеризующих состояние и перспективы развития законодательного, корпоративного, договорного регулирования и использования иных правовых средств в сфере обращения КЗИ, организационного, правового и научно-методического обеспечения деятельности по охране конфиденциальности информации.

Автор, понимая сложность рассматриваемых в монографии проблем и небесспорность ряда предлагаемых путей их решения, выражает искреннюю признательность ученым и практикующим юристам, чьи критические замечания и оценки во многом помогли доработке этого труда и, прежде всего, заведующему кафедрой коммерческого права и основ правоведения юридического факультета МГУ им. М.В.Ломоносова, заслуженному юристу РФ, доктору юридических наук, профессору Б.И. Пугинскому.

<sup>1</sup> Настоящая работа выполнена при информационной поддержке компании «Консультант Плюс».



стороны, всемерного ограждения интересов отечественного бизнеса от нездоровой конкуренции, пресечения любых попыток незаконного заимствования информации субъектами хозяйственной деятельности. *Во-вторых*, экономическими интересами коммерческих организаций и индивидуальных предпринимателей, обусловленных объективными условиями рыночной экономики, конституционного признания и защиты частной формы собственности, осуществления предпринимательской деятельности, формирования конкурентной среды в сфере производства и реализации товаров, выполнения работ и оказания услуг, правовой режим которых устанавливается нормами гражданского и коммерческого права, и, соответственно, во многом определяющих перспективы развития института коммерческой тайны, являющегося их составной частью. Предпринятое исследование требует определения его границ и конкретизации методов изучения научного объекта.

Правовой институт коммерческой тайны, как объект настоящего исследования, выполняет в рыночной экономике две важнейшие функции — регулирует гражданский (торговый) оборот КЗИ и определяет пределы (границы) возможной и дозволенной деятельности организаций по применению правовых средств, связанной с защитой частных интересов на информацию.

Для выработки теоретических основ формирования механизма правового регулирования и обеспечения охраны коммерческой тайны используются методы<sup>1</sup>, применяемые в науках частного права, в том числе и публичного права, учитывая их познавательный потенциал. В частности, методы, применяемые при установлении режима коммерческой тайны и его обеспечении путем осуществления правоприменительной деятельности, носят комплексный характер и связаны с элементами корпоративного регулирования определения степени конфиденциальности информации, предупреждения причин и обстоятельств, способствующих совершению правонарушений в этой сфере. При этом не исключается в случае нарушения права организации на коммерческую тайну обращение в правоохранительные органы и суд. Это обстоятельство определяет методологию ис-

<sup>1</sup> См.: Философия науки. 3-е изд. / Под ред. С.А. Лебева. М., 2006. С. 163–273; Керимов Д.А. Общественная методология и методология права // Теоретико-методологические проблемы права. М., 2007. С. 12, и др.

## ГЛАВА 1

### Теоретические основы правового института коммерческой тайны в России

#### § 1. Теоретико-методологические и историко-правовые проблемы охраны коммерческой тайны в России

*Методологические проблемы исследования правового института коммерческой тайны.* Определение места и роли правового института коммерческой тайны в формировании механизма правового регулирования обращения коммерчески значимой информации (далее — КЗИ) и охраны ее конфиденциальности, на наш взгляд, в настоящее время следует рассматривать в качестве *самостоятельного*, причем одного из весьма важных, *направлений современной науки частного права*, достижения которой призваны активно содействовать утверждению цивилизованных форм рыночных отношений в нашей стране. Это обусловлено, *во-первых*, происходящей в России информационной революцией<sup>1</sup>, логика развития которой требует, с одной стороны, максимально полного использования в целях упрочения экономической базы государства новейших технологий, безотлагательного внедрения в социальную практику достижений передовой науки и позитивного опыта экономически грамотного хозяйствования, а с другой

<sup>1</sup> См.: Садовничий В.А. Обеспечение устойчивого развития мирового сообщества в XXI веке через образование и науку // Международная конференция 25 июня 2001 г. М.: МГУ. С. 9.

следования явлений и процессов в сфере обращения КЗИ, включающей различные по своему назначению и характеру методы.

Оценка результатов исследования в рассматриваемой сфере зависит от *правильного выбора и корректного использования научных методов*. Термин «метод», обозначающий в русском языке способ теоретического исследования или практического осуществления чего-нибудь, достаточно широко используется в юридической науке. В философском смысле слово «метод» — это комплекс интеллектуальных действий, с помощью которых наука предполагает установить истину, к которым она стремится. А.Г. Спиркин считает, что «метод — это система регулятивных принципов преобразующей, практической или познавательной, теоретической деятельности»<sup>1</sup>. С помощью методов наука доказывает либо опровергает эти истины. Иначе формулируют понятие «метод» Б.И. Пугинский и Д.Н. Сафуллин, по мнению которых, «научные методы представляют собой идеи особого рода. Они являются инструментарием, созданным для работы с конкретным, строго определенным эмпирическим материалом». Далее, авторы указывают, «... что выбор методов познания помимо технических возможностей определяется наиболее существенными свойствами познаваемого объекта»<sup>2</sup>. Содержательное понятие «метод» используется применительно к познанию различных явлений, изучаемых в рамках данного исследования. *Методика*, в отличие от понятия «метод», означает совокупность методов обучения чему-нибудь, практического выполнения чего-нибудь. Существенными для освещения темы исследования представляются методики: формирования договорных условий об охране конфиденциальности научно-исследовательских и опытно-конструкторских работ (НИОКР); создания системы мониторинга угроз информационной безопасности (ИБ) организаций; определения степени конфиденциальности КЗИ; выявления возможных каналов утечки (ВКУ) информации и изучения системы предупреждения нарушений при обращении КЗИ, которые могут быть использованы в практической деятельности.

<sup>1</sup> Спиркин А.Г. Философия. М., 2002. С. 452.

<sup>2</sup> Пугинский Б.И., Сафуллин Д.Н. Правовая экономика: проблемы становления. М., 1991. С. 25.

Каждый из используемых в исследованиях методов имеет бесспорное значение для применения в настоящей работе. При этом, однако, последовательно и неуклонно должна учитываться специфика предмета и объекта изучения. *Всеобщий философский метод познания* используется в познании существа любых явлений, происходящих в сфере обращения КЗИ. Основные категории философии отражают в нашей мысли универсальные законы объективного мира<sup>1</sup>, помогают осмыслить появление новой категории «коммерчески значимая информация» в науке гражданского и коммерческого права, в связи с изучением процессов правового регулирования обращения КЗИ и охраной ее конфиденциальности в рыночной экономике. Концептуальные положения о правовом регулировании отношений и использовании правовых средств в сфере обращения КЗИ, организационном и правовом обеспечении процесса установления режима и охраны конфиденциальности КЗИ базируются на философском понимании движения информации в пространстве и времени, о существовании диалектических противоречий, о связи и взаимодействии явлений, обуславливающих внутренние и внешние угрозы деятельности организации, о причинной связи явлений, ведущих к утечке КЗИ, обстоятельствах, способствующих нарушениям трудовых обязанностей или договорных обязательств при обращении КЗИ. Важное значение для формулирования теоретических положений, объясняющих существование в рыночных условиях категории «коммерчески значимая информация», имеет изучение философских категорий, таких, как: часть и целое, система, содержание, структура и форма, внутренняя и внешняя сторона обращения КЗИ (внутренняя и внешняя среда), причины и условия (обстоятельства), возможность, действительность и вероятность, качество, количество и мера и другие категории философии.

*Общественные методы* в силу своей общенаучности непосредственно связаны с всеобщим методом познания и расширяют границы исследования объекта, играют важную роль в соединении философских понятий и категорий с частнонаучными методами правоведения. Преломляясь, образно говоря, через общие философские методы, общественные методы оказывают влияние на формирование научной базы частнонаучных методов, позволяющих более конкретно раскрыть закономерности исследуемого объекта. Охарактеризуем те

<sup>1</sup> См.: Спиркин А.Г. Философия. М., 2002. С. 262–307.

методы, которые имеют непосредственную связь с направлениями данного исследования.

*Метод логического подхода.* Логика определяется как наука о мышлении, о закономерностях в связях и развитии мыслей. Сам процесс правильного логического мышления истолковывается как такая связь мыслей, которая дает возможность прийти к верному выводу в результате рассуждения и делает наши мысли, обреченные в материальную языковую оболочку, понятными и убедительными для других людей.

Логическое мышление означает, что оно подчинено определенным правилам, принципам и законам, по которым мысль движется к истине, от одной истины к другой, более глубокой! В.И. Ленин по этому поводу писал: «Чтобы действительно знать предмет, надо охватить, изучить все его стороны, все связи и «опосредования». Мы никогда не достигнем этого полностью, но требование всесторонности предостережет нас от ошибок и от омертвления. Это, во-первых. Во-вторых, диалектическая логика требует, чтобы брать предмет в его развитии, «самодвижении» (как говорил иногда Гегель), изменинии... В-третьих, вся человеческая практика должна войти в полное «определение» предмета и как критерий истины и как практический определитель связи предмета с тем, что нужно человеку. В-четвертых, диалектическая логика учит, что «абстрактной истины нет, истина всегда конкретна...»<sup>2</sup>. В процессе изучения явлений, имеющих отношение к сфере обращения КЗИ, мы имеем дело с такими логическими формами мыслей, как понятия, суждения и умозаключения, которые позволяют, например, выделить признаки, характеризующие категорию КЗИ, судить об эволюционном процессе правового регулирования КЗИ в России, формулировать выводы и рекомендации по результатам исследования на основании дедуктивного (от общего рассуждения информационной безопасности страны к частному, касающегося коммерческой безопасности) и индуктивного (выведение общего положения о состоянии обеспечения безопасности организации из ряда частных утверждений, касающихся охраны конфиденциальности информации, например, на этапе преддоговорных контактов) умозаключения.

<sup>1</sup> См.: Спиркин А.Г. Указ. соч. С. 440.

<sup>2</sup> Ленин В.И. Полн. собр. соч. Т. 42. С. 290.

*Метод формирования гипотез.* При формировании содержания программы аналитических исследований могут быть выдвинуты предположения о существовании ВКУ КЗИ на конкретных направлениях деятельности организации. Обоснование этого предположения потребует объяснения фактов совершения правонарушений в сфере обращения КЗИ, причин и обстоятельств, обусловивших невыполнение или ненадлежащее выполнение трудовых обязанностей либо гражданско-правовых обязательств. Процесс проверки гипотезы позволяет глубже осмыслить объект и конкретный предмет, и сформулировать нетрадиционные варианты решения проблем обеспечения безопасности организации.

*Метод наблюдения* в философском понимании представляет собой преднамеренное, планомерное восприятие, осуществляемое с целью выявить существенные свойства и отношения объекта познания! Наблюдатель, в роли которого выступает исследователь, фиксирует вполне определенное поведение работников, занятых в сфере обращения КЗИ. Различают невключенное (сторонний наблюдатель) и включенное (наблюдатель является участником трудового коллектива либо коммерческой сделки) наблюдение. Метод наблюдения предполагает не только сбор информации о явлениях в сфере обращения КЗИ, но и объяснение событий. Применение этого метода позволяет получить исходные эмпирические данные для разработки теоретических положений и практических рекомендаций.

*Метод сравнительного правоведения* основан на изучении и использовании правового регулирования сходных отношений. Теоретические обобщения исследования основаны на сравнении различия и сходства предметов, относящихся к изучаемому объекту в системе частного права. Сравнение правовых норм носит всегда в правовой системе конкретно-исторический характер<sup>2</sup>, что использовано при характеристике эволюционного процесса формирования законодательства о коммерческой тайне. Применение этого метода позволило получить характеристику сходства и различия сравнимых отдельных элементов изучаемого объекта в рамках корпоративных, трудовых и гражданско-правовых отношений в сфере обращения КЗИ и охраны ее конфиденциальности.

<sup>1</sup> См.: Спиркин А.Г. Указ. соч. С. 435.

<sup>2</sup> См.: Гражданское право. Т. 1 / Отв. ред. проф. Е.А. Суханов. М., 2000. С. 50.

*Метод аналогии* исходит из философского принципа, что новое может быть понято через образы старого. Осмысление процесса охраны конфиденциальной информации в современный период основывалось на определении его сходства с защитой государственных секретов в советское время по конкретным однопорядковым признакам при соблюдении конкретно-исторического подхода. Применение *метода анализа и синтеза* имело определяющее значение для раскрытия сущности и основных форм развития изучаемого объекта в гражданском обороте информации, группировки проблем, подлежащих исследованию, по их значению и взаимосвязям, систематизации по признакам и проведения типологизации. Источником познания явлений, происходящих при обращении КЗИ, служат накопленные знания и практика правового, организационного и методического обеспечения безопасности организаций. Отсюда вытекают определение сущности анализа и синтеза как приемов мышления, состоящих в комплексе, органически взаимосвязанном изучении фактов, событий и явлений, связанных с проблемами охраны КЗИ; выявлении ВКУ КЗИ, причин и обстоятельности, способствующих утечке такой информации, и мерах по их предупреждению. Анализ и синтез может быть представлен и как вид практической деятельности организации, связанный с необходимостью обеспечения работы службы безопасности, и поэтому является основной частью аналитической работы.

Применение *метода эксперимента* имеет существенное значение для практической проверки чистоты и основных результатов научного исследования. В этом плане он является необходимым элементом системы научного познания, выполняющая важную прогнозную функцию. Производство экспериментов необходимо тогда, когда: *во-первых*, целесообразность и эффективность того или иного режима мероприятия, связанного с прогнозированием, нельзя обосновать с помощью иных методов; *во-вторых*, невозможно научно предсказать какие-либо конкретные результаты решения прогнозируемых проблем в сфере обеспечения безопасности организации, так как научное предвидение объясняет, как правило, лишь общие направления и характер этих результатов.

Эксперимент позволяет подтвердить выдвинутую гипотезу и служит источником фактического материала, дает возможность перейти от гипотезы к теории, а от теории — к практике, к выработке научно обоснованных рекомендаций по предупреждению утечки КЗИ. Эксперимент выступает, с одной стороны, как способ проверки, напри-

мер, установленного в организации режима коммерческой тайны, а с другой — как инструмент, способствующий поиску новых правовых средств, направленных на обеспечение эффективности деятельности по охране КЗИ.

Общепризнанным является факт проникновения математики во многие отрасли знания, в том числе и гуманитарные. *Математические методы* широко используются при исследовании социальных явлений. Высказанное К. Марксом положение о том, что «наука только тогда достигнет совершенства, когда ей удастся пользоваться математикой»<sup>1</sup>, не потеряло своей актуальности в современном периоде. В этой связи следует подчеркнуть, что криминологическая наука, например, обнаруживает тенденции к переходу от чисто качественного анализа к количественно-математическому. Это, впрочем, характерно сегодня, хотя и в меньшей степени, для других юридических наук, включая науку частного права. Математические формулы выражают не только количественные отношения действительности, но и улавливают качественную сторону объекта исследования. Математические методы использованы при разработке методик определения степени конфиденциальности информации, выявления ВКУ информации и изучения системы предупреждения нарушений в сфере обращения КЗИ, а также для обоснования расчетов, подтверждения тенденции развития того или иного явления. Математический аппарат может быть использован при проведении расчета данных о вероятности возникновения угроз организации, моделирования ВКУ КЗИ и решения других задач в рамках создания автоматизированной системы управления режимным обеспечением работ, выполняемых с использованием КЗИ.

Данные *кибернетики*, исследующей различные системы живой природы и автоматические системы, созданные человеком, а также изучающей законы управления в любых системах, в том числе и социальных, используются в данном исследовании. Задача заключается в изучении возможностей использования кибернетических методов при выявлении угроз организации, планировании мер по охране КЗИ и других, которые использовались, например, при разработке экспертных систем в области правосудия и законотворчества.

В исследовании широко использованы *частнонаучные методы*, которые позволили получить данные о проблемах конфиденциаль-

<sup>1</sup> См.: Лафарг П. Воспоминания о Марксе. М., 1958. С. 10.

ности информации в гражданском обороте с использованием правовых средств, о существовании ВКУ КЗИ, причин и обстоятельств, их обуславливающих, а также об эффективности принимаемых мер защиты. Наиболее характерными в этой группе являются методы, которые чаще всего применялись для решения задач исследования.

*Письменный и устный опрос* достаточно часто используется для сбора эмпирических материалов. Опрос, как выборочный метод сбора социально-правовой информации в сфере обращения КЗИ, проводился в виде *анкетирования*, представляющего собой сбор сведений об имеющихся недостатках в работе, связанном с корпоративным регулированием обращения КЗИ, формированием контрагентами доверительных условий о конфиденциальности информации, принятием адекватных мер угрозам безопасности организации. При этом использовались различные формы сбора сведений, в основном в виде устного опроса и заполнения анкет.

*Анализ документов* — один из широко используемых и эффективных методов, который применялся для сбора первичной информации о состоянии дел в сфере обращения КЗИ и охраны ее конфиденциальности. Анализировались документы на традиционном (бумажном) носителе и электронные документы, официальные и неофициальные, письменные и статические и другие в зависимости от возможности доступа к ним, их целостности и легитимности.

Кроме того, использовался и *метод экспертных оценок*, который позволил учесть мнение специалистов по определенному кругу вопросов. Экспертами являлись руководители организаций и менеджеры, хорошо знающие проблемы безопасности коммерческих структур. Экспертам были заданы следующие вопросы: каково состояние охраны коммерческой тайны в организации, какова величина латентности (т.е. нераскрытых, неизвестных администрации нарушений) в сфере обращения КЗИ, каковы причины нарушений в этой сфере, какие меры следует предпринять по закрытию ВКУ КЗИ. В отличие от опроса информация, полученная от экспертов, носила концептуальный, а не эмпирический характер, поэтому была менее детализированной.

Итак, каждый из рассмотренных методов выполняет свою определенную роль и не может быть абсолютизирован. Поэтому необходимо комплексное их использование. Следование этому требованию позволило повысить уровень достоверности результатов исследования.

**Историко-правовые аспекты охраны коммерческой тайны в России** до настоящего времени не являлись предметом отдельного исследования. Исторический подход к изучению данной проблемы позволил установить зависимость содержания деятельности хозяйствующих субъектов от особенностей экономического строя и политической обстановки в стране и действия ряда других факторов, обновать необходимость введения в научный оборот правовой категории «коммерчески значимая информация», являющейся предметом правового регулирования института коммерческой тайны, и определить состояние и тенденции развития законодательства в этой сфере общественных отношений.

*Эволюционный характер формирования товарно-денежных отношений и утверждение частной собственности оказали влияние на степень урегулирования правом КЗИ в исторической ретроспективе.* При анализе проблемы эволюции этапов формирования института коммерческой тайны, на наш взгляд, необходимо учитывать явления и процессы, которые обуславливали специфику различных периодов экономического поведения субъектов хозяйственной деятельности.

*Во-первых*, это влияние «формационного» и «цивилизационного» подходов, объясняющих эволюционный характер общества в зависимости от конкретного способа производства и культурного развития, определяющих саму возможность возникновения института коммерческой тайны в силу появления товарно-денежных отношений и признания государством частной собственности (главный критерий).

*Во-вторых*, это влияние последствий научно-технической и информационной, торговой революций на содержание форм и методов защиты КЗИ.

*В-третьих*, это влияние экономической и политической обстановки в стране на развитие рыночных условий хозяйства (поощрение конкуренции, необратимость процессов приватизации, гарантии защиты частной собственности и др.), на правовую оценку нарушений в области защиты КЗИ (эффективность мер ответственности за нарушение договорных обязательств, разглашение КЗИ и др.).

*В-четвертых*, это влияние хозяйственной ситуации, сложившейся в организации, т.е. внутренних и внешних, объективных и субъективных обстоятельств, обуславливающих прибыльность либо убыточность деятельности, на формирование условий, обеспечивающих закрепление гражданских прав на КЗИ, их самозащиту и реализацию мер оперативного воздействия на нарушителей.

Названные критерии носят производный характер от общей периодизации исторического процесса развития нашего государства.

Процесс формирования и развития правового института коммерческой тайны, его законодательной базы, определяющей рамки возможного и дозволенного поведения субъектов гражданского права при выборе правовых механизмов исполнения и защиты КЗИ и обеспечения баланса частных и публичных интересов, исторически включает этапы, характерные для периодизации истории государства и права России<sup>1</sup>.

**На первом этапе** с момента возникновения феодального государства и права до крестьянской реформы (IX в. — 1861 г.) выделяется несколько периодов, предшествовавших появлению КЗИ. **Первый период** характеризуется ведением общинного натурального хозяйства, основанного на коллективной форме собственности, и образованием крупной церковной, княжеской и боярской собственности<sup>2</sup>. Для этого периода характерны межгосударственные торговые отношения Киевской Руси с Византией и другими государствами<sup>3</sup>. Договоры содержали условия, позволявшие сторонам защищать свои национальные интересы (государственная тайна). Внутри государства между представителями различных слоев населения заключались договоры с участием торговцев и ремесленников, предусматривавшие условия по защите торговых и профессиональных секретов. При согласовании условий договора купли-продажи кушпы, ростовщики, мастеровые люди пользовались информацией, содержащейся в торговых книгах, где отражались их деятельность и материальное положение. Тайна торговых книг охранялась законом<sup>4</sup>. Торговой тайной считались знание мест закупки товаров, списки покупателей и др. информация.

**Второй период** характеризуется разделением труда с его последующей кооперацией, использованием ремесленной техники, возникновением мануфактурного производства и появлением понятия

<sup>1</sup> См.: История государства и права России: Учебник / Под ред. Ю.П. Титова. М., 2004. С. 7–11, и др.

<sup>2</sup> См.: Семенникова Л.И. Россия в мировом сообществе цивилизаций. М., 2003. С. 64–65, 178, 255, и др.

<sup>3</sup> См.: Карамзин Н.М. История государства Российского. М., 2005. С. 48–56, 83–88, 991–1015, и др.

<sup>4</sup> См.: Розенберг В. Промысловая тайна. СПб., 1910. С. 10–24.

«промысловой тайны»<sup>1</sup>, позволявшей промышленникам защищать свои имущественные интересы. Во времена «петровской модернизации» значение «промысловой тайны» возрастает в связи с распространением частной собственности, рыночных отношений и постепенным переходом от мануфактурного к фабрично-заводскому, индустриальному производству.

**Третий период** ознаменован началом промышленного переворота в России (30–40-е годы XIX в.), ростом крупных предприятий и возникновением конкуренции, переходом от мануфактуры к фабрике, появлением понятия «фабричной тайны». Начиная с этого периода, как правильно отмечает Р.М. Гасанов<sup>2</sup>, коммерческие тайны начали приносить деньги, которые давали торговцам и банкирам власть, подпачивая устои феодализма.

**На втором этапе** в период утверждения и развития капитализма в России (1861–1917 гг.) происходит постепенное понимание того, что использование КЗИ является важным средством увеличения прибыли предприятий, служит защитой их частных интересов и требует адекватной правовой охраны. Реформы, проведенные в этот период, способствовали развитию частной собственности в промышленности и других сферах, активному расширению рыночных отношений, созданию акционерных обществ, усилению процессов монополизации в экономике. Россия к концу XIX в. вплотную подошла к стадии индустриального общества<sup>3</sup>. Законодательство того времени адекватно реагировало на обострившиеся конкурентные отношения в экономике. «Промысловая тайна» была введена в рыночный оборот как средство защиты предпринимателей от недобросовестной конкуренции: всякое ее нарушение вызывало правовое реагирование со стороны лиц, чье право было нарушено. Понятие «промысловая тайна» прочно утвердилось в законодательных актах Российской империи и включало в себя различные виды промышленной, или фабричной, тайны, тайны коммерческой, т.е. тайны торговой<sup>4</sup>. Под промышленной тайной понималось привнесение чего-либо нового в процесс создания благ: фабричным секретом считался не только предмет па-

<sup>1</sup> См.: Дозорцев В.А. Вестник Высшего Арбитражного Суда Российской Федерации. 2001. № 7. С. 99–113.

<sup>2</sup> См.: Гасанов Р.М. Шпионаж особого рода. М., 1989. С. 29–35.

<sup>3</sup> См.: Семенникова Л.И. Указ. соч. С. 280–391.

<sup>4</sup> См.: Розенберг В. Указ. соч. С. 12–15.

тента, но и всякая особенность производства. Торговая тайна включала элементы индивидуальности, исключительности ведения торговли (например, знание мест закупки товаров и др.), т.е. свойственные данному предприятию особенности, индивидуальные детали его коммерческой деятельности. Правовую охрану тайны, не связанной с «телесным предметом», В. Розенберг<sup>1</sup> считал одной из труднейших проблем законодательства того времени. Нужно сказать, что эта проблема осталась нерешенной и в начале XXI в. Правовая наука того времени не признавала абсолютного характера соблюдения промышленных тайн. Аналогичной точки зрения придерживаются современные исследователи (И.А. Зенин и др.), дополняя указанием на фактическое монопольное обладание коммерческой тайной. Таким образом, рассмотренные виды промысловой тайны защищали от разглашения техническую, технологическую и деловую информацию, имевшую коммерческую значимость для предпринимателей. По существу, указанные понятия стали исходной базой для модифицированного формулирования некоторых признаков, определяющих современное понятие «коммерческая тайна», содержащееся в ФЗ «О коммерческой тайне», и явились основанием для определения термина КЗИ, более объемного по своему содержанию и широте применения в гражданском обороте, чем понятие «коммерческая тайна».

**На третьем этапе** в период существования Советского государства (1917–1991 гг.), была уничтожена частная собственность и значительно ослаблены товарно-денежные отношения<sup>2</sup>, что привело к видоизменению «промысловой тайны» и превращению ее в «государственную» и «служебную» тайну с приобретением новых функций по защите государственных интересов на уровне предприятий. Изменение формы (внешнего названия правового института) тайны частично отразилось и на ее содержании. Промышленные (фабричные) тайны по-прежнему были востребованы государством. Это объясняется тем, что наращивание экономической мощи, производство более совершенных товаров, правда, в основном для нужд обороны и безопасности, не могли обойтись без использования новых технологий и техники. Техническая, технологическая, экономическая и иная информация в зависимости от ее значимости для интересов

<sup>1</sup> См.: Розенберг В. Указ. соч. С. 21–60.

<sup>2</sup> См.: История отечественного государства и права. Ч. 2 / Под ред. О.И. Чистякова. М., 2004. С. 7–535, и др.

государства имела три степени секретности: «секретно», «совершенно секретно» и «особой важности», что определялось перечнями сведений, утверждаемых Правительством СССР. Торговая (коммерческая) тайна с учетом направленности ее использования в дореволюционный период практически не имела внутреннего хождения между предприятиями и использовалась в основном во внешнеторговых отношениях.

**Первый период (1917–1920 гг.)** — «военного коммунизма» — характеризовался ликвидацией частной собственности, искоренением товарно-денежных отношений, установлением рабочего контроля над производством и финансовой стороной деятельности предприятий. Законы Российской империи, позволявшие защищать производственную и коммерческую тайны, были отменены в связи с принятием Всероссийским Центральным Исполнительным Комитетом (ВЦИК) Положения о рабочем контроле от 14 (27) ноября 1917 г.<sup>1</sup> Национализация промышленности и торговли, перевод предприятий в разряд государственных обусловили трансформацию понятия «промысловая тайна» в государственную тайну. Важное место в создаваемой системе защиты государственных секретов занимает институт перечней сведений, составляющих государственную тайну. Первое упоминание о таком перечне содержалось в Положении о военной цензуре (1918 г.)<sup>2</sup>.

**Второй период (1921–1929 гг.)** — новой экономической политики (*нэп*) — характеризуется созданием экономических стимулов для развития производства. Были восстановлены рыночные отношения, разрешена частная торговля, денационализированы предприятия и др., что позволило к середине 20-х годов восстановить промышленность. Оживление частного предпринимательства сопровождалось конкуренцией на рынке товаров и необходимостью защиты КЗИ. Однако ввиду отсутствия нового законодательства о недобросовестной конкуренции (*нэп* рассматривался большевиками как временное явление) защита информации осуществлялась договорным путем на уровне предприятий с использованием обычаев и обыкновений.

Укрепление государственного сектора требовало защиты его интересов. В 1921 году Совет народных комиссаров (СНК) РСФСР утверждает Перечень сведений, составляющих тайну и не подлежа-

<sup>1</sup> См.: Декреты Советской власти. М., 1957. Т. 1. С. 83–85.

<sup>2</sup> См.: Сборник приказов Военного Совета республики. 1918. № 97. С. 987.

ших распространению. Вводится военная цензура печатных изданий. В связи с образованием СССР в 1924 году утверждается новый перечень, включивший раздел об экономических сведениях. Нужно сказать, что история Советского государства знает три открытых общесоюзных перечня (1926, 1947, 1956 гг.) и девять закрытых перечней, последний из которых был утвержден в 1980 году.

*Третий период* (1930—1985 гг.), в течение которого были сформированы основные параметры системы защиты государственных секретов. Специфика направлений по охране государственных секретов определялась крупномасштабными задачами, решаемыми государством на различных этапах своего развития. В 30-х годах в нашей стране были созданы основы социализма, включавшие обобществление всех средств производства, отсутствие частной собственности, плановое ведение экономики. Плановость ограничивала инициативу и вела к снижению заинтересованности в результатах труда. Система стимулирования труда, построенная на социалистическом соревновании, не смогла заменить частные интересы, связанные с получением прибыли. Реформы<sup>1</sup> по совершенствованию хозяйственного механизма, проведенные в 50—60-е годы, несколько улучшили положение дел в экономике, однако в 70-е годы темпы роста замедлились, а в 80-е упали до уровня застоя<sup>2</sup>. Это происходило оттого, что государственный сектор был малоподвижен и отторгал все новое. Промышленная продукция была неконкурентоспособной на мировом уровне. Одной из причин такого состояния экономики можно назвать излишнюю, тотальную секретность, когда КЗИ надолго оседала в специальных хранилищах и не была доступна организациям, которые остро в ней нуждались.

В послевоенный период, вплоть до 1985 года, происходил процесс постепенного усиления режима секретности и наращивания объема секретной документации. Периодически менявшиеся перечни главнейших сведений (ПГС) увеличивали объем категорий сведений, отнесенных к государственной тайне. Это объясняется существованием не только объективных причин, связанных с использованием в оборонном комплексе достижений НТР, состоянием «холодной войны» с Западом, но и действием субъективных «перестраховочных» фак-

<sup>1</sup> См.: Егiazарян Г. Перестройка и уроки хозяйственных реформ // Вопросы экономики. 1988. № 2, и др.

<sup>2</sup> См.: Семенишкова Л. И. Указ. соч. С. 704—709, и др.

торов на уровне министерств и предприятий. Ведомственные перечени, утверждаемые министерствами и ведомствами, расширяли круг таких сведений с учетом решаемых ими задач. Аналогичная работа велась и предприятиями, которые руководствовались не только ведомственными перечнями, но и Положением о порядке подготовки материалов, предназначенных для открытого опубликования, утвержденным Главным управлением по охране тайн в печати при Совете Министров СССР (далее — Главлит). Таким образом, информация о нововведениях технического и технологического характера надолго становилась закрытой и труднодоступной для специалистов, что отрицательно сказывалось на развитии экономики. Нужно отметить, что в этот период на предприятиях была создана отлаженная система правовой защиты государственных интересов<sup>1</sup>, которая во многом теперь заимствована современными службами безопасности для защиты частных интересов предпринимателей.

*Четвертый период* (1985—1991 гг.) характеризуется формированием законодательной базы о коммерческой тайне. Это период «перестройки», то есть реформирования системы в рамках социализма, гласности, повышения личной заинтересованности, совершенствования хозяйственного механизма, завершившийся, как известно, распадом СССР. Политические и экономические изменения, произошедшие в СССР в период с 1985 по 1991 г., явились причиной возрождения правового института коммерческой тайны. Важнейшими факторами, обусловившими процесс разделения массива сведений, ранее всецело принадлежавших государству, на две составляющие — государственную тайну и секреты предприятий (коммерческая тайна), — являются следующие.

1) *Политический фактор*. Впервые за долгие годы в стране осуществлялись преобразования производственных отношений, предпологалось введение многообразия форм собственности, развитие товарно-денежных отношений, кооперации и самоуправления трудовых коллективов. Благодаря перестройке активно развивался международный политический диалог, укреплявший взаимопонимание и доверие между СССР и другими странами.

Положительные перемены на международной арене позволили значительно, причем не всегда обоснованно, под лозунгами глас-

<sup>1</sup> См.: Северин В. А. Правовое регулирование охраны государственных секретов в СССР // Советское государство и право. 1991. № 1.



ности снять ограничения на большой массив информации, ранее действовавшей в закрытом режиме, и внести коррективы в государственную систему защиты секретов в СССР. Решением Комитета конституционного надзора СССР от 29 ноября 1990 г. был отменен существовавший в стране порядок, допускавший применение неопубликованных нормативных актов о правах, свободах и обязанностях граждан (например, Общесоюзная инструкция № 0126-72 и др.). В тот период примерно 70 процентов таких актов в той или иной мере носили закрытый характер<sup>1</sup>. Главлит 18 июня 1990 г. отменил режим хранения и использования иностранных изданий, ограниченных для общего пользования (отмеченных знаком «шестигранник»). Теперь эти вопросы решались по усмотрению руководителей предприятий. Вместе с тем был сохранен режим секретности материалов, предназначенных для открытой публикации, раскрывавших сведения об оборонном и экономическом потенциале страны (около 75% разведывательной информации иностранных спецслужбы получали из открытых источников)<sup>2</sup>.

Были рассекречены наименования и дислокация некоторых режимных предприятий. Отменены условные наименования режимных объектов в виде «почтовых ящиков». На режимных предприятиях допускалось создание кооперативов и совместных с иностранными фирмами предприятий. Значительно был сокращен перечень городов и районов страны, закрытых для посещения иностранцами. Некоторые из них в последующем приобрели статус открытых экономических зон. Был несколько упрощен прием иностранных делегаций, групп и отдельных граждан, прибывших в СССР по экономическим, торговым и научно-техническим вопросам. В стране была проведена большая работа по рассекречиванию информации. Объем секретной информации в ряде отраслей промышленности уменьшился на 30–40 процентов<sup>3</sup>. Значительная часть массива этой информации была отнесена к коммерческой тайне предприятий.

2) *Экономический фактор*. Экономические реформы, проводившиеся в этот период, не смогли решить главную проблему — лега-

<sup>1</sup> См.: Известия. 1990. 30 ноября. «Отменены секретные акты».

<sup>2</sup> См.: Рубанов В., Никитин Л. Не забывать об экономической безопасности // Социалистическая законность. 1987. № 10, и др.

<sup>3</sup> См.: Угаров В. Гриф «секретно»: шпионomanия или необходимость? // Экономика и жизнь. 1990. № 30.

лизации частной собственности на законодательном уровне. Собственность по-прежнему безраздельно оставалась в руках государства. Введение хозяйственного расчета и проведение иных мероприятий по совершенствованию хозяйственного механизма не смогли изменить экономическую ситуацию в стране. Причиной было отсутствие частного интереса предприятий к результатам своей деятельности. Господство социалистической собственности обуславливало существование однополярной государственной системы режима секретности на любую информацию. Постепенно, с приходом в СССР зарубежного частного капитала, начали формироваться отношения по поводу использования и охраны информации. Создание первых совместных предприятий с участием иностранного капитала<sup>1</sup> выявило проблемы в сфере правового регулирования и защиты права на коммерческую тайну в СССР<sup>2</sup>. Вопросы обмена деловой конфиденциальной информацией и охраны торговых секретов частично были решены в соглашениях между СССР и США, подписанных в 1990 г., о научно-техническом сотрудничестве в области мирного использования атомной энергии и торговых отношениях.

3) В рамках экономических реформ проводилась *конверсия предприятий оборонных отраслей промышленности*, что способствовало переводу части государственных секретов в разряд коммерческой тайны. Часть предприятий, наряду с разработкой вооружения и военной техники, и прежде занимались созданием продукции суверенно-гражданского назначения. Это обстоятельство эффективно использовалось для легендривания оборонных работ. Ставились задачи без ущерба для безопасности и обороноспособности страны полнее использовать потенциал военно-промышленного комплекса<sup>3</sup>. Например, по результатам создания ракетно-космической системы «Буран» в гражданские отрасли народного хозяйства были переданы для использования более 600 современных технологий, новых материалов и технических средств. Вместе с тем хозяйственный механизм оборонных предприятий оставался административным. Предприятия были лишены возможности на своем уровне определять загрузку

<sup>1</sup> См.: Брагинский М. Совместные хозяйственные организации // Социалистическая законность. 1988. № 7.

<sup>2</sup> См.: Рубанов В., Дмитриев Ю. К вопросу о защите «промышленных секретов» совместных предприятий // Хозяйство и право. 1989. № 1, и др.

<sup>3</sup> См.: Рубанов В. А. Оборонный достаток и экономический остаток // Международная жизнь. 1990. № 12.

производственных мощностей с учетом выгодности заказов. Многие НИОКР, результаты которых не были востребованы оборонными ведомствами, по-прежнему оставались недоступными для предприятий, выпускающих гражданскую продукцию<sup>1</sup>.

4) *Нерешенность фундаментальных вопросов собственности отразилась и на содержании законопроектных работ по регулированию КЗИ*, которые активно велись в этот период (1988–1991 гг.). Межведомственной рабочей группой при Гостехкомиссии СССР был подготовлен ряд законопроектов: «О защите секретной информации», «О недобросовестной конкуренции», «О коммерческой тайне» и другие. К сожалению, основные положения названных законопроектов были сформулированы в русле официальной политической доктрины перестройки, то есть обновления существующей государственной системы режима секретности без учета возрождения частной собственности и защиты интересов предприятий на КЗИ.

5) *В обществе в этот период зреют настроения о необходимости внесения изменений в действующую правовую систему защиты секретов*. Начинается гласное обсуждение этих проблем в печати<sup>2</sup>. Этому способствует необходимость организации защиты КЗИ с учетом сформировавшихся первых кооперативов и совместных с инфирмами предприятий. В период 1990–1991 гг. было принято свыше 16 законов СССР и 8 законов РСФСР, а также иные правовые акты, в которых содержались отдельные нормы о защите КЗИ. Важнейшими являются законы о собственности, о предприятиях и предпринимательской деятельности, которые заложили основу для нового законодательства России в этой сфере.

*На четвертом этапе* — период «реставрации капитализма» (с 1992 г. по настоящее время) — характерным является переход от социализма к капитализму, от плановой к рыночной экономике, что обуславливает коренные изменения в правовой системе<sup>3</sup>, включая регулирование обращения КЗИ и охрану ее конфиденциальности. Произшедшие революционные преобразования в производстве

<sup>1</sup> См.: *Никитин П.* Конверсия секретности: неразумная недостаточность // Коммунист. 1990. № 9, и др.

<sup>2</sup> См.: *Рубанов В.* От «культы секретности» — к информационной культуре // Коммунист. 1988. № 13; *Никитин П., Сидовский В.* Укреплять правовые гарантии защищенности личности // Социалистическая законность. 1988. № 12, и др.

<sup>3</sup> См.: *История отечественного государства и права. Ч. 2 /* Под ред. О.И. Чистякова. С. 512–535.

ных отношениях, появление и признание государством частной собственности потребовали адекватных изменений в правовом регулировании системы секретности. Движение России по рыночному пути развития привело к сужению сферы государственных экономических и научно-технических интересов, в связи с чем уменьшился объем информации ограниченного доступа, защищаемой на уровне организации. Перераспределение объемов информации, защищаемой обладателем на основании законов и договоров, внесло коренные изменения в теорию и практику защиты государственных, коммерческих и иных секретов. В Российской Федерации были приняты специальные законы «О государственной тайне» (1993 г.) и «О коммерческой тайне» (2004 г.), определившие, правда в разное время, интересы государства и хозяйствующих субъектов в сфере обращения и защиты информации с ограниченным доступом.

При этом следует учитывать, что если в советский период осуществлялась правовая защита только государственных секретов, то в настоящее время на законодательном уровне урегулирована защита различных видов информации с ограниченным доступом, разглашение (утечка) которой может причинить вред интересам личности, общества и государства. Например, В.Н. Лопатин различает 34 вида тайн и называет 89 федеральных законов, в которых содержатся правовые нормы, регулирующие отношения по поводу того или иного вида информации ограниченного доступа<sup>1</sup>, в том числе 37 законов, содержащих нормы об охране коммерческой тайны.

Сегодня в России сформированы законодательные основы гражданско-правового регулирования коммерческой тайны. Важным этапом развития законодательства о коммерческой тайне было принятие части первой ГК РФ, где впервые информация была определена как самостоятельный объект гражданских прав (ст. 128 ГК РФ), а также указаны общие условия отнесения ее к коммерческой тайне (ст. 139 ГК РФ), части второй ГК РФ, закрепившей условия о конфиденциальности в ряде обязательств, связанных с производством и реализацией товаров, выполнением работ и оказанием услуг. Большое влияние на формирование механизма правового регулирования коммерческой тайны оказал ныне утративший силу Федеральный закон

<sup>1</sup> См.: *Лопатин В.Н.* Концепция развития законодательства в сфере обеспечения информационной безопасности Российской Федерации (проект). М., 1998. С. 147–158.

от 25 января 1995 г. № 24-ФЗ «Об информации, информатизации и защите информации», который по праву считался в течение более 10 лет базовым в области информационных отношений. В названном Законе впервые был установлен порядок документирования информации и закреплено право собственности на материальные носители информации, определены правовые режимы защиты информации. В последнем ему на смену новом ФЗ от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» уточнены основополагающие понятия с учетом развития информационных технологий и вхождения России в мировое информационное сообщество. Часть четвертая ГК РФ, вступающая в действие с 1 января 2008 г.<sup>1</sup>, регулирует право на результаты интеллектуальной деятельности и средства индивидуализации. В отдельных главах закреплено право на секреты производства (ноу-хау) (гл. 75) и право использования результатов интеллектуальной деятельности в составе единой технологии (гл. 77).

Вместе с тем результаты анализа показывают, что за последние 15 лет существующий в стране механизм защиты сведений, доступ к которым ограничен на законных основаниях, еще не в полной мере адаптировался к изменившимся условиям рыночной экономики. Практика деятельности государственных предприятий и коммерческих структур особым образом продолжает отражать гонимыми складывавшиеся в стране общественные отношения в сфере защиты государственных секретов. Ей присущи известные пороки административно-командной системы: бюрократизм процедуры установления и обеспечения режима секретности (конфиденциальности), экстенсивный путь развития системы охраны секретов, игнорирование объективных рыночных законов конкуренции, невосприимчивость к потребностям научно-технического прогресса и происходящей в стране информационной и торговой революций. Решение этих проблем во многом зависит от повышения уровня информативной культуры в обществе.

Современный этап развития общества и государства характеризуется тем, что информационные процессы стали неотъемлемым свойством обеспечения деятельности государственных органов, предприятий и граждан. Информационные ресурсы по своей значимости, наряду с природными, финансовыми, трудовыми и иными,

<sup>1</sup> См.: СЗ РФ. 2006. № 52. Ст. 5496.

составляют важнейший потенциал хозяйствующих структур. В предпринимательской деятельности используется информация, имеющая коммерческую ценность. Создание в России реального сектора экономики за счет расширения сферы деятельности субъектов малого предпринимательства повлечет, по оценке специалистов, увеличение спроса на КЗИ. Данные опросов подтверждают, что в условиях проведения рыночных реформ три четверти предпринимателей интересуются коммерческой, маркетинговой и нормативно-правовой информацией<sup>1</sup>, использование которой они связывают с экономической устойчивостью работы фирм и желанием расширить сферу своей деятельности.

Учитывая то обстоятельство, что частью четвертой ГК РФ установлено исключительное право на секрет производства (ноу-хау) и что обладателем в отношении таких сведений на законном основании вводится режим коммерческой тайны, организации вынуждены по своему усмотрению применять различные правовые средства, регулирующие обращение КЗИ и охрану ее конфиденциальности. Вышеизложенное подчеркивает необходимость научного поиска путей разработки такого механизма и обеспечения эффективности его функционирования в рыночной экономике.

Важное место в системе периодизации законодательства о КЗИ занимают третий и четвертый этапы, имеющие определенные особенности, что предопределило необходимость их более глубокого изучения. Формирование механизма регулирования и обеспечения охраны коммерческой тайны в России должно осуществляться, по нашему мнению, с использованием опыта защиты секретов в советский период, учетом форм проявления КЗИ в гражданском обороте и решением проблем, связанных с практическим применением Закона «О коммерческой тайне».

**Концепция исследования проблем формирования механизма правового регулирования обращения КЗИ и охраны ее конфиденциальности.**  
Характеристика механизма правового регулирования обращения и защиты КЗИ требует первоочередного анализа влияния базисных явлений собственности в рыночной экономике, связанных с частными интересами предпринимателей, на процесс появления такого рода информации и регулирования общественных отношений по поводу ее исполь-

<sup>1</sup> См.: Информационное обеспечение предпринимательской деятельности: год 2001. М., 2001. С. 11, и др.

зования и защиты в гражданском обороте. В экономическом смысле общеизвестным является утверждение о том, что основу производственных отношений составляет собственность. Ведущее место в отношениях между различными субъектами по использованию средств и результатов производства занимает информация, которая сегодня признается даже более важным ресурсом, чем сырье и энергия.

*Секретность (конфиденциальность) при этом выступает как специфический способ организации отношений по использованию этого ресурса.* Следовательно, складывающиеся в России рыночные отношения по поводу использования и защиты информации с ограниченным доступом — это часть экономических отношений собственности, а сами секреты как регуляторы доступа к информационным ресурсам, в зависимости от статуса их обладателя (собственника), могут быть предметом публично-правового (государственная и служебная тайна) или частного правового регулирования (коммерческая тайна). Государственная тайна при этом связывается с реализацией политических (государственных) интересов Российской Федерации, а коммерческая тайна — с экономическими (частными) интересами коммерческих организаций в процессе их хозяйственной деятельности. При разграничении названных интересов нужно исходить из понятия интереса как категории общественных наук и учитывать, что «...интерес есть по форме общественное отношение, имеющее содержанием потребность субъекта, носящую социальный характер и проявляющуюся в сознании и реализации целей»<sup>1</sup>.

*Правовые отношения между субъектами государственной и частной собственности по поводу использования в экономическом обороте информационных ресурсов являются основополагающим фактором, существенно влияющим на формирование механизмов защиты информации с ограниченным доступом.* Данное обстоятельство предопределяет необходимость адекватного отображения в системе защиты КЗИ всех происходящих в развитии общества и государства изменений экономического и правового характера. Здесь возникает много новых и сложных теоретико-методологических и практических вопросов, решение которых связано с разработкой концепции механизма

<sup>1</sup> Михайлов С.В. Категория интереса в российском гражданском праве. М., 2002. С. 26.

правового регулирования обращения КЗИ и охраны ее конфиденциальности.

Одним из наиболее важных вопросов, лежащих в основе данной концепции, является *учет частных интересов предпринимателей в сфере обращения КЗИ.* Общественные отношения, существующие в российской рыночной экономике по поводу использования и защиты КЗИ, непосредственно связаны с частными интересами предпринимателей, которые нуждаются в охране. На практике в концентрированной форме охрана частного интереса обеспечивается защитой коммерческой тайны. Сущность частноправовых интересов выражают взаимосвязанные категории «производственные отношения» и «собственность»<sup>1</sup>. Экономические отношения собственности, по мнению Е.А. Суханова, подвергаются правовому оформлению и таким образом регулируют отношения между людьми по поводу приобретения конкретного лицом конкретного имущества, использующим его в своих интересах, в пределах установленных границ его дозволенного использования<sup>2</sup>. Объектом экономических отношений выступают товары, которые по форме представляют не только вещи, но и работы, услуги, результаты интеллектуальной деятельности — короче, любые продукты труда, включая и *информационные ресурсы*, удовлетворяющие ту или иную общественную потребность посредством купли-продажи. В зависимости от того, кто является субъектом присвоения товаров, различают частную, государственную, муниципальную и иные формы собственности, которые на основании Конституции РФ (ч. 2 ст. 8) признаются и защищаются равным образом. В объективной реальности существования рыночных отношений, как справедливо замечает Е.А. Суханов, «...никаких иных „форм собственности“, кроме частной и публичной, в действительности нет и быть не может», а «...частная собственность обозначает лишь противоположность государственной („публичной“) собственности, т.е. принадлежность имущества конкретным физическим или юридическим (частным) лицам...»<sup>3</sup>.

<sup>1</sup> Краткий философский словарь / Под ред. А.П. Алексеева. 2-е изд. М., 2002. С. 307.

<sup>2</sup> См.: Гражданское право. Учебник. В 2 т. Т. 1 / Отв. ред. проф. Е.А. Суханов. 2-е изд. М., 2000. С. 477.

<sup>3</sup> См.: Суханов Е.А. Гражданское право России — частное право / Отв. ред. В.С. Ем. М., 2008. С. 39—40.

Государственная (публичная) и частная собственность обуславливает различные интересы государства в лице своих предприятий, собственников которых оно выступает, и предпринимателей в рыночной экономике. Нужно сказать, что государственные предприятия непосредственно участвуют в производстве, распределении, обмене и потреблении товаров и услуг<sup>1</sup>, т.е. занимают, по сути, государственным предпринимательством. Презюмируется, что они находятся в более привилегированном положении по отношению к частным организациям. Они вправе рассчитывать на государственный заказ с гарантированным сбытом продукции. Им не должно грозить в этой связи банкротство. Финансовое благополучие зависит от финансирования государственного заказа. Доходы, полученные от производства государственной деятельности, находятся в распоряжении государства. Поэтому говорить об экономических интересах предприятия можно лишь с позиций интересов государства как его собственника<sup>2</sup> и с учетом более широкого арсенала правовых средств, которые используются для охраны государственных интересов, в том числе и правового института государственной тайны.

Успешное развитие предпринимательства зависит от той экономической и правовой среды, в которой оно осуществляется. Предприниматель, как ведущий участник рыночных отношений, находится в совершенно особых условиях ведения предпринимательской деятельности. Интересы предпринимателей основываются на частной собственности, на возможности индивидуального или коллективного владения и распоряжения не только основными фондами производства (землей, зданиями, оборудованием, трудом, капиталом), но и «человеческим капиталом» (знаниями, интеллектуальной собственностью, информацией), обеспечивающими ее субъектам доход.

Уровень этого дохода напрямую зависит от новаторства предпринимателей и степени активности использования КЗИ. Говоря о новаторстве, Й.А. Шумпетер в своей теории экономического развития писал, что «рынок относится к нововведениям скептически, но если предпринимателю удается реализовать эти нововведения, то меха-

<sup>1</sup> См.: Губин Е.Л. Правовые формы взаимодействия предпринимательства с государством // Научные труды РАЮН. 2001. № 1; Дойников И. В. Правовое регулирование государственного предпринимательства. М., 2001, и др.

<sup>2</sup> См.: Экономическая теория: Учебник / Под ред. В.Д. Камаева. 8-е изд. М., 2002. С. 43–63, 454–491; Сажина М.А., Чибриков Г.Г. Экономическая теория. М., 2003. С. 328–345, и др.

низм конкуренции вытесняет с рынка предпринимателей, использующих устаревшие технологии. Именно новаторство способствует переходу экономики из одного равновесия в другое, содействуя прогрессу<sup>3</sup>. Предприниматель реализует свой частный интерес, связанный с получением прибыли, через новаторство, путем введения в дело на коммерческой основе новых производственных технологий, новых форм организации бизнеса, новых товаров. Причем их появлению на рынке предшествует использование предпринимателем ранее никому не известной информации технического, технологического и делового характера, имеющей коммерческую значимость. Безусловно, предприниматель идет на риск, когда вводит на рынок новые товары, причем рискует он не только своими временем, деловой репутацией, но и капиталом. Однако частный интерес в получении прибыли заставляет его осуществлять деятельность на свой риск и свою имущественную ответственность.

Конкуренция на рынке диктует постоянное обновление ассортимента и улучшение качества выпускаемой продукции, что заставляет организации выделять КЗИ и заботиться о ее правовой защите. Однако это под силу только крупным организациям, имеющим в своей структуре юридические подразделения и службы безопасности. Большинство руководителей малых и средних предприятий сегодня не имеют финансовых возможностей содержать такие службы и даже отдельных специалистов и слабо осведомлены об эффективности использования средств и методов защиты КЗИ.

Наличие государственных (публичных) и частных интересов<sup>2</sup> в экономических общественных отношениях объективно обуславливает существование различных видов информации с ограниченными доступом<sup>3</sup>, адекватно отражающей интересы собственников в гражданском обороте. Разделение всего массива информации с учетом данного критерия способствовало решению задач правового регулирования большей части действующих в стране секретов, появлению реально-го хозяина, заинтересованного в их рациональном использовании и защите. При этом ограничение на доступ к информации (так назы-

<sup>1</sup> Цит. соч. Шумпетера Й.А. по: Экономическая теория: Учебник / Под ред. В.Д. Камаева. С. 258.

<sup>2</sup> См.: Малько А.В. Основы теории законных интересов // Журнал российского права. 1999. № 5, 6, и др.

<sup>3</sup> См.: Алексеев А.И. О классификации конфиденциальной информации по видам тайн // Безопасность информационных технологий. 1999. № 3, и др.

ваемая «секретность») обеспечивается путем установления правового режима секретности (государственная тайна) или конфиденциальности (коммерческая тайна) и регулирует, по существу, правовые отношения по поводу использования и защиты информации в гражданском обороте. Товары (работы, услуги), при производстве которых используются сведения, составляющие государственную тайну, изъяты из гражданского оборота. Их оборот осуществляется на основании специального законодательства. Аналогичная ситуация и с КЗИ, которая изымается и вводится в гражданский оборот по решению ее обладателя. Отношения между субъектами по поводу документированной КЗИ носят обязательственный характер. Обладатель по договору передает свое право на КЗИ третьему лицу на возмездной основе.

*Особенности использования информации с ограниченным доступом определяют различные системы ее защиты, регулируемые соответственно правовыми институтами государственной, коммерческой и иной охраняемой законом тайны. В настоящей работе рассмотрены проблемы правового регулирования и защиты КЗИ с использованием института коммерческой тайны. В рыночной экономике роль этого института является доминирующей по сравнению с институтом государственной тайны, задачи которого ограничены в экономике рамками обеспечения обороноспособности и безопасности государства. Это объясняется местом, которое занимают частные хозяйствующие субъекты в структуре рыночной экономики по формированию и развитию структуры и инфраструктуры товарного рынка.*

*При разработке и построении систем защиты КЗИ следует иметь в виду, что частная организация выступает собственником своих информационных ресурсов, которые могут быть предметом гражданско-правовых сделок. Поэтому документированная информация не может быть использована вопреки частным интересам другими субъектами, включая и государство, и предполагает возможность ее относительного обособления рамками деятельности организации. Вместе с тем имеется необходимость согласования государственных, общественных и личных интересов при установлении частными организациями режима коммерческой тайны и его обеспечения.*

*Деятельность частной организации по установлению и обеспечению режима коммерческой тайны, осуществляемая при выполнении договорного обязательства, в том числе государственного заказа, связанного с необходимостью соблюдения условия конфиденциальности, должна рассматриваться как возмездное оказание услуг заказ-*

чику (покупателю). Стоимость таких услуг и иные условия определяются сторонами в договоре.

*Функционирование механизма правового регулирования обращения КЗИ и охраны ее конфиденциальности должно рассматриваться как неотъемлемая составная часть производственной и иной деятельности частной организации, направленной на получение прибыли. При таком отношении любые достижения и промахи, связанные с установлением режима коммерческой тайны и его обеспечением, будут непосредственно отражаться на уровне доходов организации и материальном благополучии каждого работника. На основе сочетания личных и корпоративных интересов у работников формируется внутренняя потребность в защите ценной для организации информации, поскольку ее разглашение (утечка) повлияет на уровень их материального вознаграждения и получения иных благ.*

*Деятельность частной организации по охране конфиденциальности информации должна быть построена на принципах самофинансирования и экономической целесообразности, что позволит решить проблему определения действительной необходимости засекречивания информации и осуществления достаточных, связанных с ее защитой, мероприятий. Установленный организацией режим коммерческой тайны не является нейтральным по отношению к развитию производительных сил. Он отлекает на проведение специальных мероприятий производственные мощности, финансовые и трудовые ресурсы, а также отрицательно сказывается на уровне информационного обмена между производителями и оптовыми покупателями. Эффективность осуществления мероприятий по обеспечению режима секретности (конфиденциальности) будет проявляться, прежде всего, в готовности заказчика, включая и государство, оплатить оказываемые ему услуги на договорной основе, что требует применения целесообразных методов и разработки методик определения критериев целесообразности выделения и защиты КЗИ и создания, таким образом, надежного механизма противодействия неоправданной секретности.*

Исходя из общего понятия научной категории «правовое регулирование»<sup>1</sup>, объединяющей, по мнению С.С. Алексеева<sup>2</sup>, в один ряд

<sup>1</sup> См.: Алексеев С.С. Механизм правового регулирования в социалистическом государстве. М., 1966. С. 5–79; Общая теория государства и права. Академический курс в 3-х томах. 2-е изд. / Отв. ред. проф. М.Н. Марченко. Т. 3. М., 2001. С. 89–109.

<sup>2</sup> См.: Алексеев С.С. Право: азбука — теория — философия: Опыт комплексного исследования. М., 1999. С. 347–387.

«механизм правового регулирования», «правовые средства», «правовой режим» и др., область научного анализа права института коммерческой тайны как объекта исследования включает комплекс теоретико-методологических и практических проблем частного правового характера, непосредственно связанных с гражданским (торговым) оборотом КЗИ и обеспечением деятельности по охране ее конфиденциальности. Использование КЗИ и обеспечение ее конфиденциальности должны, по нашему мнению, рассматриваться системно в составе правового института в качестве единого правообразующего фактора, поскольку, с одной стороны, имеют тенденцию к нормативно организованной интеграции в самостоятельный институт коммерческой тайны, а с другой стороны, влияют на иные виды гражданских правоотношений в области предпринимательской деятельности. Исходя из названных соображений **исследование проблем формирования и реализации механизмов правового регулирования обращения КЗИ и охраны ее конфиденциальности, в рамках правового института коммерческой тайны, рассматривается на концептуальном уровне как совокупность признаков:**

характеризующих теоретико-методологические аспекты проблемы исследования правового института коммерческой тайны как составной части наук гражданского и коммерческого права, историко-правовые предпосылки и эволюционный характер появления КЗИ и ее законодательного регулирования в экономическом обороте;

раскрывающих понятие и сущность КЗИ, формы ее проявления в гражданском (торговом) обороте в связи с производством и реализацией товаров, выполнением работ и оказанием услуг;

отражающих опыт правового регулирования отношений по поводу защиты информации в советский период и перспективы развития современного российского законодательства о коммерческой тайне;

характеризующих возможность использования правовых средств в сфере обращения КЗИ в рамках корпоративных, трудовых и гражданско-правовых отношений, связанных с охраной конфиденциальности информации;

характеризующих организационное обеспечение деятельности по установлению режима коммерческой тайны в коммерческой организации;

раскрывающих основные направления правового и научно-методического обеспечения деятельности по охране конфиденциальности информации.

Названные группы признаков находятся между собой в тесной взаимосвязи и, взаимно дополняя друг друга, позволяют в совокупности получить **характеристику механизма правового регулирования обращения КЗИ и охраны ее конфиденциальности в гражданском обороте и определить пути его дальнейшего совершенствования.** В обобщенном виде роль каждой группы признаков с этих позиций может быть обозначена следующим образом.

**Первая группа признаков** определяет влияние базисных явлений собственности в рыночной экономике, связанных с частными интересами предпринимателей, на процесс появления коммерчески значимой информации в исторической ретроспективе, требующий правового регулирования и обуславливающий формирование и развитие правового института коммерческой тайны.

**Вторая группа признаков** показывает реальную среду гражданского оборота, где в силу рыночных условий (конкурентность, максимизация прибыли и др.) существует КЗИ и благодаря новаторству предпринимателей обеспечивается собственное «воспроизводство», что имеет значение для прогрессивного развития экономики. Появление КЗИ в экономическом обороте связано с легальным признанием ее государством. Отсюда важно проследить путь эволюции законодательства в этой сфере, который напрямую связан с частными интересами.

**Третья группа признаков** представляет законодательную базу, определяющую рамки возможного и дозволенного поведения субъектов при выборе правовых механизмов использования и охраны конфиденциальности КЗИ. Эти признаки выявляются при сравнительном исследовании правового регулирования обращения КЗИ в советский и современный периоды развития России.

**Четвертая группа признаков** базируется на наличии связи между правовыми средствами, используемыми на корпоративном уровне при взаимоотношении работодателя и работника, в процессе заключения гражданско-правовых договоров и исполнения обязательств, связанных с соблюдением условия конфиденциальности. Она позволяет учитывать при решении задач по охране конфиденциальности информации специфику проявлений нарушений, связанных с разглашением (утечкой) КЗИ, обусловленные особенностями лиц, совершающих такие нарушения, и учитывать их в предупредительной работе по обеспечению информационной безопасности организаций.

**Пятая группа признаков** отражает деятельность организаций по установлению режима коммерческой тайны с учетом реальных и потенциальных угроз безопасности организации, определению степени конфиденциальности информации и осуществлению других мер до начала производства и реализации товаров (работ, услуг). Между этими явлениями существует тесная взаимосвязь по схеме: интересы — угрозы — защита, которая обуславливает контуры системы мер по охране конфиденциальности.

**Шестая группа признаков** отражает социальные явления и процессы, имеющие место в обществе, государстве и в конкретной организации, обуславливающие нарушения режима коммерческой тайны, причины и обстоятельства, им способствующие, показывает необходимость их учета в определении мер предупреждения, а также использования методов, методик и технологий обеспечения деятельности по охране конфиденциальности информации.

Имея в виду принятую структуру настоящей работы, в первой главе изложение ограничивается рассмотрением первых трех групп признаков. Другие группы, требующие освещения целого комплекса определяющих их содержание специальных вопросов, будут освещены в последующих главах монографии.

## § 2. Понятие коммерчески значимой информации и сущность ее обращения в рыночной экономике

**Понятие информации в гражданском обороте.** Ученые неоднократно обращались к определению понятия информации, пытаясь установить ее общие характерные признаки, независимо от отраслей научных знаний. Каждый исследователь, исходя из общего понятия информации, определяемого как сведения об окружающем мире и протекающих в нем процессах либо как сообщения, осведомляющие о положении дел, которые воспринимаются человеком или специальными устройствами, трансформировал его на интересующую область научных знаний. Отсюда и различия в определении понятия информации, которые зависят от предметной области знаний, целей и задач, стоящих перед получателями информации.

Понятие информации, которая имеет коммерческую значимость, является производным от общей категории «информация». Информация является одной из фундаментальных характеристик

мирознания наряду с материей, энергией, пространством — временем<sup>1</sup>. Термин «информация», используемый для раскрытия ее как правовой категории, впервые встречается в ныне утратившем силу ФЗ «Об информации, информатизации и защите информации» от 25 января 1995 г.<sup>2</sup> Формально это понятие не претерпело изменений в ФЗ «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 г. № 149-ФЗ<sup>3</sup> и определяется как сведения (сообщения, данные) о лицах, предметах, фактах, событиях, явлениях и процессах, независимо от формы их представления, пригодного для характеристики любых видов информации. Специфика КЗИ определяется ее коммерческой ценностью для лиц, занимающихся предпринимательством. Информация как объект коммерческой ценности, обремененная в форме книг, брошюр, содержащаяся в электронных базах данных и др. имеет стоимостную оценку, является товаром, производимым для продажи и получения прибыли.

Большинство ученых-юристов, определяя понятие «информация» в гражданском обороте, подчеркивают, что она не может быть объектом правоотношений безотносительно к ее материальным носителям — физическим объектам (отдельные документы и массивы документов в информационных системах и др.), социальным и экономическим процессам<sup>4</sup>. Информация постоянно обращается в социальной среде, удовлетворяя, таким образом, потребности личности, общества и государства, что дает основание для вывода об обособлении нового вида общественных отношений — информационных<sup>5</sup>, являющихся объектом правового регулирования.

Говоря о понятии информационных правоотношений в контексте гражданского оборота информации, нельзя однозначно согласиться с позицией О.А. Гаврилова, который определяет их как урегулированные нормами права отношения, при которых «один субъект (физическое или юридическое лицо) вправе требовать от другого субъекта получения определенной информации, а второй — обязан

<sup>1</sup> См.: Гаврилов О.А. Информатизация правовой системы России. Теоретические и практические проблемы. М., 1998. С. 10.

<sup>2</sup> См.: Собрание законодательства РФ. 1995. № 8. Ст. 609.

<sup>3</sup> См.: СЗ РФ. 2006. № 31. Ст. 3448.

<sup>4</sup> См.: Бачило И.Л. Информационное право: основы практической информатики: Учебное пособие. М., 2003. С. 61–71, и др.

<sup>5</sup> См.: Право и информатика / Под. ред. Е.А. Суханова. М., 1990. С. 5.



передать первому определенному виду информации»<sup>1</sup>. При этом не учитывается тот факт, что информационный рынок регулируется исключительно договорными отношениями, в рамках которых субъекты обладают равными гражданскими правами. Порядок обязательной передачи организациями документов на безвозмездной основе или за плату установлен законом.

Объектом информационных отношений, по мнению О.А. Гаврилова, выступают информация и информационные ресурсы<sup>2</sup>. На наш взгляд, исходя из понятия информации как правовой категории, используемой в гражданском обороте, она не может существовать вне материального носителя. Поэтому объектом гражданско-правового регулирования могут быть только информационные ресурсы, информационные системы, технологии и средства их обеспечения, а не информация как таковая.

Отношения между субъектами по поводу информации урегулированы нормами публичного и частного права<sup>3</sup>. Такие нормы, как регуляторы информационных отношений, содержащиеся в различных отраслях правовых актов, регламентируют права, обязанности и ответственность субъектов при производстве, распространении и использовании информации, содержащейся на материальных носителях. Нормы права могут запрещать участникам информационных отношений совершать некоторые действия, предписывать конкретное поведение либо разрешать самим свободно определять характер взаимоотношений друг с другом на договорной основе.

Исключение из общей части ГК РФ, определяющей объекты гражданских прав, в процессе принятия части четвертой ГК РФ того объекта, как «информация» (128 ГК РФ<sup>4</sup>), заставляет вновь обратиться к результатам обсуждения вопроса о *соотношении и разграничении понятий «информация», «вещи» и «результаты интеллектуальной деятельности (исключительные права)»*.

В ныне утратившем силу ФЗ «Об информации, информатизации и защите информации», ФЗ «Об участии в международном информа-

ционном обмене»<sup>1</sup> провозглашалось право собственности на информацию. ФЗ «Об информации, информационных технологиях и о защите информации», по существу, не решает этот вопрос и содержит отсылочную норму, что «право собственности и иные вещные права на материальные носители, содержащие документированную информацию, устанавливаются гражданским законодательством» (п. 5 ст. 11). Такая общая формулировка вызывает на практике ряд вопросов о возможности использования категории собственности к информационным правоотношениям.

Весьма убедительной является позиция Л.К. Терещенко о соотношении категорий информации и собственности<sup>2</sup>, которая считает, что классическая «триада» правомочий собственника, обладающего абсолютным правом на вещь, не может применяться в отношении информации. К ней неприменимо правомочие «владения», поскольку нельзя физически обладать нематериальными объектами. Информация может находиться одновременно в пользовании бесчисленного круга субъектов и в этой связи к ней неприменимо правомочие «пользования». Правомочие «распоряжения» также неприменимо по отношению к информации, поскольку, отчуждая право на ее использование, продавец не лишается при этом возможности ее дальнейшего использования.

Поэтому право собственности и иные вещные права могут быть применимы только по отношению к материальным носителям, содержащим документированную информацию<sup>3</sup>, которая в системе гражданско-правовых отношений является средством оформления любых сделок, фактом исполнения обязательств и подтверждения любых сделок, фактом разрешения споров. Информации, обращаемой в гражданском обороте, с одной стороны, присущи общие признаки информации как правовой категории, с другой стороны, как правильно отмечает М.С. Зельцер, «не будучи товаром в классическом политэкономическом смысле, она все чаще реализуется в возмездной форме, внешне напоминающей товарно-денежный обмен»<sup>4</sup>.

<sup>1</sup> СЗ РФ. 1996. № 28. Ст. 3347.

<sup>2</sup> См.: Терещенко Л.К. Информация и собственность // Защита прав создателей и пользователей программ для ЭВМ и баз данных. М., 1996. С. 3–11.

<sup>3</sup> См.: ФЗ от 29 декабря 1994 г. № 77-ФЗ «Об обязательном экземпляре документов» // СЗ РФ. 1995. № 1. Ст. 1; ФЗ от 29 декабря 1994 г. № 78-ФЗ «О библиотечном деле» // СЗ РФ. 1995. № 1. Ст. 2, и др.

<sup>4</sup> Зельцер М.С. Гражданско-правовой режим информации. Автореф. дисс. канд. юрид. наук. М., 2004. С. 11.

Документированная информация традиционно включается в состав имущества организаций и вводится в гражданский оборот по усмотрению собственника или в силу действия закона, с учетом специфических свойств информации<sup>1</sup>. Во-первых, это физическая неотчуждаемость информации. Процедура отчуждения информации должна состоять в передаче прав на ее использование. Во-вторых, это обособленность информации. Информация овеществляется в виде символов, знаков и тому подобное и, таким образом, может существовать обособленно, то есть независимо от своего создателя. В-третьих, информация, участвующая в гражданском обороте, всегда отображается на материальном носителе, вследствие чего возникает двуединство информации и того материального носителя, на котором она отображена. В-четвертых, это тиражируемость (распространяемость) информации, означающая, что одна и та же информация может принадлежать одновременно неограниченному кругу лиц. В-пятых, это существование информации в организационной форме. Информация обращается в строго определенных организационных формах (документ, база данных, фонд документов, архив и т.п.).

Названные свойства информации обуславливают правовой режим информации при введении ее в гражданский оборот. Однако понимание отдельных свойств информации носит дискуссионный характер<sup>2</sup>. Исходной посылкой к дискуссии является правовая природа информации, точнее, ее отображение, овеществленное на материальном носителе. При включении информации в гражданский оборот она всегда (по словам В.А. Копылова) отображается на материальном носителе, в связи с чем возникает двуединство информации и материального носителя. Такое явление, которое, по нашему мнению, может носить физический, а не правовой характер, позволило В.А. Копылову сформулировать понятие сложной вещи, состоящей из носителя информации и самой информации, отображенной на носителе. Регулирование информационной вещи должно осуществляться, по мнению В.А. Копылова, институтами авторского права и вещной собственности<sup>3</sup>.

<sup>1</sup> См.: Копылов В. А. О модели гражданского оборота информации // Журнал российского права. 1999. № 9. С. 35–45.

<sup>2</sup> См.: Щербак Н. Информация как объект гражданско-правового регулирования // Законодательство. 2004. № 7; Ефремов А. Информация как объект гражданских прав // <http://www.Russianlaw.net>, и др.

<sup>3</sup> См.: Копылов В. А. Информационное право. М., 2003. С. 166–174.

Несколько иной, хотя и совпадающей по многим аспектам, позиции придерживается И.Л. Бачило, которая считает, что гражданско-правовую защиту документированной информации (информационного продукта), представляющей собой одновременно нематериальный объект (информация) и овеществленный предмет (собственно документ, содержащий информацию), можно осуществлять с помощью институтов интеллектуальной собственности и вещной собственности<sup>1</sup>.

Анализ судебно-арбитражной практики показывает, что данная проблема нередко вызывает затруднения даже у судов, не говоря уж о субъектах предпринимательской деятельности. Так, по мнению Е. Зверевой, в зависимости от того, что считать первичным, исходным — информационный продукт в его идеальном выражении или материальный предмет, в котором он воплощен, — сделки, в которых реализуется оборот информационных продуктов, можно рассматривать как куплю-продажу либо как передачу имущественных прав на информационный продукт<sup>2</sup>.

Нужно сказать, что концепция права собственности на информационные ресурсы («информационной вещи», по словам В.А. Копылова) была закреплена в ныне утратившем силу ФЗ «Об информации, информатизации и защите информации» от 20 февраля 1995 г. № 24-ФЗ. Положения названного Закона о праве собственности на информационные ресурсы оценивались многими учеными критически. При этом отмечалось явное противоречие между нормами названного Закона и ГК РФ. В новом Законе «Об информации, информационных технологиях и о защите информации» понятие «информационные ресурсы» не упоминается, а используется термин «документированная информация». Раздел II «Право собственности и другие вещные права» ГК РФ не содержит права собственности «информационных ресурсов» и «документированной информации». Доктриной гражданского права убедительно доказаны безуспешные попытки приспособить «проприетарную» (от лат. *proprietas* — собственно-сть) концепцию к нематериальным результатам интеллектуальных продуктов, включая и информацию<sup>3</sup>. Это положение получило зако-

<sup>1</sup> См.: Бачило И. Л. Информационное право. М., 2003. С. 241–252.

<sup>2</sup> См.: Зверева Е.А. Информация как объект нематериальных гражданских прав // Право и экономика. 2003. № 9.

<sup>3</sup> См.: Гражданское право / Под ред. проф. Е.А. Суханова. Т. 1. М., 2000. С. 634–635.

нодательное закрепление. Пунктом 4 ст. 129 ГК РФ (в ред. ФЗ от 18 декабря 2006 г. № 231-ФЗ) установлено, что результаты интеллектуальной деятельности (включая и секрет производства. — *Прим. авт.*) не могут отчуждаться или иными способами переходить от одного лица к другому. Однако права на такие результаты и средства, а также материальные носители, в которых выражены соответствующие результаты или средства, могут отчуждаться или иными способами переходить от одного лица к другому в случаях и в порядке, которые установлены ГК РФ. Как отмечает Е.А. Суханов, обладатель исключительного (имущественного) права по своему усмотрению может как использовать соответствующий результат интеллектуальной деятельности, так и распоряжаться своим правом на него, используя для этого: 1) договор об отчуждении исключительного права, при котором у первоначального правообладателя остаются лишь неимущественные права, и 2) лицензионный договор, по которому лицензиат получает право использовать объект интеллектуальной собственности в соответствующих пределах, тогда как исключительное право остается у лицензиара-правообладателя<sup>1</sup>.

Не менее спорным является вопрос о *правомерности отнесения информации к такому объекту гражданских прав, как результаты интеллектуальной деятельности (исключительные права)*. В литературе высказано мнение о том, что «помимо традиционных объектов охраняемых авторским и патентным правом, а также законодательством о средствах индивидуализации участников гражданского оборота, российское законодательство предоставляет охрану информации, составляющей служебную и коммерческую тайну...»<sup>2</sup>. К результатам интеллектуальной деятельности относятся секреты производства (ноу-хау), которым с 1 января 2008 г. предоставляется правовая охрана. В гражданском обороте обращается и другая информация, которую трудно отнести к результатам интеллектуальной деятельности, например, коммерческая информация, используемая при заключении договора. При этом нужно исходить из содержания информации и определения способов ее правовой охраны в ГК РФ, а также учитывать, что информационные правоотношения могут возникнуть и по поводу общедоступной информации либо информации, в от-

<sup>1</sup> См.: Суханов Е.А. Гражданское право — частное право / Отв. ред. В.С. Ем. М., 2008. С. 148–149.

<sup>2</sup> Сергеев А.П. Право интеллектуальной собственности в Российской Федерации. М., 1996. С. 30.

ношении которой установлен специальный режим (государственная, коммерческая, служебная, профессиональная, личная и другие виды тайн). Правовой режим информации, как подчеркивал В.А. Дозорцев, строится на ином принципе, чем для классических объектов интеллектуальных прав. На ознакомление со сведениями не закрепляется исключительное право, действует начало свободы ознакомления с информацией, свободы познания сведений, кроме случаев, когда их конфиденциальность специально охраняется законом<sup>1</sup> либо урегулирована договорными отношениями.

Были высказаны предложения «не перекраивать гражданское законодательство под нужды информационного, а всего лишь замечать упоминание о праве собственности на информационные ресурсы в Законе об информации на более обширную формулировку «права на информационные ресурсы»<sup>2</sup>. Предложение А.А. Ефремова было высказано в свое время В.А. Дозорцевым, о включении конфиденциальности (сохранении тайны) содержательного результата в систему исключительных прав<sup>3</sup>. Речь идет о концепции исключительного права на информацию и отнесения ее к объектам интеллектуальной собственности, которую сформулировал В.А. Дозорцев.

Однако с таким предложением трудно согласиться. Информация, как это было показано выше, обладает специфическими свойствами, которые не позволяют в полной мере распространить на ее режим исключительных прав. Поэтому законодатель в ст. 1465 ГК РФ специально устанавливает правило, что в отношении сведений, составляющих секрет производства (ноу-хау), обладателем вводится режим коммерческой тайны, который, собственно, и выполняет функцию правовой охраны по поддержанию исключительного права на секрет производства. По мнению И.А. Зенина, «ноу-хау — это неохраямая конфиденциальная научно-техническая, коммерческая, финансовая и иная информация, обладающая экономической ценностью, а также различные производственные навыки и опыт их применения»<sup>4</sup>. В режиме ноу-хау функционирует, прежде всего, неохраямая техниче-

<sup>1</sup> См.: Дозорцев В.А. Понятие исключительного права // Проблемы современного гражданского права: Сборник статей. М., 2000. С. 303.

<sup>2</sup> См.: Ефремов А.А. Информация как объект гражданских прав. Адрес: www.vic.spb.ru/law/doc/a76.htm.

<sup>3</sup> См.: Дозорцев В.А. Интеллектуальные права. Понятие. Система. Задачи кодификации. М., 2005. С. 24.

<sup>4</sup> Зенин И.А. Гражданское и торговое право зарубежных стран. М., 2008. С. 171.

ская и технологическая информация. Такая информация не является всеобщим достоянием. Как подчеркивает И.А. Зенин, «на ноу-хау не существует исключительного права, а есть лишь фактическая монополия»<sup>1</sup>. Обладатель ноу-хау «передает по договору не право использования (поскольку такового нет), а само ноу-хау как совокупность разнородной неохраямемой информации»<sup>2</sup>. В данном случае речь идет о совокупности различных технических и других знаний, навыков для освоения технологического процесса производства. Как пишет И.А. Зенин, единственной формой приобретения ноу-хау является договор о его передаче. В силу специфики ноу-хау на него не могут быть установлены исключительные права<sup>3</sup>. Это в полной мере относится и к информации делового характера.

Вместе с тем законодатель пошел по другому пути, а именно: раскрывает в части четвертой ГК РФ понятие секрета производства (ноу-хау) и обязывает обладателя таких сведений вводить режим коммерческой тайны (ст. 1465), закрепляет за обладателем исключительное право на секрет производства, которое не требует специальной регистрации (ст. 1466), и определяет время его действия в зависимости от сохранения конфиденциальности соответствующих сведений, составляющих секрет производства (ст. 1467)<sup>4</sup>. В часть первую ГК РФ было внесено дополнение о том, что права на результаты интеллектуальной деятельности (секрет производства), а также материальные носители, в которых выражены соответствующие результаты, могут отчуждаться или иными способами переходить от одного лица к другому в случаях и в порядке, которые установлены Кодексом (п. 4 ст. 129 ГК РФ). Законодательное закрепление права на секрет производства (ноу-хау) отражает результаты многолетней работы ученых в этой области и подтверждает либо опровергает основные тенденции, сложившиеся в юридической науке относительно определения понятия ноу-хау и его включения в систему исключительных прав. Принятие части четвертой ГК РФ связано с внесением изменений в Закон о коммерческой тайне, в котором понятие информации, со-

<sup>1</sup> Зенин И.А. Указ. соч. С. 171.

<sup>2</sup> См.: Там же. С. 174.

<sup>3</sup> См.: Гражданское право / Под ред. проф. Е. А. Суханова. Т. 2. Полутом 1. М., 2000. С. 580.

<sup>4</sup> См.: ГК РФ. Часть четвертая от 18.12.2006. № 230-ФЗ // СЗ РФ. 2006. № 52. Ст. 5496.

ставляющей коммерческую тайну, с одной стороны, отождествляется с понятием «секрет производства» и подчеркивается, что к такой информации при определенных условиях могут быть отнесены сведения любого характера (п. 2 ст. 3 Закона), а с другой стороны, в пункте 1 этой же статьи коммерческая тайна определяется как режим конфиденциальности информации.

Итак, при определении понятия «информация» в гражданском обороте нужно исходить из того, что информационные отношения — это новый вид общественных отношений, требующий в рамках частного права правовой регламентации нормами гражданского права<sup>1</sup> и договорного регулирования информационного обеспечения торгового оборота с учетом предмета коммерческого права<sup>2</sup>. Вместе с тем нужно учитывать, что производство и реализация товаров (работ, услуг) связаны с использованием различной по своему правовому режиму научной, технической, технологической, коммерческой и иной информации. Причем одна часть этой совокупности информации является открытой, а другая — закрытой. *Открытая информация* — это та, которая не скрывается производителем и коммерсантом. Она общезвестна, представляет познавательный и чисто прикладной интерес и используется в процессе производства и реализации товаров, выполнения работ и оказания услуг. *Закрытой является информация*, которая специально скрывается и защищается производителем товаров (работ, услуг) от посторонних лиц. Ее использование в процессе производства и сбыта товаров дает предпринимателю преимущество перед конкурентами на рынке.

Успех в производстве конкурентоспособных товаров (работ, услуг) определяется не только возможностью доступа предпринимателей к сырью и энергоресурсам. Одна из его важных предпосылок — информационные ресурсы коммерческой организации, используемые так, чтобы произвести и предложить потребителям товары более дешевые, более экономичные и удобные в обращении, чем у аналогичных фирм. Для решения этой задачи используется коммерчески значимая информация. В условиях конкуренции получение прибыли зависит от умения сохранить КЗИ, неизвестную кон-

<sup>1</sup> См.: Гражданское право. Т. 2. Полутом 1 / Отв. ред. проф. Е.А. Суханов. М., 2000. С. 563–635.

<sup>2</sup> См.: Пугинский Б.И. Коммерческое право России: Учебник. 2-е изд. М., 2006. С. 247–251.

курентам, а также от способности правильно распорядиться ею на рынке. Известно, что экономически устойчивой считается фирма, прибыли которой непрерывно увеличиваются. Важнейшим элементом процесса экономического роста является обладание КЗИ путем установления на нее режима коммерческой тайны (фактическая монополия) и умелое использование фирмой такой информации на договорной основе.

КЗИ может относиться к разным сферам (технике, технологии, экономике, организации производства, торговли и т.д.), отражать любую сторону деятельности организации, быть продуктом внутреннего производства либо может быть получена (передана) по договору, но в силу неизвестности ее партнерам (конкурентам), благодаря сохранению в тайне фирменного «секрета», имеет коммерческую ценность в рыночном обороте. Используемая в таком качестве информация, хотя и составляющая не более 5% от ее общего объема, является важнейшим ресурсом организации, ее инструментом (средством) получения прибыли в условиях существования конкуренции, а ее разглашение (утечка) может стать причиной экономических потерь. Таким образом, *под коммерчески значимой информацией следует понимать совокупность сведений технического, технологического и делового характера, составляющих коммерческую тайну, включая и секреты производства (ноу-хау), которые участвуют в гражданском (торговом) обороте с учетом присущих им особенностей гражданско-правового режима и являются связующим звеном во всех направленных деятельности организации.*

**Характеристика обращения коммерчески значимой информации.** Гражданский оборот КЗИ определяется ГК РФ, Законом о коммерческой тайне и иными актами или самими участниками, имеющими право отчуждать и приобретать такую информацию. В гражданском праве различают информацию по признаку ее оборотоспособности. Выделяют информацию, не изъятую и не ограниченную в гражданском обороте (общедоступная информация, которая свободно извлекается и распространяется любым лицом), изъятую из оборота (государственная тайна, рассекречивание и передача сведений, ее составляющих, допускается в установленном законом порядке) и ограниченную в обороте (коммерческая и иные виды тайн, сведения о которых отчуждаются по разрешению их обладателей).

Объективно коммерческая тайна возникает в процессе производства конкурентоспособного товара или осуществления иной деятельности, содержащей элементы новизны, основывающейся на ис-

пользовании КЗИ. Производитель получает преимущество на рынке благодаря использованию прогрессивных технологий, методов и приемов, сведения о которых не известны конкурентам. В результате товары (работы, услуги) пользуются большим спросом, чем те, при производстве которых такие технологии или приемы не использовались. Предприниматель, заботясь об увеличении своей прибыли, вынужден выделять определенные сведения в процессе хозяйственной деятельности и вводить в целях их сохранности режим коммерческой тайны.

В этой связи можно говорить об объективном процессе возникновения коммерческой тайны на любом этапе жизненного цикла производства товаров (работ, услуг), что обусловлено конкуренцией в условиях рыночной экономики. Очевидно, что тот предприниматель, который принимает меры в отношении сведений, благодаря использованию которых его товар (работа, услуга) становится конкурентоспособным, в состоянии получить стабильную прибыль и держаться в условиях жесткой борьбы, образно говоря, «на плаву». И наоборот, тот, кто пренебрегает этим правилом и недооценивает преимущества использования КЗИ, рискует оказаться банкротом. Можно было бы привести немало примеров того, как благодаря своевременному ограничению доступа к сведениям фирмы-производители до сих пор держат мировое лидерство в производстве товаров. Среди отечественных компаний — это авиационные, ракетно-космические, судостроительные и другие фирмы, входящие в состав высокотехнологичного сектора экономики.

В процессе производства и обмена товаров (работ и услуг) коммерческая тайна может существовать в различных формах, в зависимости от содержания КЗИ. Исходя из общепринятого определения товара как продукта труда, произведенного для продажи, проследим путь появления сведений, которые предприниматель «закрывает» с целью изготовления товара с такими полезными свойствами, которые необходимы для максимального удовлетворения нужд потребителя, формирования и обеспечения спроса на товар.

Для раскрытия особенностей возникновения коммерческой тайны в сфере производства и обмена товаров необходимо рассмотреть ее формы на основе такой классификации, которая с наибольшей полнотой отражала бы специфику факторов, определяющих необходимость выделения и закрытия сведений, делающих товар конкурентоспособным, благодаря сокрытию этих сведений от лиц, не имеющих к ним доступа на законных основаниях.

Как представляется, продуктивным в данном отношении может быть путь изучения форм появления коммерческой тайны в гражданском обороте применительно к принятой в экономической науке общей классификации производственных процессов, на основе которых выделяются *обеспечивающие, обслуживающие, вспомогательные и основные процессы*. Сведения об экономических, материальных и организационных условиях производства, процессах, обслуживающих производство, вспомогательных процессах и процессах, связанных с созданием основного вида продукции и ее реализацией, позволят установить наиболее уязвимые участки производства и сбыта товаров, где обращается КЗИ. Они могут быть связаны с подбором и расстановкой кадров, выполнением различных этапов НИОКР, использованием новой техники и оборудования, планированием и финансированием развития производства, разработкой конструкции инструмента и приспособлений, оснасткой моделей и подготовкой их производства, проектированием и конструированием изделий, разработкой их технологий, испытанием опытных образцов, постановкой продукции на производство и, наконец, реализацией (сбытом) готовой продукции. Определение участков в технологической цепочке производства и сбыта товаров, на которых имеется угроза возникновения экономических потерь, снижения прибыли, позволит своевременно предпринять меры противодействия, исключая или затрудняющие разглашение (утечку) КЗИ. Более конкретно участки возникновения коммерческой тайны в сфере производства и реализации продукции рассматриваются, в зависимости от содержания КЗИ, на различных этапах выполнения НИОКР и маркетинговых исследований, заключения и исполнения договоров на передачу информационных продуктов, оказание информационных услуг, включая коммерческую концессию. Отдельно определены участки сосредоточения КЗИ на стадиях подготовки производства автомобилей и их сбыта на рынке.

Полученные данные исследования позволяют сделать вывод о том, что КЗИ появляется в процессе разработки и внедрения новой техники (НИОКР), выполнения маркетинговых исследований и оказания услуг, а также совершения внутренних и внешнеторговых коммерческих сделок. Установлено, что секрет привлекательно-сти и конкурентоспособности товара (работы, услуги) заложен в технических и технологических особенностях производства и организации сбыта товара, выполнения работы или оказания услуги. Речь идет о неохраняемой научно-технической, технологической, произ-

водственной и иной информации, обладающей экономической ценностью, о конструкции машин, использовании формул (физических, химических и т.п.), применении методов производства, схем и чертежей отдельных узлов изделий, сведения о которых могут быть использованы конкурентами для налаживания производства аналогичных товаров, о различных приемах и хозяйственном опыте, котормы в советское время на безвозмездной основе обменивались предприятиями. Относясь к категории «ноу-хау», такого рода информация характеризует научно-техническую и технологическую стороны производства. Сказанное относится и к коммерческой (деловой) информации, характеризующей управленческую, финансовую, маркетинговую и другую деятельность, позволяющую успешно вести дела и заключать взаимовыгодные сделки. Следовательно, в сфере общественного производства на этапе разработки и освоения новой техники КЗИ проявляется в форме технических и технологических секретов (ноу-хау), а на этапе обмена (купли-продажи) товаров (торговли) — в форме коммерческих (деловых) секретов. Обе эти формы, содержащие КЗИ, охраняются правовым институтом коммерческой тайны.

Определенная специфика присуща обращению коммерческих (деловых) секретов. В рыночной экономике мало изготовить хорошую вещь, ее нужно еще выгодно продать. «Товары не могут сами отправляться на рынок и обмениваться»<sup>1</sup>. Для этих целей субъектами используется различная по содержанию и степени доступа коммерческая информация, которая обеспечивает продвижение товаров от производителей к потребителям. Результаты исследования подтверждают связь закрытой коммерческой информации с различными процессами коммерческой деятельности. Центральное место в торговом обороте занимают коммерческие сделки, с помощью которых осуществляется разнообразная деятельность российских хозяйствующих субъектов и их зарубежных партнеров. Сделка, применительно к торговому обороту, характеризует, во-первых, организационный процесс обмена товаров, включающий волево отношение собственников к заключению договора и исполнению обязательств, во-вторых, внутреннюю связь этапов сделки с торговой деятельностью субъектов, занимающихся продвижением товаров от изгото-

<sup>1</sup> Маркс К. Капитал. Критика политической экономии. Т. 1. Кн. 1: Процесс производства капитала. М.: ОАО «ЦЭФ», 2001. С. 85.

товителя к потребителю с целью получения прибыли. Как отмечал К. Маркс: «Процесс обмена товара осуществляется, таким образом, в виде двух противоположных и друг друга дополняющих метаморфозов — превращения товара в деньги и его обратного превращения из денег в товар. Моменты товарного метаморфоза представляют собой в то же время сделки товаровладельца — продажу, обмен товара на деньги; куплю, обмен денег на товар, и единство этих двух актов: продажу ради купли»<sup>1</sup>.

Внутренние и внешнеторговые сделки по реализации товаров, в течение всего периода их существования, требуют использования сторонами открытой и закрытой информации. Необходимость и степень использования закрытой информации определяется стороной в зависимости от этапов сделки. Для раскрытия особенностей возникновения закрытой информации в сфере торгового оборота необходимо рассмотрение действий субъектов на примере совершения *внешнеторговой сделки*, которая по многим параметрам является более сложной в правовом отношении, чем внутренняя коммерческая сделка. Сложность объясняется тем, что внешнеторговые сделки, как отмечает И.С. Зыкин, обладают двумя существенными признаками: «во-первых, в сделке участвуют лица (субъекты) различной национальной принадлежности, во-вторых, очерчивается круг отношений, в сфере которых заключаются такого рода сделки»<sup>2</sup>. Местонахождение коммерческих организаций на территории разных государств, где действуют различные правовые системы, серьезно осложняет процесс заключения и осуществления сделок. В результате, в них появляется ряд дополнительных условий, в том числе по соблюдению конфиденциальности, которые не всегда имеются во внутренних коммерческих сделках. Алгоритм деловой практики международной торговли в полной мере подчинен нормам Венской конвенции «О договорах международной купли-продажи товаров», а также учитывает возможность применения торговых обычаев базовых условий поставки товаров, содержащихся в Международных правилах толкования торговых терминов (Инкотермс) и Принципах международных коммерческих договоров (УНИДРУА), которые отражают обновленные международные нормы и учитываются сторонами в той мере, в какой это не запрещено императивными нормами во внутрен-

<sup>1</sup> Маркс К. Указ. соч. С. 103.

<sup>2</sup> Зыкин И.С. Договор во внешнеэкономической деятельности. М., 1990. С. 8.

него права. Такой подход с учетом действия национального законодательства<sup>1</sup> позволяет учитывать специфику различных этапов сделки, определяющих необходимость выделения и закрытия сведений, использование которых способствует формированию конкурентной стратегии продвижения товаров на рынке.

В теории серьезное внимание обоснованно уделяется анализу *основных этапов внешнеторговой сделки*. Принято считать, что *первый этап* представляет собой предконтрактную подготовку для продавца и покупателя. Соответственно состоит в исследовании рынка, которое ведет продавец и покупатель по двум взаимосвязанным направлениям: первое — изучение и анализ условий рынка; второе — изучение форм и методов торговли. Анализ практики показывает, что изучение спроса проводится в тесной взаимосвязи с изучением предложений и цен. Формы и методы торговли изучаются с целью анализа деятельности предприятий-изготовителей и фирм, выступающих на рынке в качестве покупателей конкретного товара, выявления позиций на рынке, каналов и методов сбыта и коммерческой практики, используемой в торговле данным товаром<sup>2</sup>. Продавец в этот период, на основании данных маркетинговых исследований, которые носят конфиденциальный характер, активно воздействует на рынок, прежде всего с помощью рекламы, с тем чтобы возбудить интерес к своей продукции потенциальных покупателей. Нужно сказать, что покупатель (импортер) товаров также изучает рынок, ставится во взаимодействие с ним, с тем чтобы обострить конкуренцию между продавцами (экспортерами), активизировать предложение товара, побудить экспортеров к понижению цен на товары и, таким образом, выбрать наиболее подходящего партнера. Данные, определяющие выбор потенциального продавца-партнера, носят конфиденциальный характер, поскольку получены покупателем в результате проведения собственных маркетинговых исследований. По результатам позиционирования товара на рынке<sup>3</sup> продавец (экспортер) делает свое предложение на продажу товара. Организация-импортер знакомит с этим предложением будущего потребителя товара и, убедив-

<sup>1</sup> См.: ФЗ от 13 октября 1995 г. № 157-ФЗ «О государственном регулировании внешнеторговой деятельности» // СЗ РФ. 1995. № 42. Ст. 3923.

<sup>2</sup> См.: Герчикова И.Н. Международное коммерческое дело: Учебник. М., 1996. С. 33–58.

<sup>3</sup> См.: Котлер Ф. Основы маркетинга / Пер. с англ. М., 1992. С. 93 — 95, 109.

шись, что параметры товара удовлетворяют требованиям заказчика, направляет запрос экспортеру с просьбой направить коммерческое предложение на товар, содержащее, в том числе, и закрытую информацию, необходимую для принятия решения о заключении контракта. Экспортер изучает запрос и согласовывает с изготовителем товара возможность его поставки. В этом задействованы различные службы организации — экспортера и изготовителя товара (финансово-экономические, юридические, маркетинга, транспортные и др.). По результатам согласования готовится оферта и направляется покупателю (импортеру). Получив оферту, импортер согласовывает с потребителем товара целесообразность заключения сделки на предложенных условиях и направляет экспортеру акцепт оферты. Такие действия означают решимость импортера заключить договор. На этапе предконтрактной подготовки стороны должны учитывать взаимные коммерческие интересы и исключать случаи, ведущие к потере конфиденциальности коммерческой информации. В этих целях они могут заключать соглашение о конфиденциальности информации, используемой в процессе ведения коммерческих переговоров.

*Второй этап* связан с проведением коммерческих переговоров<sup>1</sup> по согласованию условий и заключению контракта. Представляется, правильными будут действия сторон по взаимному информированию друг друга о степени конфиденциальности представляемой информации, касающейся предмета договора. Причем обязательство сторон о неразглашении полученной конфиденциальной информации можно закрепить документально в протоколе о намерениях либо в соглашении о неразглашении конфиденциальной информации (о секретности) Confidentiality (Secrecy) Agreement. Целесообразно такой протокол или соглашение подписать до начала переговоров. В нем нужно определить принципы соблюдения конфиденциальности; круг сведений, не подлежащих разглашению или передаче третьим лицам. Затем эти условия будут записаны в самом контракте или в отдельном документе, прилагаемом к нему. После решения вопроса о гарантиях соблюдения конфиденциальности стороны переходят непосредственно к переговорам по выработке условий контракта. Речь идет о согласовании предмета договора, коммерческих, технических, транспортных, юридических и

<sup>1</sup> См.: Соловьев Э.Я. Искусство проведения переговоров. М., 2006. С. 6 — 137, и др.

иных условий. Перед подписанием контракта стороны должны получить в соответствующих организациях своих стран экспортную и импортную лицензии, в случае если товар подлежит лицензированию. О получении лицензии стороны обязаны уведомить друг друга. После решения этого вопроса стороны подписывают контракт о поставке товара. Вместе с контрактом могут быть подписаны отдельные соглашения о командировании специалистов, техническом обслуживании и другие. В контракте стороны предусматривают условия о конфиденциальности. Как показывает анализ ряда контрактов, это условие носит общий характер и его можно применить к предмету любого контракта. Например, первая сторона обязуется сохранять режим конфиденциальности в течение неограниченного срока в отношении сведений, относящихся к товарам, а также любой иной информации, полученной от другой стороны, которую обособленно можно считать конфиденциальной, не разглашать никакую такую информацию третьим сторонам и не использовать ее иначе, как в целях выполнения настоящего договора.

*Третий этап* сделки связан с ее исполнением со стороны экспортера. Экспортер заказывает изготовителю товар, подлежащий поставке импортеру, согласно контракту. Затем в соответствии с условиями договора купли-продажи изготовителем товара, либо импортером, либо экспортером осуществляется фрахтование транспорта для перевозки товара. Импортер обеспечивает платеж за товар. Это может быть подтверждено либо банковской гарантией оплаты, либо открытием аккредитива, либо переводом аванса, а также использованием других способы расчета. Экспортер после получения от покупателя гарантий оплаты направляет поручение на экспедирование и таможенное декларирование груза<sup>1</sup>, а также оформляет через свой банк паспорт сделки, который вместе с таможенной декларацией является основанием для пропуска товара через таможенную границу России. Кроме того, в соответствии с законом импортером могут быть затребованы от экспортера сертификаты соответствия товара требованиям безопасности и происхождения товара. После оформления названных выше документов экспортер информирует импортера о готовности товара к отгрузке, отгружает товар покупателю и ставит его в известность о факте отгрузки. В своем банке экспортер получает валюту в оплату за товар, осуществляет платежи в бюджет, рассчитывает

<sup>1</sup> См.: Халилов С.В. Таможенное право: Учебник. 2-е изд. М., 2005. С. 84—141.



вается с изготовителем товара и иными кредиторами. Органы валютного контроля в соответствии с Законом РФ «О валютном регулировании и валютном контроле» от 9 октября 1992 г. № 3615-1 (в ред. от 7 июля 2003 г. № 116-ФЗ) могут запрашивать любую, в том числе и закрытую, информацию, касающуюся обоснованности платежей в иностранной валюте, учета и отчетности валютных операций. В данном случае субъекты внешнеэкономической деятельности обязаны по запросу государственного органа предоставлять такую информацию для проверки.

*Четвертый этап* сделки связан с ее исполнением со стороны импортера. Отгруженный экспортером товар поступает на таможенный склад в стране покупателя-импортера, который оплачивает таможенную пошлину, налоги и сборы<sup>1</sup>. Для получения товара из таможенного покупателя должен предьявить таможенным органам ввозную грузовую декларацию, товарораспорядительные документы, квитанции об оплате налогов и сборов и другие документы. Речь идет о документах, которые следуют с грузом от пункта отправления до пункта назначения. Это коммерческие, транспортные и таможенные документы. После получения товара импортер продает его потребителю и производит расчеты с бюджетом и кредиторами.

Для третьего и четвертого этапов характерным является соблюдение сторонами условий конфиденциальности сделки, кроме случаев, когда в силу закона они обязаны предоставить сведения, составляющие коммерческую тайну по мотивированному запросу в таможенные, налоговые и иные государственные органы.

В теории практически остается вне поля зрения исследователей вопрос о том, что по мере совершения сделок хозяйствующие субъекты накапливают ценный опыт и знания, которые составляют закрытую часть коммерческой информации и требуют защиты. Совокупность отдельных сведений, используемых в торговом обороте, раскрывает планы конкурентной стратегии, результаты маркетинговых исследований и рекламной деятельности, новые приемы и технологии сбыта товаров, списки клиентов, посредников, особенности финансовых, страховых и иных операций. Знание подобных сведений дает конкурентам преимущество при завоевании рынков сбыта товаров. В условиях конкуренции любая организация принимает меры по сохранению такой информации. Недобросовестные конкуренты

<sup>1</sup> См.: Халилов С.В. Указ. соч. С. 247–315.

ты зачастую прибегают к использованию методов «промышленного шпионажа»<sup>1</sup>, хотя используются и вполне доступные легальные средства для ведения конкурентной разведки. Поэтому достижение конкурентных преимуществ на рынке требует от хозяйствующих субъектов охраны своей информации с использованием имеющихся в их распоряжении правовых средств.

### § 3. Опыт правового регулирования информации с ограниченным доступом в советский период

Исследование проблем правовой природы коммерчески значимой информации в советский период и ее защита в рамках существовавшей в то время единой системы охраны государственных секретов имеет исключительно важное значение для понимания процесса трансформации части государственных секретов в промышленные (коммерческие) секреты предприятий и формирования, в этой связи, предложений о направлениях, формах, методах и средствах правовой защиты КЗИ в современных условиях. Предметом изучения в данном случае является процесс осуществления правовой защиты технической, технологической и иной информации с использованием правового режима, который был установлен на основании общесоюзных и ведомственных актов для охраны государственных секретов, включая и «служебную тайну», а также сведений, отнесенных к информации «для служебного пользования».

Доминирующая роль государства со всей определенностью проявлялась в том, что производство такой информации, ее использование, передача и правовая охрана осуществлялись предприятиями в рамках выполнения государственного заказа и под контролем соответствующих государственных структур. Причем этот процесс происходил по вертикали (орган государственного и хозяйственного управления — предприятие) на основании директивных указаний и по горизонтали (предприятие — предприятие) путем заключения и исполнения хозяйственных договоров<sup>2</sup>. Предприятия являлись одновременно производителями и потребителями охраняемой инфор-

<sup>1</sup> См.: Ярочкин В.И. Безопасность информационных систем. М., 1996. С. 143–154, и др.

<sup>2</sup> См.: Хохлов С.А. Договорная работа. Свердловск, 1986. С. 24–78, и др.

мации. Они могли использовать такого рода информацию при выполнении научно-исследовательских и опытно-конструкторских работ (НИОКР) в рамках госзаказа. Передача охраняемой информации контрагентам по госзаказу либо использование ее при выполнении собственных хозяйственных работ осуществлялись исключительно по разрешению министерства, являвшегося полномочным органом государства, обладавшего правом распоряжения такой информацией. Интересы предприятия по поводу производства, использования и защиты охраняемой информации напрямую были связаны с размещением госзаказа и выполнением хозяйственных работ, которые обеспечивали ему получение прибыли в рамках социалистической системы хозяйства. Следовательно, можно говорить об экономической ценности охраняемой информации для предприятий и ее потенциальной коммерческой значимости в плане заключения договоров и исполнения обязательств. Однако в частных интересах такая информация не могла быть использована предприятиями, помимо государства, в период существования социалистических производственных отношений.

*Признавая аксиоматичным положение о существовании в советский период охраняемой информации технического, технологического и иного характера, позволявшей предприятиям получать прибыль в интересах государства, представляется важным исследование форм, методов и правовых средств, применявшихся для защиты такой информации. При этом следует исходить из функционирования единой системы защиты государственных секретов, в рамках которой осуществлялось обращение КЗИ. В этой связи первоочередного рассмотрения требуют вопросы урегулирования правоотношений в сфере охраны государственных секретов и организации защиты секретов на предприятиях.*

**Регулирование правоотношений в сфере охраны государственных секретов.** Характеристика советского законодательства об охране государственных секретов основывается на совокупности административно-правовых и уголовно-правовых норм, регулировавших правоотношения по поводу определения, использования и защиты сведений, составлявших государственную и служебную тайну. Отношения, связанные с определением сведений, составлявших государственную и служебную тайну, их использованием, сохранением и обеспечением режима секретности проводимых работ регулировались, прежде всего, нормами административного права.

*Существовавшая в СССР система защиты секретов представляла собой иерархическую административную структуру, которая была*

*основана на властном подчинении и полностью отражала тоталитарный характер государства. Она являлась в определенном смысле опорой государства в проведении его внутренней и внешней политики. Большинство исследователей<sup>1</sup> в целом правильно называют причины, обусловившие в советский период тотальный характер закрытия информации во многих сферах деятельности государства. Система защиты секретов, как отмечает В.А. Рубанов, «...зародилась в трагический для советского народа период „обострения классовой борьбы“, выкристаллизовалась в годы Великой Отечественной войны и укрепилась во времена войны „холодной“»<sup>2</sup>. В данном случае фиксируется влияние в основном объективных факторов, но немалую роль играли и субъективные причины.*

*Структура управления системой защиты секретов в СССР характеризовалась единым организационным содержанием и юридическим неравенством сторон. Субъектами правоотношений в сфере защиты государственных секретов являлись Комитет государственной безопасности (КГБ) СССР и его органы на местах, министерства оборонных отраслей промышленности и подведомственные им предприятия, военные представительства и учреждения Министерства обороны (МО) СССР, отдельные министерства и ведомства на основании предоставленных им Советом Министров СССР (далее — СМ СССР) прав по вопросам обеспечения режима секретности, а также подчиненные им предприятия. В министерствах и ведомствах, на предприятиях, в организациях и учреждениях функционировали специально создаваемые «режимно-секретные органы» (РСО), которые непосредственно занимались деятельностью по обеспечению режима секретности при выполнении секретных работ, использовании и хранении секретных документов и специальных изделий.*

*Отношения между основными субъектами, которыми являлись министерство и подчиненные ему предприятия, регулировались с помощью административно-правовых методов. Министерство было наделено необходимыми государственно-властными полномочиями по отношению к подчиненным ему предприятиям. Оно принимало решения по поводу определения степени секретности категорий све-*

<sup>1</sup> См.: Никулин Л. Конверсия секретности: неразумная недостаточность // Коммунист. 1990. № 9, и др.

<sup>2</sup> Рубанов В. От «культы секретности» — к информационной культуре // Коммунист. 1988. № 13. С. 25.

дений, их использования и передачи контрагентам, осуществляло контроль обеспечения режима секретности на предприятиях и при необходимости применяло меры воздействия к руководящему составу предприятий в случаях совершения правонарушений в сфере защиты государственных секретов. Аналогичным образом выстраивались отношения на предприятиях между администрацией и руководителями структурных подразделений, между ними и работниками в рамках трудовых правоотношений, на основании действовавших в организации локальных актов. Соответствующее поведение сторон обеспечивалось действием императивных административных норм, содержащихся в общесоюзных и ведомственных нормативных правовых актах.

*Административно-правовые нормы, которые устанавливали правовой статус субъектов и предписывали определенные варианты поведения лиц, допущенных к секретным работам, документам и изделиям, можно подразделить на различные виды, в зависимости от содержащихся в них предписаний.*

*Обязывающие нормы* содержали предписание лицам, допущенным к секретным работам, документам и изделиям, совершать определенные действия по обеспечению режима секретности в соответствии с требованиями общесоюзной Инструкции от 12 мая 1987 г. № 556-126 (далее — Инструкция № 0126-87), ведомственных инструкций и приказов министерств, локальных актов предприятий.

*Запрещающие нормы* устанавливали ограничения для лиц, допущенных к секретным работам, документам и изделиям, и указывали на недопустимость совершения действий, предусмотренных общесоюзными, ведомственными и локальными актами. Речь идет о запретах, установленных администрацией предприятий в отношении лиц-секретносителей. Это выражалось в ограничении прав работников на посещение посольств и представительств иностранных компаний, ведение служебных переговоров по секретным вопросам с использованием незащищенных линий связи, сообщение в устной или письменной форме кому бы то ни было (в том числе и родственникам) секретных сведений и других ограничениях.

*Уполномочивающие нормы* предоставляли возможность предприятиям и их РСО действовать по своему усмотрению при планировании, организации и реализации мероприятий по обеспечению режима секретности проводимых работ в пределах, установленных общесоюзными и ведомственными актами.

*Стимулирующие нормы* определяли возможность применения мер морального характера к лицам, допущенным к секретным работам, документам и изделиям (например, вручение почетных грамот и др.).

Нормы, содержащиеся в общесоюзных и ведомственных актах, подразделялись на *материальные*, определявшие права и обязанности субъектов, и *процессуальные*, предусматривавшие порядок осуществления контроля по обеспечению режима секретности и проведения служебного расследования по факту разглашения секретных сведений. Кроме того, законодательством была определена процедура привлечения лиц к ответственности за разглашение государственных секретов, утрату документов или изделий, содержащих такие сведения.

*Правовой статус субъектов в сфере охраны государственных секретов и обеспечения режима секретности определялся не Конституцией и законами СССР, а директивными указаниями Центрального Комитета Коммунистической партии Советского Союза (далее — ЦК КПСС), в виде отдельных или совместных с СМ СССР постановлений. Важнейшими правовыми актами ЦК КПСС и СМ СССР, определявшими политику в области защиты государственных секретов, являлись постановления от 1 октября 1970 г. № 840-285 «О мерах по усилению режима секретности», от 15 ноября 1976 г. № 941-323 «О мерах по дальнейшему совершенствованию системы сохранения государственных секретов» и другие.*

Особое место в регулировании прав и обязанностей в области защиты государственных секретов занимали постановления СМ СССР. На уровне правительства были приняты все перечни главнейших сведений, составивших в различные периоды государственную тайну СССР, общесоюзные инструкции по обеспечению сохранения государственной тайны и режима секретности проводимых работ в учреждениях и на предприятиях СССР (последняя из них была принята 12 мая 1987 г. № 556-126), положения о порядке установления степени секретности категорий сведений и определения степени секретности сведений, содержащихся в работах, документах и изделиях (последнее из них было принято 3 декабря 1980 г. № 12-378). Правительством принимались решения по наиболее важным направлениям защиты государственных секретов, в которых содержались нормы административного и хозяйственного права. Например, постановление СМ СССР от 12 августа 1982 г. № 751-194

«О дополнительных мерах по обеспечению сохранности государственных секретов по оборонной тематике» и другие.

*Названные постановления партии и правительств, за исключением некоторых актов, например, отдельных перечней сведений, составляющих государственную тайну, были секретными.* Доступ к ним имел ограниченный круг людей, включая и исполнителей секретных работ. Поэтому трудно говорить о гарантиях реализации гражданами прав на защиту в области охраны государственных секретов, поскольку, например, при рассмотрении уголовных дел суд руководствовался секретными постановлениями, неизвестными обвиняемому. Нужно сказать, что с принятием СМ СССР открытого постановления от 27 апреля 1926 г. «Об утверждении перечня сведений, являющихся по своему содержанию специально охраняемой государственной тайной»<sup>1</sup> на правоохранительные органы были возложены обязанности по руководству этим перечнем при решении вопросов о привлечении лиц, виновных в разглашении сведений, составляющих государственную тайну, к уголовной ответственности.

*Общесоюзная инструкция № 0126-87 содержала, как и все предыдущие аналогичные акты, начиная с момента утверждения первой такой инструкции в 1959 году, отсылочные нормы об ответственности лиц за разглашение сведений, составляющих государственную и служебную тайну.* Лица, допустившие правонарушение в этой сфере, привлекались к юридической ответственности в соответствии с нормами действовавшего в то время законодательства. Причем ответственность была установлена дифференцированно, в зависимости от грифа секретности. Так, за разглашение сведений, составлявших служебную тайну, утрату документов и изделий, содержащих такие сведения, либо иные нарушения режима секретности и виновные лица привлекались к дисциплинарной ответственности и могли быть, по согласованию с органами КГБ, отстранены от секретных работ путем аннулирования им соответствующей формы допуска. За эти же действия, если они были связаны с передачей сведений, составляющих служебную тайну, иностранным организациям, законом предусматривалась возможность привлечения лиц к уголовной ответственности. *Никакие другие виды юридической ответственности, кроме уголовной и дисциплинарной ответственности, законодательством того времени не были установлены.*

*Советское уголовное законодательство содержало нормы об уголовной ответственности за разглашение государственной тайны.* Основные начала уголовного законодательства Союза ССР и союзных республик, которые были приняты 31 октября 1924 г. ЦИК СССР, отнесли к компетенции Союза ССР издание законодательства об уголовной ответственности за государственные преступления. Уголовный кодекс РСФСР (далее — УК РСФСР) 1926 года включал нормы об уголовной ответственности за разглашение государственных секретов. Указ Президиума Верховного Совета СССР от 9 июля 1947 г. «Об ответственности за разглашение государственной тайны и за утрату документов, содержащих государственную тайну»<sup>1</sup>, принятый на следующий день после принятия 8 июля 1947 г. СМ СССР открытого постановления «Об установлении Перечня сведений, составляющих государственную тайну, разглашение которых карается по закону»<sup>2</sup>, закрепил три самостоятельных состава преступлений, посягающих на сохранность государственной тайны. Указ предусматривал усиленные меры наказания за разглашение сведений, составляющих государственную тайну, утрату материалов, документов и изделий, содержащих такие сведения, а также за передачу за границу изобретений, открытий или технических усовершенствований невоенного характера. Принятые акты адекватно отражали политическую и экономическую обстановку, в которой находилась наша страна после окончания Великой Отечественной войны. Усиление режима секретности было продиктовано объективной необходимостью укрепления обороноспособности страны, связанной с разработкой новых видов вооружения и военной техники, в частности, с созданием ракетно-ядерного щита СССР.

Перечень 1947 г. в этой связи включал значительно расширенный, по сравнению с аналогичным актом 1926 г., раздел о сведениях экономического характера. Например, сведения о планах по ввозу и вывозу отдельных товаров, состояний экспортных фондов товаров, о промышленности в целом и отдельных ее отраслях, сельском хозяйстве, торговле и другие. В названном перечне практически был заново сформирован раздел, содержащий сведения о научных открытиях, изобретениях и технических усовершенствованиях невоенно-

<sup>1</sup> См.: Ведомости Верховного Совета СССР. 1947. № 20.

<sup>2</sup> См.: Сборник документов по истории уголовного законодательства СССР и РСФСР 1917–1952 гг. М., 1953. С. 431–432.

<sup>1</sup> См.: Сборник законов СССР. М., 1926. № 32.

го характера. *Исследовательские и экспериментальные работы в любых областях науки и техники до их окончательного завершения являлись секретными.* В рамках действовавшего в то время законодательства была определена процедура получения разрешения со стороны государства на их открытое опубликование. Контроль обеспечения режима секретности и цензура опубликования открытых изданий научно-технического и иного характера находились в ведении органов КГБ и Главного управления по охране государственных тайн в печати при СМ СССР (Главлит СССР).

Усиление военного противостояния СССР — США и создание в 1955 году военно-политического блока НАТО потребовали от нашей страны уточнения круга сведений, подлежащих защите. Постановлением СМ СССР от 28 апреля 1956 г. был утвержден новый «Перечень сведений, составляющих государственную тайну, разглашение которых карается законом»<sup>1</sup>. В этом перечне раздел о технической, технологической и иной информации дополняется новыми категориями сведений, которые ранее не включались в прежние перечни. Верховным Советом СССР 25 декабря 1958 г. были приняты Основы уголовного законодательства Союза ССР и союзных республик и Закон об уголовной ответственности за государственные преступления<sup>2</sup>, ныне утратившие свою юридическую силу. Необходимость их принятия обуславливалась тем, что некоторые нормы действовавшего в то время законодательства устарели, другие нуждались в уточнении ввиду их недостаточной четкости, третьи в связи с изменением обстановки потеряли актуальность и их необходимо было исключить из числа государственных преступлений<sup>3</sup>. Общесоюзное законодательство явилось юридической базой для принятия 27 октября 1960 г. УК РСФСР, который действовал на территории нашей страны до 1 января 1997 г., т.е. до момента вступления в силу нового УК РФ.

УК РСФСР 1961 г. включал семь статей, обеспечивавших правовую охрану государственной, военной и служебной тайны<sup>4</sup>. В част-

<sup>1</sup> См.: Справочник по законодательству для работников органов прокуратуры, суда и МВД. Т. 26. Ч. 1. М.: Юрид. лит., 1971. С. 30.

<sup>2</sup> См.: Ведомости Верховного Совета СССР. 1959. № 1. Ст. 8 (с изм. и доп.); Уголовное законодательство СССР и союзных республик. Т. 1. М., 1963. С. 29–50.

<sup>3</sup> См.: Материалы второй сессии Верховного Совета СССР пятого созыва. Стенографический отчет. М., 1959. С. 413.

<sup>4</sup> См.: Комментарий к Уголовному кодексу РСФСР / Под ред. Ю.Д. Северина. М., Юрид. лит., 1980.

ности, к преступным посягательствам на государственную, военную и служебную тайну относились следующие составы преступлений. Во-первых, особо опасные государственные преступления, такие как: измена Родине (ст. 64 УК) и шпионаж (ст. 65 УК). Одной из форм измены Родине являлась выдача государственной или военной тайны иностранному государству. Основным признаком шпионажа являлись сведения, составлявшие государственную или военную тайну, а также иные сведения, не относящиеся к этим видам тайн. Во-вторых, иные государственные преступления. Это разглашение государственной тайны (ст. 75 УК) и утрата документов, содержащих государственную тайну (ст. 76 УК). Статья 259 УК предусматривала уголовную ответственность за разглашение военной тайны или утрату документов, содержащих такую тайну. Понятием военной тайны охватывались сведения военного характера, составлявшие государственную тайну.

Обязательным признаком названных выше составов преступлений являлся предмет преступления, включавший круг сведений, относящихся к государственной и военной тайне, который определялся в соответствии с «Перечнем главнейших сведений, составляющих государственную тайну» и ведомственными перечнями.

В-третьих, в числе общеуголовных преступлений впервые в советском законодательстве была установлена уголовная ответственность определенной категории работников органов связи за нарушение тайны переписки граждан (ст. 135 УК) и за разглашение данных предварительного следствия или дознания (ст. 184 УК). Речь в данном случае идет о разглашении сведений, составляющих служебную тайну. Таким образом, действовавшее в советский период уголовное законодательство позволяло надежно защищать государственные секреты, включая сведения технического и технологического характера.

*Дисциплинарная ответственность лиц, допустивших разглашение сведений, составляющих служебную тайну, либо утрату документов и изделий, содержащих такие сведения, и иные нарушения режима секретности, действовавшим в то время трудовым законодательством не устанавливалась.* Хотя общесоюзная инструкция № 0126-87 содержала отсылочные нормы к трудовому законодательству о возможности привлечения правонарушителей к дисциплинарной ответственности и отстранения их от работы, связанной с использованием и защитой сведений, составлявших государственные секреты. В данном случае речь шла о применении к нарушителям режима секретности

общих норм Кодекса законов о труде РСФСР (далее — КЗоТ)<sup>1</sup> об ответственности работников за нарушения дисциплины труда. В трудовом законодательстве не были закреплены требования к работодателям, допускаемым к государственной и служебной тайне. Не были определены их трудовые обязанности по соблюдению режима секретности. В КЗоТ отсутствовали правовые основания увольнения работников в случае невыполнения или ненадлежащего выполнения ими обязанностей по сохранению государственных секретов. Применение по аналогии норм трудового законодательства к лицам, допустившим нарушения режима секретности, было связано на практике с нарушением принципа законности в деятельности администрации предприятий и правоохранительных органов. Так, например, ст. 33 КЗоТ предусматривала возможность увольнения рабочего или служащего за систематическое невыполнение им без уважительной причины обязанностей, возложенных на него трудовым договором и правилами внутреннего трудового распорядка, и только в том случае, если к нему ранее применялись меры дисциплинарного взыскания<sup>2</sup>. Применение к нарушителям мер дисциплинарного взыскания в виде объявления выговора или строгого выговора не всегда позволяло получить нужный эффект. Дело в том, что часто даже одно грубое нарушение требований режима секретности, допущенное лицом, могло причинить угрозу интересам предприятия и в конечном итоге государству. Однако увольнение такого нарушителя или перевод его на работу, не связанную с государственными секретами, законом не были предусмотрены. Нечеткая регламентация процедуры отстранения работника от работы с секретными документами и инструкциями, возможность применения которой упоминается в Инструкции № 0126-87, и, что самое главное, отсутствия правовых оснований в КЗоТ приводили на практике к весьма спорным ситуациям. Отстранение от работы с последующим увольнением часто осуществлялось по нелегальным и незаконным основаниям. Чаше всего администрация, не без помощи РСО, создавала ситуацию, компрометирующую поведение работника. В такой обстановке у работника не оставалось другого варианта, как написать заявление об увольнении по собственному желанию. Использовались и другие способы уволь-

<sup>1</sup> См.: Ведомости Верховного Совета РСФСР. 1971. № 50. Ст. 1007.

<sup>2</sup> См.: Кодекс законов о труде РСФСР // Ведомости Верховного Совета РСФСР. 1971. № 50. Ст. 1007.

нения в рамках действовавшего в то время КЗоТ. Например, увольнение оформлялось по сокращению штатов и другим, фактически не существующим, основаниям.

**Характеристика защиты секретной информации на предприятии в советский период.** Накопление исследовательских материалов, приоткрытие занавеса «секретности» с момента «перестройки» повзвали в рассматриваемый исторический период обобщить данные о состоянии правового регулирования в сфере защиты секретной информации, проанализировать недостатки в практике применения законодательства об ответственности за нарушения в данной сфере<sup>1</sup>.

В Советском Союзе была создана и действовала надежная в правовом отношении система секретности, хотя некоторые исследователи в своих публикациях справедливо отмечали ее громоздкость на отдельных уровнях управления и бюрократически извращения<sup>2</sup>. Правовое регулирование общественных отношений, которые складывались в рамках этой системы, было обеспечено со стороны государства изданием Перечня сведений, составляющих государственную тайну, Закона об уголовной ответственности за государственные преступления, принятого 25 декабря 1958 г., с последующими изменениями и дополнениями от 11 января 1984 г., в который были включены нормы об ответственности за разглашение государственной тайны, утрату документов, содержащих государственную тайну, передачу иностранным организациям сведений, составляющих служебную тайну; установлением порядка защиты секретных сведений; созданием в структурах государственного управления, на предприятиях специальных органов и подразделений — РСО, занимавшихся вопросами защиты информации, и наделением их соответствующими полномочиями.

Сложность и многоплановость работы по защите секретной информации не позволили в советский период получить всестороннего и единообразного разрешения этой проблемы в теории, что в определенной мере отражается и сегодня в практике защиты информации,

<sup>1</sup> См.: Северин В.А. Правовое регулирование охраны государственных секретов в СССР // Советское государство и право. 1991. № 1, и др.

<sup>2</sup> См.: Гласность и демократия // Правда. 1988. 19 июня; Рубанов В. От «культы секретности» — к информационной культуре // Коммунист. 1988. № 13. С. 24—36; Перестройка, гласность... шпионаж // Красная звезда. 1989. 11 мая; Рейзберг Б. Плата за неразглашение // Поиск. 1989. № 15, и др.

имеющей коммерческую значимость. Внимание ученых<sup>1</sup> в тот период было сосредоточено в основном на изучении уголовно-правовых аспектов охраны государственных секретов. Перестройка, происходившая в стране, напрямую коснулась разрешения проблем в сфере охраны секретов, что в последующем было связано с проведением широкомасштабного комплексного исследования по программе «Секрет»<sup>2</sup>. Но при всей их теоретической значимости проблемы защиты технологической, технической и иной информации, охраняемой в правовом режиме «государственной тайны», засекречивания и рассекречивания такой информации, исследования личности нарушителей режима секретности, причин и обстоятельств, способствующих таким нарушениям, и меры предупреждения не получили в то время должного рассмотрения. Вместе с тем полученные результаты исследований позволили сделать вывод, что вопросы защиты секретной информации, накопившиеся в результате деятельности органов государственной власти и управления, государственных и кооперативных предприятий и организаций требуют законодательного регулирования.

В СССР на государственном уровне были установлены три степени секретности сведений: особой важности, совершенно секретно и секретно. Сведения, имевшие степень секретности «особой важности» и «совершенно секретно», составляли государственную тайну, а гриф «секретно» — служебную тайну. Проводимая в стране работа по рассекречиванию информации позволила в конце 80-х годов значительно уменьшить объем секретных сведений, охраняемых государством, и выделить часть информации, производство которой осуществлялось предприятием и относившейся к его «промышленным секретам», с грифом «секретно». Вместе с тем она выявила несовершенство механизма засекречивания информации. В частности, в рассматриваемый период не было четкого разграничения между сведениями, которым устанавливалась степень секретности особой важности и совершенно секретно. В первом случае при отнесении информации к сведениям особой важности предусматри-

валось наступление особо тяжелых последствий, во втором — тяжелых последствий одного и того же круга сведений, касающихся обороны и безопасности, политических и экономических интересов СССР. Качественные критерии оценки не всегда позволяли на практике правильно определить степень секретности. Поэтому было высказано предложение о том, что в проекте Закона о государственной тайне должны быть установлены иные критерии, например, *стоимостные* оценки ущерба. Речь шла о разработке шкалы материального ущерба, в зависимости от значений которой устанавливается соответствующая степень секретности. Например, к категории «особой важности» относятся сведения, ущерб от разглашения которых превышает 2 млрд руб.; к категории «совершенно секретно» — ущерб в пределах от 1 млн руб. до 1 млрд руб.; к категории «секретно» — ущерб в пределах от 100 тыс. руб. до 1 млн руб. Нужно отметить условность стоимостных значений, составленных с использованием метода экспертных оценок для промышленных предприятий (цены приведены по состоянию на 1 января 1991 г.). Такой подход с учетом качественной оценки позволил бы различать сведения особой важности и совершенно секретные. Среди критериев оценки ущерба следует выделить *характер сведений* (относимость их к защищаемым областям деятельности государства), их *важность* (новизна, актуальность, эффективность, степень обобщенности), *возможность защиты* и *материальные затраты* на их охрану. Это предложение в полной мере относится к сведениям категории «секретно», выделенных предприятиями и защищаемых сегодня с помощью института коммерческой тайны. Представляется, что эти сведения, относимые к КЗИ, также могут быть классифицированы по степени важности и их характеру.

Порядок определения степени секретности информации, ее просмотра и обеспечения сохранности был урегулирован Общесоюзной инструкцией № 0126-87. В соответствии с ее требованиями право на засекречивание информации было предоставлено СМ СССР, который утверждал Перечень главнейших сведений (ПГС), составляющих государственную тайну; руководителям министерств и ведомств, которые на основании ПГС утверждали ведомственные перечни сведений, подлежащих засекречиванию, с учетом специфики их деятельности.

На основании требований указанных выше перечней исполнители и их руководители обязаны присвоить соответствующий гриф секретности работам, документам и изделиям, содержащим секретные сведения. Степень секретности сведений по НИОКР,

<sup>1</sup> См.: Дьяков С.В., Игнатъев А.А., Карпушин М.П. Ответственность за государственные преступления. М., 1988. С. 118—140; Мелникова Л.А. Совершенствование законодательства об охране государственной тайны // Советское государство и право. 1989. № 6. С. 123, и др.

<sup>2</sup> См.: Материалы «круглого стола» «Известий». Гриф «секретно» в эпоху гласности // Известия. 1989. 28 апреля.

подлежащих защите, определялась заказчиком в техническом задании на проведение работы, что было предусмотрено соответствующими государственными и ведомственными стандартами. Порядок рассекречивания информации был основан на учете факторов и условий, требовавших корректировки степени секретности. Применительно к НИОКР такая корректировка была возможна на каждом этапе их проведения.

Анализ практики засекречивания и рассекречивания информации позволил выявить ряд недостатков, связанных, во-первых, с нарушениями установленного порядка, которые выражаются в неадекватном засекречивании или рассекречивании исполнителями работ, документов и изделий, невыполнении требований о периодическом пересмотре степени секретности, в особенности по НИОКР. Основные причины указанных недостатков — в невыполнении или незнании исполнителями нормативных требований в области защиты секретной информации. Нужно отметить, что более половины из числа опрошенных на ряде предприятий не были ознакомлены с основополагающими документами или были ознакомлены в общих чертах. Отмечался недостаточный контроль РСО за засекречиванием и рассекречиванием информации.

Во-вторых, это недостатки, связанные с несовершенством общих и ведомственных перечней (так, 27% опрошенных заявили о необходимости конкретизации Перечней, 15% — о регулярности их пересмотра, 10% — об их сужении); установление в них излишне высокой степени секретности отдельным категориям сведений, несвоевременное включение в них сведений, требующих защиты, особенно в части НИОКР, а также сохранение сведений, утративших свою актуальность.

В целях устранения отмеченных недостатков было высказано предложение о разработке нового проекта Перечня главнейших сведений, с учетом определенной методики (об этом заявили 59% опрошенных на предприятиях). Основу предложенной методики составили следующие положения. Засекречивание сведений должно быть направлено на предотвращение причинения ущерба обороноспособностям, государственной безопасности, политическим, экономическим и научно-техническим интересам СССР. Описание возможного ущерба должно сопровождаться соответствующими качественными и количественными показателями (например, в виде материального ущерба), полученными расчетным или экспертным путем.

*Концепция учета факторов при оценке ущерба от разглашения секретной информации*, отдельные элементы которой получили свое отражение в принятых после 1991 года законодательных и иных правовых актах, используются в современной правоприменительной и хозяйственной практике применительно к установлению и обеспечению коммерческими организациями режима коммерческой тайны. Ее суть сводится к следующему.

Если возможный ущерб незначителен и не представляет опасности для общества и государства, или отсутствует принципиальная возможность защиты сведений, или затраты на защиту сведений, несмотря на возможный ущерб, превышают его, то сведения подлежат отнесению к категории несекретных и должны быть исключены из дальнейшего рассмотрения.

Засекречивание информации всегда связано с наступлением определенных отрицательных последствий для общества и государства, в число которых входят, с одной стороны, затраты на обеспечение режимных мероприятий, а с другой — потери от ограничений в пользовании секретной информацией. При определении затрат на защиту сведений необходимо оценить, какие материальные, трудовые и финансовые ресурсы потребуются для осуществления мероприятий по обеспечению соответствующих видов режима секретности. Такие затраты могут потребоваться при проведении необходимых инженерно-технических работ; организации охраны секретных работ, оформлении нужного числа сотрудников, допускаемых к секретным работам и документам; финансировании вновь создаваемых РСО и внесении дополнений в штаты предприятий; осуществлении иных мероприятий в зависимости от объема работ по обеспечению режима секретности.

Определяя отрицательные последствия засекречивания сведений, необходимо оценить факторы, которые обуславливают недополученную при этом выгоду. К числу таких факторов относятся политическая целесообразность открытого опубликования сведений; значительный экономический эффект от широкого использования сведений в отраслях народного хозяйства; ускорение научно-технического прогресса страны; укрепление внешнеэкономических позиций государства на мировом рынке и другие.

Для обеспечения полноты и объективности определения преимуществ открытого опубликования сведений, если предполагается экономический эффект, как представляется, следует произвести его стоимостную оценку, получаемую расчетным или экспертным пу-



тем. Если отрицательные последствия засекречивания сведений преобладают возможный ущерб в случае их разглашения, то они подлежат отнесению к категории несекретных и должны быть исключены из дальнейшего рассмотрения. При возможном ущербе, в совокупности превышающем затраты на защиту этих сведений и отрицательные последствия их засекречивания, сведения подлежат засекречиванию и отнесению к соответствующей степени секретности. Категоризация секретности определяется экспертным путем, исходя из размера ущерба государственным интересам, а также требуемой надежности защиты данной категории сведений, т.е. мер режимного характера, предусмотренных правовыми актами.

Принятие решения о засекречивании сведений должно учитывать объективное свойство информации, заключающейся в утрате со временем своей актуальности. Поэтому на законодательном уровне целесообразно указать контрольный срок пересмотра степени секретности сведений либо обстоятельства, при наступлении которых встает вопрос о ее изменении или полном рассекречивании.

Представляется, что современный уровень развития экономических моделей в рыночной экономике не вызывает сомнения в возможности получения объективных оценок ущерба от разглашения сведений о деятельности коммерческих организаций.

Выборочные данные исследований позволили составить примерную характеристику на лиц, нарушавших режим секретности, который был установлен нормативными актами, приказами и инструкциями на предприятиях с учетом направлений их деятельности и оперативной обстановки. Исполнители и должностные лица нередко допускали нарушения преступного характера, выразившиеся в фактическом невыполнении или ненадлежащем выполнении своих служебных обязанностей, что приводило к разглашению государственной тайны или утрате секретных документов. Отсюда важным было на раннем этапе осуществлять профилактику таких нарушений.

Борьба с нарушениями режима секретности, в рассматриваемый период, проводилась недостаточно. Администрация, РСО и общественные организации оперировали часто суженным представлением о формах проявления нарушений режима секретности, ведущих к возможной утечке информации. Это проявлялось в том, что нарушения пропускного режима находятся на виду и чаще могут фиксироваться проверяющими, тогда как нарушения, допускаемые при выполнении НИОКР с использованием конфиденциальной информа-

ции, — более сложные для восприятия явления и поэтому не всегда в полной мере могут выявляться администрацией, а виновные нести ответственность. Показательно, что 98% лиц, допустивших нарушения, были ознáкомлены с обязанностями, однако в должностных инструкциях не были указаны обязанности по защите информации секретного характера. Нарушения режима секретности были совершены в совокупности (в 40% случаев) с другими нарушениями трудовой и производственной дисциплины. Значительное число нарушений, связанных с защитой информации, не попадало в поле зрения компетентных органов, осуществлявших контроль в этой сфере. Эти недостатки характерны и сегодня для коммерческих организаций.

Результаты исследования позволили установить общую причину нарушений режима секретности. Она была обусловлена тем, что допускались ошибки, просчеты в ходе преодоления трудностей в социально-экономическом развитии страны, что, безусловно, проявлялось в использовании форм и методов защиты информации. Имелись недостатки, относящиеся к системе реализации ответственно-сти за ненадлежащее выполнение служебных обязанностей, связанных с защитой секретов. Анализ дисциплинарной практики на ряде предприятий за пятилетний период показывает, что в 38% случаев нарушениям режима секретности был объявлен выговор, в 31% — замечание, в 12% — строгий выговор, в 10% — переведены на нижеоплачиваемую работу или понижены в должности. На руководителей предприятий и структурных подразделений только в 1% случаев были наложены дисциплинарные взыскания. Лишь в 5% случаев виновным применялись меры материального характера за причиненный ущерб. Недостаточно применялись меры морального воздействия, что способствовало неправильному формированию жизненной позиции лиц, допустивших нарушения режима.

Анализ обстоятельств организационно-управленческого характера позволил выявить недостатки, которые были связаны с отсутствием должного порядка и дисциплины в охране секретов. Это — отсутствие единого подхода в определении структуры и численности РСО, нечеткое определение функций каждого органа, занимающегося защитой информации, чрезмерная служебная загруженность, возложение на РСО несвойственных функций, неукomплектованность служб режима. Имелись недостатки в подборе и расстановке кадров, их обучении. Это проявлялось в приеме на работу лиц, не имеющих опыта и квалификации по защите секретов. В стране отсутствовала развитая база профессиональной подготовки и переподготовки кадров для

подразделений, занимавшихся защитой секретов. Наиболее распространенными, по нашему мнению, были следующие недостатки:

а) недостаточное использование средств вычислительной техники в защите секретов (работы по автоматизации функций РСО велись на отдельных предприятиях и носили фрагментарный характер);

б) отмечалась по ряду позиций неувязка плановых заданий с их финансированием, что приводило к ненадлежащему выполнению работ по защите секретов;

в) на отдельных предприятиях имела место непродуманная система оплаты труда, не позволявшая стимулировать выполняемую работу по защите секретов и приводившая в отдельных случаях к дефициту квалифицированных кадров в РСО.

В борьбе с нарушениями режима секретности недостаточно использовать правовые средства. В числе недостатков нужно выделить несовершенство правового регулирования режимно-секретной деятельности (засекречивание и рассекречивание информации, порядок функционирования подразделений по защите секретов, установление льгот для исполнителей секретных работ и т.п.); несовершенство действующего законодательства по защите секретов, что создавало трудности в практике РСО, контрольных и судебных органов по реализации принципа неотвратимости ответственности за совершение правонарушений режима секретности. В СССР отсутствовал Закон о государственной тайне, в котором была бы определена правовая основа защиты секретов. На законодательном уровне не были определены требования, предъявляемые к лицам, которым доверены секреты по службе, не урегулирован процесс их деятельности, не определены критерии определения существенного вреда при разглашении или утрате документов. В трудовом законодательстве не были зафиксированы права и обязанности лиц, выполняющих секретные работы, поощрения и взыскания в сфере охраны секретов<sup>1</sup>, в административном законодательстве отсутствовали нормы о нарушениях в области защиты секретной информации<sup>2</sup>.

В большинстве случаев, как показывают данные исследования, поводом к возбуждению уголовных дел являлись материалы проверки контрольных органов. Непосредственное обнаружение админи-

<sup>1</sup> См.: Кодекс законов о труде РСФСР. М.: Юрид. лит., 1986. С. 52–54.

<sup>2</sup> См.: Кодекс РСФСР об административных правонарушениях. М., 1989.

страцией признаков преступных нарушений режима секретности — явление весьма редкое (только в 3% случаев материалы передавались в правоохранительные органы). Это объясняется тем, что, во-первых, администрации невыгодно было вскрывать нарушения, поскольку ответственность за защиту информации возлагалась на руководителей предприятий и подразделений, во-вторых, работники контрольных органов порой недостаточно знали специфику обслуживаемых объектов, его уязвимых участков с точки зрения возможности утечки информации, недооценивали общественную опасность иных государственных преступлений, посягающих на сохранность секретов. У отдельных работников правоохранительных органов иногда возникало неправоильное представление, будто борьба с нарушениями режима секретности — дело министерства и администрации предприятий. В этой связи следует отметить, что, безусловно, меры, принимаемые администрацией, имеют важное предупредительное значение, однако они не должны подменять уголовно-правовые, когда имеются признаки преступного разглашения сведений или утраты документов и изделий.

В целом повышение эффективности работы по защите секретной информации, в рассматриваемый период зависело, на наш взгляд, от закрепления правовой основы защиты секретной информации в Законе с учетом произошедших политических и экономических изменений после 1985 года; четкого определения в Законе порядка засекречивания и рассекречивания информации на основе методики, доступной для понимания исполнителями; определения на основе методики новых вариантов ПГС и ведомственных перечней; совершенствования структуры управления защитой секретов в зависимости от вида секретной информации и ее носителей; закрепления в трудовом законодательстве прав и обязанностей лиц, выполняющих секретные работы, и отражения их в должностных инструкциях; установления административной ответственности за совершение нарушений в области защиты секретов, определения перечня нарушений, за которые наступает административная ответственность, субъектов ответственности и санкций; улучшения подбора, расстановки и обучения кадров, занимающихся защитой секретной информации; установления исполнителям секретных работ надбавок к заработной плате; проведения целенаправленной работы с исполнителями по изучению нормативных документов в области защиты секретов; создания в стране единого учебного и научного центра по подготовке специалистов в области защиты секретов; увязки плани-

рования мероприятий по защите секретов с их финансированием; использования ЭВМ в практике защиты секретов в целях повышения оперативности прохождения секретных документов, а также моделирования процессов выявления возможных каналов утечки секретной информации и прогнозирования мер по их предупреждению.

Большинство названных предложений были реализованы в современный период при подготовке правовых актов, связанных с обеспечением режима, регулированием государственной или коммерческой тайны, практикой защиты информации, используемой в предпринимательской деятельности. Многие недостатки организационно-управленческого, воспитательного и правового характера, имевшие место в советский период, являются характерными и сегодня, применительно к деятельности организаций по охране конфиденциальности информации. Их анализ и меры предупреждения изложены в последующих главах.

#### § 4. Современное законодательство о коммерческой тайне

*Роль и место правового института коммерческой тайны в системе частного права.* Правовое регулирование отношений, связанных с обеспечением защиты коммерческой тайны, приобрело высокую актуальность и практическую значимость в условиях перехода страны к рыночной экономике. Впервые *право на коммерческую тайну и ее защиту* было закреплено в ныне утративших силу Законе СССР от 4 июня 1990 г. № 1529-1 «О предприятиях в СССР» (ст. 33), Законе РСФСР от 25 декабря 1990 г. № 445-1 «О предприятиях и предпринимательской деятельности» (ст. 28), Законе РСФСР от 24 декабря 1990 г. «О собственности в РСФСР» (ст. 2). Положения названных законов применялись на территории Российской Федерации до 1 января 1995 г.<sup>1</sup> Позднее был принят Закон РСФСР от 22 марта 1991 г. № 948-1 «О конкуренции и ограничении монополистической деятельности на товарных рынках», который с 26 октября 2006 г. утра-

<sup>1</sup> См.: ФЗ от 30 ноября 1994 г. № 52-ФЗ «О введении в действие части первой Гражданского кодекса Российской Федерации» с изм. // Собрание законодательства РФ. 1994. № 32. Ст. 3302; 2001. № 17. Ст. 1644.

тил силу в связи с введением в действие Федерального закона от 26 июля 2006 г. № 135-ФЗ «О защите конкуренции»<sup>1</sup>.

Поэтому возрождение института коммерческой тайны произошло в СССР именно с момента принятия названных выше законов. Статья 33 Закона СССР «О предприятиях в СССР» от 4 июня 1990 г.<sup>2</sup> определяла коммерческую тайну как «не являющиеся государственными секретами сведения, связанные с производством, технологической информацией, управлением, финансами и другой деятельностью предприятий, разглашение (передача, утечка) которых может нанести ущерб его интересам». В соответствии со ст. 2 Закона РСФСР «О собственности в РСФСР» от 24 декабря 1990 г.<sup>3</sup> секреты производства относились к охраняемым объектам интеллектуальной собственности. Закон РСФСР «О предприятиях и предпринимательской деятельности в РСФСР» от 25 декабря 1990 г.<sup>4</sup> подтвердил право предприятия на коммерческую тайну. Закон РФ «О конкуренции и ограничении монополистической деятельности на товарных рынках» от 22 марта 1991 г.<sup>5</sup> относил к формам недобросовестной конкуренции «получение, использование, разглашение научно-технической, производственной или торговой информации, в том числе коммерческой тайны, без согласия ее владельца».

Дальнейшее развитие институт коммерческой тайны (с включением в него ноу-хау) получил в Основах гражданского законодательства Союза ССР и республик от 31 мая 1991 г., введенных в действие на территории России 4 августа 1992 г.<sup>6</sup> (далее — Основы гражданского законодательства), которые с 1 января 2008 г. признаны не действующими на территории Российской Федерации<sup>7</sup>. Анализ условий охраноспособности информации, при соблюдении которых обладатель технической, организационной или коммерческой инфор-

<sup>1</sup> См.: СЗ РФ. 2006. № 31 (1 ч.). Ст. 3434.

<sup>2</sup> См.: Ведомости Съезда народных депутатов РСФСР и Верховного Совета РСФСР. 1990. № 25. Ст. 460.

<sup>3</sup> См.: Там же. 1990. № 30. Ст. 416.

<sup>4</sup> См.: Там же. № 30. Ст. 418.

<sup>5</sup> См.: Там же. 1991. № 16. Ст. 499.

<sup>6</sup> См.: Ведомости Съезда народных депутатов СССР и Верховного Совета СССР. 1991. № 26. Ст. 733.

<sup>7</sup> См.: Федеральный закон от 18 декабря 2006 г. № 231-ФЗ «О введении в действие части четвертой Гражданского кодекса Российской Федерации» (ст. 3 п. 3).

мации, составляющей секрет производства (ноу-хау), имеет право на защиту от незаконного использования этой информации третьими лицами, наглядно демонстрирует преемственность и системную связь статьи 151 Основ гражданского законодательства с главой 75 части четвертой ГК РФ, устанавливающей аналогичные критерии охраноспособности секрета производства (ноу-хау), охраняемого в режиме коммерческой тайны.

Названные законы явились основой для развития современного российского законодательства о коммерческой тайне. Систему законодательства, регулирующего отношения, связанные с коммерческой тайной, образуют нормы конституционного, гражданского, трудового, административного, уголовного, информационного и иных отраслей права. В литературе содержится анализ отдельных законов и даны предложения по совершенствованию законодательства в этой сфере, в основном с использованием методов публично-правового регулирования отношений<sup>1</sup>.

Для становления рыночной экономики России характерным является совершенствование гражданского и торгового законодательства, что получает свое выражение в упрочение правовых начал в сфере обращения КЗИ. Дозволительный метод регулирования<sup>2</sup> открывает простор практическим действиям коммерческих организаций при взаимоотношении их с контрагентами, партнерами и иными лицами по поводу использования и охраны конфиденциальности КЗИ.

По мере накопления организационными организациями опыта в сфере обращения КЗИ встает вопрос о правовой базе использования гражданско-правовых и иных средств, установления режима коммерческой тайны и его организационного, правового и методического обеспечения, имеющих специфику по сравнению с иными объектами гражданских прав. Отсюда, важно выявить признаки, раскрывающие комплексный и самостоятельный характер существования правового института коммерческой тайны в системе частного права.

*Правовое регулирование обращения КЗИ охватывает систему гражданско-правовых и иных норм, ядро которой составляет правовая ин-*

<sup>1</sup> См.: Бачило И.Л., Лопатин В.Н., Федотов М.А. Информационное право: Учебник / Под ред. акад. РАН Б.Н. Топоркина. СПб., 2001. С. 503–522, и др.

<sup>2</sup> См.: Алексеев С.С. Общие дозволения и общие запреты в советском праве. М., 1989. С. 132–163, и др.

*ститут коммерческой тайны в рамках частного права, носящей комплексный характер.* Это проявляется в существовании совокупности связанных друг с другом правовых норм, относящихся к различным отраслям частного права, регулирующих обращение и защиту КЗИ.

В юридической науке к частному праву<sup>1</sup> относят гражданское, коммерческое и частично трудовое право, а также некоторые другие отрасли права. Е.А. Суханов отмечает, что «...частное право отнюдь не исчерпывается гражданским правом, составляющим лишь его основу». В частности, он говорит о торговом праве как всегда рассматриваемом и рассматриваемом относящимся к специальной части частного права<sup>2</sup>. Такого же мнения Б.И. Пугинский, который подчеркивает, что «коммерческое право представляет собой специальную область частного права»<sup>3</sup>. В литературе нет единого мнения относительно частноправовых начал трудового права. Бесспорно, как самостоятельная отрасль права оно «имеет свой „предмет“ и „метод правового регулирования“ и характеризующие ее и закрепленные в ТК РФ основные принципы трудового права, как бы „компиллирующие“ (вбирающие в себя) частноправовые и публично-правовые начала (принципы) в их неразрывной связи, что выделяет трудовое право из частного и публичного права»<sup>4</sup>. Поэтому прав Е.А. Суханов, который пишет: «Что касается трудового права, то его природу в настоящее время нельзя определить однозначно. В пользу его частноправового характера свидетельствуют многие правила о трудовом договоре, составляющие основу этой отрасли и получившие теперь новое развитие»<sup>5</sup>.

Безусловно, *предпринимательское право*, как «комплексная интегрированная отрасль права, совокупность правовых норм, связанных предметным единством, регулирующих... взаимодействия частных и публично-правовых начал отношения в сфере... пред-

<sup>1</sup> См.: Суханов Е.А. Система частного права // Вест. Моск. ун-та. Сер. II «Право». 1994. № 4, и др.

<sup>2</sup> Суханов Е.А. Современное развитие частного права в России // Российская академия юридических наук. Научные труды. Вып. 1 (том 1). М., 2001. С. 14.

<sup>3</sup> Пугинский Б.И. Коммерческое право России: Учебник. 2-е изд. М., 2006. С. 27.

<sup>4</sup> Дмитриева И.К. Принципы российского трудового права. М., 2004. С. 184.

<sup>5</sup> Гражданское право: Учебник. В 2 т. Т. 1 / Отв. ред. проф. Е.А. Суханов. 2-е изд. М., 2000. С. 9.

принимательской деятельности»<sup>1</sup>, несмотря на критику его предмета и метода регулирования (Е.А. Суханов,<sup>2</sup> Б.И. Пугинский<sup>3</sup> и др.), занимает важное место в системе формирования механизма правового регулирования обращения и защиты КЗИ. Важнейшие правовые категории предпринимательской деятельности (абз. 3 п. 1 ст. 2 ГК РФ), связанные с получением систематической прибыли, являются основой обращения КЗИ и обуславливают необходимость ее защиты в рыночной экономике.

Поэтому можно утверждать, что правовое регулирование обращения КЗИ и охрана ее конфиденциальности осуществляются в основном в рамках названных отраслей частного права и комплексной отрасли предпринимательского права.

*Правовой институт коммерческой тайны занимает особое место в системе гражданского и коммерческого права и включает совокупность общих и специальных гражданско-правовых норм, регулирующих гражданский оборот коммерчески значимой информации<sup>4</sup>, «овеществленной», т.е. выраженной в производимых и реализуемых товарах, выполняемых работах и оказываемых услугах. Гражданский кодекс содержит целый ряд общих норм. В частности, непосредственное отношение к регулированию коммерческой тайны в гражданском обороте имеют положения статей 1, 2, 9, 10, 11, 12, 14, 15, 16 и другие ГК РФ. Правовые нормы, регулирующие отношения по поводу КЗИ, содержатся в различных частях ГК РФ. Они закрепляют обязанности коммерческого предпринимателя по сохранению в тайне ставших ему известными сведений о торговых сделках (ст. 184 ГК РФ). Регулируют права сторон на КЗИ и порядок соблюдения условий конфиденциальности по договорам подряда (ст. 727 ГК РФ), на выполнение научно-исследовательских, опытно-конструкторских и технологических работ (ст. 772 ГК РФ), коммерческой концессии (ст. 1027, 1032 ГК РФ), простого товарищества (ст. 1042, 1045 ГК РФ), об отчуж-*

дении исключительного права на секрет производства (ст. 1468 ГК РФ) и передачи права на технологию (ст. 1557, 1560 ГК РФ), а также по лицензионным договорам о предоставлении права использования секрета производства (ст. 1469 ГК РФ) или технологии (ст. 1560 ГК РФ). Определенные особенности присущи договорным отношениям по сохранению банковской тайны (ст. 857 ГК РФ) и тайны страхования (ст. 946 ГК РФ) в рамках института коммерческой тайны, что подтверждает необходимость их самостоятельного исследования. Кроме перечисленных, используются и непоименованные в ГК РФ договоры (договоры на выполнение маркетинговых исследований, на передачу коммерческой информации и др.). Как видно, соблюдение условий конфиденциальности касается выполнения работ и оказания услуг, производства и реализации товаров, правовое регулирование которых является предметом наук гражданского и коммерческого права.

Теория коммерческого права определяет роль и место института коммерческой тайны в торговом обороте. Деятельность по обеспечению охраны коммерческой тайны в торговом обороте может быть представлена в виде совокупности продолжающихся в течение длительного времени действий, направленных на увеличение доходов коммерческой организации, исключение неоправданных расходов, сохранение положения на рынке товаров или получение иной коммерческой выгоды. Субъектами такого рода деятельности выступают лица, относящиеся к различным субъектам коммерческого права. Они реализуют свои коммерческие цели в условиях оборотоспособности товаров, являющихся объектами торгового права. Деятельность по обеспечению охраны коммерческой тайны заключается в оказании помощи субъектам в достижении целей путем реализации мер организационного, правового и научно-методического характера.

*В регулировании отношений по использованию КЗИ и охране ее конфиденциальности применяются отдельные нормы трудового права. В частности, в трудовом договоре работодатель и работник могут предусматривать условия обеспечения конфиденциальности работ, при выполнении которых используется КЗИ (ст. 57 ТК РФ). Трудовой кодекс РФ, в частности, предусматривает основание для увольнения работника за разглашение коммерческой тайны (подп. «в» п. 6 ст. 81 ТК РФ).*

*Специальные гражданско-правовые нормы, регулирующие отношения по поводу КЗИ, содержатся в Федеральном законе «О коммерче-*

<sup>1</sup> Предпринимательское право Российской Федерации / Отв. ред. Е.П. Губин, П.Г. Лахно. М., 2004. С. 20.

<sup>2</sup> См.: Суханов Е.А. Современное развитие частного права в России. С. 5–19.

<sup>3</sup> См.: Пугинский Б.И. Коммерческое право и предпринимательство // Актуальные проблемы коммерческого права: Сб. статей. Вып. 2. М., 2005. С. 21.

<sup>4</sup> Словосочетание «коммерчески значимая информация» означает «имеющая ценность, важное значение для ведения предпринимательской (коммерческой) деятельности. См.: Ожегов С.И. Словарь русского языка. М., 1988. С. 190. Слово «значимый» означает «выражающий что-нибудь, имеющий какое-нибудь значение».

ской тайне» от 29 июля 2004 г. № 98-ФЗ<sup>1</sup> (в редакции от 18 декабря 2006 г. № 231-ФЗ), который устанавливает право организаций на отнесение сведений к информации, составляющей коммерческую тайну; закрепляет права и обязанности обладателей такой информации и иных лиц; определяет меры по охране конфиденциальности информации в трудовых и гражданско-правовых отношениях.

Ряд важных положений о коммерческой тайне содержат другие законодательные акты. Закон о конкуренции запрещает незаконное использование информации, составляющей коммерческую тайну, определяет функции и права антимонопольных органов, а также санкции, применяемые к нарушителям. Закон РФ «О частной деятельности и охранной деятельности в Российской Федерации» от 11 марта 1992 г.<sup>2</sup> запрещает «разглашать собранную информацию, использовать ее в каких-либо целях вопреки интересам своего клиента...», в том числе и коммерческую тайну организаций (ст. 7). Особо нужно выделить ФЗ «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 г. № 149-ФЗ<sup>3</sup>, который содержит определения информации, информационной системы, документированной информации и другие базовые положения, применяемые при защите коммерческой тайны, однако он не регулирует корпоративные и договорные отношения по поводу использования и охраны КЗИ.

В числе подзаконных актов следует назвать Указ Президента РФ «Об утверждении перечня сведений конфиденциального характера» от 6 марта 1997 г. № 188<sup>4</sup>, а также ныне утратившее силу в связи с принятием ФЗ «О коммерческой тайне» постановление Правительства РСФСР «О перечне сведений, которые не могут составлять коммерческую тайну» от 5 декабря 1991 г. № 35<sup>5</sup>. Последний названный акт в течение почти 13 лет являлся единственным документом, кото-

<sup>1</sup> См.: ФЗ от 29 июля 2004 г. № 98-ФЗ «О коммерческой тайне» // СЗ РФ. 2004. № 32. Ст. 3283.

<sup>2</sup> См.: Ведомости Съезда народных депутатов РФ и Верховного Совета РФ. 1992. № 17. Ст. 888.

<sup>3</sup> См.: ФЗ от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // СЗ РФ. 2006. № 31. Ст. 3448.

<sup>4</sup> См.: Собрание законодательства РФ. 1997. № 10. Ст. 1127.

<sup>5</sup> См.: Собрание постановлений Правительства РСФСР. 1992. № 1—2.

рый устанавливал ограничения на отнесение информации к коммерческой тайне.

Взаимоотношения хозяйствующих субъектов с государственными органами и органами местного самоуправления по поводу предоставления им КЗИ, вопросы охраны конфиденциальности такой информации регулируются нормами публичного права (административное и уголовное, материальное и процессуальное законодательство).

Гражданско-правовые и иные нормы предоставляют владельцу КЗИ возможность по своему усмотрению определять характер и направление использования права на информацию и меры по охране ее конфиденциальности. Разработка и осуществление таких мер предполагают создание определенных правовых механизмов с использованием норм других отраслей права, что существенно расширяет границы гражданско-правового регулирования КЗИ.

*Правовой институт коммерческой тайны следует рассматривать, как самостоятельный институт частного права, в котором существуют гражданско-правовые нормы отдельно регулирующей обработке КЗИ и охрану ее конфиденциальности, независимо от правового регулирования смежного объекта гражданского права на результаты интеллектуальной деятельности (исключительные права).* В цивилистической науке вопрос о самостоятельности правового института коммерческой тайны носит дискуссионный характер. Следует отметить наличие двух взаимоисключающих подходов при отнесении информации, составляющей коммерческую тайну, к объектам исключительных прав. *Первый подход*, сторонником которого является В.А. Дозорцев, исходит из отнесения прав на информацию к системе исключительных прав. Концептуальные положения, объясняющие основания возникновения исключительных прав и способы их закрепления, позволили В.А. Дозорцеву сформулировать и обосновать принципы «системы, основанной на конфиденциальности (сохранении тайны) содержательного результата»<sup>1</sup>.

В.А. Дозорцев пишет: «Для результатов интеллектуальной деятельности, имеющих содержательный характер, имеется потребность в закреплении абсолютных прав на объекты, не обособленные или даже не поддающиеся обособлению на основе четких формальных признаков. Единственным способом обособления таких объек-

<sup>1</sup> См.: Дозорцев В.А. Интеллектуальные права: Понятие. Система. Задачи квалификации. Сб. статей / Исслед. центр частного права. М., 2005. С. 24.

тов является сохранение их конфиденциальности, и эта конфиденциальность одновременно составляет содержание правовой охраны... С помощью конфиденциальности в этом случае охраняется объект, именуемый „ноу-хау“, который может относиться к любой сфере, независимо от своего профиля»<sup>1</sup>. Далее В.А. Дозорцев подчеркивает, что «ноу-хау охраняется только при нарушении конфиденциальности», и «в этом случае правомерно говорить не об абсолютной „охране“ объекта, а о „защите“ прав и интересов субъекта»<sup>2</sup>. В этой связи В.А. Дозорцев вводит в научный оборот понятие «квазиабсолютное право». Он отмечает: «Абсолютной защиты у обладателя ноу-хау нет (в отличие, например, от патентообладателя). Его право можно характеризовать только как квазиабсолютное. Оно менее надежно, чем полноценное абсолютное право, хотя более универсально и шире. От этого оно не перестает быть исключительным, но содержание этой „исключительности“ отличается от традиционного исключительного права, основанного, например, на патенте. Поэтому ноу-хау нельзя вывести из числа объектов исключительных прав...»<sup>3</sup>. В.А. Дозорцев считал, что система исключительных прав «включает в себя не только традиционные результаты интеллектуальной деятельности, но и нетрадиционные (точнее — нетрадиционно охраняемые) типа ноу-хау...»<sup>4</sup>.

*Второй подход* аргументированно обоснован в трудах И.А. Зенина<sup>5</sup>. По его мнению, ноу-хау, в состав которого включается охраняемая конфиденциальная научно-техническая, коммерческая, финансовая и иная информация, не является объектом исключительных прав. И.А. Зенин считает, что «в отличие от охраняемого патентом изобретения на ноу-хау не существует исключительного права, а есть лишь фактическая монополия»<sup>6</sup>. К этому следует добавить, что, по нашему мнению, фактическая монополия организации на такую информацию возможна при соблюдении определенной проце-

<sup>1</sup> Дозорцев В.А. Указ. соч. С. 44.

<sup>2</sup> Там же. С. 46.

<sup>3</sup> Там же. С. 65 — 66.

<sup>4</sup> Там же. С. 68.

<sup>5</sup> См.: Зенин И.А. Коммерческая тайна и ноу-хау // Законодательство. 2005. № 12, и др.

<sup>6</sup> Зенин И.А. Гражданское и торговое право зарубежных стран. М., 2008. С. 171.

дуры, связанной с установлением режима коммерческой тайны и его последующим обеспечением защиты, т. е. охраны конфиденциальности КЗИ. Подобную позицию занимает Э.П. Гаврилов, который считает, что «поскольку коммерческая тайна известна третьим лицам, она не может быть объектом исключительного права, ибо на третье лицо не может быть возложена обязанность не использовать и не разглашать объект, который ему неизвестен»<sup>1</sup>.

*Несколько иную*, можно сказать, *колпромиссную позицию* занимает А.П. Сергеев, который считает коммерческую тайну самостоятельным нетрадиционным объектом интеллектуальной собственности (исключительные права) (на этой же позиции стоит В.А. Дозорцев) и, вместе с тем, допускает монополию лица на такого рода информацию после принятия им превентивных мер охраны<sup>2</sup> (по существу, разделяет позицию И.А. Зенина). Нужно подчеркнуть, что позиция А.П. Сергеева частично нашла свое законодательное подтверждение в части четвертой ГК РФ (гл. 75 и 77) относительно секрета производства (ноу-хау) и технологии, относящихся к понятию информации, составляющей коммерческую тайну (ст. 3 Закона о коммерческой тайне), в отношении которых обладателем таких сведений введен режим коммерческой тайны.

Признавая правомерность существования в науке различных подходов относительно включения конфиденциальности информации в систему исключительных прав, хотелось бы высказать некоторые *соображения о целесообразности выделения общественных отношений по поводу обращения и защиты КЗИ в самостоятельный правовой институт коммерческой тайны*.

1) Безусловно, решение задачи укрепления правовой базы регулирования КЗИ допускает использование различных вариантов. Вместе с тем отнесение института коммерческой тайны к системе исключительных прав (интеллектуальная собственность) не вполне обоснованно. Большинство исследователей отмечают, что институты гражданского права, опосредствующие интеллектуальную собственность и ее результаты, закрепляют за обладателями право на легальную монополию совершения различных действий по использо-

<sup>1</sup> См.: Гаврилов Э.П. О кодификации законодательства, относящегося к интеллектуальной собственности // Вестник Высшего Арбитражного Суда Российской Федерации. 2002. № 10. С. 96.

<sup>2</sup> См.: Сергеев А.П. Право интеллектуальной собственности в Российской Федерации: Учебник. М., 1996. С. 30, 619—625.

ванию и распоряжению результатами творчества, тогда как институт коммерческой тайны, наоборот, закрепляет право на КЗИ только при установлении обладателем определенных условий неизвестности и охраноспособности такой информации. В противном случае лицо лишено возможности доказывать свое право на КЗИ.

Государством специально установлены порядок оформления, способы приобретения и защиты исключительных прав. Закон о коммерческой тайне не требует государственной регистрации права на КЗИ. Исключительное право на секрет производства действует до тех пор, пока сохраняется конфиденциальность сведений, составляющих его содержание (ст. 1467 ГК РФ). Возможность защиты нарушенного права на КЗИ возникает у обладателя с момента установления в отношении такой информации режима коммерческой тайны, т.е. фактической монополии.

2) Обращение КЗИ в гражданском обороте имеет определенные особенности. Предметом регулирования КЗИ являются многообразные отношения по поводу ее производства (получения), использования, хранения и передачи с соблюдением условий конфиденциальности. Часто регулирование этих отношений выходит за рамки гражданско-правовых. В этих случаях используются иные правовые средства для установления режима коммерческой тайны и его обеспечения мерами организационного, правового и иного характера.

3) Цель выделения сферы обращения КЗИ как самостоятельной области правового регулирования состоит в том, чтобы упорядочить законодательное, корпоративное и договорное регулирование в этой сфере на основе изучения правовой практики, для устранения имеющихся пробелов и согласовывать применение правовых средств, с тем чтобы их использование соответствовало решению хозяйственных задач.

4) Правовой институт коммерческой тайны выполняет важные функции в гражданском обороте. Он признает право юридических лиц и индивидуальных предпринимателей на КЗИ; устанавливает правовой режим обращения КЗИ; позволяет на законном основании обладателю КЗИ использовать или при необходимости изъять такую информацию в процессе производства и реализации товаров, выполнения работ и оказания услуг; защищает права обладателей КЗИ с помощью норм гражданского, трудового, административного, уголовного и иных отраслей права.

5) Решение проблем организационного, правового и иного обеспечения деятельности по охране конфиденциальности информации

требует создания теоретической базы правового регулирования сферы обращения КЗИ, которая в настоящее время отсутствует. Ранее границы исследования названных проблем определялись в основном рамками изучения применения норм публичного права, а проблемам частноправового характера при обращении КЗИ не уделялось должного внимания.

6) Основологающее значение для раскрытия содержания части неправовых проблем регулирования деятельности при обращении КЗИ, разработки предложений по совершенствованию ее механизма имеет изучение практики правосотворчества и реализации норм в этой сфере отношений.

**Характеристика условий режима охраноспособности коммерческой тайны.** В Законе о коммерческой тайне информация, составляющая коммерческую тайну, определяется как сведения любого характера, которые имеют действительную или потенциальную коммерческую ценность в силу неизвестности их третьим лицам, к которым у третьих лиц нет свободного доступа на законном основании и в отношении которых обладателем таких сведений введен режим коммерческой тайны (п. 2 ст. 3 Закона). Появление такой формулировки, содержащей условия, при соблюдении которых информация может быть отнесена к коммерческой тайне, в российском законодательстве не случайно. Она во многом заимствована из зарубежного законодательства, где коммерческая тайна определяется аналогичным образом.

В большинстве стран законодательство, регулирующее режим конфиденциальности информации и устанавливающее ответственность за ее неправомерное использование, представляет собой весьма развитый нормативный массив, формирование которого осуществляется на основе национальных правовых традиций с использованием международных стандартов<sup>1</sup>.

В Великобритании отсутствует законодательная (статутная) защита коммерческих секретов, не существует четкого легального определения коммерческой тайны. Регулирование коммерческой тайны включает отдельные элементы вещных и обязательственных прав и судебные прецеденты защиты конфиденциальной информа-

<sup>1</sup> См.: Обзор зарубежной практики защиты коммерческой тайны, по адресу: <http://legislature.ru/monitor/seminar/komtayna.html>; <http://legislature.ru/monitor/economics/310378-3ekspfund2.html>, и др.



ции, совокупность которых характеризует понятие «конфиденциальное право». Нормами конфиденциального права регулируются не только коммерческая, но и другие виды тайн (государственная, личная и др.). Объектом регулирования коммерческой тайны являются отношения в сфере предпринимательской деятельности. Рассмотрение судом иска о защите конфиденциальной информации возможно при выполнении обладателем следующих условий. Во-первых, информация по своему содержанию должна иметь «неотъемлемый признак конфиденциальности» в силу важности ее коммерческого использования. Во-вторых, информация должна быть связана с условиями охраны, из которых следует обязательство о ее неразглашении. И, в-третьих, должно иметь место правонарушение использования этой информации, причиняющее ущерб ее обладателю. Такой подход к определению коммерческой тайны является характерным для большинства зарубежных стран, включая Россию.

Защита коммерческой тайны в США осуществляется на уровне законодательства штатов. В основу местных законов положен единый рамочный законодательный акт — Единобразный закон о торговых секретах 1979 г. в редакции 1985 г. (The Uniform Trade Secrets Act). В соответствии с данным актом коммерческая тайна определяется как информация (включая формулы, модели, программы, механизмы, способы, технологии) или технология, которая обладает самостоятельной экономической ценностью (действительной или потенциальной) и недоступна для других лиц, которые могли бы извлечь экономическую выгоду из ее использования или разглашения, и в отношении которой приняты меры по защите ее секретности. В 1996 г. в США вступил в силу Закон об экономическом шпионаже (The Economic Espionage Act), который заложил основы федеральной системы коммерческой тайны. Он заполнил существовавшие ранее пробелы в законодательстве, расширил понятие коммерческой тайны и ввел уголовную ответственность за присвоение лицом коммерческой тайны в своих интересах.

В соответствии с законодательством Германии к коммерческой тайне относится информация, отвечающая признаку секретности (доступная только известному ограниченному кругу лиц), при условии наличия у владельца информации обоснованного интереса в ее сохранении. Нарушение коммерческой тайны рассматривается законодательством Германии как факт недобросовестной конкуренции. Закон о недобросовестной конкуренции (Unlauteren Wettbewerbsgesetz, UWG) предусматривает уголовную ответственность за престу-

пления, связанные с нарушением коммерческой тайны. Немецкое законодательство закрепляет обязанности работника по неразглашению им коммерческой тайны после прекращения трудовых отношений (расторжения трудового договора).

Закон о недобросовестной конкуренции в Германии выделяет два вида тайн. К производственной тайне могут относиться сведения организационного и технического характера, касающиеся способа производства, технологии, организации труда, а также технические открытия, изобретения либо сведения о характере и целях исследовательских работ и др. Коммерческой тайной, в отличие от производственной являются сведения, которые касаются торговых отношений фирм, организации и размеров оборота, состояния рынков сбыта, поставщиков и потребителей и др.

Защита коммерческой тайны в Таиланде осуществляется на основе Закона о коммерческой тайне, который вступил в силу в 2002 г. (Trade Secret Act). Закон разделяет коммерческую информацию на два вида. К первому виду относятся промышленные тайны, которые состоят из коммерческой информации, затрагивающей технические вопросы, связанные, например, с производственным процессом. Ко второму виду относится коммерческая информация, включающая в себя методику продаж, договорные формы, клиентскую базу, рекламные технологии, и др.

Порядок и условия защиты коммерческой тайны закреплены в законодательстве Канады, Мексики, Бразилии, Франции, Нидерландов, Бельгии, Венгрии, Чехии, Италии, Японии, Китая и других государств<sup>1</sup>.

В последние годы принят ряд международных актов, имеющих отношение к информационной сфере: Окинавская хартия глобального информационного общества, Типовой закон Комиссии ООН по праву международной торговли (ЮНСИТРАЛ), «Об электронной коммерции» (1996 г.), Общие обычаи Международной торговой палаты для удостоверения цифровым способом международной коммерции 1997 г., Международные правила толкования торговых терминов (Инкотермс) 2000 г. и другие. Особое значение для России, в рамках участия в работе Всемирной торговой организации (ВТО),

<sup>1</sup> См.: Анализ правовой концепции режима коммерческой тайны, подготовленный Аналитическим управлением Аппарата Государственной Думы РФ, по адресу: <http://www.akai.ru/pravo/iam/2.htm>.

имеют Международное соглашение по тарифам и торговле (ГАТТ) и Соглашение о коммерческом использовании интеллектуальной собственности (TRIPS)<sup>1</sup>. Минимальные международные стандарты по защите коммерческой тайны установлены в статье 10 bis Парижской конвенции по охране промышленной собственности, в которой подчеркивается, что, во-первых, страны Союза обязаны обеспечить гражданам стран, участвующих в Союзе, эффективную защиту от недобросовестной конкуренции, а во-вторых, актом недобросовестной конкуренции считается всякий акт конкуренции, противоречащий честным обычаям в промышленных и торговых делах.

Названные положения получили свою конкретизацию в тексте Соглашения ТРИПС, применительно к понятию коммерческой тайны. В частности, в процессе обеспечения эффективной защиты от недобросовестной конкуренции, как это предусмотрено ст. 10 bis Парижской конвенции (1967 г.), страны-участницы должны охранять закрытую информацию и данные, предоставляемые их правообладателям. В Соглашении впервые на международном уровне сформулированы принципы защиты информации: 1) информация является секретной в том смысле, что она либо в целом, либо в конкретном сочетании или расположении ее компонентов не является известной или легко доступной лицам, принадлежащим к определенному кругу, обычно имеющему дело с подобными видами информации, 2) информация имеет коммерческую ценность ввиду ее секретности, 3) в конкретных обстоятельствах была подвергнута определенным разумным мерам охраны лицом, контролирующим эту информацию на законных основаниях, в целях сохранения ее секретности.

Для выполнения данного Соглашения странам — членам ВТО придется охватить правовой охраной все секреты, имеющие коммерческую ценность.

*Анализ зарубежного законодательства о коммерческой тайне имеет существенное значение для оценки условий режима охраноспособности коммерческой тайны, закрепленных в ст. 1465 ГК РФ.*

*Во-первых, это коммерческая ценность информации.* В прежнем (ст. 151 Основ гражданского законодательства, ст. 139 ГК РФ) и действующем гражданском законодательстве (гл. 75 части четвертой ГК РФ) это понятие не раскрывается и по-разному объясняется в ли-

<sup>1</sup> См.: Гражданское право. Т. 2. Полутом 1 / Отв. ред. проф. Е.А. Суханов. М., 2000. С. 564.

тературе. Под коммерческой ценностью большинством авторов понимается способность информации быть объектом рыночного оборота<sup>1</sup>. Как правило, к коммерческой тайне относится информация, использование которой предоставляет ее обладателю определенные конкурентные преимущества. Коммерческая ценность может выражаться в получении прибыли от реализации продукции, продвижении которой к потребителю связано с использованием данных о состоянии рынков сбыта и т. д. Если информация не представляет для ее обладателя коммерческой ценности, она не может считаться коммерческой тайной. Как отмечает А.А. Кузьмин, «в отношении сохранения тайны должно быть наличие оправданного экономического интереса»<sup>2</sup>. Об этом писал еще в начале XX века В. Розенберг. По его мнению, «охрана тайны допустима постольку, поскольку с сохранением тайны сопряжен какой-либо защищаемый правом интерес, в сфере промышленной тайны этот интерес имеет характер имущественного»<sup>3</sup>.

Определение экономической ценности информации может быть установлено в суде различными способами. Оценка стоимости КЗИ может быть основана на рыночной цене сделок по передаче аналогичной информации, либо обладатель должен представить документы, подтверждающие понесенные им расходы в ходе выполнения НИОКР, маркетинговых исследований.

Информация, составляющая коммерческую тайну, может иметь не только действительную, но и потенциальную коммерческую ценность. Например, знания и сведения, которые не используются в настоящее время организацией, но могут быть использованы в будущем. Поэтому под коммерческой ценностью информации следует не только понимать привязку ее к денежному эквиваленту, но и учитывать возможный вред интересам субъекта вследствие разглашения такой информации.

Гражданский кодекс прямо не указывает на субъективную принадлежность лиц, имеющих право на секрет производства (ноу-хау), охраняемого в режиме коммерческой тайны, но определенный вы-

<sup>1</sup> См.: Комментарий к ГК РФ. Ч. 1 / Под ред. О.Н. Садикова. М., 1998. С. 290, и др.

<sup>2</sup> См.: Кузьмин А.А. Правовая защита коммерческой тайны // Правоведение. 1992. № 5. С. 47.

<sup>3</sup> Розенберг В. Промысловая тайна. СПб., 1910. С. 31.

вод может быть сделан исходя из анализа содержания ст. 1465 ГК РФ. В названной статье выделен признак «коммерческой ценности» сведений, которые используются субъектами в предпринимательской деятельности для получения прибыли при продаже товаров (работ, услуг). В литературе вывод о том, что субъектами права на коммерческую тайну являются предприниматели, обосновывается по-разному. Так, одни считают, что «коммерческая тайна, как защищаемый правом объект, не существует вне предприятия, она неотделима от предприятия»<sup>1</sup>. Другие полагают, что «собственником коммерческой тайны можно считать любой хозяйствующий субъект, имеющий статус юридического лица, потому что именно юридическое лицо вправе создавать локальные нормативные акты, регулирующие охрану коммерческой тайны»<sup>2</sup>. Как видно из данного определения, индивидуальные предприниматели исключены из числа субъектов права на коммерческую тайну. Такой подход представляется неверным, поскольку, в соответствии с п. 3 ст. 23 ГК РФ, к предпринимательской деятельности граждан, осуществляемой без образования юридического лица, соответственно применяются нормы, регулирующие деятельность юридических лиц, являющихся коммерческими организациями, если иное не вытекает из закона, иных правовых актов или существа правоотношения. В данном случае не имеется никаких препятствий к тому, чтобы признать индивидуальные предпринимателей субъектами права на коммерческую тайну.

Зарубежный опыт был использован в одном из первых союзных законов, в котором было дано понятие коммерческой тайны, хотя не были определены критерии охраноспособности такой информации. Так, Закон СССР «О предприятиях в СССР» (ст. 33) определял коммерческую тайну как сведения, не являющиеся государственным секретом, связанные с производством, технологической информацией, управлением, финансами и другой деятельностью предприятия. В Законе не были определены субъекты, имеющие право на установление режима коммерческой тайны. Нужно сказать, что этот пробел был восполнен в Законе РСФСР о предприятиях и предпринимательской деятельности, где субъектом был уже назван руководитель предприятия. Основы гражданского законодательства (ст.

<sup>1</sup> См.: Кузьмин А.А. Указ. соч. С. 49, и др.

<sup>2</sup> См.: Плаксин В.А., Макогон Ю.В. Коммерческая тайна: правовые проблемы // Государство и право. 1992. № 8. С. 76.

151) определяли в числе других видов информации и коммерческую информацию, которая могла быть отнесена при определенных условиях к секретам производства (коммерческой тайне).

В зарубежном законодательстве субъектами права на коммерческую тайну также признаются лица, осуществляющие предпринимательскую (коммерческую) деятельность. Так, например, в соответствии с § 90 Германского торгового уложения<sup>1</sup> владельцем коммерческих и производственных секретов является предприниматель.

*Во-вторых, информация не подпадает под перечень сведений, доступ к которым не может быть ограничен, и перечень сведений, отнесенных к государственной и иной тайне.* Действующее законодательство представляет руководителю организации право самостоятельно решать вопрос об объеме сведений, подлежащих отнесению к коммерческой тайне. При этом организация руководствовалась, до вступления в силу Закона о коммерческой тайне, постановлением Правительства РСФСР от 5 декабря 1991 г. № 35 «О перечне сведений, которые не могут составлять коммерческую тайну»<sup>2</sup>. Этот акт устанавливал определенные ограничения для субъектов по отнесению сведений к коммерческой тайне.

*В-третьих, отсутствие свободного доступа к информации на законном основании.* Наличие доступа означает, что информация не должна быть общезвестна. Как писал В. Розенберг, «общезвестное одно только индивидуально волею не может быть превращено в тайну». Под общезвестным он понимал то, что «известно неопределенно большому кругу лиц и доступно восприятию каждого желающего»<sup>3</sup>. Общеизвестная информация, даже если она имеет экономическую ценность, не может считаться коммерческой тайной, хотя в литературе высказано мнение, что такая информация будет признаваться коммерческой тайной. Как подчеркивает Г. Штумпф, «если секретом будет тот факт, что предприятие использует именно этот способ или устройство и в связи с этим добивается наибольшего успеха»<sup>4</sup>. Такой подход представляется спорным. Если какие-то зна-

<sup>1</sup> См.: Германское право. Ч. 2. М.: Исследовательский центр частного права, 1996. С. 81, и далее.

См.: Собрание актов Президента РСФСР и Правительства РСФСР. 1992. № 1–2. Ст. 7.

<sup>3</sup> См.: Розенберг В. Указ. соч. С. 31.

<sup>4</sup> См.: Штумпф Г. Договор о передаче ноу-хау. М., 1976. С. 30.

ния, используемые коммерсантом, позволяют ему добиваться коммерческих успехов, однако организация формально не выделяет и не охраняет такие сведения, то такие знания могут считаться коммерческой тайной, но при соблюдении условий, указанных в ст. 1465 ГК РФ.

Определение понятия доступа к информации содержится в Едином образном законе о торговых секретах США, в котором сказано, что информация «не может быть легко получена законными средствами». В качестве законных средств получения информации Закон называет «деконструирование» или «обратный инжиниринг» (reverse engineering). Суть процесса «обратного инжиниринга» в том, что приобретается какой-либо продукт конкурента и подвергается исследованию с целью выяснения его характеристик для создания своего, аналогичного продукта. Такое получение и последующее использование информации не является нарушением коммерческой тайны первоначального производителя. Хотя многие компании за рубежом стремятся обезопасить себя от раскрытия своих торговых секретов и включают в контракты оговорку о запрещении подобного рода действий<sup>1</sup>.

*В-четвертых, это меры по охране конфиденциальности информации.* Речь идет о принятии владельцем информации мер по охране ее конфиденциальности. Как писал В. Розенберг, «то, что могло бы быть по своим объективным признакам тайною, не есть таковая, если тот, ради интересов которого охраняется тайна, не пожелал сделать из этого тайны»<sup>2</sup>. Наличие мер по охране конфиденциальности информации — это условие, подлежащее доказыванию в суде при возникновении спора; условие, подтверждающее соблюдение критериев отнесения информации к коммерческой тайне. Например, суды в США при рассмотрении споров о нарушении коммерческой тайны требуют, чтобы «истец доказал, что им предпринимались меры по защите информации»<sup>3</sup>.

Невыполнение требований по охране конфиденциальности информации существенным образом влияет на юридическое значение других признаков охраноспособности коммерческой тайны. Если

информация не содержится в секрете, то она, в принципе, доступна, по крайней мере, доступ к ней существенно облегчен. Таким образом, перестает выполняться условие о том, что «к информации нет свободного доступа на законном основании». А если информация становится доступной, то она теряет и качество коммерческой ценности в силу ее неизвестности третьим лицам.

Большинство авторов (И.Л. Бачило, И.А. Зенин, В.Н. Лопатин, А.П. Сергеев и др.) условно выделяют *три группы мер* по охране конфиденциальности информации: технические, организационные и юридические меры.

*Технические* меры связаны с использованием различных технических средств, препятствующих несанкционированному доступу к информации. Например, кодирование сообщений, передаваемых по каналам электронной или факсимильной связи; установление различных устройств, препятствующих снятию информации в процессе ее прохождения по каналам связи, и другие. *Организационные* меры направлены на ограничение доступа работников к конфиденциальной информации. К *юридическим* мерам относятся такие способы охраны информации, которые предполагают использование определенного комплекса правовых средств, предоставленных законом и подзаконными актами владельцам информации. К ним следует отнести разработку и принятие корпоративных актов, регулирующих процесс установления и обеспечения режима коммерческой тайны.

В зарубежной практике применяются различные способы защиты интересов владельцев коммерческой тайны<sup>1</sup>, например, соглашение о неконкуренции (covenants not to compete). Такое соглашение представляет собой письменное обязательство увольняющегося работника не заниматься после увольнения определенное время деятельностью в той же сфере, в какой осуществляет свою деятельность работодатель. Возможность заключения такого соглашения предусмотрена, в частности, Германским торговым уложением. В соответствии с § 60 ГТУ служащему не разрешается без согласия принципала заниматься торговым промыслом и совершать сделки в торговой отрасли принципала. Параграф 74 ГТУ предусматривает возможность заключения письменных соглашений о неконкуренции на период после окончания служебных отношений. Важным условием соглашения является получение бывшим служащим денежного возмеще-

<sup>1</sup> См.: *Stim R. Intellectual Property: Patents, Trademark and Copyrights*. N. Y., 1994. P. 221–248.

<sup>2</sup> См.: *Розенберг В.* Указ. соч. С. 31.

<sup>3</sup> См.: Практика защиты коммерческой тайны в США. М., 1990. С. 31.

<sup>1</sup> См.: Protecting Trade Secrets, Patents, Trademarks and Copyrights. P. 74–75.

ния, составляющего не менее половины месячного его содержания. Такие соглашения заключаются на срок не более 2 лет с момента окончания служебных отношений<sup>1</sup>.

Аналогичные соглашения практикуются и в США. Они признаются действительными в том случае, если целесообразны и необходимы для защиты торговых секретов; сфера деятельности, на которую распространяется соглашение, должна быть четко очерчена и не являться слишком широкой; они должны быть разумны по срокам (не более 2–3 лет) и территории действия (в пределах 1–2 штатов); должно предусматриваться соразмерное вознаграждение<sup>2</sup>. Возможность использования подобных соглашений в российской практике<sup>3</sup> ранее была установлена п. 3 ч. 3 ст. 11 Закона о коммерческой тайне, утратившим силу с 1 января 2008 г. в связи с введением части четвертой ГК РФ. Статья 1470 ГК РФ обязывает гражданина сохранять конфиденциальность полученных сведений до прекращения действия исключительного права на секрет производства.

**Анализ тенденций, предшествовавших принятию Закона о коммерческой тайне и перспективы его совершенствования.** Долгое время в нашей стране не было единого закона прямого действия, регулирующего порядок отнесения информации к коммерческой тайне, права и обязанности субъектов, гражданский оборот такой информации и ее защиты. Нельзя сказать, что такая работа не велась. Попытки разрабатывать такой акт предпринимались еще в советское время. Весьма серьезным, заслуживающим внимания является, в частности, проект Закона СССР о коммерческой тайне, подготовленный В.А. Рубановым, в котором были сформулированы положения о правах предприятий в области коммерческой тайны, и их ответственности. В предисловии к законопроекту В.А. Рубанов, говоря о роли органов государственного управления, в частности КГБ, подчеркивает: «Учиться конкуренции, учиться производить нужные людям товары в условиях рынка можно лишь самостоятельно охраняя свои секреты, избавившись от контроля КГБ»<sup>4</sup>.

<sup>1</sup> См.: Protecting Trade Secrets, Patents, Trademarks and Copyrights. P. 74–75.

<sup>2</sup> Ibid.

<sup>3</sup> См.: Коломиец А. Условие о неразглашении коммерческой тайны в трудовом договоре (контракте) // Хозяйство и право. 1998. № 5. С. 33.

<sup>4</sup> Рубанов В.А. Охрана коммерческих тайн в рыночных условиях // Вестн. агентств «Post Factum». 1990. № 11.

За более чем 15-летний период учеными, исследовавшими эту предметную область, было высказано немало ценных предложений, которые нашли отражение в различных проектах Закона о коммерческой тайне. Доработка проекта, принятого в первом чтении Государственной Думой Федерального Собрания РФ 2 апреля 1997 г.<sup>1</sup>, велась более семи лет. За этот период были проанализированы замечания, изложенные в заключении Президента РФ от 14 мая 1997 г., и даны предложения по совершенствованию законодательства о коммерческой тайне. Это свидетельствует о трудностях становления отечественного правового института коммерческой тайны, регулирующего частные интересы собственников, и разрешения существующих проблем в теории и на практике.

Проблема принятия закона о коммерческой тайне неоднократно обсуждалась учеными страны и оценивалась ими весьма неоднозначно. По этому вопросу были и сторонники, и противники принятия такого закона<sup>2</sup>. Так, например, А.П. Сергеев считает, что в принятии специального закона об охране коммерческой тайны не было необходимости, «вполне достаточно четкого понятия коммерческой тайны, определения содержания прав ее обладателя и мер их эффективной защиты. Современное законодательство такую возможность предоставляет»<sup>3</sup>. Другие авторы подчеркивали, что в современных условиях принятие закона является достаточно актуальным, и должно будет способствовать «обеспечению национальных интересов России... и препятствовать неправомерному и безвозмездному использованию отечественных ноу-хау зарубежными фирмами»<sup>4</sup>. Ряд авторов справедливо отметили, что принятие данного Закона связано с вступлением России в ВТО, поскольку защита коммерческой тайны, наряду с патентной защитой изобретений и охраной авторских прав, предусмотрена соглашением о торговых аспектах защиты

<sup>1</sup> См.: Трудное рождение законов. Заключение на проект федерального закона «О коммерческой тайне» // Российская газета. 1997. 18 июня.

<sup>2</sup> См.: Лопатин В.Н. Правовая охрана и защита коммерческой тайны // Законодательство. 1998. № 11, и др.

<sup>3</sup> См.: Сергеев А.П. Право интеллектуальной собственности в Российской Федерации. М., 1996. С. 619–620.

<sup>4</sup> См.: Мухомедшин И. Актуальные проблемы правовой защиты научно-технического потенциала России // Хозяйство и право. 1998. № 9. С. 38.

прав интеллектуальной собственности и является одним из важных требований ВТО<sup>1</sup>.

Принятый ФЗ от 29 июля 2004 г. № 98-ФЗ «О коммерческой тайне» (в ред. ФЗ от 18 декабря 2006 г. № 231-ФЗ) (далее — Закон) подтвердил тенденцию укрепления позиций рыночной экономики в России. Вместе с тем формирование механизма прав организаций на информацию, содержащую коммерческую тайну, и обеспечение их информационной безопасности сопряжено на практике с определенными трудностями. Результаты исследования позволили выделить проблемы по совершенствованию законодательства о коммерческой тайне и предложить пути их решения.

*Первая группа проблем имеет общетеоретический характер.* Их решение позволит сформировать единый подход к формированию правового механизма регулирования и защиты коммерческой тайны.

1. *О понятии «коммерческая тайна».* Определению этого понятия посвящены п. 1 и 2 ст. 3 Закона. Вместе с тем в названных пунктах Закона упущен, как представляется, частноправовой подход к определению коммерческой тайны. В ст. 1465 ГК РФ указаны условия, при соблюдении которых в отношении сведений любого характера может быть введен режим коммерческой тайны. Институт коммерческой тайны призван защищать частные интересы лиц, занимающихся предпринимательской деятельностью с целью получения прибыли. Такими лицами являются коммерческие организации (п. 1 и 2 ст. 50 ГК РФ) и индивидуальные предприниматели (ст. 23 ГК РФ), а не любые лица, как это следует из определения понятия «обладатель информации, составляющей коммерческую тайну» (п. 4 ст. 3 Закона). В литературе высказано мнение о том, что «правильнее было бы говорить не об обладателях, а о владельцах коммерческой тайны», имеющих монопольное право на такую информацию, а также о «конфидентах коммерческой тайны», т.е. лицах, которым на основании трудового или гражданско-правового договора либо законна стала известной коммерческая тайна (работники, контрагенты, государственные органы и их должностные лица)<sup>2</sup>. Представляется,

что в правовом отношении между ними имеется разница по поводу распоряжения документированной информацией, составляющей коммерческую тайну, что должно учитываться при реализации выказанных предложений по совершенствованию законодательства о коммерческой тайне. Поэтому коммерческую тайну составляет любая коммерчески значимая информация, определяемая и защищаемая коммерческой организацией или индивидуальным предпринимателем на законном основании, используемая указанными лицами в предпринимательской деятельности с целью получения прибыли.

Введение в Закон понятия «коммерчески значимая информация» позволит определить завершенную систему положений, связанных с обеспечением информационной безопасности субъектов регулируемых отношений, рассматривать в содержательном единстве понятия «коммерческая тайна» и «секрет производства (ноу-хау)», включающих различные сведения технического, технологического и делового характера, имеющих коммерческую значимость, а не отождествлять эти два понятия, как это сформулировано в ст. 34 ФЗ от 18 декабря 2006 г. № 231-ФЗ (изменения внесены в п. 2 ст. 3 ФЗ «О коммерческой тайне»). На наш взгляд, понятие «коммерческая тайна» шире понятия «секрет производства». Оно включает, наряду с секретом производства, часть коммерческой информации (торговые секреты), широко используемой в торговом обороте, и позволяет более точно выразить сущность понятия «информация, составляющая коммерческую тайну (секрет производства)», раскрываемого в п. 2 ст. 3 Закона. В таком понимании КЗИ играет важную роль в рыночной экономике.

2. *О праве организации на документированную информацию, составляющую коммерческую тайну, и возможности включения ее в состав имущества организации.* Закон прямо не содержит положений, закрепляющих это право за обладателем документированной информации, составляющей коммерческую тайну. Между тем эти вопросы возникают в случае реорганизации коммерческих организаций и принятия решения о передаче правопреемнику прав на такую информацию. Аналогичная ситуация может возникнуть и при ликвидации организации, когда после сдачи в архив документов часть из них остаются невостребованными. Речь идет о технической документации (отчеты НИОКР и др.), содержащей КЗИ. Вопрос в данном случае должен решаться с учетом того факта, что документированная информация является частью имущества организации и его реализация возможна на договорной основе.

<sup>1</sup> См.: Зеин И., Морзунова Е., Погуляев В. Что такое информация и как ее защищать // Закон. 1998. № 2; Минаев С. Коммерция перестала быть тайной // Коммерсантъ. 2004. 4 августа, и др.

<sup>2</sup> См.: Бачило И.Л., Лопатин В.Н., Федотов М.А. Информационное право. СПб., 2001. С. 509; Бельев М.В. Субъекты права на коммерческую тайну: проблемы правового статуса // СПС «Консультант Плюс», и др.

Вопрос об отнесении документированной информации к имуществу организаций в ФЗ «Об информации, информационных технологиях и о защите информации» не решен. В соответствии с п. 5 ст. 11 Закона «право собственности и иные вещные права на материальные носители, содержащие документированную информацию, устанавливаются гражданским законодательством». Однако ГК РФ не содержит соответствующих норм, регулирующих такие правоотношения. Ранее этот вопрос был решен ныне утратившим силу ФЗ «Об информации, информатизации и защите информации», содержащем положения о включении в состав имущества организации документированной информации (ст. 2, 5, п. 2, 5 и 6 ст. 6). По этому пути шли и некоторые субъекты РФ, в которых были приняты законы об информационных ресурсах, находящихся в их собственности. Например, Закон г. Москвы от 24 октября 2001 г. № 2 «Об информационных ресурсах и информации города Москвы» (в ред. Закона г. Москвы от 28 декабря 2005 г.) разрешает включение документированной информации в состав имущества организаций.

Учитывая имеющийся опыт, предлагается указывать документированную информацию с грифом «коммерческая тайна» как имущество в балансе юридического лица в разделе «учет нематериальных активов» после внесения соответствующих изменений в законодательство. В частности, потребуется внести в Положение по бухгалтерскому учету в раздел «Учет нематериальных активов» ПБУ 14/2000 от 16 октября 2000 г. № 9<sup>1</sup>н<sup>1</sup>, а также в Закон о коммерческой тайне дополнение о том, что оценка документированной информации, содержащей коммерческую тайну, производится ее обладателем на основании методики Минфина РФ. Такой порядок позволит избежать злоупотреблений со стороны хозяйствующих субъектов. Включение такой информации в состав имущества организации потребует внесения дополнений в ФЗ от 21 ноября 1996 г. № 129-ФЗ «О бухгалтерском учете». Полагаем, что фактическая монополия организации на такую информацию может быть формально закреплена путем включения документированной информации, содержащей коммерческую тайну, в состав ее имущества.

Решение этого вопроса позволит не гипотетически предполагать, что КЗИ — это ценный ресурс, а фактически учитывать экономическую составляющую коммерческой ценности информации как

<sup>1</sup> См.: Положения по бухгалтерскому учету. М.: Дело и сервис, 2002. С. 244–266.

товара. При этом условия КЗИ сама становится предметом купли-продажи и иных сделок.

3. *О возникновении и прекращении права на коммерческую тайну.* Важным вопросом является определение момента возникновения права на коммерческую тайну (секрет производства), которое по версии ст. 1467 ГК РФ связывает с введением режима коммерческой тайны. При этом упускается из виду, что это право формально представляется на основании учредительных документов (п. 1 ст. 49 ГК РФ), где оно юридически должно быть закреплено за организацией с момента ее государственной регистрации. Конечно, коммерческая тайна, как справедливо отмечает И.Л. Бачило, может появиться и не с момента регистрации и записи в учредительных документах и регистрации предпринимателя, а в процессе хозяйственной деятельности. Речь идет не только о правах, но и обязанностях обладателя коммерческой тайны (например, о защите информации при ее получении по договору), поскольку они взаимосвязаны и существуют неразрывно.

Поэтому важно закрепить право организаций на информацию, содержащую коммерческую тайну, в учредительных документах с учетом предложений по совершенствованию законодательства о коммерческих организациях<sup>1</sup>. Законодательное решение данного вопроса позволит администрации финансировать деятельность по защите коммерческой тайны с отнесением затрат на основную производственную деятельность.

4. *О закреплении принципов разработки перечня информации, составленной коммерческой тайну.* Пункт 1 ч. 1 ст. 10 Закона установил обязанности обладателя по определению перечня информации, составляющей коммерческую тайну, однако не закрепил принципы формирования структуры данного документа. На практике это приводит к разному в подходах к его составлению, что затрудняет работу государственных органов, имеющих право требовать предоставление такой информации, и затрагивает в определенной мере права других лиц, связанных с ограничениями на ознакомление с информацией. Поэтому предлагается закрепить в Законе положение о том, что при составлении Перечня обладатель должен исходить из определения прибыльных направлений своей деятельности; рыночной

<sup>1</sup> См.: Суханов Е.А. Проблемы развития законодательства о коммерческих организациях // Хозяйство и право. 2002. № 5, и др.

конъюнктуры товаров (работ, услуг), уровня сбыта аналогичных товаров и прибыльности других организаций, а также учитывать возможности установления адекватных мер защиты выделенной информации.

5. *О правомерности правил допуска, разрабатываемых организациями.* В ст. 10 Закона в общем виде сформулировано положение об ограничении доступа лиц к информации, составляющей коммерческую тайну. На практике широко применяются меры, ограничивающие допуск граждан к коммерческим секретам. Эта процедура предшествует оформлению трудового договора с гражданином. В связи с оформлением допуска острями являются вопросы получения добровольного согласия лица на проведение в отношении него проверочных мероприятий и четкого закрепления в Законе оснований для отказа гражданину в допуске к коммерческой тайне.

Между тем практика действий администрации по проведению проверочных мероприятий вызывает определенные нарекания. Речь идет об использовании службами безопасности таких методов и средств, которые порой нарушают конституционные права граждан на тайну переписки, ведения телефонных переговоров, банковскую тайну и др. Для сравнения укажем, что вопрос о защите интересов государства и проверки в этой связи лиц, допускаемых к государственной тайне, урегулирован Федеральным законом «О государственной тайне». В частности, лицо дает письменное согласие на проведение в отношении него полномочными органами проверочных мероприятий<sup>1</sup>.

Учитывая, что Конституция РФ (ч. 2 ст. 8) равным образом защищает частную и государственную собственность, предлагается внести дополнение в Закон о правомерности использования организацией определенных сил и средств для проверки лиц, допускаемых к коммерческой тайне. Решение этой задачи связано с определением пределов возможного использования сил и средств и необходимости внесения соответствующих изменений в законы «Об оперативно-розыскной деятельности» и «О частной детективной и охранной деятельности в Российской Федерации».

6. *О регулировании трудовых правоотношений.* Законом должным образом не урегулирована финансовая сторона отношений работ-

ника и работодателя по поводу защиты информации, составляющей коммерческую тайну. *Во-первых*, не предусмотрены обязанности работодателя по выплате вознаграждения работнику, получившему в процессе трудовой деятельности информацию, имеющую коммерческую значимость для организации. Размер и условия такого вознаграждения должны устанавливаться трудовым договором на основании оценки труда работника в соответствии с правовой нормой. *Во-вторых*, согласие работника о соблюдении установленного режима коммерческой тайны должно быть письменно подтверждено в трудовом договоре и дополнительно оплачено (например, в процентах к должностному окладу). *В-третьих*, после прекращения трудового договора работодатель теряет правовые основания требовать от работника сохранения коммерческой тайны. В этом случае стороны могут заключить, например, гражданско-правовой договор возмездного оказания услуг по сохранению коммерческой тайны, условия которого определяются сторонами. При отсутствии у работника желания заключить такой договор и в случае разглашения или незаконного использования им сведений, составляющих коммерческую тайну, после его увольнения действуют нормы ГК РФ и УК РФ, устанавливающие ответственность. Это в полной мере относится и к работникам организации-контрагента.

Важным является вопрос о размере возмещаемых работателю убытков, причиненных неправомерными действиями либо бездействием работника, разгласившего коммерческую тайну вопреки трудовому договору. Статья 238 ТК РФ устанавливает обязанность работника возместить работодателю прямой действительный ущерб, кроме неполученных доходов (упущенная выгода). Причем под прямым действительным ущербом понимается реальное уменьшение наличного имущества работодателем. Размер ущерба определяется по фактическим потерям, исчисляемым исходя из рыночных цен, но не ниже стоимости имущества по данным бухгалтерского учета (ст. 246 ТК РФ). Из этого следует, что без учета на балансе документированной информации, составляющей коммерческую тайну в составе имущества организации, нельзя вести речь о причинении ущерба организации и о привлечении работника к полной материальной ответственности на основании ст. 243 ТК РФ за разглашение таких сведений. Применение к работнику санкции в пределах среднего месячного заработка (ст. 241 ТК РФ) за ущерб, образовавшийся вследствие разглашения КЗИ, причиненный работодателю, не может покрыть экономические потери организации. Поэтому нужны методические

<sup>1</sup> См.: Государственная тайна и ее защита в Российской Федерации / Под общ. ред. М.А. Вуса и А.В. Федорова. СПб., 2003. С. 325–348.



рекомендации по оценке ущерба, причиненного вследствие разглашения коммерческой тайны, утвержденные Минфином РФ.

7. *О взаимоотношении организаций с государственными и муниципальными органами власти по поводу предоставления им КЗИ.* Законом предусмотрена обязанность организаций по запросам налоговых, природоохранных, антимонопольных и других государственных органов предоставлять информацию, составляющую коммерческую тайну, необходимую для решения стоящих перед ними задач. Вместе с тем процедура передачи информации фрагментарно закреплена в некоторых правовых актах, определяющих правовое положение федеральных министерств и служб. Статья 6 Закона устанавливает обязанность обладателя предоставлять такую информацию по требованию органов государственной власти, иного государственного органа, органа местного самоуправления.

По нашему мнению, правом истребования информации, содержащей коммерческую тайну, должны быть наделены только те государственные органы, которые выполняют судебные, надзорные и контрольные функции по отношению к организациям и индивидуальным предпринимателям на основании федерального закона. Полагаем, что предоставление властных полномочий всем государственным органам власти и управления, их должностным лицам, включая и местные органы власти, на изъятие информации, содержащей коммерческую тайну, не будет способствовать реализации конституционного принципа равенства защиты частной и государственной собственности.

При предоставлении информации по запросу государственного органа возникают административно-правовые, а не гражданско-правовые отношения. Поэтому в Законе должны быть прописаны гарантии того, что эта информация по вине должностных лиц не станет достоянием третьих лиц и, таким образом, обладателю не будет причинен ущерб. Однако ответственность должностных и муниципальных служащих не установлена.

На случай разглашения или неправомерного использования охраняемой информации по вине государственного органа либо органа местного самоуправления предлагается, во-первых, ввести денежную компенсацию государством либо муниципальным образованием стоимости изъятой информации, содержащей коммерческую тайну (например, в размере не менее 1000 МРОТ), во-вторых, установить дисциплинарную и уголовную ответственность служащих за ущерб, причиненный обладателю такой информации. Появление в

трудовом и уголовном законодательстве соответствующих норм позволит повысить ответственность должностных лиц за сохранность сведений, составляющих коммерческую тайну, и будет иметь общепреventивное значение для защиты частных интересов.

Учитывая предложение, предшествовавшие принятию части четвертой ГК РФ, касающейся регулирования информационных процессов<sup>1</sup>, и содержание главы 75 ГК РФ, можно констатировать, что ряд вопросов правового регулирования обращения КЗИ и ее защиты не были законодательно урегулированы. Поэтому защита интересов предпринимателей требует совершенствования законодательства о коммерческой тайне с учетом стратегии инновационного развития России.

---

<sup>1</sup> См.: Дозорцев В.А. Интеллектуальные права: Понятие. Система. Задачи кодификации: Сб. статей / Исслед. центр частного права. М., 2005. С. 224–237, 346–405.

и оказании услуг, связанные с определенными целями организации. Признаки, включаемые в понятие «правовые средства», предметно увязаны с такими целями организации, как: 1) защита законных прав организаций во взаимоотношениях с органами государственной власти и местного самоуправления, партнерами и конкурентами; 2) подержание внутреннего порядка управления; 3) повышение конкурентоспособности товаров; 4) развитие кооперированных связей и недопущение зависимости от недобросовестных конкурентов и партнеров; 5) развитие техники и технологий на уровне мировых стандартов; 6) создание благоприятной рыночной конъюнктуры и рост прибылей за счет эффективного использования КЗИ в рекламной и инновационной деятельности, при осуществлении внешней торговли.

Для достижения указанных целей организациям нужно решить ряд сложных задач по своевременному выявлению угроз жизненно важным для их бизнеса интересам, использованию правовых средств по установлению режима КЗИ, выявлению, предупреждению и пресечению правонарушений в сфере обращения КЗИ. Поэтому содержание понятия «правовые средства» не может быть универсальным, оно зависит от решаемых организацией задач и определяется направлениями ее предпринимательской деятельности.

Термин «правовые средства» был введен в научный оборот учеными-юристами еще в дореволюционный период<sup>1</sup>. Проблема содержательной интерпретации правовых средств как научной категории относится к числу наиболее актуальных и «вечных» объектов исследования юридической науки. Общетеоретическим и гражданско-правовым проблемам правовых средств посвящены многие работы<sup>2</sup>. Одной из первых фундаментальных работ, в которой рассматриваются теоретические проблемы использования гражданско-правовых средств в сфере экономики, явилась монография Б.И. Путинского «Гражданско-правовые средства в хозяйственных отношениях» (М., 1984). Несмотря на то, что со времени ее издания прошло почти 25 лет, многие содержащиеся в ней выводы и рекомендации сохра-

<sup>1</sup> См.: Шершеневич Г.Ф. Общая теория права. М., 1912; Петражицкий Л.И. Введение в изучение права и нравственности. Основы эмоциональной психологии. СПб., 1908; Иеринг Р. Цель в праве. Т. 1. СПб., 1881, и др.

<sup>2</sup> См.: Алексеев С.С. Механизм правового регулирования в социалистическом государстве. М., 1966; Быков А.Г. План и хозяйственный договор. М., 1975; Зименский Г.Л. Совершенствование хозяйственного законодательства: цель и средства. Киев, 1980; Замойский И.Е. Эффективность хозяйственно-правовой работы. Киев, и др.

## ГЛАВА 2

# Использование правовых средств при обращении коммерчески значимой информации

## § 1. Понятие правовых средств и их применение при обращении коммерчески значимой информации

**Понятие правовых средств, используемых коммерческими организациями в сфере обращения КЗИ**, относится к числу важнейших для понятийного аппарата юридической науки. Точность определения понятия «правовые средства» необходима для решения задач по установлению режима конфиденциальности организаций, имеющей информации и обеспечению безопасности субъектов своих целей. Большой важность для достижения субъектов исследования проблем ширинство ученых, труды которых посвящены исследованию проблем информационного правоотношений, не используют либо неточно излагают сущность данного понятия<sup>1</sup>.

Понятием «правовые средства» охватываются различные процессы и этапы обращения КЗИ. *Правовые средства* — это предусмотренные законом инструменты (методы, формы) обеспечения защиты КЗИ при производстве и реализации товаров, выполнении работ

<sup>1</sup> См.: Сергеев А.П. Право интеллектуальной собственности в Российской Федерации. М., 1996. С. 619–633; Фатьянов А.А. Правовое обеспечение безопасности информации в Российской Федерации. М., 2001. С. 183–218; Копылов В.А. Информационное право. М., 2003. С. 383–391, и др.

няют свою актуальность и сегодня, в период становления рыночной экономики в России, и отличаются широким масштабом анализируемых гражданско-правовых проблем<sup>1</sup>. Существенный вклад в развитие теории использования правовых средств внесли последующие работы отечественных ученых-цивилистов<sup>2</sup>.

При определении совокупности признаков, составляющих содержание понятия «правовые средства», используемого в сфере обращения КЗИ, автор исходил из общих концептуальных представлений о правовых средствах, сформировавшихся в течение последних десятилетий в отечественной юридической науке. В своей совокупности они сводятся к системе теоретических положений, раскрывающих сущность правовых средств, их место и роль в системе правового регулирования, условия и порядок их применения и т.д. Исходным и бесспорным является положение о том, что понятие «правовые средства» является составной частью общего понятия категории «правовое регулирование».<sup>3</sup> Как подчеркивает С.С. Алексеев, «правовые средства не образуют каких-то особых, принципиально отличных от традиционных, зафиксированных догмой права, в общепринятом понятийном аппарате явлений правовой действительности. Это весь арсенал, весь спектр правовых феноменов различных уровней с той лишь особенностью, что они вычленяются и рассматриваются... с позиций их функционального предназначения, тех черт, которые характеризуют их как инструменты правового регулирования...». Далее, поясняя свою мысль, С.С. Алексеев пишет, что «перед нами те же юридические нормы, хозяйственные договоры, счета в банке, меры поощрения, санкции, но предстающие в качестве функциональных явлений, инструментов реализации силы, ценности права»<sup>4</sup>.

<sup>1</sup> См.: Пугинский Б.И. Основные проблемы теории гражданско-правовых средств: Автореф. дисс. докт. юрид. наук. М., 1985.

<sup>2</sup> См.: Алексеев С.С. Правовые средства: постановка проблемы, понятие, классификация // Советское государство и право. 1987. № 11; Гойман В.И. Действие права (методологический анализ). М., 1992; Исаков В.Б. Механизм правового регулирования // Проблемы теории государства и права / Под ред. С.С. Алексеева. М., 1987; Малько А.В. Правовые средства как общетеоретическая проблема // Правоведение. 1999. № 2, и др.

<sup>3</sup> Алексеев С.С. Право: азбука — теория — философия: Опыт комплексного исследования. М., 1999. С. 347.

<sup>4</sup> Там же. С. 349.

Наиболее полно характеристика правовых средств представлена в упомянутой работе Б.И. Пугинского, который указывает ряд существенных признаков, позволяющих отличать правовые средства от других правовых явлений:

- 1) правовые средства представляют собой конкретные способы решения экономико-социальных задач участниками гражданского оборота;
- 2) это сочетание действий юридического характера, выполняемые субъектами, своего рода «пустышки» правового действия;
- 3) они имеют правовую природу в силу законодательного установления, что обуславливается сознательной направленностью действий субъектов на создание юридически значимого результата;
- 4) их использование рассчитано на определенную инициативность и свободу усмотрения субъекта в выборе соответствующего правового средства, определения его содержания и порядка работы с ним;
- 5) правовые средства — это целостные образования, составляющие комплекс средств, который характеризуется внутренней взаимосвязанностью и структурным единством; важнейшими из них являются договоры, внедоговорные обязательства, различные юридические конструкции, санкции и т.д.;
- 6) диапазон функционирования правовых средств достаточно широк, область применения конкретного правового средства определяется его адекватностью подлежащей решению задаче<sup>1</sup>.

Развивая мысль Б.И. Пугинского об использовании правовых средств по достижению желаемого результата, А.В. Малько в дополнении к перечисленным признакам называет еще три характерные черты, присущие правовым средствам. По мнению А.В. Малько, правовые средства связывают в процессе регулирования объекта «идеальное (цель) с реальным (результат)», т.е. идеальную и материальную стороны. Они приобретают особые свойства явлений, действующих в связке «цель — средство — результат». В этой связи нужно отметить, что понятие «цель» находит свое выражение применительно к обеспечению безопасности коммерческой организации. Названная цель в данном случае определяет выбор по усмотрению организации правовых средств. Их использование обусловлено част-

<sup>1</sup> См.: Пугинский Б.И. Гражданско-правовые средства в хозяйственных отношениях. М., 1984. С. 86—89, 97.

ными интересами организации, связанными с получением максимальной прибыли и иной коммерческой выгоды (результат).

Заслуживает внимания суждение А.В. Малько о том, что правовые средства объединяются в определенную систему для решения поставленных задач, воплощаются в механизме правового регулирования для того, чтобы успешно преодолевать препятствия и добиваться социально значимых результатов. И, наконец, высказанная им мысль о том, что определенное сочетание юридических средств в правовых режимах, методах правового регулирования придает специфику отраслям права, выражает особый порядок организации конкретных общественных отношений<sup>1</sup>, может рассматриваться как существенное дополнение их системной характеристики.

Разработка концепции правовых средств является результатом усилий многих ученых. Окончательное формирование концепции в силу ее чрезвычайной сложности и многогранности еще предстоит осуществить в ходе анализа и обобщения материалов правового обеспечения деятельности хозяйствующих субъектов в рыночной экономике. Это представляется важным потому, что многие исследователи, приступая к изучению конкретного объекта, независимо от отрасли права, пытаются наметить тот или иной круг существенных признаков, которые, по их мнению, достаточны для формулирования основных свойств использования правовых средств.

Практика деятельности коммерческих организаций показывает, что имеется необходимость внесения ясности по основным вопросам выбора и использования правовых средств в сфере обращения КЗИ. Это, прежде всего, решение вопроса о том, какие правовые средства охватываются данным понятием и могут быть использованы в сфере обращения КЗИ, т.е. их круг, а во-вторых, какие средства имеют доминирующий характер в технологической цепочке охраны конфиденциальности КЗИ. Учитывая направленность настоящего исследования, задача состоит в адаптации имеющейся общей концепции правовых средств, на основе накопленных данных теории и практики применительно к рассматриваемой нами проблеме. Речь идет о выявлении специфики использования правовых средств в сфере обращения КЗИ, об анализе существующего положения дел в области

охраны КЗИ, о выработке рекомендаций правовотворческого и правоприменительного характера.

При определении содержания и объема понятия «правовые средства», применяемого в сфере обращения КЗИ, в качестве исходной позиции с учетом положений общей концепции была использована классификация правовых средств, предложенная Б.И. Пугинским<sup>1</sup>. Суть ее состоит в распределении правовых средств по группам признаков, позволяющим выделить их свойства и определить место с учетом решаемых теоретических и практических задач в гражданском обороте. Группировка признаков была осуществлена, *во-первых*, в зависимости от функционального назначения правовых средств, а именно: служащие организации гражданского и, в частности, торгового оборота через создание субъективных прав и обязанностей лиц; обеспечивающие их реализацию с использованием мер имущественной ответственности, способов защиты гражданских прав, мер оперативного воздействия, мер обеспечения исполнения обязательств; содействующие исползованию других правовых средств и notably в этой связи вспомогательный характер; регулирующие деятельность участия лиц в обороте и определяющие круг их полномочий. *Во-вторых*, по кругу субъектов, управомоченных применять соответствующие правовые средства, которые используются непосредственными участниками оборота в пределах их компетенции. *В-третьих*, деление правовых средств в зависимости от порядка их применения собственными действиями участников оборота, на основе правоприменительных актов суда и административных актов государственных органов. *В-четвертых*, распределение правовых средств по степени сложности на: первичные (элементарные), т.е. субъективные права и юридические обязанности, поощрения и наказания, льготы и запреты, и на комплексные (составные) правовые средства — договор, институт, правовой режим и др. *В-пятых*, деление правовых средств на регулятивные (дозволения) и охранительные (меры защиты) в зависимости от выполняемой ими роли. *В-шестых*, распределение правовых средств с учетом характера их воздействия на материально-правовые (рекомендации) и процессуальные (иск), а также времени их действия — на постоянные и временные. *В-седьмых*, деление правовых средств в зависимости от вида правового регулирования — на

<sup>1</sup> См.: Малько А.В. Правовые средства как общетеоретическая проблема // Правоведение. 1999. № 2.

<sup>1</sup> См.: Пугинский Б.И. Указ. соч. С. 91–93.

нормативные (установленные в нормах права — запреты) и индивидуальные (например, акт реализации прав и обязанностей).

Универсальный характер названной классификации позволяет ее рассматривать как исходную базу при конкретизации понятийных признаков правовых средств применительно к проблеме охраны конфиденциальности КЗИ. Эта конкретизация необходима для выявления особенностей выбора и применения правовых средств регулирования корпоративных, трудовых и гражданско-правовых отношений в сфере обращения КЗИ. Специфика регулирования отношений в рассматриваемой сфере обусловлена особой правовой природой информации, действием в зависимости от хозяйственной ситуации обязывающих, запрещающих и управомочивающих юридических норм, зависимостью решения задач по обеспечению безопасности организаций от установленного правового режима охраны конфиденциальности КЗИ. Основной отличительной чертой понятия правовых средств, используемых в сфере обращения КЗИ, от общего, является, например, то, что оно не дублирует общее, богаче по набору признаков, выполняет конкретную служебную роль и т.д. Исходя из названных соображений **понятие правовых средств, используемых организациями, их роль и место в механизме правового регулирования обращения КЗИ и охраны ее конфиденциальности** можно определить как совокупность признаков:

1) позволяющих определить значимость правовых средств как универсальных правовых инструментов в реализации целей организации, обусловленных ее частными интересами, устанавливающих по усмотрению организаций их право на КЗИ в пределах, допускаемых законом, с учетом факторов и степени воздействия внешней среды; определяющих правоотношения организации с государством, поставщиками, потребителями, конкурентами, учредителями (акционерами), дочерними и зависимыми обществами по поводу КЗИ;

2) определяющих требования к содержанию трудовых прав и обязанностей работодателей и работников, командированных и иных лиц в сфере обращения КЗИ, и их реализацию с использованием мер юридической ответственности;

3) закрепляющих в гражданско-правовом договоре по инициативе и усмотрению сторон субъективные гражданские права и обязанности по поводу использования, передачи и охраны КЗИ и обязывающих их реализацию с использованием различных способов защиты гражданских прав на КЗИ; учитывающих особенности возникновения внедоговорных обязательств в сфере обращения КЗИ;

4) характеризующих порядок установления правового режима обращения КЗИ, определяющих систему мер режима КЗИ, обеспечивающих участие юридической службы и службы безопасности, других подразделений организации в реализации названных мер и фиксирующих круг их полномочий; отражающих особенности правовой охраны информации, переданной в связи с выполнением государственного заказа;

5) имеющих значение для выявления нарушений установленного режима коммерческой тайны с использованием методов контрольной и аналитической работы, понимания причин и обстоятельств, способствующих совершению правонарушений, осуществления предупредительной деятельности в целях обеспечения информационной безопасности организации.

Названные группы признаков находятся между собой в тесной взаимосвязи и взаимно дополняют друг друга. Их выделение носит в значительной мере условный характер и преследует главным образом цель связать работу по анализу использования правовых средств, регулирующих сферу обращения КЗИ, с решением задач по установлению режима КЗИ и обеспечению его в организациях. В обобщенном виде роль каждой разновидности признаков с этих позиций может быть обозначена следующим образом.

*Первая группа признаков* представляет информацию о выборе, моделировании и формировании на уровне конкретной организации механизма корпоративного регулирования КЗИ, представляющего собой систему правовых средств, включающую корпоративные акты, договор и иные средства, субъективные права и юридические обязанности и их реализацию. Она отражает степень закрепления в учредительных документах и иных корпоративных актах права организации на КЗИ и ее защиту; раскрывает взаимоотношения организации с учредителями (участниками) общества; показывает возможность использования по усмотрению организации позитивных обязанностей, запретов, дозволений, содержащихся в нормах гражданского, трудового, административного и уголовного законодательства, исходя из закрепленных субъективных прав и обязанностей в сфере обращения КЗИ, не противоречащих интересам личности, общества и государства. Разработка теории правовых средств, используемых в сфере обращения КЗИ, является актуальной задачей применительно к формирующемуся в рамках частного права институту коммерческой тайны, когда на практике организации пытаются до-

стичь своих частных целей с помощью конкретных средств, установленных законодательством.

*Вторая группа признаков* показывает «внутреннюю» среду обращения КЗИ в организации при возникновении и прекращении трудовых правоотношений по поводу охраны и защиты КЗИ. Она раскрывает взаимные права и обязанности работника и работодателя в этой сфере деятельности; позволяет учитывать факторы, определяющие появление возможных каналов утечки КЗИ, обусловленные социальными нарушениями в этой сфере и особенностями личности нарушителей. Знание этих факторов имеет непосредственное значение для выявления, предупреждения и пресечения правонарушений в рассматриваемой сфере деятельности организации.

*Третья группа признаков* характеризует «внешнюю» среду обращения КЗИ при взаимоотношении организации с контрагентами, партнерами и иными лицами, органами государственной власти и местного самоуправления в рамках договорных и внедоговорных обязательств. Она позволяет свободно использовать не только правовые средства, определяемые законами и иными правовыми актами, но и знать те, которые порождаются использованием самих субъектов, прежде всего, в рамках гражданско-правового договора. Эта группа признаков позволяет учитывать, что свобода принятия организацией решений в сфере обращения КЗИ ограничена в законе определенными пределами усмотрения; порядок действий при применении конкретных средств урегулирован нормами права.

В случаях злоупотребления правом на КЗИ, использования недозволенных способов ее получения либо разглашения (утечки) пресечение неправомерных действий лиц осуществляется по усмотрению организации в рамках предоставленных законом возможностей. Это может быть обращение в правоохранительные или административные органы с заявлением о возбуждении уголовного или административного дела (антимонопольный орган и др.) либо в суд с иском о возмещении убытков. ГК РФ устанавливает и иные способы защиты гражданских прав, которые могут быть использованы организацией при операциях с КЗИ.

*Четвертая группа признаков* базируется на наличии неразрывной связи между угрозами информационной безопасности организации и объемом (направлениями) устанавливаемого по ее усмотрению режима конфиденциальности КЗИ в рамках, предусмотренных законом. Эту взаимосвязь важно учитывать при определении сведений, составляющих КЗИ, урегулировании порядка допуска и до-

ступа граждан и юридических лиц к КЗИ, планировании режимных мер обеспечения технологических процессов производства товаров и сложившейся деловой практики их реализации; выполнении конфиденциальных работ, включая заказы для государственных нужд, и оказании услуг другим лицам по охране КЗИ в пределах, допускаемых законом.

*Пятая группа признаков* непосредственно связана с правовым обеспечением информационной безопасности организации, которое осуществляется путем выявления в ходе проведения контрольной и аналитической работы нарушений обращения КЗИ, установления возможных каналов утечки КЗИ, анализа причин и обстоятельств, ее обуславливающих, разработки и реализации предупредительных мер на различных этапах производства и продажи изделий, в местах наибольшего сосредоточения коммерческих секретов. Эта группа признаков раскрывает особенности технологии «связывания» и реализации субъективных прав и обязанностей между лицами внутри организации и при исполнении ими обязательств с контрагентами, касающихся сохранности КЗИ (внешний фактор).

Таким образом, правовые средства, используемые в сфере обращения КЗИ: 1) имеют правовую природу, 2) устанавливаются юридическими нормами, корпоративными актами, договором и иными средствами, 3) их выбор осуществляется по волевому усмотрению организации с учетом воздействия внешней среды и внутренней обстановки в трудовом коллективе, в пределах, допускаемых законом, 4) они представляют собой способы самостоятельной практической деятельности по закреплению прав на КЗИ и их защите, определяемые целями организации.

В рамках настоящего параграфа рассмотрим первую группу признаков, характеризующих *корпоративное регулирование отношений в сфере обращения КЗИ на уровне организации*. Остальные группы признаков будут рассмотрены в последующих главах монографии.

Анализ практики перехода хозяйствующих субъектов на рыночные отношения позволяет сделать вывод о том, что за последние 10 лет с момента введения в действие части первой ГК РФ намечалась тенденция постепенного сужения сферы государственного вмешательства в предпринимательскую деятельность. Хотя это совсем не означает, что государство устранилось от регулирования экономических преобразований. На самом деле изменились его функции

в переходной экономике<sup>1</sup>. Это проявляется, с одной стороны, в определении государством главных направлений реализации экономической политики с использованием специальных способов и методов преимущественно общедозволительного типа регулирования<sup>2</sup> деятельности хозяйствующих субъектов. Речь идет о равенстве участников гражданских отношений и неприкосновенности их собственности, о свободе договора, недопустимости вмешательства в частные дела, об обеспечении восстановления нарушенных прав и судебной их защите (ст. 1 ГК РФ).

Более конкретно роль государства применительно к деятельности коммерческих организаций выражается: во введении общих правил их создания, реорганизации и ликвидации; в легализации их деятельности с использованием средств лицензирования, аккредитации, сертификации; в установлении налогов (сборов), стандартов, квот, тарифов, ставок таможенных пошлин и др.; в осуществлении государственного контроля по ведению бухгалтерского учета и представлению отчетности; в применении законных санкций к нарушителям<sup>3</sup>.

С другой стороны, изменение порядка регулирования состоит в признании и соблюдении государством прав организаций, необходимых им для участия в рыночных отношениях. Важнейшими из них являются: право организаций на получение прибыли от пользования имуществом, продажи товаров, выполнения работ или оказания услуг (ст. 2 ГК РФ), на самостоятельное формирование и использование своих информационных ресурсов и в этой связи осуществление поиска, получения, передачи, производства и распространения информации; право на защиту КЗИ. Право юридических лиц на информацию выражается в возможности создания ими с учетом профиля их деятельности и решаемых задач собственной информационной системы. Обеспечение безопасности функционирования этой системы занимает особое место в деятельности организации. Это объясняется тем, что информация является связующим элементом, пронизывающим все производственные и коммерческие процессы,

<sup>1</sup> См.: Экономическая теория: Учебник / Под ред. В.Д. Камаева. М., 2002. С. 607–609.

<sup>2</sup> См.: Алексеев С.С. Общие дозволения и общие запреты в советском праве. М., 1989. С. 103–163.

<sup>3</sup> См.: Предпринимательское право Российской Федерации / Отв. ред. Е.П. Губин, П.Г. Лахно. М., 2004. С. 396–429.

служит важным рычагом получения прибыли и достижения иных целей организации. Именно от осуществления этого права зависит степень самостоятельности организации на представительство и защиту своих частных интересов и, в конечном итоге, реализация всех остальных прав.

По мере уменьшения масштабов государственного правового воздействия на экономику и увеличения степени самостоятельности коммерческих организаций вопрос о корпоративном регулировании хозяйственной деятельности, в том числе обращения КЗИ, приобретает все большую актуальность. В юридической науке высказаны различные мнения о правовой природе, роли и месте корпоративного права в регулировании общественных отношений<sup>1</sup>, возникающих на уровне отдельных организаций. Под корпоративным правом, являющимся составной частью гражданского права, понимается система правил, установленных собственником или администрацией коммерческой организации и регулирующих внутрифирменные отношения.

Акты, регулирующие внутреннюю деятельность организаций, чаще всего именуются в правовой литературе как «локальные» или «корпоративные» акты. Употребление наименования «локальные акты», а также «внутренние документы» являлось традиционным для советской правовой науки. Их разработка предусматривала использование предприятиями унифицированных форм организационно-распорядительной документации, утверждаемых вышестоящими государственными органами, например, о квартальном и годовом планировании, отчетности, премировании и др. Локальное «огосударвленное» нормотворчество в советский период использовалось в «усеченном» виде и не играло столь заметной роли в регулировании хозяйственной деятельности предприятий. Локальные акты, издававшиеся на предприятиях, слово в слово повторяли циркуляры министерств и центральных органов управления народным хозяйством, что реально отражало отсутствие у них необходимых хозяйственных прав.

Такое же положение было характерно и для сферы охраны секретов. На предприятиях действовали внутренние документы, определявшие режим секретности проводимых работ, в частности, порядок

<sup>1</sup> См.: Шиткина И.С. Правовое регулирование деятельности коммерческих организаций внутренними (локальными) документами. М., 2003, и др.

заключения договоров с контрагентами, разработки единых планов по сохранению государственных секретов при выполнении особо важных НИОКР. Годовой комплексный план по обеспечению режима секретности составлялся на основании аналогичного плана министерства (ведомства) с учетом оперативной обстановки, возможности использования сил и средств, имеющихся на предприятии для решения конкретных задач. Министерством (главным управлением по режиму) устанавливался порядок представления отчетности о выполнении мероприятий по обеспечению режима секретности. Перечень сведений, подлежащих засекречиванию на предприятии, различные инструкции и положения по обеспечению режима секретности составлялись на основании Общесоюзной инструкции № 0126-87, нормативных правовых актов министерств, а также Госкомиссии СССР и Главлита СССР.

Общая теория права включает корпоративные акты в число источников (форм) права в Российской Федерации и признает, что их действие имеет правовое значение<sup>1</sup>. Юридическим содержанием корпоративных актов являются правила, которые установлены самой организацией и имеют значение для ее внутренней деятельности (устав, учредительный договор, правила внутреннего трудового распорядка и др.).

В современной науке трудового права<sup>2</sup> сохранилось и раскрывается применительно к новым рыночным условиям понятие «локальные акты». Этот термин был вновь закреплён в действующем Трудовом кодексе РФ. В частности, ТК РФ относит акты локального нормотворчества, например коллективный договор, к числу источников трудового права, принимаемых в конкретной организации и действующих в ее пределах<sup>3</sup>.

Цивилистическая наука и ГК РФ, как справедливо замечает Н.В. Козлова, не предусматривают в числе источников гражданского права — локальные нормативные акты<sup>4</sup>. Обосновывая это положение ссылками на ГК РФ, автор пишет, что «...решение, принятое колле-

гиальным органом юридического лица, не может рассматриваться в качестве локального нормативного акта, являющегося источником права, но обладает признаками гражданско-правовой сделки, данная сделка есть акт реализации гражданской правосубъектности юридического лица»<sup>1</sup>.

В литературе высказана и иная точка зрения о правовой природе корпоративного акта. В частности, В.С. Ем обоснованно считает, что корпоративные акты занимают особое место в системе гражданско-правовых актов и являются необходимыми юридическими фактами в механизме возникновения, изменения или прекращения многих гражданских правоотношений<sup>2</sup>.

Признавая правомерность большинства выдвинутых учеными-правоведами суждений относительно правовой природы регулирующих корпоративных отношений, вместе с тем хотелось бы высказать некоторые соображения по поводу появления новых источников правового регулирования хозяйственной деятельности. Политический курс России на переход от плановой к рыночной экономике, конституционное признание и закрепление частной формы собственности, предоставление субъектам экономической свободы и возможности заниматься предпринимательством обусловили формирование новых общественных отношений, регулируемых частным правом. Эти отношения были законодательно урегулированы, что позволило отразить фактические изменения, происходившие в экономике. Важнейшими законодательными актами, принятыми в тот период Верховным Советом РСФСР, были законы «О собственности в РСФСР» (24 декабря 1990 г.) и «О предприятиях и предпринимательской деятельности» (25 декабря 1990 г.), утрагившие силу с 1 января 1995 г. в связи с введением в действие части первой ГК РФ. Названные законы и другие правовые акты закрепили процесс экономических преобразований в области собственности и предпринимательской деятельности. Появление новых хозяйствующих субъектов, правовой статус которых был окончательно закреплён в части первой ГК РФ, позволило им самостоятельно, без оглядки на государство регулировать хозяйственную деятельность на корпоративном уровне.

<sup>1</sup> См.: Козлова Н.В. Указ. соч. С. 382.

<sup>2</sup> Там же. С. 383.

<sup>1</sup> См.: Общая теория государства и права. Академический курс в 3-х томах / Отв. ред. проф. М.Н. Марченко. Т. 2. М., 2001. С. 248—249.

<sup>2</sup> См.: Куренной А.М. Трудовой договор: понятие, содержание и порядок заключения // Законодательство. 1997. № 1. С. 48; Российское трудовое право. М., 2004. С. 30—45.

<sup>3</sup> См.: Гейхман В.Л., Дмитриева И.К. Трудовое право. М., 2002. С. 44—45.

<sup>4</sup> См.: Козлова Н.В. Правосубъектность юридического лица. М., 2005. С. 381.



Основными источниками такого регулирования явились *корпоративные акты*, издаваемые организациями по различным направлениям их деятельности. Примечательным является тот факт, что сегодня любая организация, в зависимости от масштабов ее деятельности имеет собственную систему корпоративного регулирования, которая, по аналогии с правовым регулированием<sup>1</sup>, включает, *во-первых*, издание корпоративных актов, содержащих корпоративные нормы, регламентирующие отношения в хозяйственной деятельности, в том числе при обращении КЗИ. *Во-вторых*, правоотношения, возникающие между субъектами в процессе осуществления ими деятельности, связанной с использованием и охраной КЗИ, что находит отражение в фиксации их прав и обязанностей. *В-третьих*, речь идет о реализации прав и обязанностей субъектов, т.е. фактическом их поведении, с использованием различных способов корпоративного регулирования обращения КЗИ.

Формирование механизма корпоративного регулирования обращения КЗИ представляет собой сложный процесс учета факторов воздействия внешней среды на хозяйственную деятельность, и выработки в этой связи адекватных мер противодействия угрозам. При этом существенное значение имеет правильный выбор актов корпоративного права, использование которых позволит эффективно регулировать отношения, возникающие при обращении КЗИ. Речь идет о возможности использования обычаев, деловых обыкновений, прецедентов и корпоративных актов, выражающих содержание, прежде всего, общедозволительного метода регулирования.

Использование *обычаев делового оборота* (ст. 5 ГК РФ) в предпринимательской деятельности, включая и охрану КЗИ, система которых, в отличие от Запада, еще не полностью сложилась в России, возможно при наличии устоявшихся и широко применяемых в этой сфере правил поведения, не предусмотренных законодательством. В данном случае можно говорить о действии правил по поддержанию необходимого уровня бдительности работников и их ответственности за порученный участок работы с КЗИ. Эти правила, имевшие в советское время «идеологическую начинку», многим хорошо известны, особенно старшему поколению. Они сложились и имели широкое применение, прежде всего, в оборонных отраслях промышленности.

<sup>1</sup> См.: Общая теория государства и права. Т. 3. С. 94–95.

В настоящее время эти правила приобрели совершенно другое значение и используются в организациях для поддержания фирменного имиджа и охраны коммерческих секретов. Особенно их действие проявляется в крупных, ныне акционированных организациях, созданных еще в советский период. В трудовых коллективах этих организаций сохранилась в силу традиций обстановка ответственного отношения работников к выполнению своих обязанностей по защите охраняемой информации, что имеет важное воспитательное значение для вновь поступивших на работу лиц, а также реализации функции предупреждения разглашения (утечки) КЗИ.

Обычаи делового оборота, связанные с сохранением КЗИ, получают все большее распространение в российской коммерческой практике. Речь идет о соблюдении определенных правил поведения при деловых контактах с конкурентами, когда работники фирмы не имеют права обсуждать цены, условия продажи, расходы, производственные планы и другую КЗИ. При рекламировании качества продукции своей фирмы нельзя отрицательно отзываться о конкурентах и производимых ими изделиях, даже при наличии достоверной информации об этом. Нельзя также упоминать о трудностях конкурентов, связанных с проблемами производства, обслуживания, финансовых затруднениях, а также о наличии судебных тяжб. Конечно, такое цивилизованное поведение в деловых отношениях является пока скорее исключением, чем правилом для российских фирм. Переговоры с покупателями по вопросу о ценовой политике ведутся с соблюдением сложившихся и получивших распространение в коммерческой деятельности правил делового оборота, когда фирма не обязана предоставлять всем покупателям одинаковые цены и равные условия продажи. Различия в ценах допускаются при разном количестве продаваемых изделий. Фирма также не обменивается прогнозами о будущих предельных, т.е. самых высоких и самых низких, ценах на товар. Такая информация в силу установившихся правил поведения в предпринимательской среде представляет коммерческую значимость для организации-продавца, и, естественно, не подлежит разглашению.

ГК РФ содержит ряд статей, имеющих отсылки о возможности использования обычаев делового оборота (ст. 474, 478, 508, 510, 513 и др.). Речь может идти об устоявшейся практике прохождения поставщиками, с которыми фирма уже имеет деловые отношения, дополнительной проверки при передаче им заказов на новые комплектующие узлы, материалы или сервисное обслуживание. Проверка

проводится на основании информации о поставщиках, которая характеризует их отношение к выполнению своих договорных обязательств с данной фирмой. При этом устанавливается соответствие спецификации параметрам качества и надежности, определяется возможность стабильности поставок качественных изделий. Поставщики могут получить новые заказы в том случае, когда качество их товаров и услуг отвечает требованиям фирмы, а цена не выше, чем у других поставщиков. При необходимости решается вопрос о заключении с добросовестными в хозяйственном отношении поставщиками долгосрочных договоров, стимулировании их деятельности, связанной с расширением производства, номенклатуры изделий и повышении качества товаров.

В хозяйственной деятельности используются правила, прочно вошедшие в повседневную практику регулирования сферы обращения КЗИ и получившие в литературе название «*деловых обыкновений*». На многих фирмах действует порядок, в соответствии с которым запрашивается совмещение трудовой деятельности на конкурирующей фирме. Работа по совместительству у покупателей или поставщиков фирмы возможна только с письменного разрешения руководства организации. Работник не имеет права продавать изделия, лично им изготовленные или взятые на реализацию, если аналогичные товары предлагаются к продаже фирмой, с которой у него имеется трудовой договор. Он не должен оказывать помощь конкурентам в продаже изделий, например, по более низким ценам, а также содействовать улучшению работы конкурирующих фирм. Другими словами, работники не должны извлекать собственную коммерческую выгоду из деловых контактов, если они противоречат интересам фирмы.

Деятельность, связанная с охраной конфиденциальности информации, требует принятия организацией различного рода решений. Отдельные решения могут служить в будущем образцом для разрешения вновь возникающих аналогичных дел. Примерами *прецедента на корпоративном уровне в сфере обращения КЗИ* могут быть решения, принятые однажды общим собранием в отношении одного из учредителей или администрации к работнику, разгласившим сведения, составляющие КЗИ. В первом случае собрание может принять решение, в соответствии с которым учредитель теряет право на получение части своей прибыли, если иное не предусмотрено законом и учредительными документами. Во втором случае работник, разгласивший КЗИ, помимо возможного привлечения его по усмотрению администрации к юридической ответственности, не может в буду-

щем претендовать на занятие руководящей должности в данной организации. Если последующие аналогичные случаи, возникающие в организации, разрешаются таким же образом, то можно говорить, что имеет место корпоративный прецедент, хотя к его оценке следует подходить с большой степенью осторожности и учитывать действие внутренних факторов в организации (смена собственника, руководителем органов управления обществом и др.).

Основным источником корпоративного права, используемого организациями в сфере обращения КЗИ, является *корпоративный нормативный акт*, которому присущи общие признаки. Он имеет правовореческий характер, издается по усмотрению органа управления в пределах его компетенции, в письменной форме, его содержание не должно противоречить законодательству и иным нормативно-правовым актам.

Корпоративные акты, издаваемые в этой сфере, не только воплощают имеющиеся пробелы в Законе о коммерческой тайне, но и конкретизируют правовые нормы применительно к воздействию факторов внешней среды на хозяйственную деятельность, в рамках которой происходит процесс получения, использования, передачи и защиты КЗИ. Акты дополняют и расширяют диапазон действия правовых норм и тем самым формируют механизм регулирования обращения КЗИ. Однако в Законе не указана процедура принятия корпоративных актов в данной сфере. Поэтому применяются общие нормы ГК РФ, определяющие правосубъектность юридического лица и компетентность его органов управления. Из смысла Закона нетрудно понять, что первоочередными объектами корпоративного регулирования являются: установление режима коммерческой тайны и обеспечение в целом безопасности организации. В Законе установлены пределы корпоративного регулирования, в частности, перечисляются сведения, которые организация не вправе включать в свой перечень сведений, составляющих коммерческую тайну (ст. 5 Закона).

*Анализ корпоративных актов, действующих в сфере обращения КЗИ, показывает, что они существенно образом отличаются от аналогичных актов советского периода по направленности (целям) регулирования и юридическому содержанию.* Формирование локальных актов по вопросам защиты государственных секретов осуществлялось при строжайшем соблюдении интересов государства. В этих целях была установлена обязательная процедура их согласования с министерством и органом КГБ. Мнение предприятий не всегда учитывалось, трудовому коллективу навязывалось «сверху» определенное

поведение в сфере обеспечения режима секретности. Содержание локальных актов того периода было обусловлено рамками разрешенного поведения со стороны государства. Общесоюзной инструкцией № 0126 и ведомственными актами устанавливался алгоритм обязательных действий предприятия в сфере защиты информации. Реализация правовых норм по вопросам защиты государственной тайны предполагала безусловное соблюдение их в неизменном виде и допускала лишь некоторую конкретизацию мер по обеспечению режима секретности применительно к специфике производственной деятельности предприятия. Собственных санкций за нарушения требований по обеспечению режима секретности предприятия не использовали, что, впрочем, соответствовало общему положению дел в области локального регулирования того периода<sup>1</sup>. Предприятия лишь воспроизводили в своих актах (приказы, положения, инструкции и др.) санкции об ответственности за нарушения требований режима секретности, установленные общесоюзным законодательством, постановлениями Правительства СССР, нормативно-правовыми актами министерств.

*По юридическому содержанию действующие сегодня корпоративные акты являются в основном регулятивными.* Корпоративные нормы в этой области устанавливают режим коммерческой тайны и определяют поведение администрации и работников по поводу использования, передачи и защиты КЗИ. Эти нормы постепенно обособились в отдельную группу. Наряду с акционерными, финансовыми, трудовыми и иными нормами они регулируют одно из важных направлений деятельности организации, связанное с обеспечением ее информационной безопасности. Корпоративные нормы в этой сфере являются регулятором не только внутренних процессов обращения КЗИ и в этой связи являются обязательными для работников и работодателей, но и регулируют их взаимоотношения с внешней средой. В литературе содержатся предложения по принятию коммерческими структурами кодекса корпоративного поведения. Реализация этого предложения с участием представителей не только крупного, но и среднего бизнеса способствовала бы поддержанию элементарного порядка по соблюдению этических норм в сфере бизнеса и защите прав на КЗИ. Решение названной задачи требует значительных

<sup>1</sup> См.: *Смирнов В. Н.* Внутренний трудовой распорядок на предприятии. Ленинград, 1980. С. 40–47, и др.

организационных усилий участников, объединенных единой целью добросовестного ведения бизнеса.

В корпоративных актах указываются санкции, установленные и обеспеченные мерами государственного принуждения, и процедура привлечения лиц к ответственности. Это может быть указание о порядке проведения служебного расследования по факту разглашения сведений, составляющих коммерческую тайну, и об обращении по его результатам с заявлением в правоохранительные органы с просьбой о возбуждении уголовного дела. Организации могут ввести меры поощрения за труд, связанный с сохранением КЗИ. В актах предусматриваются основания предоставления работникам различных льгот, надбавок к заработной плате, например, в процентном отношении к должностному окладу за секретность. Для этих целей используются и иные формы материального стимулирования, которые применяются за счет прибыли организации. Однако они не вправе устанавливать какие-то новые, дополнительные санкции за совершение правонарушений в сфере охраны КЗИ, поскольку это является прерогативой государства. Закон о коммерческой тайне (ст. 14 и 15) устанавливает возможность привлечения лиц к дисциплинарной, гражданско-правовой, административной и уголовной ответственности за совершение правонарушений в сфере обращения КЗИ, которая применяется в соответствии с действующим законодательством.

Механизм права организаций на КЗИ формируется на основе концепции общих дозволений и запретов<sup>1</sup>, содержащихся в нормах законодательства, и конкретных дозволений, запретов и позитивных обязываний, установленных Законом о коммерческой тайне, иных нормативно-правовыми актами, регулирующими процесс обращения КЗИ. Их соотношение позволяет определить преимущество определенных способы правового регулирования, характерные для обращения КЗИ. В этой связи необходимо подчеркнуть, что общедозволительный метод регулирования, свойственный гражданскому праву, имеет исходное и направляющее правовое воздействие применительно к сфере регулирования обращения КЗИ. Это объясняется тем, что информация в виде информационных ресурсов участвует в гражданском обороте с присущими ей особенностями при совершении ак-

<sup>1</sup> См.: *Алексеев С. С.* Общие дозволения и общие запреты в советском праве. М., 1989. С. 8–102.

тов купли-продажи.оборот КЗИ напрямую связан с частными интересами организации. Их реализация при занятии бизнесом требует от организаций надежного обеспечения их безопасности. Кроме дозволительных норм регулирование обращения КЗИ обеспечивается с помощью императивных обязывающих и запрещающих норм. В частности, права на доступ к КЗИ, которые предоставляет администрация в разрешительном порядке своим работникам, другим лицам, построены на конкретных обязывающих и запретах, содержащихся в различных корпоративных актах.

Закон о коммерческой тайне предоставляет организациям право на отнесение сведений о различных сторонах их хозяйственной деятельности к информации, составляющей коммерческую тайну (ст. 4). Фактическая монополия организации на такую информацию возможна при соблюдении определенной процедуры, связанной с установлением режима коммерческой тайны. В ст. 10 Закона перечислены основные меры, которые должны быть предприняты по охране конфиденциальности информации. Формально право организации на КЗИ фиксируется в ее учредительных документах, и в этом нет противоречия правовым нормам, определяющим право собственности коммерческих организаций. Таким способом организация публично уведомляет других лиц о возможности обладания и использования в своей деятельности КЗИ, охраняемой в режиме «коммерческая тайна».

В учредительном договоре и (или) уставе определяется орган управления или должностное положение лица, которые правомочны определять состав и объем сведений, составляющих КЗИ, устанавливать соответствующие режимы, обеспечивающие конфиденциальность ее охраны, осуществлять в необходимых случаях защиту права организации на КЗИ. Включение в учредительные документы основополагающих положений по использованию и защите КЗИ позволяет организации осуществлять регулирование взаимоотношений с учредителями и контрагентами, финансирование подразделений, обеспечивающих безопасность, научно-методическое, организационное и правовое обеспечение порядка установления и реализации мер режима коммерческой тайны; предупреждение возникновения каналов утечки КЗИ.

*Субъективное право организации на КЗИ* образуют три возможных правомочия: право требования исполнения или соблюдения юридической обязанности от работников и других лиц, право на совершение собственных активных действий, имеющих юридическое зна-

чение и право на защиту субъективных гражданских прав в связи с их нарушением<sup>1</sup>. Названные правомочия в различных комбинациях в зависимости от области регулирования отдельных направлений и участков, где сосредоточены коммерческие секреты, находят свое выражение в конкретных по названию и назначению корпоративных актах.

Важнейшими из них являются *акты общего характера*, регулирующие управленческие и финансовые вопросы. К ним относятся учредительные документы, коллективный договор, правила внутреннего трудового распорядка, а также положения о фондах и резервах, об организации отчетности, о правовом статусе совета директоров, правлении, генеральном директоре, структурном подразделении, об оплате труда, о порядке заключения и исполнения договоров и другие, в которых содержатся ряд прав и обязанностей, определяющих поведение лиц при обращении КЗИ.

Предметно и конкретно вопросы охраны конфиденциальности КЗИ закрепляются в *специальных корпоративных актах*, таких как: перечень сведений, составляющих коммерческую тайну, инструкция по обеспечению сохранности коммерческой тайны, положение о разрешительной системе и ряд других. В литературе были высказаны различные предложения по структуре и содержанию названных выше актов. Их анализ содержится в этой и других главах книги.

Таким образом, корпоративное регулирование обращения КЗИ отражает общую концепцию воздействия норм корпоративного права на процесс управления организацией и ее имуществом и создает необходимые предпосылки для обеспечения охраны конфиденциальности информации в рамках трудовых и гражданско-правовых отношений. Корпоративное регулирование в сфере обращения КЗИ, выполняет, на наш взгляд, *регулятивную* (устанавливает и уточняет взаимные субъективные права и юридические обязанности по поводу КЗИ), *конкретизирующую* (оперативно, применительно к конкретной ситуации, сложившейся в сфере обращения КЗИ, уточняет общие положения Закона о коммерческой тайне), *правовосполнительную* (по необходимости и усмотрению организации осуществляет регулирование отношений по поводу КЗИ, которые не охвачены нормами законодательства) функции. Реализация названных функций позволяет организациям значительно расширить границы

<sup>1</sup> См.: Грибанов В.П. Осуществление и защита гражданских прав. 2-е изд. М., 2001. С. 104–108, и др.

гражданско-правового регулирования и охраны КЗИ с использованием корпоративных актов и иных правовых средств.

## **§ 2. Роль норм трудового права в регулировании обращения коммерчески значимой информации**

*Сущность проявления трудовых отношений в механизме корпоративного регулирования использования и охраны КЗИ.* В системе правовых средств, используемых коммерческими организациями в сфере обращения КЗИ, важное место занимают нормы трудового права. Однако их наличие вовсе не означает их всеобщность, обязательное и прямое действие при регулировании трудовых отношений по поводу использования и защиты КЗИ. Для этого в организациях формируется и действует определенный механизм корпоративного регулирования отношений в сфере обращения КЗИ. Регламентация трудовых отношений по поводу КЗИ нормами трудового права в рамках одной организации образует определенный порядок, который является составной частью механизма корпоративного регулирования отношений в этой сфере. В данном случае, понятие «порядок» в числе важнейших признаков включает не только правила внутреннего трудового распорядка, но и иные нормы корпоративного права, специально устанавливаемые для регулирования обращения КЗИ.

Механизм приводится в действие путем закрепления в трудовом договоре на основе норм трудового и корпоративного права конкретных прав и обязанностей работодателя и работника. Его функционирование обеспечивается фактическим поведением сторон на тех участках хозяйственной деятельности, где обращается КЗИ.

Трудовой кодекс Российской Федерации (ТК РФ)<sup>1</sup> юридически закрепил возможность для работодателя осуществлять по соглашению с работником правовую защиту КЗИ путем включения в трудовой договор дополнительных (факультативных) условий. Практика включения в трудовой договор (контракт) дополнительных условий о неразглашении коммерческих секретов была заимствована отечественными предпринимателями у зарубежных инвесторов в конце 80-х гг. XX в. В этот период на территории СССР шел интенсивный

<sup>1</sup> См.: Собрание законодательства РФ. 2002. № 1(1). Ст. 3.

процесс создания совместных с иностранными фирмами предприятий. Зарубежные фирмы уделяли серьезное внимание защите своих технологий, внедряемых в производство. Наша страна была вынуждена принять ряд правовых актов, регулирующих правовой статус совместных хозяйственных организаций, имевший определенные особенности, что позволило им надежно сохранять коммерческие секреты. Правовые акты того периода, регулировавшие деятельность совместных предприятий<sup>1</sup>, содержали нормы о защите конфиденциальной информации, которые находили отражение в корпоративных актах, в том числе коллективных договорах, на основании которых стороны включали соответствующие условия в трудовые договоры.

Правовая база регулирования трудовых отношений в сфере обращения КЗИ, первоначально созданная для нужд совместных предприятий, долгое время использовалась и иными хозяйствующими субъектами. В КЗоТ соответствующие изменения были внесены Законом РФ от 6 мая 1998 г. № 69-ФЗ<sup>2</sup> «О внесении изменений и дополнений в статью 15 КЗоТ РФ», который утратил силу с введением нового ТК РФ. Закон предусматривал возможность включения в трудовой договор условия о неразглашении работником сведений, составляющих коммерческую тайну. Норма, регулировавшая трудовые отношения в этой сфере, была включена в трудовое законодательство в силу назревшей объективной необходимости.

В рыночных условиях защита частных интересов собственника работодателя и соблюдение при этом личных интересов работников наемного труда по поводу сохранности КЗИ отражается на производственном процессе и получении прибыли. Законодатель при включении этой нормы в КЗоТ учитывал существующую на предприятиях в этой сфере развитую систему локального нормотворчества. Вместе с тем вопросы, имевшие практическое значение для предприятий в тот период, не были решены на законодательном уровне. При этом такая ситуация сохранялась вплоть до принятия нового ТК РФ. Речь идет о привлечении работников к дисциплинарной и материальной ответственности, включая и их увольнение по инициативе администрации за нарушения требований сохранности КЗИ, поскольку эти

<sup>1</sup> См.: Постановление Верховного Совета РСФСР от 22 февраля 1991 г. № 684-1 «О соглашениях российских организаций с иностранными фирмами» // Ведомости Съезда народных депутатов РСФСР и Верховного Совета РСФСР. 1991. № 9. Ст. 199.

<sup>2</sup> См.: Собрание законодательства РФ. 1998. № 12. Ст. 1382.

вопросы требовали законодательного регулирования и не могли решаться на корпоративном уровне.

Закрепление диспозитивной нормы в ТК РФ (ч. 3 ст. 57), установившей возможность включения в трудовой договор условия о защите КЗИ, изменило прежнюю ситуацию, когда регулирование осуществлялось только на основании корпоративных актов. ТК РФ предусматривает основание для увольнения работника за разглашение коммерческой тайны, ставшей ему известной в связи с исполнением трудовых обязанностей (подп. «в» п. 6 ст. 81). Сложившийся в течение ряда лет субъективный корпоративный подход организаций по поводу использования и охраны КЗИ в рамках трудовых отношений получил свое законодательное закрепление, что соответствует принципам трудового права<sup>1</sup> в условиях рыночной экономики и открывает новые возможности для защиты частных интересов.

Трудовые правоотношения, возникающие между работодателем и работниками по поводу КЗИ, характеризуются общими признаками, которые достаточно полно раскрыты в теории трудового права. Вместе с тем они имеют определенную специфику. С трудовыми правоотношениями непосредственно связаны и иные отношения, получившие в теории трудового права название «производных» (от трудовых) или «непосредственно связанных» с ними. В зависимости от времени возникновения «производных» отношений от трудовых И.К. Дмитриева выделяет три группы отношений: «предшествующие, сопутствующие и вытекающие из трудовых»<sup>2</sup>, которые анализируются применительно к целям настоящего исследования.

*Во-первых*, это отношения, связанные с проверкой лиц, вновь поступающих на работу, и оформлением им допуска к КЗИ. Эти отношения непосредственно связаны с трудовыми правоотношениями и по времени предшествуют им. Как отмечает И.К. Дмитриева: «Предшествующие отношения появляются до трудовых, а прекращаются с их возникновением»<sup>3</sup>. Данное суждение в первой части предложения с учетом целей настоящего исследования не вызывает возражений, но вторая его часть нуждается, по нашему мнению, в определенной конкретизации применительно к рассматриваемой нами сфере. Дело

в том, что отношения, возникшие между работодателем и работником в связи с оформлением допуска к КЗИ, в последующем не прекращаются. Администрация после оформления допуска и издания приказа о назначении лица на должность продолжает вести проверку вновь поступающих на работника данных в процессе его трудовой деятельности. По результатам последующей проверки руководством организации может быть принято решение об аннулировании допуска и прекращении трудовых отношений.

*Во-вторых*, «сопутствующие правоотношения» по поводу КЗИ возникают и существуют вместе с трудовыми отношениями, обеспечивая эффективное использование такого рода информации, содержащейся в документах и изделиях, а также охрану ее конфиденциальности. К их числу следует отнести условия трудового договора, связанные с охраной конфиденциальности КЗИ, осуществлением контроля за выполнением работниками требований по обеспечению информационной безопасности на конкретном участке работы, и другие отношения.

*В-третьих*, это правоотношения, вытекающие из трудовых, которые могут возникнуть при нарушении сторонами условий трудового договора в части охраны КЗИ, выразившемся в возможном причинении ущерба и применением в этой связи мер юридической ответственности.

Названные выше «производные», непосредственно связанные с трудовыми, отношения, возникающие между работодателем и работником по поводу КЗИ, являются важнейшей частью механизма корпоративного регулирования обращения КЗИ и обеспечивают его функционирование благодаря усилиям администрации и работников, права, обязанности и ответственность которых в сфере обращения КЗИ непосредственно закреплены в коллективном договоре, правилах внутреннего трудового распорядка, иных корпоративных актах и в трудовых договорах. Факультативный характер применения норм трудового права в рассматриваемой сфере определяет их роль в механизме правового регулирования обращения КЗИ и охраны ее конфиденциальности, которая может быть обозначена совокупностью следующих признаков:

- 1) определяющих сущность трудовых отношений в механизме корпоративного регулирования обращения и охраны КЗИ;
- 2) раскрывающих формы и методы использования правовых средств при проведении проверочных мероприятий в отношении принимаемых на работу лиц, допускаемых к КЗИ, а также в процессе их трудовой деятельности;

<sup>1</sup> См.: Гейхман В.Л., Дмитриева И.К. Трудовое право: Учебник. М., 2002. С. 30–39, и др.

<sup>2</sup> См.: Гейхман В.Л., Дмитриева И.К. Указ. соч. С. 53, 54.

<sup>3</sup> Там же. С. 54.

- 3) характеризующих содержание корпоративного регулирования допуска и доступа лиц к КЗИ;
- 4) объясняющих особенности формирования условий по охране конфиденциальности КЗИ, включаемых в трудовой договор, и определения прав и обязанностей работодателя и работника при обращении КЗИ.

Результаты проведенного исследования подтверждают наличие проблемы использования форм, методов и процедур в рамках трудового права, решение которых напрямую связано с функционированием механизма корпоративного регулирования обращения КЗИ. Первоочередного решения требуют вопросы, которые позволяют судить о законности действий администрации при проведении проверочных мероприятий в отношении лиц, поступающих на работу, и в процессе их трудовой деятельности в коммерческой организации; о правовых средствах, используемых для сбора и проверки данных на лиц, поступающих на работу, и в процессе их трудовой деятельности, связанной с КЗИ; о содержании корпоративных актов, определяющих порядок допуска и доступа лиц к КЗИ; о правовой природе взаимоотношений между администрацией и гражданином, представившим необходимые документы при приеме на работу в период, предшествующий оформлению ему допуска к КЗИ; о правомерности отказа гражданину в приеме на работу; о согласовании условий по охране конфиденциальности информации в трудовом договоре и определении прав и обязанностей работодателя и работника в корпоративных актах.

**Формы и методы проверки лиц, допускаемых к КЗИ.** Соблюдение коммерческими организациями законности при проведении *проверочных мероприятий* в отношении лиц, поступающих на работу, деятельность которых будет связана с использованием КЗИ, является весьма острой проблемой, затрагивающей частную жизнь граждан. В нашей стране действует система правовых норм, обеспечивающих неприкосновенность частной жизни граждан. К их числу относятся нормы: Конституции РФ (ст. 21, 23, 24, 51, 53), Гражданского кодекса РФ (ст. 150, 151, 152, 1069, 1070) и иных правовых актов.

При проведении проверочных мероприятий администрация обязана руководствоваться нормами Конституции РФ, запрещающими произвольное вмешательство в частную жизнь (ст. 22, 23). Сбор, хранение, использование и распространение информации о частной жизни граждан разрешается только с их согласия (ст. 24). Ограничение прав граждан на неприкосновенность их частной жизни допу-

скается на основании судебного решения. Речь идет о праве граждан на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений (ст. 23).

Конституция РФ содержит конкретные основания для вмешательства в частную жизнь граждан. Это связано с необходимостью защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства или чрезвычайного положения (ст. 23, 55, 56), что в полной мере соответствует международным нормам о защите прав и свобод человека и гражданина.

*Административной организацией* на основании Конституции РФ, ТК РФ, законов «Об оперативно-розыскной деятельности», «О частной детективной и охранной деятельности» и иных правовых актов *используются различные правовые средства для сбора и проверки данных на лиц, допускаемых к КЗИ. Сбор и проверка данных, характеризующих личность, осуществляется на начальном этапе приема лиц на работу и в течение всей последующей их трудовой деятельности, при условии, что их работа связана с КЗИ.*

Можно говорить в этой связи о двух самостоятельных, но вместе с тем тесно связанных между собой *этапах проверки*, имеющих свои особенности в плане использования форм, методов и приемов сбора, оценки личностных данных. На практике в зависимости от будущего должностного положения лица и совокупности КЗИ, передаваемой ему для выполнения обязанностей, условно выделяют *поверхностный (простой) и глубокий (сложный) уровни (этапы) проверки*. Названные этапы проверки различаются по глубине и объему проводимых проверочных мероприятий. Под глубиной проверки данных кандидата на работу за соответствующий период его деятельности. Например, подтверждение личностных данных за последние 5–10 лет, начиная с 18-летнего возраста. Объем проверочных мероприятий также может быть различным с точки зрения совокупности использования форм, методов и приемов проверки.

*Первый этап, получивший название «поверхностный» уровень проверки, осуществляется преимущественно работниками отдела кадров и службы безопасности организации в отношении лиц, поступающих на работу, связанную с использованием КЗИ.* Такой уровень проверки предполагает получение информации от лица, претендующего на занятие конкретной должности и представившего в этой связи необходимые документы в отдел кадров. При приеме на работу с канди-

датом проводится собеседование, в процессе которого работник отдела кадров выясняет интересующие его вопросы, касающиеся его жизнедеятельности. В частности, уточняются паспортные данные, дата и место рождения, гражданство, адрес регистрации проверяемого лица, фактическое место проживания, образование, семейное положение; наличие собственности (квартира, земельный участок, дачные постройки, автотранспорт и т.д.), возможная судимость и ряд других.

Сбор информации осуществляется с помощью методов анкетирования, тестирования, изучения представленных кандидатов на работу документов, рекомендаций и резюме. Вопросы, включаемые в анкету, касаются различных аспектов жизнедеятельности кандидата на работу. Используется тестирование для получения дополнительных данных. Изучение документов предполагает установление их подлинности и достоверности сделанных в них записей. Это касаются документов, представляемых кандидатом на работу в обязательном порядке: паспорт, трудовая книжка, диплом о высшем (среднем) профессиональном образовании.

Способ визуального осмотра документов, применяемый работниками отделов кадров, не всегда позволяет выявить, например, подделку фотографии в паспорте, подделку и искажение записей в трудовой книжке или дипломе об образовании. При наличии сомнений в подлинности документов администрация может на коммерческой основе обратиться за помощью в экспертные учреждения министерства юстиции или внутренних дел, используя при этом свои личные связи, поскольку разрешение этих вопросов не регламентировано законом.

При устройстве на работу многие кандидаты представляют различные письменные рекомендации в виде характеристик, которые не носят правового характера, но подтверждают эффективность прежней трудовой деятельности. Информация, содержащаяся в таких документах, носит в основном объективный характер, но при ее оценке доминирует субъективный корпоративный подход нового работодателя. Что касается представляемых кандидатом резюме, то в них содержится информация субъективного характера, которая рассчитана на то, чтобы вызвать профессиональный интерес у будущего работодателя. Поэтому такая информация требует тщательной проверки.

Названные обстоятельства следует учитывать администрации при формировании мнения о профессиональном и психологическом облике кандидата, претендующего на занятие конкретной должно-

сти. Таким образом, проверка информации, полученной от кандидата на работу, и его документов ведется по трем основным направлениям: 1) уточнение достоверности информации, сообщенной лицом в письменной и устной форме; 2) подтверждение подлинности документов, предоставляемых лицом при приеме на работу; 3) выявление обстоятельств, препятствующих приему лица на работу, связанную с использованием КЗИ.

*Второй этап характеризуется более «глубоким» уровнем проверки. На данном этапе проверки предполагается возможное использование сил и средств внешних организаций, и, прежде всего, правоохранительных и иных государственных органов, располагающих необходимой информацией о проверяемом лице.*

Практическое решение этой задачи представляет значительную трудность. Порядок взаимодействия коммерческих организаций с государственными органами по этому вопросу Законом о коммерческой тайне и иными правовыми актами не урегулирован. Поэтому работники служб безопасности организаций для получения информации их информации часто прибегают к помощи сотрудников органов Министерства внутренних дел (МВД) РФ и Федеральной службы безопасности (ФСБ) РФ на доверительной основе, используя в этих целях свои старые профессиональные связи.

Более тщательной проверке подвергаются лица, претендующие на занятие руководящих постов и допускаемые в этой связи к наиболее ценной коммерческой информации. Периодически проверке подвергаются работники, связанные в процессе своей трудовой деятельности с КЗИ. Необходимость проведения такой проверки объясняется тем, что в жизни любого работника происходят события, которые впоследствии могут оказать влияние на его отношение к исполнению трудовых обязанностей, в том числе и по сохранению КЗИ. Поэтому задача администрации состоит в выявлении такого рода ситуаций, имеющих связь с возникновением угроз для нормального функционирования организации.

В процессе проведения проверки используются «независимые» источники. Это могут быть осведомители (агентура, доверенные лица), подобранные службой безопасности организации из числа ее работников, а также скрытое наблюдение, включая систему видеонаблюдения. Применяются и иные приемы проверки, порой нарушающие требования Конституции РФ, например, прослушивание служебных телефонных переговоров, ведущихся в сети предприятия.



Использование названных выше сил и средств позволяет администрации фиксировать поведение работников, отклоняющееся от установленных корпоративных норм, регулирующих порядок использования и защиты КЗИ, устанавливать дополнительный режим КЗИ и, таким образом, заблаговременно предупреждать правонарушения в этой сфере.

Причем проверка ведется целенаправленно с учетом имеющихся данных на работника. Речь идет о выяснении источников дохода и связанного с ним материального положения и жилищных условий кандидата на работу, о причинах увольнения с предыдущих мест работы, включая возможные обвинения в некомпетентности, о возможных конфликтных ситуациях, имевших место в предшествующий период жизнедеятельности, в том числе и в период занятия индивидуальным предпринимательством, о привлечении лица в качестве истца или ответчика и другие.

Оцениваются имевшие место события в личной жизни проверяемого лица. Известно, что негативные факты аморального поведения лица, граничащие порой с правонарушениями (злоупотребление алкогольными напитками, эмоциональная неустойчивость, психические отклонения и др.), могут быть использованы конкурентами в своих интересах путем оказания на него выгодного влияния.

Анализ деятельности ряда организаций показывает, что наряду с традиционными гласными формами проверки службы безопасности порой используют и негласные методы. Причем в зависимости от целей проверки негласные формы могут использоваться как на первом, так и на втором ее этапе. При использовании негласных методов проверки администрация обязана учитывать существующие законодательные ограничения в этой сфере деятельности. Федеральный закон «Об оперативно-розыскной деятельности» от 12 августа 1995 г.<sup>1</sup> устанавливает исчерпывающий перечень государственных органов, которые могут осуществлять оперативно-розыскные мероприятия, иметь оперативно-технические силы и использовать различные средства, в том числе и для негласного получения информации.

На основании судебного решения органам ФСБ и МВД предоставлено право осуществлять контроль почтовых отправлений; про-

слушивание телефонных переговоров с подключением к стационарной аппаратуре организаций, независимо от их форм собственности; негласное снятие информации с технических каналов связи и проведение иных мероприятий с использованием тайных осведомителей (агентуры и доверенных лиц).

Коммерческие организации и их службы безопасности такими полномочиями законом не наделены. Закон прямо запрещает им проведение оперативно-розыскных мероприятий с использованием технических и иных средств негласного получения информации. Несмотря на существующий запрет, многие крупные организации под видом защиты своих прав на коммерческую тайну устанавливают специальное оборудование цифровых АТС, позволяющих вести в автоматическом режиме запись разговоров работников по телефону (не только служебного, но личного характера); ведут с помощью видеосъемки наблюдение за поведением персонала не только на рабочих местах, например, при работе с документами или изделиями, содержащими коммерческую тайну, но и в местах, предназначенных для кратковременного отдыха работников внутри организации, а также осуществляют иные мероприятия, относящиеся по своему содержанию к числу оперативно-розыскных. Такие действия могут свидетельствовать о попытках грубого вмешательства администрации в частную жизнь работников и должны быть предметом проверки со стороны органов прокуратуры.

**Корпоративное регулирование порядка допуска и доступа лиц к КЗИ.**  
Анализ материалов деятельности организаций по охране конфиденциальности информации показывает, что в большинстве из них действуют специальные корпоративные акты, определяющие порядок и процедуру допуска и доступа лиц к КЗИ. В крупных и средних организациях, имеющих дочерние общества, представительства и филиалы, наибольшую распространенность получили акты, именуемые как «Номенклатура должностей работников, допускаемых к работам, документам и изделям, содержащим коммерческую тайну» (далее — номенклатура). На малых предприятиях чаще всего вместо номенклатуры составляется список работников, допущенных к таким сведениям.

Номенклатура представляет собой документ внутреннего пользования с расшифровкой подразделений организации и указанием должностей работников, которым необходим допуск к соответствующим категориям (разрядам) сведений, составляющих коммерческую тайну. В этом документе содержится правовое обоснование

<sup>1</sup> См.: Собрание законодательства РФ. 1995. № 33. Ст. 3349; 1997. № 29. Ст. 3502; 1998. № 30. Ст. 3613; 1999. № 2. Ст. 233; 2000. № 1 (ч. 1). Ст. 8; 2001. № 13. Ст. 1140; 2003. № 2. Ст. 167.

допуска лиц, занимающих определенные должности, к соответствующим категориям сведений, составляющих коммерческую тайну. Номенклатура разрабатывается службой безопасности совместно с руководителями подразделений и утверждается руководителем организации. Основанием для разработки номенклатуры является структура управления организацией, ее штатное расписание, положение о подразделениях, должностные инструкции и перечень сведений, составляющих коммерческую тайну. В положении о порядке допуска лиц к сведениям, составляющим коммерческую тайну (далее — положение), содержится требование о том, что работники, должности которых включены в номенклатуру, могут быть назначены на эти должности только после оформления им допуска к КЗИ.

В данном случае требование корпоративных норм не согласуется с нормами трудового законодательства, не предусматривающего соблюдение такой процедуры при приеме граждан на работу. При этом следует учитывать то обстоятельство, что проверка лиц порой проводится продолжительное время, которое никак не регламентируется, даже корпоративными актами.

Администрация в течение всего периода проверки находится, образно говоря, «в двойственном положении». С одной стороны, у нее нет оснований для отказа лицу в приеме на работу, а с другой, она не может заключить с ним трудовой договор и издать приказ о приеме на работу до получения результатов проверки. Фактически администрация в период проведения проверки нарушает трудовое законодательство, запрещаящее истребование от лиц, поступающих на работу, других документов, помимо перечисленных в ст. 65 ТК РФ.

Нарушение проявляется в том, что, во-первых, при заключении трудовых договоров иные требования к лицам, поступающим на работу в коммерческие организации, не могут быть предъявлены со стороны администрации (ч. 3 ст. 67 ТК РФ), кроме государственных и муниципальных унитарных предприятий. Речь идет о требованиях, предъявляемых к лицам, оформляемым на допуск к КЗИ. Во-вторых, администрация снимает копии с документов, предъявляемых лицом при заключении трудового договора, в которых содержатся персональные данные работника, и без письменного его согласия, в нарушение требований ст. 88 ТК РФ, передает сведения третьей стороне для проведения проверки. Это происходит потому, что трудовое законодательство не предусматривает обязанности администрации заключить в определенный срок трудовой договор после передачи лицом документов, перечисленных в ст. 65 ТК РФ.

В ТК РФ отсутствуют гарантии соблюдения прав лица (ст. 64) в преддоговорный период установления трудовых отношений, когда администрацией проводится проверка его персональных данных. В данном случае администрация не несет ответственности за сохранность персональных данных. Из закона (гл. 14 ТК РФ) прямо не следует, что администрация обязана защищать персональные данные лиц, в отношении которых проводятся проверки. В состоянии такой неопределенности стороны могут находиться достаточно продолжительное время, когда администрация не принимает решение о приеме лица на работу и фактически не допускает его к работе под различными предлогами. Например, объясняет сложившуюся ситуацию необходимостью согласования кандидатуры советом директоров (правлением) общества либо нахождением генерального директора в длительной командировке и иными причинами.

*Анализ корпоративных актов, регулирующих порядок допуска и доступа лиц к сведениям, составляющим коммерческую тайну, показывает, что эти понятия не разграничиваются, а порой и смешиваются.* По этому пути идет и законодательство. В частности, Закон о коммерческой тайне не использует такую терминологию, как «допуск лиц к информации, составляющей коммерческую тайну». Закон предоставляет обладателю лишь право «разрешать или запрещать доступ к информации, составляющей коммерческую тайну, определять порядок и условия доступа к этой информации» (п. 2 ч. 1 ст. 10). Между тем употребляемые в литературе термины «допуск» и «доступ» лиц к коммерческой тайне имеют различное правовое содержание.

*Под допуском лиц к КЗИ* следует понимать установленное Законом право представителей органов государственной власти, иного государственного органа, органа местного самоуправления на истребование информации, составляющей коммерческую тайну, а также учредителей (акционеров), наемных работников, организационных контрагентов на использование в своей деятельности конфиденциальных сведений. Перечисленные категории лиц проходят соответствующую проверку при поступлении на государственную или муниципальную службу либо зачислении на должность в коммерческие организации. Право на использование КЗИ предоставляется субъектам в зависимости от занимаемой ими должности. Доступ работников к КЗИ осуществляется при наличии у них допуска к таким сведениям.

Право допуска лиц к конфиденциальным сведениям оформляется распоряжением генерального директора либо лицом, им уполно-

моченным. Факт допуска работника организации к конфиденциальным сведениям отражается в учетной карточке, подписанной руководителем службы безопасности. Карточка содержит установочные сведения на лицо, имеющее доступ к КЗИ. В частности, в ней указаны фамилия, имя, отчество, год и место рождения работника, его паспортные данные, отношение к воинской службе, адрес регистрации и фактическое место проживания, занимаемая должность и наименование подразделения, в котором он трудится, номер и дата распоряжения руководителя организации, в соответствии с которым предоставлено право доступа к КЗИ, и срок, на который предоставлено такое право. В карточке делается отметка о лишении работника (ряда) конфиденциальности сведений, к которым ранее было допущено лицо.

*Доступ лиц к КЗИ* означает фактическое ознакомление определенных лиц с конкретными работами, документами и изделиями, содержащими конфиденциальные сведения при условии соблюдения ими порядка, установленного в организации. Следует иметь в виду обстоятельство, что работник в силу различных причин может в процессе своей трудовой деятельности и не ознакомиться с соответствующими категориями сведений, к которым он имел доступ.

Формальная процедура допуска лиц к КЗИ всегда предшествует по времени фактическому доступу к такой информации. Исключением, пожалуй, являются представители государственных органов и командированные лица из числа организаций-контрагентов, которые допускаются к КЗИ на основании закона или договора. В отношении названных лиц допускная работа, связанная с осуществлением проверочных мероприятий, организацией не проводится.

Должностным лицам государственных органов предоставлено законом право на безвозмездное получение КЗИ в связи с исполнением ими служебных обязанностей. В этих целях государственный орган направляет руководителю организации требование о предоставлении КЗИ, в котором указывается основание для истребования таких сведений. Чаще всего с такими запросами в организации обращаются территориальные органы налоговой и таможенной службы, правоохранительные и контролирурующие органы, действующие на основании законодательства, определяющего их права по истребованию такого рода информации.

Руководитель организации рассматривает требование государственного органа и принимает решение о предоставлении либо от-

казе в предоставлении КЗИ. Закон о коммерческой тайне обязывает обладателя КЗИ предоставить такую информацию в суд, органы прокуратуры, предварительного следствия и дознания по делам, находящимся в их производстве (п. 3 ст. 6). Государственным органам предоставлено законом право истребования КЗИ в судебном порядке (п. 2 ст. 6).

Допуск командированных лиц к сведениям, составляющим КЗИ, осуществляется на основании договора о проведении совместных работ с предъявлением предписания на выполнение задания. Договором предусмотрены обязательства сторон по передаче КЗИ и охране ее конфиденциальности, по оформлению допуска лицам, участвующим в совместных работах, составляющих коммерческую тайну.

В предписании на выполнение задания, которое подписывается руководителем организации-контрагента, указываются должность, фамилия, имя и отчество командированного лица, цель его командировки, номер и дата договора о проведении совместных работ и другие данные. Необходимость доступа командированных лиц к конкретным сведениям определяется руководителем принимающего подразделения, участвующего в совместных работах.

Допуск командированных лиц к сведениям, составляющим коммерческую тайну, осуществляется по разрешению руководителя организации либо иного уполномоченного лица с последующей отметкой об этом в предписании на выполнение задания. При завершении работ в предписании на выполнение задания (оборотная сторона) принимающей стороной указывается, с какими сведениями, составляющими коммерческую тайну, было ознакомлено командированное лицо. Правильность записей в справке подтверждается подписью командированного лица. Предписание на выполнение задания вместе со справкой об осведомленности командированного лица находится на хранении в службе безопасности. Сроки хранения таких документов определяются номенклатурой дел, которая ведется в организации согласно требованиям государственной архивной службы.

*Содержание «допускной работы» и процедуры принятия решений о допуске лиц к КЗИ.* В практике хозяйствующих субъектов деятельность по проверке лиц, допускаемых к секретам, получила название «допускной работы». Она представляет собой специфический вид деятельности любой организации, которая имеет дело с КЗИ. Ее содержательная часть является составным и наиболее важным структурным элементом общего комплекса мер, направленных на обеспе-

чение безопасности организации. Значимость этой работы предопределяет необходимость создания в организациях с большим объемом КЗИ и хозяйственных связей специальных подразделений в составе служб безопасности, штатные работники которых на профессиональной основе осуществляют функциональную деятельность по допуску лиц к КЗИ.

Обобщение данных об опыте работы таких подразделений позволяет выделить направления их деятельности. *Во-первых*, это работа с участием руководителей подразделений номенклатуры должностей работников, оформляемых на допуск к различным категориям (разрядам) конфиденциальности КЗИ. *Во-вторых*, это подготовка рекомендаций кадровым органам по оформлению материалов на лиц, допускаемых к КЗИ, и изучение документов, представленных лицом, поступающим на работу. Работа по оформлению и переоформлению материалов на допуск лиц к КЗИ ведется кадровой службой. Работник кадрового органа после проведения ознакомительной беседы с лицом, поступающим на работу, оказывает ему помощь в заполнении формализованных документов (анкета, личная карточка работника и др.), которые затем передает в службу безопасности. В процессе беседы уточняется, была ли связана прежняя работа оформляемого лица с коммерческими секретами и оформлялось ли в этой связи письменное обязательство о неразглашении коммерческой тайны. Полученные данные используются для принятия решения о направлении запроса в организацию по прежнему месту работы лица. Такое предусмотрительное уведомление бывает весьма кстати в случаях возможных последующих претензий со стороны организации о якобы имевшем место разглашении коммерческих секретов ее бывшим работником.

Переоформление допуска работнику может быть связано с повышением или понижением степени конфиденциальности КЗИ, обусловленной изменением хозяйственной ситуации. Администрацией может быть принято решение об аннулировании действия допуска в том случае, если работник в течение одного года не пользовался и в дальнейшем не будет использовать в работе сведения, составляющие коммерческую тайну. Этот вопрос находится в компетенции руководителя организации, который принимает решение по представлению начальника службы безопасности.

*В-третьих*, это подготовка и направление запросов в организации, учреждения и на предприятия по прежним местам работы (службы) лиц, оформляемых на допуск к КЗИ. Нужно отметить, что

трудовое законодательство не устанавливает легальной возможности обмена информацией о персональных данных работника между коммерческими организациями в связи с заключением трудового договора. Тем более что передача персональных данных работника третьей стороне без его письменного согласия запрещена законом (ст. 88 ТК РФ). Это создает трудности в проверке данных, полученных от лица, поступающего на работу.

*В-четвертых*, представление руководителю организации или лицу, им уполномоченному, материалов для оформления и переоформления допусков, инструктаж лиц, допущенных к КЗИ, а также увольняемых лиц, имевших такой допуск, и оформление письменных обязательств о неразглашении сведений, составляющих коммерческую тайну, ведение и хранение документов по допускной работе. *В-пятых*, это контроль за деятельностью лиц, прибывающих в организацию для выполнения совместных договорных работ с использованием КЗИ, и учет сведений, с которыми они были ознакомлены.

Выборочный анализ материалов коммерческих организаций показал, что *используются различные процедуры для принятия решения о допуске лица к КЗИ*. Действия по оформлению допуска заключаются в основном в том, чтобы убедиться, что принимаемые на работу лица могут без риска для частных интересов организации ознакомиться с КЗИ в объеме, необходимом для выполнения ими трудовых обязанностей. Собственно, для этого и проводится проверка персональных данных, характеризующих личность кандидата на определенную должность.

При предоставлении лицу допуска к КЗИ администрация должна убедиться в том, что лицо обладает уравновешенным характером, а его прежние поступки характеризуются надежностью и ответственностью в любой хозяйственной ситуации. Результаты проверки должны свидетельствовать о том, что у лица развито чувство фирменного патриотизма, которое при надлежащем материальном и моральном стимулировании позволит поддерживать необходимый уровень его лояльности по отношению к частным интересам организации. Поэтому решение о допуске лица к КЗИ принимается по результатам комплексного изучения полученной о нем информации и анализа факторов, позволяющих получить целостное представление о личности.

Выборочный опрос работников кадров и служб безопасности показывает, что *при решении вопроса о предоставлении лицу допуска к*

*КЗИ чаще всего анализируются следующие обстоятельство. Во-первых,* выясняются факты привлечения лица, поступающего на работу, к юридической ответственности, в том числе за нарушения в сфере безопасности организаций. Оценивая уравновешенность характера, благоразумие и рассудительность лица, необходимо проанализировать данные о допущенных им правонарушениях.

Речь идет об оценке лицом факта привлечения его к уголовной ответственности, о возможных повторных нарушениях, которые имели место в последующий период работы. Изучение практики служб безопасности показывает, что, как правило, приговор суда за совершение преступления является достаточным основанием для отказа лицу в оформлении допуска.

В отдельных случаях, когда преступление совершено давно и имеются основания полагать, что лицо в последующий период жизнедеятельности не вступало в конфликт с социальными нормами, администрацией может быть принято положительное решение о допуске такого лица к КЗИ. Неоднократное нарушение лицом корпоративных норм, регулирующих обращение КЗИ, свидетельствует о пренебрежительном его отношении к интересам собственника и трудового коллектива, о недостаточном чувстве ответственности и служит основанием для отказа в допуске.

*Во-вторых,* уточняется возможное наличие скорее отрицательных черт характера лица, поступающего на работу, которые могут подтверждаться результатами проверки. Предоставление такому лицу допуска к КЗИ может быть сопряжено с определенным риском для безопасности организации. При оценке сведений, отрицательно характеризующих лицо, важно учитывать источник получения информации. К числу наиболее выраженных и тесно связанных между собой психологических свойств личности, которые проявляются в различных видах деятельности, могут относиться признаки, свидетельствующие о нежелании соблюдать установленный порядок охраны конфиденциальности информации; о безответственности в финансовых делах и попытках ухода от удовлетворения исков кредиторов; о наличии судебных исков работодателей и иных лиц в отношении проверяемого; о случаях проявления нечестности со стороны проверяемого лица, выразившейся в сокрытии отдельных автобиографических данных, например, о наличии судимости.

*В-третьих,* это учет данных, свидетельствующих об эмоциональной устойчивости и о возможных психических отклонениях в поведе-

нии лица<sup>1</sup>. Эмоциональная неустойчивость и расстройств психики могут повлиять на правильное восприятие лицом объективной действительности, в силу чего оно не сможет должным образом выполнять трудовые обязанности, в том числе осуществлять защиту КЗИ. Признаки возможных отклонений в поведении лица могут быть выявлены в процессе ознакомительной беседы. Такие сведения можно получить официально путем обращения в медицинские учреждения в порядке ст. 88 ТК РФ (абзац б) о состоянии здоровья лица, в целях решения вопроса о возможности выполнения работником трудовой функции, связанной с КЗИ.

Требует внимания анализ достоверности информации об имевших место случаях злоупотребления лицом, поступающим на работу, спиртными напитками и употребления наркотических средств. Общеизвестным является факт их отрицательного влияния на трудовой процесс. В частности, это проявляется в поведенческих актах лица, свидетельствующих о его осторожности и рассудительности, так необходимых для соблюдения режима КЗИ. Оценка данных необходима для определения возможности рецидива со стороны таких лиц. Важно выяснить, имели ли место прогулы и другие нарушения трудовой дисциплины по причине злоупотребления спиртными напитками. Что касается употребления наркотиков, то это не только правовая, но и медицинская проблема, решение которой во многом зависит от действий государственных органов. Федеральный закон от 8 января 1998 г. № 3-ФЗ «О наркотических средствах и психотропных веществах»<sup>2</sup> определяет наркоманию как заболевание, обусловленное зависимостью от наркотических средств или психотропных веществ. Употребление лицом наркотиков должно автоматически исключать его допуск и доступ к коммерческим секретам.

Названные отклонения в поведении лица могут быть использованы, при определенных обстоятельствах, конкурентной разведкой для оказания на него давления с целью незаконного получения КЗИ. Допуск таких лиц к КЗИ представляет потенциальную угрозу безопасности организации.

<sup>1</sup> См.: *Войсунский А.Е.* Психологические аспекты информационной безопасности // Глобальная информатизация и безопасность России. М.: Изд-во Моск. ун-та, 2001. С. 168–175, и др.

<sup>2</sup> См.: СЗ РФ. 1998. № 2. Ст. 219.

Анализ практики коммерческих организаций показывает, что причинами отказа гражданину в приеме на работу, связанную с использованием сведений, составляющих коммерческую тайну, чаще всего являются судимость лица, совершение им аморальных поступков, медицинские противопоказания, препятствующие выполнению работы в сфере обращения КЗИ. Названные основания для отказа гражданину в допуске к коммерческой тайне широко используются в практике, однако в ТК РФ либо иным правовом акте официально не установлены. В литературе названы и другие основания, такие как признание лица недееспособным или ограничением дееспособным в судебном порядке, не санкционированная руководством фирмы работа по совместительству, которые, на наш взгляд, носят обиходный характер.

Для сравнения укажем, что в Законе о государственной тайне четко перечислены основания для отказа гражданину в допуске к государственной тайне<sup>1</sup>. Порой эти основания по аналогии используются для отказа в допуске к коммерческой тайне. В правовом отношении является некорректным предложение о том, что «сотруднику предприятия или организации может быть отказано в допуске к информации, составляющей его коммерческую тайну, в случаях... уклонения сотрудника от проверочных мероприятий»<sup>2</sup>. Это правило действует в отношении государственной тайны<sup>3</sup>, поскольку установлено законодательством. Применительно к коммерческой тайне ТК РФ не предусматривает такое основание для отказа гражданину в приеме на работу, хотя организации широко используют его в допускной работе.

Итак, ТК РФ, Законом о коммерческой тайне и иными правовыми актами не установлены формы, методы и процедуры проверки лиц, допускаемых к работе, связанной с использованием КЗИ. Каждая организация на корпоративном уровне устанавливает свои правила, регулирующие порядок допуска и доступа лиц к КЗИ. Анализ материалов ряда организаций позволяет сделать вывод, что су-

<sup>1</sup> См.: ФЗ от 6 октября 1997 г. № 131-ФЗ «О государственной тайне» // СЗ РФ. 1997. № 41. Ст. 4673.

<sup>2</sup> См.: Справочник директора предприятия / Под ред. М.Г. Лапусты. 5-е изд. М., 2001. С. 554.

<sup>3</sup> См.: Федеральный закон «О внесении изменений и дополнений в Закон РФ «О государственной тайне» от 19 сентября 1997 г. № 131-ФЗ // СЗ РФ. 1997. № 41. Ст. 4673.

ществует тенденция проведения в основном простой, получившей на практике название «стандартной», проверки лиц, допускаемых к КЗИ. Что касается более основательной «глубокой» проверки, то она в силу известных причин проводится крайне редко. Первоначальная проверка проводится, как правило, в отношении всех поступающих на работу лиц. Анализ содержания проверочных мероприятий по допуску лиц к КЗИ показывает, что многие из них связаны с вторжением в личную жизнь граждан и поэтому требуют их письменного согласия. Однако, в отличие от порядка, установленного для допуска лиц к государственной тайне<sup>1</sup>, Закон о коммерческой тайне не регулирует процедуру получения письменного согласия лица, в отношении которого проводятся проверочные мероприятия.

Поэтому необходимо узаконить существующую практику допускной работы в коммерческих организациях по этому вопросу и внести соответствующие изменения в ТК РФ и Закон о коммерческой тайне.

**Формирование условий о конфиденциальности информации в трудовом договоре.** Содержанием трудового договора являются условия, определяемые ст. 57 ТК РФ. Законодатель различает существенные и дополнительные (факультативные) условия. Круг существенных и дополнительных условий договора законодательно закреплён и не может быть изменён сторонами. Условия о неразглашении коммерческой тайны работодателя отнесены к числу дополнительных условий, определяемых самими сторонами. При формулировании этого условия стороны руководствуются законодательством РФ, регулирующим защиту коммерческой тайны, прежде всего, Законом о коммерческой тайне и корпоративными актами организации.

**Круг условий о неразглашении коммерческой тайны определяется работодателем и по его инициативе обсуждается с работником.** Анализ материалов организаций показывает, что важнейшими, по мнению работодателя, являются следующие условия, которые должен соблюдать работник: не разглашать информацию, составляющую коммерческую тайну организации, которая будет ему доверена или станет известна по работе; не передавать третьим лицам и не раскрывать публично такую информацию без согласия администрации; со-

<sup>1</sup> См.: Инструкция о порядке допуска должностных лиц и граждан Российской Федерации к государственной тайне. Утв. пост. Правительства РФ от 28 октября 1995 г. № 1050 // СЗ РФ. 1997. № 41. Ст. 4987.

хранять такого рода информацию тех организаций, с которыми имеются договорные отношения; выполнять относящиеся к нему требования корпоративных актов по сохранности коммерческой тайны; не использовать такую информацию, которая в качестве конкурентного действия может нанести ущерб организации; в случае попытки посторонних лиц получить от работника информацию, составляющую коммерческую тайну, незамедлительно известить об этом администрацию; незамедлительно сообщать об утрате носителей информации, составляющей коммерческую тайну, удостоверений, пропусков, ключей от режимных помещений, хранилищ, сейфов и о других фактах, которые могут привести к разглашению (утечке) КЗИ; в случае увольнения передать администрации все носители информации, составляющей коммерческую тайну (документы, чертежи, рукописи, диски, дискеты, кино- и фотоматериалы и др.), которые находились у работника в связи с выполнением обязанностей.

Названные типовые условия являются предметом обсуждения сторон при заключении трудового договора, и чаще всего в различных комбинациях отражены в договоре или иных документах (письменное обязательство, подписка о неразглашении и др.), являющихся его составной частью. По мнению Ю.В. Гаврилина, «прямое включение в контракт оговорки о конфиденциальности — лучшая, но отнюдь не единственно возможная форма решения данной проблемы. Лучшей указанная форма является потому, что она наиболее проста и надежна, так как прямо опирается на ст. 57 ТК РФ. Однако, в принципе, обязанность по неразглашению сведений, составляющих коммерческую тайну, может быть возложена на работника и иным путем, в частности, посредством оформления особого письменного обязательства работника, путем дачи им подписки о неразглашении»<sup>1</sup>.

Далее Ю.В. Гаврилин подчеркивает, что «целесообразно увязывать подобные соглашения с трудовым договором либо прямо указывать на то, что они становятся составной частью последнего». Трудно согласиться с первой частью предложения, сформулированного Ю.В. Гаврилиным, насчет «увязывания подобных соглашений с трудовым соглашением», поскольку единственным правовым докумен-

том, регулирующим трудовые правоотношения, является трудовой договор (ст. 56 ТК РФ).

Условия по сохранности коммерческой тайны могут содержаться в тексте самого договора или в виде отдельного документа, являющегося неотъемлемым приложением к договору. Представляется, что второй вариант может быть более предпочтительным. Далеко не все работники с момента приема на работу могут быть допущены к коммерческой тайне. У большинства из них такая потребность может возникнуть в процессе работы. Поэтому удобно, в данном случае, будет оформить дополнение к трудовому договору с возложением на работника обязанностей по защите коммерческой тайны.

Разработка формы и внутреннее содержание соответствующего раздела трудового договора или отдельного приложения к нему в части, касающейся сохранения коммерческой тайны, имеют важное правовое значение. В случае разглашения работником сведений, составляющих коммерческую тайну организации, эти документы будут являться основанием для обращения в суд с иском о возмещении ущерба.

Условия, которые включены в трудовой договор, представляют собой «выраженные» сторонами условия. Безусловно, в теории и на практике признается, что включение в трудовой договор оговорки о конфиденциальности является предпочтительным как для работодателя, так и для работника<sup>1</sup>. Работодатель при наличии такой оговорки обеспечивает себе точное понимание работником пределов использования КЗИ. Ему значительно проще доказывать в суде факт нарушения работником своих обязанностей в части нарушения условия конфиденциальности. Со своей стороны работник приобретает преимущества, так как обеспечивается четкое понимание требований работодателя в отношении сохранения в тайне КЗИ. Выраженные условия несут легитимный характер, однако лежат как бы на поверхности и отражают лишь организационную часть проблемы, они не затрагивают поведения работника при использовании им КЗИ в гражданском обороте.

Речь в данном случае идет о «подразумеваемых» работодателем условиях, которые не включены в трудовой договор в виде условия о конфиденциальности. Работодатель считает, что в течение действия трудового договора работник должен вести себя по отношению к

<sup>1</sup> См.: Коломиец А. Условие о неразглашении коммерческой тайны в трудовом договоре (контракте) // Хозяйство и право. 1998. № 5, и др.

<sup>1</sup> Гаврилин Ю.В. Понятие и правовая охрана коммерческой тайны в РФ (Научно-практический комментарий к ч. 1 ст. 139 ГК РФ) // СПС «Консультант Плюс», 2004.

нему честным образом. Под этой общей обязанностью, которая никак не зафиксирована в договоре, имеется в виду и обязанность работника не раскрывать определенную КЗИ. Такое положение было характерным для советского периода, когда в трудовом договоре не указывалось условие по охране секретов. В этом не было необходимости, поскольку в обществе царил общественно-политический климат, поддерживаемая в силу общественного воздействия КПСС, профсоюзами и др. организациями. В рыночных условиях надежды коммерческих организаций на честность работников не всегда оправдываются. Поэтому «подразумеваемые» работодателем условия должны быть отражены в трудовом договоре.

*Результаты исследования позволили сформулировать ряд предложений, которые необходимо учитывать при формировании условий о защите КЗИ в трудовом договоре.*

1) При отсутствии «выраженного» условия в трудовом договоре работодатель не имеет возможности препятствовать бывшему работнику в том, что он займется на работу в конкурирующую организацию или организует непосредственно дело, находящееся в прямой конкуренции с его собственным делом с последующим риском раскрытия и использования КЗИ или деловой репутации, достигнутый работодателем.

2) Недобросовестное использование работником внутренней цели информации до ее официального опубликования, в целях осуществления своей собственной деятельности. Во многих организациях действуют правила, когда работник не имеет права продавать изделия, собственные или чужие, а также выполнять все виды работы, если его фирма аналогичную продукцию предлагает к продаже или выполняет те же работы. Работники организации не должны содействовать конкурентам в продаже изделий, в частности, по более низким ценам, а также содействовать им в работе. Другими словами, работники не могут извлекать собственную выгоду из деловых контактов, если эти контакты задевают интересы организации. От коммерческих сделок работники не должны иметь доход, дополнительный по отношению к заработной плате. В трудовой договор может быть включено условие, в соответствии с которым работник должен избегать конфликта между личными и корпоративными интересами, не допуская даже видимости неправомерного поведения в отношении организации.

3) При деловых контактах с конкурентами работники, с одной стороны, не должны обсуждать внутренние дела организации (цены,

условия продажи, производственные планы и т.д.), а другой — профессиональные контакты абсолютно необходимы по вопросам технических разработок и новшествах, о тенденциях хозяйственного развития. В данном случае существует опасность договоренностей между работниками в обход корпоративных интересов. Поэтому представители организаций должны избегать дискуссий о ценах и внутренних делах своих фирм, что должно быть одним из условий трудового договора.

4) Организация должна четко сформулировать условие о том, что работник не должен применять недопустимые способы и средства получения чужой секретной информации о деятельности конкурентов, и он не должен иметь самостоятельный доступ к чужой секретной информации. Это в полной мере относится к любым контрагентам. Такой подход будет способствовать разрешению возможных конфликтных ситуаций с другими организациями.

**Содержание прав и обязанностей работодателя и работника по защите КЗИ.** Выборочное изучение трудовых договоров в ряде коммерческих организаций показывает, что условие о конфиденциальности, как правило, сформулировано сторонами весьма кратко. Вместе с тем наличие в трудовом договоре условия о сохранении коммерческой тайны является основанием для конкретизации прав и обязанностей работодателя и работника, которые закреплены в различных корпоративных актах, положениях о статусе подразделений, положениях к трудовому договору и должностных инструкциях. В названных выше документах отражены императивные нормы Закона о коммерческой тайне (ст. 11), определяющие обязанности работодателя и работника. В частности, Закон обязывает *работодателя* ознакомить под расписку работника, доступ которого к информации, составляющей коммерческую тайну, необходим для выполнения им своих трудовых обязанностей, с перечнем информации, составляющей коммерческую тайну, обладателями которой являются работодатель и его контрагенты; с установленным режимом коммерческой тайны и с мерами ответственности за его нарушение; создать работнику необходимые условия для соблюдения им установленного режима. Кроме того, получение работником сведений, составляющих коммерческую тайну, должно осуществляться с его согласия, которое письменно оформляется при поступлении на работу или в процессе исполнения трудовых обязанностей. В случае незаконного установления режима коммерческой тайны работник вправе обжаловать действия администрации в судебном порядке.



Реализация работодателем обязанностей по ознакомлению работников с требованиями режима требует от него разработки корпоративных актов, определяющих перечень сведений, составляющих коммерческую тайну и меры по установлению режима такой тайны. В этой связи важным корпоративным актом, в котором ведущее место занимают нормы трудового права, является *Инструкция по обеспечению сохранности коммерческой тайны организации*. Она составляется, как правило, при большом объеме сведений, когда к ним имеет доступ значительный круг работников. В этом случае необходимо детализировать порядок действий исполнителей, предусмотреть четкую систему документооборота и организацию работ в реальных помещениях.

Содержание такой *инструкции* должно соответствовать конкретной обстановке и учитывать специфику организации, в зависимости от которых в том или ином объеме в ней следует определить порядок присвоения и снятия грифа документам и работам, содержащим коммерческую тайну; доступа работников и контрагентов к КЗИ; обращения с конфиденциальными документами; приема представителей других организаций и ведения коммерческих переговоров; предоставления информации государственным органам и органам местного самоуправления; проведения контроля за обеспечением сохранности таких сведений; привлечения к ответственности работников, разгласивших сведения, составляющие коммерческую тайну, и допустивших другие нарушения установленного режима.

В небольших по численности организациях вместо *инструкции* составляется *памятка работнику, допущенному к КЗИ*. Она содержит основные положения по обеспечению режима и вполне может заменить инструкцию по данному вопросу. В *памятке работника* должны быть указаны положения, обязывающие его работать только с теми документами, к которым он получил доступ в силу выполнения трудовых обязанностей; знать, какие конкретно сведения подлежат защите; кому и в каком объеме эти сведения могут быть доведены, включая представителей контрагента.

Трудовым кодексом РФ (гл. 43) и иными правовыми актами предусмотрены *особенности регулирования труда руководителя организации*. Учитывая, что руководитель организации возглавляет исполнительную власть, на него возлагаются обязанности управленческого характера по защите коммерческой тайны и ответственность за состояние дел на этом участке работы. При заключении с ним трудового договора общее собрание акционеров или совет директоров об-

щества определяет его права и обязанности в этой части деятельности. *Во-первых*, должны быть письменно закреплены его полномочия по определению состава и содержания сведений, составляющих коммерческую тайну. *Во-вторых*, необходимо обязать его не использовать коммерческую тайну в своих интересах для занятия деятельностью, которая может причинить ущерб организации. *В-третьих*, следует определить ответственность за создание необходимых условий для обеспечения сохранности коммерческой тайны и порядок возмещения убытков, причиненных его виновными действиями в соответствии с ГК РФ. *В-четвертых*, он должен быть предупрежден о том, что нарушение им порядка защиты коммерческой тайны может повлечь расторжение с ним трудового договора, а также привлечение к ответственности.

На работника Законом возложены несколько иные обязанности по охране коммерческой тайны, а именно: выполнять установленный работодателем режим коммерческой тайны; не разглашать такого рода информацию и не использовать без согласия работодателя и его контрагентов в личных целях; вернуть, в случае увольнения, имеющиеся у него документы, содержащие КЗИ; не разглашать сведения после увольнения в течение срока, предусмотренного трудовым договором или соглашением, дополнительно заключаемым с работодателем.

Подробный перечень обязанностей работника содержится в отдельном приложении к трудовому договору либо в должностной инструкции, с которыми он знакомится под расписку. В основном они носят императивный характер в виде требований администрации к работнику. Работник предупреждается об ответственности за нарушение требований по охране коммерческой тайны с указанием срока действия. Обобщение таких документов позволяет сформулировать некоторые общие положения, которые используются большинством организаций. Перечень обязанностей, возлагаемых на работников, изложенных в приложении к трудовому договору или в должностной инструкции, по существу, совпадает с типовыми условиями, обсуждаемыми при заключении трудового договора.

В теории и на практике весьма остро стоит вопрос о пределах ограничения, которые налагаются на работников в связи с охраной конфиденциальности КЗИ. Как отмечает Ю.В. Гаврилин, «ограничения, добровольно принятые на себя работником (но не навязанные ему работодателем), могут идти сколь угодно далеко, но при этом не ве-

сти к ограничению его право- и дееспособности»<sup>1</sup>. Прямых ответов относительно пределов ограничения, к сожалению, не содержится в Законе о коммерческой тайне.

Правда, можно говорить об условиях, при которых меры по охране конфиденциальности КЗИ признаются *разумно достаточными*, применительно к частным интересам. Автор разделяет подход к решению этой проблемы, сформулированный Ю. В. Гаврилиным, который состоит «в поиске оптимального баланса интересов работодателя и работника (в том числе бывшего), которые в равной степени заслуживают защиты»<sup>2</sup>, и, добавив, не должны быть направлены против публичных интересов.

Суть «оптимального баланса интересов работодателя и работника» может быть охарактеризована следующим образом. Для признания ограничений *разумно достаточными* (п. 5 ст. 10 Закона) необходимо выполнение четырех условий.

*Во-первых*, информация, которая защищается, должна быть отнесена в установленном порядке к коммерческой тайне. Это означает, что работодатель не может искать защиты там, где работник использует свои полученные знания и опыт.

*Во-вторых*, ограничение должно носить адекватный характер и не должно быть слишком широким, запрещающим работнику быть вовлеченным в дело, в котором данная информация является бесполезной и не может быть использована по прямому назначению.

*В-третьих*, ограничения должны распространяться на разумный период времени. Работодатель должен возлагать ограничения на возмодно короткий период времени, который адекватно защищает его интересы. При этом важно учитывать характер информации, должность работника и специфику его работы. В зависимости от этих факторов КЗИ может оставаться таковой в течение различных периодов времени.

*В-четвертых*, ограничения должны распространяться на географическую (территориальную) сферу, которая может разумно считаться относящейся к сфере деятельности работодателя. Поэтому ограничения, которые географически распространяются за пределы территории деловой сферы работодателя, не могут считаться разумными и не подлежат защите.

Представляется, что нарушение данных условий работодателем может стать причиной обращения работника в суд о незаконном установлении режима коммерческой тайны (п. 8 ст. 11 Закона).

*Изменения, происходящие в трудовой деятельности работника, оказывают влияние на функционирование механизма корпоративного регулирования обращения КЗИ.* Чаще всего речь идет об исключении администрации из Перечня сведений, составляющих коммерческую тайну, тех сведений, которые необходимы работнику и к которым он был допущен в силу выполнения трудовых обязанностей. В данном случае действуют общие нормы трудового законодательства, регулирующие порядок перевода на другую постоянную работу и перемещение (ст. 72 ТК РФ) либо временный перевод на другую работу в случае производственной необходимости (ст. 74 ТК РФ). Права и обязанности сторон, в связи с изменением организационных или технологических условий труда по поводу использования КЗИ, могут быть изменены с соблюдением условий, предусмотренных ст. 73 ТК РФ.

Права работника в сфере обращения КЗИ могут быть прекращены на основании закона. ТК РФ предусматривает увольнение за неоднократное грубое нарушение работником своих трудовых обязанностей, связанных с разглашением коммерческой тайны, ставшей известной работнику в связи с выполнением им трудовых обязанностей (подп. «в» п. 6 ст. 81 ТК РФ). Ранее такая норма отсутствовала в КЗОТ РСФСР. Увольнение работника по этому основанию возможно, если в трудовом договоре содержится условие о неразглашении коммерческой тайны (ст. 57 ТК РФ) и до работника были доведены требования работодателя по охране таких сведений, а также выполнены условия, предусмотренные ст. 1465 ГК РФ. Применение к работнику иных дисциплинарных мер не должно отражаться на его доходе к КЗИ.

Закон о коммерческой тайне прямо предусматривает обязанность заключения соглашения между работником и работодателем о неразглашении коммерческой тайны. Вместе с тем на практике такой документ, как «Обязательство о неразглашении коммерческой тайны» (далее — Обязательство), используется организациями с 1991 г. и оформляется в связи с расторжением трудового договора. Обязательство содержит определенные ограничения, налагаемые на работника после его увольнения, а именно: не разглашать сведения, составляющие коммерческую тайну организации, которые ему были доверены или стали известны по работе; не передавать третьим ли-

<sup>1</sup> Гаврилин Ю. В. Указ. соч. // СПС «Консультант Плюс», 2004.

<sup>2</sup> Там же.

цам и не раскрывать публично сведения, составляющие коммерческую тайну организации, без ее согласия, а также тех организаций, с которыми у работодателя имеются деловые отношения; не использовать знание коммерческой тайны организации для занятия любой деятельностью, которая в качестве конкурентного действия может нанести ущерб организации. Анализ таких документов показывает, что ограничение прав работника в большинстве случаев установлено на срок от 2 до 5 лет. Закон не содержит норм о необходимости выплаты денежной компенсации работнику в случае ограничения его прав после прекращения с ним трудовых отношений. Поэтому при отсутствии материальных стимулов Обязательство в рыночной экономике не работает. Изменение этой ситуации возможно путем заключения возмездного договора с лицом, права которого ограничиваются обладателем коммерческой тайны на определенный срок. Предметом договора является сохранение лицом коммерческой тайны после расторжения трудового договора, ставшей ему известной по работе в организации. Для принятия работодателем решения о заключении такого договора ему важно выяснить, в состоянии ли работник оказывать влияние на коммерческие связи организации после своего увольнения и какие ограничения в этой связи необходимо установить, с тем чтобы их можно было отнести к категории разумных мер.

### § 3. Гражданско-правовое регулирование обращения коммерчески значимой информации

*Роль гражданско-правовых средств в механизме регулирования обращения КЗИ и охраны ее конфиденциальности.* В формирующихся в нашей стране рыночных условиях характерной является тенденция все более полного использования организациями гражданско-правовых средств в регулировании хозяйственной деятельности, включая и обращение КЗИ. По мере накопления опыта применения таких средств для охраны конфиденциальности информации этот вопрос приобретает все большую актуальность. Проблема состоит в установлении особенностей использования средств применительно к охране конфиденциальности КЗИ, используемой при производстве товаров (работ, услуг).

Доктрина гражданско-правовых средств в хозяйственных отношениях, объясняющая порядок реализации дозволенных установлений и механизмов правового регулирования, принятых в частном праве, была разработана в начале 80-х гг. XX в.<sup>1</sup> Сегодня система гражданско-правовых средств последовательно внедряется в практику хозяйствования и активно используется организациями для защиты своих частных интересов. Важное значение для понимания механизма использования таких средств в сфере регулирования обращения КЗИ имеют следующие положения. Во-первых, правовые средства выступают действенными инструментами хозяйственной деятельности фирмы. В их выборе и конкретизации участвуют сами стороны, исходящие из законных интересов, чем достигается детальное и точное определение содержания субъективных прав и обязанностей, включая передачу, использование и охрану конфиденциальности КЗИ. Каждое средство образует некоторый комплекс действий юридического характера. Примером может служить подготовка и реализация такого документа, как совместное заключение организацией о наличии условий для проведения конфиденциальных работ. Его утверждению предшествует согласование условий договора. Такое предварительное регулирование обеспечивает соответствие работы по применению средств требованиям Закона о коммерческой тайне и интересам самой организации.

Во-вторых, правовые средства — интегрированные образования, соединения действий, основанных на правовых установлениях и усмотрениях субъектов<sup>2</sup>. Их применение выражает особый аспект правового регулирования, неразрывно связанный с нормативным, но не сводимый к последнему. Раздел между нормативной регламентацией отношений и использованием средств проходит там, где возникает возможность свободного решения организациями на правовой основе своих жизненных задач. При использовании правовых средств у субъекта появляется необходимость не просто пользоваться предложенной законодателем моделью поведения, а проводить конструктивную работу по выбору пригодного средства и приспособлению его к конкретным условиям в целях достижения желаемого результата.

<sup>1</sup> См.: Пушинский Б.И. Гражданско-правовые средства в хозяйственных отношениях. М., 1984. С. 90–97.

<sup>2</sup> См.: Там же. С. 100–102.

Последующие изменения, произошедшие в нашей стране, позволили расширить парадигму применения гражданско-правовых средств с учетом рыночных условий. При этом неизменным остается определение самого понятия правовых средств, сформулированное еще в конце 70-х гг.<sup>1</sup>, неоднократно подтвержденное хозяйственной практикой. В частности, «под правовыми средствами понимаются основанные на дозволениях закона совокупности инициативных юридических действий лиц, служащих достижению соответствующих целей... главным в данной системе является договор»<sup>2</sup>.

Учитывая особенности, присущие обращению КЗИ, необходимо определить возможные правовые средства, пригодные для использования в деятельности по охране конфиденциальности информации. Речь идет о разработке упорядоченного алгоритма юридических действий организации, позволяющего обеспечить ей охрану такой информации в рамках гражданско-правовых отношений.

ГК РФ, Закон о коммерческой тайне содержат целый ряд норм, закрепляющих возможность охраны конфиденциальности КЗИ с использованием режима коммерческой тайны. Наличие этих норм представляет организациям регулирующего договорные отношения сного правового механизма, регулирующего договорные отношения с контрагентами и иными лицами при обращении КЗИ.

В цивилистической науке аксиоматичным является утверждение о том, что важнейшим элементом системы гражданско-правовых средств является *договор*. Благодаря договору стороны определяют свой субъективные права и обязанности по использованию полученной КЗИ, ее передаче и охране конфиденциальности при взаимоотношении с третьими лицами. В теории договорного права, на наш взгляд, недостаточно раскрыты права и обязанности сторон, связанные с режимом охраны конфиденциальности информации при производстве и реализации товаров (работ, услуг).

Между тем практикой накоплен богатый опыт режимного сопровождения договорных работ, выполнявшихся в основном для нужд обороны в советский период, нуждающейся в обобщении и анализе в целях использования в договорной работе коммерче-

<sup>1</sup> См.: Пугинский Б.И. Исследование эффективности гражданско-правовых средств // Вестн. Моск. ун-та. Сер. 11 «Право». 1977. № 6.

<sup>2</sup> Пугинский Б.И., Неверов О.Г. Правовая работа. Учебник. М., 2004. С. 77.

ских организаций. Практика включения в хозяйственные договоры условий о соблюдении режима секретности имела правовую основу и была подкреплена действовавшими в то время ГОСТ В2.907-75 «Тактико-техническое задание на разработку изделий военного назначения» и разработку составных частей изделия военного назначения», ГОСТ В15.101-79 «Тактико-техническое задание на выполнение опытно-конструкторских работ». В названных стандартах был обязательный раздел по обеспечению сохранения государственных секретов. Аналогичные требования содержались в отраслевых стандартах и стандартах предприятий. Нормативные акты министерств дополнительно к ГОСТам обязывали предприятия согласовывать с контрагентами договорные условия по обеспечению режима секретности. Заключение договоров, предусматривавших в ходе их выполнения использование закрытой информации, предшествовала большая подготовительная работа, связанная с подписанием совместного заключения о наличии условий по обеспечению режима секретности выполняемых работ, согласованием требований по хранению государственной и служебной тайны, включаемых в техническое задание.

Легальная возможность охраны конфиденциальности информации появилась у организаций еще в советский период. Это стало очевидным после принятия законов о собственности, о предприятиях и предпринимательской деятельности, а затем и ГК РФ. Включение в законодательство норм о коммерческой тайне и практическая деятельность по ее защите были продиктованы необходимостью упорядочивания появившихся новых общественных отношений по защите частных интересов на информационный продукт<sup>1</sup>, ставший предметом гражданского оборота.

Обязательственные отношения по поводу формирования и соблюдения условий конфиденциальности КЗИ, с одной стороны, характеризуются общими признаками, присущими обязательствам, сущность которых достаточно полно раскрыта в гражданском праве, а с другой — содержат специфические признаки применения гражданско-правовых средств обращения КЗИ. Последнее обстоятельство необходимо учитывать **при определении роли и места гражданско-правовых средств в механизме правового регулирования обращения**

<sup>1</sup> См.: Дозорцев В.А. Интеллектуальные права: Понятие. Система. Задачи квалификации: Сб. статей // Исслед. центр частного права. М., 2005. С. 52–60, и др.

**КЗИ и охраны ее конфиденциальности**, характеристика которых включает следующие группы признаков:

характеризующие различные этапы договорного регулирования отношений в информационной сфере по поводу производства, получения, использования, передачи и охраны конфиденциальности информации в процессе ее обращения;

определяющие основные черты формирования структуры и инфраструктуры информационного рынка в России, включая различные виды коммерческой информации;

дифференцирующие договоры на обращение КЗИ по группам в зависимости от специфики регулируемых ими отношений.

Каждая группа признаков тесно связана с регулирующей ролью договора, выражающего волю сторон на установление конфиденциальных отношений при согласовании условий и исполнении обязательств. Для получения *характеристики гражданско-правового регулирования обращения КЗИ* названные признаки рассматриваются в совокупности как образующие систему гражданско-правового регулирования обращения КЗИ.

**Этапы договорного регулирования отношений в информационной сфере.** Исследуемая сфера обращения КЗИ является частью общей информационной сферы хозяйствующих субъектов, где обращается открытая и закрытая информация, по поводу которой в различные исторические периоды нашей страны существовали те или иные договорные отношения, в том числе охраны конфиденциальности информации. В этой связи необходимо выделить основные историко-правовые аспекты договорного регулирования отношений в информационной сфере.

*Первый этап (с 60-х гг. XX в.) характеризуется созданием и освоением в производстве новой техники, технологии и материалов.* Динамика инновационной деятельности, связанной с использованием технической и технологической информации, характеризуется в разные периоды ростом и падением числа созданных и внедренных образцов новых типов машин, оборудования, приборов и средств автоматизации. Технологический кризис конца 80-х годов привел к падению конкурентоспособности отечественной продукции. Уменьшилось число инноваций, и изменился их характер<sup>1</sup>.

<sup>1</sup> См.: Кузык Б.Н., Яковец Ю.В. Россия — 2050. Стратегия инновационного прорыва. М., 2005. С. 58, 72, 74—75.

Объектом договорных отношений была продукция научных организаций, предприятий и учреждений<sup>1</sup>. К научно-технической продукции относились законченные научно-исследовательские, опытные, опытно-конструкторские и технологические работы; опытные и экспериментальные образцы или партии изделий. К этой же категории были отнесены и научно-технические услуги, связанные с внедрением новой техники и технологии, консультациями методического характера, координацией научных исследований.

Договорные отношения в этой сфере были в тот период урегулированы правовыми актами Госкомитета СССР по науке и технике (ГКНТ СССР), Академией наук СССР и отраслевых общесоюзных министерств, а затем и Основами гражданского законодательства Союза ССР и республик от 31 мая 1991 г. (ст. 97 гл. 12)<sup>2</sup>. В настоящее время эти отношения регулируются главой 38 ГК РФ.

В договорной практике, начиная с 80-х годов, широко использовались типовые тексты договоров на создание (передачу) научно-технической продукции, утвержденные постановлением ГКНТ СССР<sup>3</sup>. Этот документ отличался значительной степенью общности формулировок, что позволяло предприятиям на его основе конструировать различные виды договоров на выполнение подрядных работ и оказание услуг в этой области.

Основными видами договоров, которые активно использовались предприятиями в конце 80-х годов, были следующие.

1) *Договор на создание научно-технической продукции.* Особенностью договора являлось определение и согласование сторонами содержания и объема работы в целом и отдельных ее этапов. Важное внимание при этом уделялось согласованию договорной цены. Этот этап предшествовал заключению договора и оформлялся в виде согласованной и утвержденной сторонами программы работ, содержанием которой было, например, создание технологической линии основного производства завода. Как правило, такой вид договора

<sup>1</sup> См.: Общее положение о научно-исследовательских, конструкторских, проектно-конструкторских и технологических организациях было утверждено постановлением Госкомитета СССР по науке и технике от 13 ноября 1970 г. // Бюллетень нормативных актов министерств и ведомств СССР. 1983. № 7. С. 3.

<sup>2</sup> См.: Вестник Высшего Арбитражного Суда Российской Федерации. 1993. № 3. С. 4—63.

<sup>3</sup> См.: Положение о договорах на создание (передачу) научно-технической продукции. Постановление ГКНТ СССР от 19 ноября 1987 г. № 435.

предусматривал выполнение полного цикла работ: научные исследования — разработки — производство — сбыт — обслуживание. Для этих целей создавались специальные научно-производственные объединения<sup>1</sup>. Сроки выполнения отдельных этапов работы определялись календарным планом работ. Использование (внедрение) научно-технической продукции являлось обязанностью заказчика. Договором предусматривалось, что в случае необеспечения заказчиком приемки работы в течение 10 дней после получения уведомления исполнитель вправе был составить односторонний акт, который являлся основанием для расчета.

Опубликование результатов научно-технической продукции или передача ее третьим лицам разрешались с согласия исполнителя. В случае коммерческой реализации продукции заказчиком он был обязан проинформировать исполнителя и перечислить ему часть прибыли, определяемой по отдельному соглашению сторон.

Особо в договоре выделялись положения, регулирующие поведение сторон по соблюдению условий конфиденциальности. *Во-первых*, стороны согласовывали условия о том, что создаваемая научно-техническая продукция должна соответствовать нормативным техническим требованиям (ГОСТ, ОСТ, СТП), предъявляемым к обеспечению конфиденциальности при ее разработке, испытании и эксплуатации. *Во-вторых*, стороны принимали на себя обязательства по соблюдению режима конфиденциальности работ, установленно-го общесоюзными и отраслевыми правовыми актами (Инструкция № 0126 и др.). Речь идет об обеспечении охраны конфиденциальности информации, касающейся содержания предмета договора, уровня договорной цены, сроков поставки продукции, научно-технической характеристики изделий, технологических условий их эксплуатации.

*В-третьих*, в отношениях между сторонами действовало правило, когда заказчик не вправе был требовать от исполнителя передачи ему его деловых секретов вместе с документацией по научно-технической продукции. Нужно сказать, что аналогичные требования по охране конфиденциальности при создании научно-технической продукции предъявляются и сегодня в рамках действия института коммерческой тайны.

2) *Договор на проведение научно-исследовательских и опытно-конструкторских (технологических) работ*. Этот вид договора мало

чем отличается от предыдущего, пожалуй, только меньшим объемом работы и возможностью раздельного или совместного проведения научно-исследовательских и опытно-конструкторских (технологических) работ. Договор может предусматривать как весь цикл проведения исследований, разработки и изготовления образцов нового изделия и конструкторской документации на него, новую технологию производства или иное техническое новшество, так и отдельные виды исследований, разработки и изготовления новшеств.

Договором установлен порядок привлечения исполнителем контрагентов для выполнения отдельных частей исследования и изготовления опытного образца, проведения испытания и сдачи-приемки работ. Стоимость работ при заключении договора устанавливается на основании соглашения о договорной цене научно-технической продукции и окончательно определяется по сметной калькуляции, составленной исполнителем. Требования к сторонам по соблюдению условий конфиденциальности аналогичны тем, которые изложены к предыдущему договору.

3) *Договор на передачу (тиражирование) научно-технической продукции*. Договор такого вида отчасти регулировался упомянутым выше Положением, утвержденным ГКНТ СССР, которым предусматривалась возможность многократной передачи научно-технической продукции по договорной цене, кроме продукции массового тиража. Сторонами по такому договору могли быть только юридические лица.

Особенностью этого договора, во-первых, является подтверждение передающей стороной своего права на ранее созданную научно-техническую продукцию. Это могут быть данные о регистрации НИОКР в установленном порядке, об источнике финансирования и т.д. Во-вторых, на передающую сторону возлагаются обязанности по авторскому надзору и сопровождению освоения данной продукции на объекте получающей стороны. В-третьих, заказчик может поручить передающей стороне работы по приспособлению объекта передачи к своим производственным условиям, что будет связано с увеличением стоимости передаваемой продукции.

Что касается тиражирования научно-технической продукции, то речь идет об этом же договоре в пользу третьих лиц. Заказчик в данном случае может поручить исполнителю произвести дополнительные усовершенствования или дооснащение тиражируемой продукции. Работы выполняются исполнителем на основании дополни-

<sup>1</sup> См.: СП СССР. Отдел первый. 1983. № 24; 1984. № 6. Ст. 31.

тельного соглашения за отдельную плату или установления надбавки к договорной цене, определяемой сторонами договора.

Договором предусмотрено условие, что заказчик обязан обеспечить конфиденциальность сведений, составляющих договорную цену на продукцию, косвенно вытекающих из отдельных отчетов, передаваемых исполнителем. Нужно отметить, что перечисленные выше виды договоров по-прежнему пользуются спросом на практике, хотя в ГК РФ правовое регулирование получили только договоры на НИОКР (ст. 38 ГК РФ).

Второй этап (с 80-х гг.) договорного регулирования был связан с широким внедрением в различные отрасли народного хозяйства электронно-вычислительной техники (ЭВМ), персональных компьютеров и программных средств (ПС) к ним. Появление машинной информации (МИ) и необходимость ее обработки с помощью программных средств ЭВМ потребовали разработки предложений по их правовой охране<sup>1</sup>, принятия специального законодательства и Федеральной целевой программы «Электронная Россия (2002–2010 гг.)», определившей направления и темпы информатизации общества, а также обеспечения конфиденциальности проводимых работ.

Исследования А.Е. Шерстобитова в 80-е годы позволили ему предложить научно обоснованную типизацию гражданско-правовых договоров в сфере информатики<sup>2</sup>, актуальность которой подтверждается современной практикой хозяйствующих субъектов; раскрыть особенности их содержания и наметить тенденции развития договорных отношений в этой сфере. По мнению А.Е. Шерстобитова, договоры в сфере творческой деятельности могут быть сгруппированы следующим образом.

1) *Договор на разработку и передачу программных средств.* Предметом этого договора являются отношения по выполнению НИР и ОКР, передача результатов заказчику, оказание научно-технических и информационных услуг, направленных на внедрение и обслуживание ПС. Договор урегулирован нормами ст. 769–778 ГК РФ и оформляется по усмотрению сторон с учетом ранее действовав-

<sup>1</sup> См.: Защита прав создателей и пользователей программ для ЭВМ и баз данных / Л.К. Терещенко, Е.К. Волчинская, Г.В. Виталиев и др. М., 1996, и др.

<sup>2</sup> См.: Шерстобитов А.Е. Вопросы гражданско-правового регулирования отношений по передаче программных средств ЭВМ // Вестн. Моск. ун-та. Сер. 11 «Право». 1983. № 2; *Он же.* Правовое регулирование договорных отношений в сфере информатики // Сб.: Право и информатика / Под ред. Е.А. Суханова. М., 1990. С. 24–40.

ших типовых форм<sup>1</sup>, регулировавших договоры в области научно-технического прогресса на создание и передачу научно-технической продукции.

В договоре должны быть предусмотрены условия по соблюдению прав разработчика на ПС с учетом нематериальной природы объекта. Это может быть установление запрета на внесение изменений в переданные ПС и передачу их третьим лицам без разрешения исполнителя, на разглашение сведений об эффективности использования ПС в определенных сферах с учетом конкурентоспособности. Изготовление и передача ПС могут осуществляться на основе договора поставки, включающего услуги потребителя ПС. Хотя, по соглашению сторон, информационное и консультационное обслуживание может быть предметом самостоятельного договора.

2) *Договор на оказание научно-технических услуг пользователям программных средств.* Поставляемые ПС включают программы на материальных носителях и эксплуатационную документацию. Состав программ указывается в приложении к договору на передачу ПС. Качество программной продукции подтверждается сертификатами. Договор заключается в целях обучения персонала заказчика работе на ЭВМ с установленными в организации новыми ПС.

Договорные отношения в сфере оказания услуг ранее регулировались названным выше постановлением ГКНТ СССР от 19 ноября 1987 г. № 435 и ведомственными нормативными актами. В настоящее время эти отношения урегулированы гл. 39 ГК РФ («Возмездное оказание услуг»).

Условия о конфиденциальности содержат требования о соблюдении сторонами режима информации, получаемой в ходе консультаций, включающей особенности хозяйственной ситуации заказчика в сфере использования установленных новых ПС и деловую информацию исполнителя.

3) *Договор на выполнение информационно-вычислительных работ (услуг).* Как отмечает А.Е. Шерстобитов<sup>2</sup>, договоры на выполнение информационно-вычислительных работ вычислительными центрами и на аренду ЭВМ имели широкое распространение в конце 70-х —

<sup>1</sup> См.: Положение о договорах на создание (передачу) научно-технической продукции. Постановление ГКНТ СССР от 19 ноября 1987 г. № 435.

<sup>2</sup> См.: Шерстобитов А.Е. Правовое регулирование договорных отношений в сфере информатики // Сб.: Право и информатика / Под ред. Е.А. Суханова. М., 1990. С. 35.

начале 80-х годов. Пользователям оказывались информационно-вычислительные услуги с предоставлением машинного времени ЭВМ (в тот период в основном использовались большие ЕС-ЭВМ и средние ЭСМ-4 машины), получившие название «машинная обработка» информации. Обработка информации пользователями могла осуществляться и по договору аренды ЭВМ либо проката программных средств.

По такому договору исполнитель обязан был предоставить пользователю работоспособные технические и программные средства в аренду и обеспечить выделение по графику машинного времени ЭВМ, в сроки и в объеме, согласованные между сторонами. Работа по обработке информации могла выполняться персоналом исполнителя либо пользователя. Стоимость услуги по обучению персонала пользователя дополнительно включалась в договорную цену. В большинстве случаев обработка информации производилась персоналом вычислительного центра (исполнитель), реже ЭВМ, и программное обеспечение предоставлялось в аренду, как правило, подведомственным предприятиям.

Конфиденциальность процессов обработки информации, накопление банка данных и формирование баз информационных массивов обеспечивались следующими условиями договора:

1) Исполнитель обеспечивает занесение на магнитные диски, хранение данных и программных средств в установленном режиме (архивный, страховой, дубликат); принимает меры по исключению несанкционированного доступа к данным пользователя; не вносит изменения в программные средства пользователя без его письменного разрешения; не передает программные средства третьим лицам без разрешения пользователя.

2) Пользователь назначает администратора банка данных, регулирующего вопросы ведения баз данных и режима их использования; письменно уведомляет исполнителя о праве доступа к информационным массивам третьих лиц; согласовывает со службами исполнителя средства защиты баз данных, кроме имен ключей; выполняет установленные исполнителем требования внутриобъектового режима.

В начале 90-х годов происходит массовое внедрение компьютерной техники на предприятиях. Надобность в таком роде услугах по выполнению информационно-вычислительных работ постепенно отпадает. Начиная с этого времени, появляется информационно-аналитический рынок в нашей стране. Актуальной становится проб-

лема информационного обеспечения предпринимателей и защита их интересов.

Третий этап (с 90-х гг.) связан с обособлением нового вида общественных отношений — информационных<sup>1</sup>, с освоением экономической информационного ресурса как товара<sup>2</sup>. Появление субъектов информации требовало от государства правового регулирования этих отношений. Были приняты ГК РФ, ряд законов и иных правовых актов, регулирующих оборот КЗИ и позволяющих предпринимателям защищать свои частные интересы с использованием условия конфиденциальности на договорной основе. Закрепление в части первой ГК РФ информации как полноправного объекта гражданских прав явилось основой формирования в нашей стране легального информационного рынка, в условиях которого происходит торговля информационными продуктами, выполняются работы по обработке информации, предоставляются информационные услуги пользователям. Коммерческие организации, располагая собственными информационными ресурсами, составляющими КЗИ, участвуют в информационном обмене на договорной основе.

Выявление особенностей развития данного этапа предполагает определение структуры информационного рынка и классификацию договоров, регулирующих обращение КЗИ.

**Формирование структуры и инфраструктуры информации — го рынка в России. Становление рыночных отношений в России требует формирования структурных информационных услуг и решения существующих инфраструктурных проблем.** Современный мировой информационный рынок, по мнению специалистов, включает четыре основные области: электронная информация (базы данных деловой, научно-технической, юридической, профессиональной и иной информации), электронные сделки с участием информационных посредников-брокеров, системы банковских операций, электронные торги и др. (внедрение электронного обмена данными в коммерческой деятельности подразумевает прямой ввод оформленного заказа в компьютер фирмы-производителя, что ускоряет процесс купли-продажи товаров, а также их оперативного производства

<sup>1</sup> См.: Право и информатика / Под ред. Е.А. Суханова. М., 1990. С. 5.

<sup>2</sup> См.: Бачило И.Л. Информационное право: основы практической информатики. М., 2003. С. 14 — 60.



и учета), системы сетевых коммуникаций и программное обеспечение (Интернет, технические информационно-вычислительные комплексы, программные и информационные системы, средства передачи данных, системы управления базами данных и др.), которые системно взаимосвязаны и обуславливают эволюционный переход государств к этапу постиндустриальной (информационной) цивилизации.

Названные области информационного рынка еще не получили должного развития в России, что подчеркивается в Доктрине информационной безопасности РФ. Охарактеризуем рынок деловой коммерческой информации. В начале перехода страны к рыночной экономике была разрушена ранее существовавшая система информационного обеспечения управления народным хозяйством, которая не была рассчитана на обслуживание легализованной предпринимательской деятельности. Предприятия вошли в рыночные отношения, не имея соответствующего этим отношениям рынка информационных услуг. Информационный рынок практически стал формироваться в России с нулевой отметки в 1991 г., тогда как в развитых странах он зародился в 60-х годах XX века,<sup>1</sup> а в 2000 г. соотношение стоимости информационных ресурсов, программного обеспечения и топливно-энергетического комплекса составляло в западных странах пропорцию 70:30<sup>2</sup>.

Действовавшая в советский период государственная информационная система, по существу, не занималась, кроме научно-технической сферы, сбором и анализом деловой коммерческой информации. Усилия хозяйственных органов управления были направлены в тот период на сбор отчетной информации о выполнении директив и решений партии и правительства. Поэтому с переходом на рыночные условия остро встал вопрос о сборе, получении и распространении коммерческой информации, необходимой для деятельности организаций.

Анализ спроса организаций на информацию показывает, что в 70% случаев постоянный интерес вызывает правосубъектность партнеров — юридических лиц, их надежность и честность в ведении

<sup>1</sup> См.: Родонов И.И. Мировой рынок информационных услуг: электронная деловая и коммерческая информация. М., 1992. С. 5–21.

<sup>2</sup> См.: Подберезкин А. Проблемы глобализации мира: взгляд слева // Независимая газета. 2001. 10 июня.

§ 3. Гражданско-правовое регулирование обращения коммерчески значимой информации

бизнеса. Особенно это является актуальным при установлении долговосрочных взаимоотношений, связанных с выполнением совместных работ. Однако со временем этих общих сведений о предприятии, его названии и видах деятельности, получаемых из справочников или баз данных, стало недостаточно.

Обоснованный выбор деловых партнеров, сопряженный с вложением капитала, требует получения более подробной информации об учредителях, руководителях организации, о владении ими пакетами акций, о структуре капитала фирмы и источниках его происхождения, о номенклатуре и объемах выпускаемой продукции по видам стоимости и натуральном выражении, численности основных категорий работающих и их профессиональном уровне, остаточной стоимости и износе основных производственных фондов, сведения о взаимоотношении с контрагентами при экспортных и импортных операциях и другие данные.

Ретроспективный анализ показывает, что необходимость в таких сведениях появилась при проведении чековой приватизации, когда для принятия решения требовалась более полная информация о приобретаемых предприятиях. Покупателей в данном случае интересовала информация о состоянии платежей в бюджет, расчетах с поставщиками и потребителями продукции, задолженность по зарплате, взаимоотношения с органами власти, наличие неиспользованных ресурсов. Прокатившиеся в стране банковские кризисы увеличили спрос на финансовую информацию о деятельности банковской системы, причем данные были необходимы в реальном режиме времени. С возникновением рынка ценных бумаг возникла необходимость в прогнозировании и анализе ситуации на фондовом рынке. Сегодня в период мирового финансового кризиса получение такой информации является весьма актуальной задачей. Эти данные можно было получить путем проведения аналитических и маркетинговых исследований.

**Спрос на ту или иную информацию способствовал формированию различных видов информационных ресурсов, становлению субъектов информационного рынка и инфраструктуры его обеспечения.** Информация, которая используется коммерческими организациями для принятия решений, может быть условно сгруппирована следующим образом.

*Первая группа — открытая, общедоступная информация, которую можно почерпнуть из деловых изданий и средств массовой информации.* В этой группе можно выделить справочную информацию специализи-

рованных агентств и служб новостей, электронные журналы; профессиональную информацию, включающую научно-техническую и деловую (документальную, реферативную, сведения в области фундаментальных и прикладных технических, естественных и общественных наук) информацию, а также информацию, находящуюся в библиотеках, в том числе электронных, и специализированных банках данных государственных и коммерческих структур. Названные сведения можно получить на рынке деловой литературы<sup>1</sup>. Большим спросом пользуются базы данных на CD-ROM, содержащие профессиональные узкоспециализированные издания. В разных формах широко представлены справочно-правовые продукты с известными марками «Консультант Плюс» и «Гарант». Значительный объем деловой информации предприниматели могут получить в сети Интернет. Действует ряд деловых информационных порталов для предпринимателей. Например, Российский деловой портал «Альянс-Медиа», объединяющий более 25 серверов (система межрегиональных центров, электронный торговый центр, деловые предложения, государственный заказ, деловая пресса, производители товаров и услуг, картах информации и др.).

*Вторая группа — это закрытая, недоступная информация, включающая техническую и технологическую информацию (в т.ч. ноу-хау) и деловую информацию.* Что касается технической и технологической информации, то ее основным источником являются полученные результаты выполнения НИОКР, которые в консолидированном виде передаются заказчику в виде научных отчетов, технической, технологической и конструкторской документации.

Однако не менее ценная часть такой информации сосредоточена в промежуточных отчетах подразделений, отделных документах, подготовленных исполнителями по конкретной тематике. Такие документы могут храниться в специальных хранилищах и архивах предприятий продолжительное время, а передача их в государственные архивы законодательством не предусмотрена.

*Деловая информация формируется с учетом опыта деятельности организации на конкретных ее направлениях.* Основная ее доля приходится на получаемые результаты маркетинговых исследований, содержащие экономические, финансовые и коммерческие сведения. Экономическая информация является результатом исследования

ний и консалтинга в виде прогнозных моделей и оценок. Финансовая информация — это данные о котировках ценных бумаг, тенденции валютного курса, учетных ставках, состоянии рынка товаров и капиталов, ценах и инвестициях. Коммерческая информация включает в себя данные о компаниях и направлениях их работы, ассортименте выпускаемой продукции, ценах, финансовом состоянии, хозяйственных связях, учредителях, руководителях, контрагентах, клиентах, о заключении договоров и исполнении обязательств, обслуживании кредитов и другие сведения, имеющие коммерческую значимость. Процесс обращения КЗИ вполне укладывается в рамки модели гражданского оборота открытой информации, однако ее оборот определяется субъектами по их разрешению с учетом существующей монополии лиц на такого рода информацию. Отсюда можно говорить об ограниченном обороте КЗИ. Условие конфиденциальности охраны КЗИ сопровождает весь жизненный цикл обращения такой информации: ее производство (создание), обработку, хранение, тиражирование, передачу, распространение, поиск, получение и потребление.

**Структура информационного рынка представляет собой совокупность звеньев, участвующих в производстве (создании), распространении и потреблении информации.** Гражданский оборот информации предполагает участие *создателя или производителя информации*, в результате интеллектуальной деятельности которого создается информация; *обладателя (держателя) информации*, который приобретает информационные правомочия по договору с создателем информации; *потребителя информации*, который является конечным получателем и пользователем информации<sup>1</sup>.

В зависимости от участия субъектов информационного рынка в процессах обращения КЗИ их можно подразделить на две группы. *Первая группа — это государственные и коммерческие структуры, специализирующиеся на накоплении первичных массивов информации.* Промышленные информационные продукты и услуг осуществляется путем организации доступа к данным с предоставлением возможности их выборки. К ним относятся издатели деловых справочников, держатели баз данных и другие. В эту группу входят структуры, которые форми-

<sup>1</sup> См.: Копылов В.А. О модели гражданского оборота информации // Российское право. 1999. № 9; Дозорцев В.А. Информация как объект исключительного права // Дело и право. 1996. № 4, и др.

<sup>1</sup> См: <http://top100.rambler.ru/top100/Literature/>.

руют вторичные информационные массивы. Результатом их деятельности являются создание электронных архивов по отдельным видам информации, обзоры рынка товаров и услуг, мониторинг законодательства и коммерческой практики по направлениям бизнеса.

Эти организации имеют мощные информационно-аналитические службы и работают с клиентами «под заказ» либо предлагают к продаже имеющуюся продукцию. Дальнейшее развитие телекоммуникаций в России в определенной мере связано с открытием доступа к ранее закрытым сетям. Важное место в структуре рынка принадлежит брокерам, приобретающим информационные продукты у производителей и обладателей информации и определяющим условия ее продажи.

*Вторая группа — это информационно-аналитические подразделения коммерческих организаций, работающие в интересах данной структуры.* Сбор, накопление КЗИ и производство информационных продуктов осуществляется в процессе научной, производственной и коммерческой деятельности.

Важными источниками такой информации являются результаты НИОКР, аналитических и маркетинговых исследований. Информация, имеющая коммерческую значимость, используется для собственных нужд организации и включается по мере необходимости в гражданский оборот при выполнении работ по кооперации путем передачи КЗИ (купля-продажа) и оказания услуг.

Итак, структуру рынка образуют две группы субъектов, взаимодействующих между собой и вступающих в договорные отношения по поводу оказания информационных услуг, выполнения работ в информационной сфере и возмездной передачи информационных продуктов.

Развитие структуры информационного рынка требует надежного обеспечения его *инфраструктуры*. Речь идет о создании развитой общероссийской телекоммуникационной инфраструктуры, обеспечивающей оперативную связь, использование электронной цифровой подписи и совершенствование мер по защите информации.

Компьютерный рынок в России начал формироваться в конце 80-х годов (фирма IBM в 1981 г. выпустила свой первый вариант персонального компьютера — IBM PC). С тех пор существенным образом изменился процесс сбора и обработки информации. Создание компьютерной инфраструктуры потребовало урегулирования новых информационных отношений. Позднее Интернет, вошедший в коммерческую практику в середине 90-х годов, породил иные правовые

проблемы, например, в регулировании деятельности электронных магазинов<sup>1</sup>, Интернет-трейдинга (имеется в виду связь инвестора с брокером через Интернет), платности и бесплатности информации в Интернет.

Важной составляющей компьютерной инфраструктуры является рынок программного обеспечения, в частности, для информационных систем предприятий. В специальной литературе выделяют: локальные системы, предназначенные для автоматизации одного или двух направлений деятельности организации; финансово-управленческие системы с расширенным диапазоном функциональных возможностей; средние и крупные интегрированные системы, выполняющие информационно-аналитические, учетные, контрольные, управленческие и производственные функции. Разработка этих систем и их совершенствование осуществляется зарубежными и отечественными производителями, которые широко представлены на российском рынке.

*Телекоммуникационные услуги* — важная часть инфраструктуры информационного рынка. Они представлены в России ведущими операторами сотовой связи: ОАО «Мобильные телесистемы» (МТС) и ОАО «Вымпелком» (торговая марка «Билайн»). Наиболее распространена, причем не только среди предпринимателей, является услуга службы коротких сообщений (SMS), которая придает мобильному телефону свойства пейджера. Новейшие информационные технологии позволяют использовать сотовый телефон в качестве мобильного модема. Уже сегодня через ноутбук можно выходить в Интернет в любой точке Москвы, в других городах и районах России и мира.

Важной составляющей частью информационного рынка является обеспечение защиты информации с использованием новейших технологий. Этому вопросу в специальной литературе уделяется достаточно много внимания<sup>2</sup>. Проблемы возникают с обеспечением электронного бизнеса, требующего серьезного подхода к управлению уровнем риска. Организации в зависимости от их финансовых возможностей сами занимаются внедрением технологий либо пользуются услугами

<sup>1</sup> См.: <http://topshop.gambler.ru>, и др.

<sup>2</sup> См.: Герасименко В.А., Малюк А.А. Основы защиты информации. М., 1997. С. 418–499; Ярошкин В.И. Безопасность информационных систем. М., 1996. С. 205–290, и др.

внешних организаций по обеспечению безопасности корпоративных информационных систем.

Кроме использования традиционных систем безопасности, связанных с реализацией мер технического, программного, организационно-правового характера, используются *возможности страхования электронных рисков*. Понятием электронных рисков охватываются не только атаки хакеров и распространение вирусов, но и неправомерные действия работников организации, по вине которых чаще всего и наступают ощутимые потери. Если на Западе такой вид страхования получил признание, прежде всего, со стороны финансовых институтов, охотно покупающих страховки от электронных рисков, то в нашей стране ему не уделяется должного внимания. Российские страховые компании не развивают этот вид страхования, поскольку крайне низок спрос страхователей на эту услугу. Этим, пожалуй, можно объяснить тот факт, что только отдельные ведущие страховые компании имеют лицензии на страхование электронных рисков.

Страхование электронных рисков связано с потерей или порчей нематериального ресурса-информации, что затрудняет процесс оценки риска. Возмещение по электронным страховым случаям имеет свою особенность. Страховая компания оплачивает страхователю только прямой ущерб, связанный с затратами на реализацию электронного архива, без учета упущенной выгоды. Это объясняется отсутствием единой методики расчета стоимости информации, разглашение (утечка) которой приводит, например, к уменьшению числа потенциальных покупателей продукции.

**Классификация договоров в сфере обращения КЗИ.** Отдельная классификация договоров в сфере обращения КЗИ ранее не предпринималась. Она может быть осуществлена на основе общей классификации, принятой в гражданском праве, выделения договоров в предпринимательском и коммерческом праве, а также в зависимости от согласованного сторонами целевого назначения информации по ее получению, использованию, передаче и охране конфиденциальности.

Договорные отношения в информационной сфере, подчиняясь в целом общим закономерностям правового регулирования гражданского оборота, обладают определенной *спецификой*<sup>1</sup>, вытекающей из

<sup>1</sup> См.: Шерстобитов А.Е. Гражданско-правовое регулирование обязательств по передаче информации. М., 1980. С. 24–27.

свойств информации как особого объекта гражданских правоотношений, о чем справедливо пишут большинство ученых, специализирующихся в этой области научных знаний. Поэтому при конструировании договорных связей между субъектами нужно учитывать особенность информации в обороте:

информация представляет собой идеальный объект, она не может быть объектом правоотношений безотносительно к ее материальным носителям — физическим объектам (отдельные документы и массивы документов в информационных системах и др.) либо к связанным передающим и принимающим устройствам;

категории владения, пользования и распоряжения, характерные для классического права собственности, неприменимы к КЗИ, поэтому можно лишь говорить об относительных, а не абсолютных правах сторон при актах купли-продажи информационных продуктов и применять, по предложению В.А. Дозорцева, термины «обладание, использование и передача»<sup>1</sup>;

объектом договорных отношений обычно выступает информация, имеющая коммерческую ценность, и в этой связи доступ к ней ограничен ее обладателем и осуществляется только с его согласия; информация, создаваемая в рамках патентного и авторского права, не входит в группу информационных отношений и относится к самостоятельному виду объектов гражданских прав;

КЗИ, являясь предметом договорных отношений, включает технологическую и техническую (ноу-хау), коммерческую (деловую) информацию, составляющую секрет фирмы, и в этих случаях регулируется институтом коммерческой тайны.

Договор в информационной сфере как источник обязательных правил для сторон, реализует функцию защиты гражданских прав на КЗИ. Принцип свободы договора в гражданском праве позволяет участникам самостоятельно регулировать отношения по поводу охраны конфиденциальности КЗИ путем заключения договора. Для выбора его модели в целях защиты своих частных интересов стороны могут использовать как поименованные в ГК РФ договоры, так и непоименованные, но не противоречащие общим началам и смыслу гражданского законодательства.

<sup>1</sup> См.: Дозорцев В.А. Законодательство и научно-технический прогресс. М., 1978. С. 22–23.

В *гражданском праве* традиционно выделяются такие типы договоров, как договоры, направленные на передачу имущества в собственность (или иное вещное право) либо в пользование, на производство работ или на оказание услуг. Такое деление договоров составляет их «*базовую*» *общую классификацию*, отраженную в системе второй части ГК РФ, где они представлены в виде четырехленной типизации договорных обязательств по отчуждению имущества (гл. 30–33), по передаче его в пользование (гл. 34–36), по производству работ (гл. 37–38) и по оказанию услуг (гл. 39–53). На этой основе по различным юридическим критериям выделены отдельные виды и подвиды договоров. Нормы, регулирующие информационную сферу, включая обращение КЗИ, не содержатся в какой-либо отдельной главе ГК РФ, кроме секрета производства (ноу-хау), а рассредоточены в различных видах обязательств. В этой связи нужно отметить, что в части четвертой ГК РФ в рамках интеллектуальной собственности (исключительные права) в главе 75 за обладателем закрепляется исключительное право на секрет производства (ноу-хау) до тех пор, пока сохраняется конфиденциальность составляющих его содержание сведений. Гражданский оборот секрета производства регулируется договором об отчуждении исключительного права на секрет производства и лицензионным договором о предоставлении права на секрет производства и использовании секрета производства. Закон не требует регистрации исключительного права на такой секрет, но требует от обладателя введения режима коммерческой тайны для таких сведений. Кроме того, часть четвертая ГК РФ регулирует право использования результатов интеллектуальной деятельности в составе единой технологии (гл. 77) и закрепляет за лицом, создавшим или организовавшим ее создание право вводить в отношении соответствующей информации режим сохранения тайны. В данном случае установление и обеспечение режима коммерческой тайны в отношении секрета производства (ноу-хау) и единой технологии является составной частью предмета настоящего исследования.

В отдельных отраслях частного права с учетом предмета их правового регулирования разработаны свои подходы к классификации договоров. В *предпринимательском праве* классификация договоров проводится, в *одном случае*, «исходя из содержания предпринимательской деятельности» (абз. 3 п. 1 ст. 2 ГК РФ) соответственно выделяются предпринимательские договоры по продаже (реализации) товаров, передаче имущества в пользование, выполнению (производ-

ству) работ, оказанию услуг и некоторые другие<sup>1</sup>. Во *втором случае*, критерием систематизации является учет предпринимательских целей. Как отмечает О.А. Макарова, «договоры можно систематизировать по следующим видам: договоры, преследующие целью передачу имущества в собственность, преследующие целью передачу имущества в пользование, имеющие целью выполнение работ или оказание услуг, имеющие целью посредничество (представительство)»<sup>2</sup>. Как видно из сопоставления регулирования деятельности в предпринимательских целях, приведенные выше подходы к классификации предпринимательских договоров мало чем отличаются, кроме субъ-ектного состава сторон, от общей классификации договоров в гражданском праве.

Отдельные виды договоров, поименованные в ГК РФ и относимые представителями предпринимательского права к числу предпринимательских, имеют непосредственное отношение к сфере обращения КЗИ. В их числе следует назвать: договор купли-продажи (это может быть договор передачи коммерческой информации, который не поименован ГК РФ), договор подряда (конфиденциальность полученной сторонами информации — ст. 727 ГК РФ), договор на выполнение научно-исследовательских, опытно-конструкторских и технологических работ (конфиденциальность сведений, составляющих предмет договора, — ст. 771 ГК РФ), договор возмездного оказания услуг (услуги в различных сферах, предусмотренные ст. 779 ГК РФ с использованием КЗИ), договор банковского счета (банковская тайна — ст. 857 ГК РФ, может рассматриваться по отношению к банку как разновидность КЗИ), договор коммерческой концессии (использование и охрана конфиденциальности КЗИ — ст. 1027, 1032 ГК РФ), договор простого товарищества (вклад товарища в общее дело, в том числе профессиональные и иные знания, навыки и умения — ст. 1042 ГК РФ, которые могут содержать КЗИ, а также охрана их конфиденциальности).

В *современном коммерческом праве* разработана и научно обоснована классификация торговых договоров<sup>3</sup>. В качестве общих кри-

<sup>1</sup> Предпринимательское право Российской Федерации: Учебник / Отв. ред. Е.П. Губин, П.Г. Лахно. М., 2004. С. 924.

<sup>2</sup> Коммерческое право: Учебник. В 2 ч. / Под ред. В.Ф. Попондопуло, В.Ф. Яковлевой. 3-е изд. М., 2002. Ч. 1. С. 302.

<sup>3</sup> См.: *Лугинский Б.И.* Коммерческое право России: Учебник. 2-е изд. М., 2006. С. 118–121, 247–251.

териев для выделения договоров коммерческого права Б. И. Пугинский называет: «1) связь с торговым оборотом, процессом продвижения товаров от изготовителей к потребителям; 2) наличие хотя бы с одной стороны субъекта, действующего в качестве предпринимателя (коммерческой организации); 3) возмездный характер, наличие экономического интереса у каждой из сторон». С учетом предмета и метода коммерческого права выделены четыре группы договоров: реализационные, посреднические, содействующие торговле и организационные договоры.

В числе названных торговых договоров непосредственное отношение к сфере обращения КЗИ имеют договоры на проведение маркетинговых исследований, на предоставление коммерческой информации, непоименованные в ГК РФ (в этом подвиде выделены договоры на оказание информационных услуг; передачу информации, опосредованную договором купли-продажи; переработку информации), и договоры коммерческой концессии, отнесенные к группе договоров, содействующих торговле.

Классификация договоров, принятая в частном праве, имеет методологическое значение для выделения договоров в информационной сфере, включая обращение КЗИ. Анализ договорной практики организаций показывает, что в большинстве случаев информационные отношения в гражданском обороте регулируются с помощью договоров на оказание информационных услуг, реже с помощью договоров подряда на выполнение работ. Договор на выполнение НИОКР практически не претерпел существенных изменений с советского периода относительно соблюдения требований конфиденциальности.

Договор купли-продажи информационных продуктов, за исключением купли-продажи технических систем накопления и обработки информации на ЭВМ, информационных технологий, практически не используется. Причина кроется в несовершенстве действующего законодательства, регулирующего информационные отношения, непонимании участниками рынка сущности информации и недооценке ее коммерческой значимости.

Вместе с тем функционирование рынка требует *определения видовой принадлежности договоров, предназначенных для регулирования отношений в информационной сфере. Первую группу* образуют договоры на оказание информационных услуг, которые следует признавать традиционными и общепризнанными. Этот вид договора повсеместно используется участниками рыночных отношений. *Вторую группу* со-

ставляют договоры на выполнение работ в информационной сфере, связанные с проведением маркетинговых исследований, анализом и обработкой информации на ЭВМ и другие. *Третью группу* образуют договоры, касающиеся возмездной передачи информационных продуктов. К их числу относятся договоры купли-продажи и поставки информационных продуктов.

Анализ особенностей использования и защиты закрытой информации в структуре информационного рынка позволил сформулировать подход к *типизации договоров в сфере обращения КЗИ*, в основе которого лежат критерии их отграничения от общегражданских, предпринимательских и торговых договоров, а также сходства с договорами, регулирующими информационные отношения, формирующиеся под влиянием следующих факторов.

1) Связь договоров в сфере обращения КЗИ с общей и частными классификациями договоров, принятыми в частном праве.

2) Отношение договоров, регулирующих сферу обращения КЗИ, как части и целого процесса договорного регулирования информационной сферы коммерческих организаций.

3) Идентичность подходов к классификации договоров, которые предložены наукой частного права, выработаны практикой регулирования информационных отношений и обращения КЗИ.

4) Связь этапов цикла производства и реализации товара с этапами использования КЗИ, обуславливающая степень необходимости соблюдения условий охраны ее конфиденциальности.

5) Субъектный состав договорных отношений по поводу КЗИ представлен коммерческими организациями или индивидуальными предпринимателями, которые устанавливают (производители — обладатели такой информации) или приобретают по договору (контроленты) фактическую монополию на КЗИ, охраняемую в режиме «коммерческой тайны».

6) Договоры в сфере обращения КЗИ заключаются ограниченным числом работников организации. Данные о коммерческих переговорах и фактах заключения договоров, как правило, не публикуются в открытой печати. Такая информация может быть общедоступной только по согласению сторон и в их интересах. К исполнению обязательств, связанных с раскрытием КЗИ, допускаются отдельные работники, а не весь персонал подразделений, занятых договорной работой.

Таким образом, договорные отношения сторон, осложненные элементом соблюдения условия конфиденциальности, отражают спе-

цифику их регулирования при обращении КЗИ. Причем условие конфиденциальности, по усмотрению сторон, в различной степени сопровождает договорный процесс производства и реализации товаров (работ, услуг), в зависимости от целей и объема использования КЗИ.

На основании изложенного можно сделать вывод о *формирующихся определенных видах договорных отношений в сфере обращения КЗИ*. Их существование обусловлено действием названных выше факторов. *Первая группа договоров*, предметом которых является получение (создание, производство) КЗИ технического и технологического характера и коммерческого (делового) характера. Таковы договоры на выполнение научно-исследовательских, опытно-конструкторских и технологических работ, на проведение маркетинговых исследований. *Вторая группа* — это договоры на передачу информационный продуктов, содержащих КЗИ. Это договоры на передачу секрета производства (ноу-хау) и коммерческой (деловой) информации. *Третья группа* составляют договоры на оказание возмездных информационных услуг (консультативное и техническое содействие, юридический консалтинг и др.) с использованием сведений, составляющих КЗИ. Имеется, на наш взгляд, и *четвертая группа договоров*, которая носит комплексный характер. Системообразующим договором в этой группе является договор коммерческой концессии. В рамках этого договора правообладатель предоставляет пользователю возможность использования КЗИ. В этих целях он передает (купля-продажа) ему документацию технического и коммерческого характера, осуществляет информационное (консультативное и техническое содействие) обслуживание. Самостоятельное значение при обращении КЗИ имеет договор о соблюдении конфиденциальности информации, заключаемый организациями по их усмотрению на любой стадии договорного процесса.

Характеристика названных групп договоров может быть получена путем анализа содержания и порядка согласования с контрагентом условий по охране конфиденциальности КЗИ.

#### § 4. Формирование договорных условий об охране конфиденциальности информации

*Сущность определения договорных условий по охране конфиденциальности информации.* Механизм использования гражданско-право-

вых средств при обращении КЗИ включает признаки, раскрывающие содержание и порядок согласования с контрагентами условий конфиденциальности. Выработка сторонами условий любого договора в сфере обращения КЗИ связана с охраной конфиденциальности сведений, которые могут представлять, по их мнению, интерес для третьих лиц, не имеющих к ним доступа на законных основаниях. Закон о коммерческой тайне не содержит требования к сторонам о том, что в договоре должны быть определены условия охраны конфиденциальности информации. ГК РФ применительно к договорам подряда, на выполнение НИОКР и др. не раскрывает содержание таковых условий. В цивилистической теории условия о конфиденциальности информации практически не разработаны, за исключением договоров на выполнение НИОКР<sup>1</sup> и маркетинговых исследований<sup>2</sup>. Тем не менее, как показывает анализ выборочного исследования, на практике повсеместна тенденция включения в договор условия о конфиденциальности информации, без расшифровки его содержания и формулирования иных условий, обеспечивающих исполнение этого обязательства. Это условие чаще всего помещают в раздел «Дополнительные условия» договора. В соответствующих разделах договора не определены способы защиты прав на КЗИ и ответственность за нарушение обязательств по охране КЗИ.

Методика формирования условия о конфиденциальности информации в литературе не разработана. Хотя по всем поименованным и большей части непоименованным в ГК РФ договорам имеются методики определения договорных условий<sup>3</sup>. Нужно выделить методику формирования условий договора поставки продукции, разработанную И.Г. Вахниным<sup>4</sup>, однако в ней не раскрыты условия конфиденциальности на этапах преддоговорных контактов, заключения договора и исполнения обязательств.

Сложившееся положение о регулировании условия конфиденциальности информации в законодательстве, теории и на практике не

<sup>1</sup> См.: Гражданское право: Учебник. Т. II. Полутом 1 / Отв. ред. Е.А. Суханов. 2-е изд. М., 2000. С. 611—617, и др.

<sup>2</sup> См.: *Измайлова Е.В.* Правовое регулирование маркетинга. М., 2002. С. 116—117, и др.

<sup>3</sup> См.: *Брагинский М.И., Витрянский В.В.* Договорное право. В 4-х т. М., 2000—2005.

<sup>4</sup> См.: *Вахнин И.Г.* Формирование условий и заключение договора поставки продукции // *Хозяйство и право*. 1996. № 9, 11, 12; 1997. № 1, 2, 3.

способствует защите частных интересов сторон. Особенно это происходит в случаях разглашения (утечки) КЗИ, когда практически стороны оказываются беззащитными, поскольку ими предварительно не был согласован механизм использования гражданско-правовых средств защиты.

В цивилистической науке разработано общее понятие договорных условий. По мнению М.И. Брагинского, «договорные условия представляются собой способ фиксации взаимных прав и обязанностей<sup>1</sup>. Господствующим в науке гражданского права является мнение о «трехчленном делении договорных условий» на существенные, обычные и случайные<sup>2</sup>. Их содержательный анализ дается в работах О.С. Иоффе, И.Б. Новицкого, З.Г. Крыловой, Р.О. Халфиной, Б.И. Пугинского, Е.А. Суханова и др. ученых. Критика взглядов ученых-цивилистов по вопросу разграничения названных договорных условий подробно рассматривается в названной работе М.И. Брагинского и В.А. Витрянского.

Под существенными понимаются те условия, которые непосредственно установлены п. 1 ст. 432 ГК РФ. Это, во-первых, названные в законе или иных правовых актах как существенные (для всех договоров таким условием является предмет договора); во-вторых, названные в законе или иных правовых актах как необходимые для договоров данного вида; в-третьих, условия, относительные которых по заявлению одной из сторон должно быть достигнуто соглашение.

Как отмечает Е.А. Суханов, «законодательство не использует понятия обычных и случайных условий»<sup>3</sup>, они используются лишь «в теоретической и учебной литературе»<sup>4</sup>. По его мнению, «условия, включенные в договор по желанию сторон, называются случайными, противопоставляя их условиям обычным, которые вообще не согласуются сторонами, но входят в содержание их договорного обязательства»<sup>5</sup>.

По мнению О.С. Иоффе, наличие или отсутствие обычных и случайных условий не оказывает никакого влияния на факт заключения договора. Объясняя свою позицию, О.С. Иоффе отмечал: «Более того, практически нет необходимости включать обычные условия в договор, так как они сформулированы в законе или иных нормативных актах и, поскольку контрагенты согласились заключить данный договор, они тем самым признаются выразившими согласие подчиниться тем условиям, которые по закону распространяются на договорные отношения соответствующего вида или на все договоры вообще. Наконец, как случайные должны рассматриваться условия, которые тоже «не имеют значения для заключения договора. Но если обычные условия предусматриваются законом и потому вступают в действие в силу одного только факта заключения договора, то случайные условия могут возникнуть и приобрести юридическое действие только в том случае, что они будут включены в самый договор»<sup>1</sup>.

Более практичным и хорошо понятным для хозяйствующих субъектов является предложенный Б.И. Пугинским подход к порядку определения условий договоров. Он наряду с существенными выделяет предписываемые, инициативные и отсылочные условия<sup>2</sup>. Гражданско-правовая доктрина относит к числу иных условий договора<sup>3</sup> — предписываемые законом («необходимость включения которых в текст договора предусмотрена законодательством»<sup>4</sup>) и инициативные («...не упоминаемые в законодательстве о договорах данного вида. Включение их в соглашение определяется усмотрением контрагентов»<sup>5</sup>). В последующих работах Б.И. Пугинский уточняет свою позицию. Он пишет: «В любом договоре можно выделить два вида условий: прямые (вырабатываемые самими сторонами) и подразумеваемые. Подразумеваемые условия входят в договор из закона, иных правовых актов и обычаев делового оборота. Подразумеваемые условия не записываются в текст договора, ибо они и так обя-

<sup>1</sup> Цит. О.С. Иоффе по кн.: Брагинский М.И., Витрянский В.В. Договорное право. Книга первая. 2-е изд. С. 297.

<sup>2</sup> См.: Гражданское право. Учебник. В 2-х т. Т. 2 / Под ред. проф. Е.А. Суханова. М., 1994. С. 49–51.

<sup>3</sup> См.: Гражданское право. Т. II. Полумтом I / Отв. ред. проф. Е.А. Суханов. 2-е изд. М., 2000. С. 165.

<sup>4</sup> Гражданское право. Т. 2. М., 1994. С. 50.

<sup>5</sup> Там же.

<sup>1</sup> Брагинский М.И., Витрянский В.В. Договорное право. Книга первая: Общие положения. 2-е изд. М., 2005. С. 295.

<sup>2</sup> См.: Там же. С. 295–296.

<sup>3</sup> Гражданское право. Т. II. Полумтом I / Отв. ред. проф. Е.А. Суханов. 2-е изд., М., 2000. С. 166.

<sup>4</sup> Там же. С. 165.

<sup>5</sup> Там же.



зательны для сторон»<sup>1</sup>. По мнению Б.И. Пугинского, важно уделить внимание второй группе условий — прямым, которые вырабатываются самими сторонами. При этом необходимо учитывать «способы воздействия закона на усмотрение договорных контрагентов при выработке таких условий»<sup>2</sup>. Можно выделить ряд принципиальных положений, раскрывающих суть этих способов<sup>3</sup>: 1) закон может предписывать сторонам выработать определенные условия, не касаясь их содержания, с использованием для этих целей управомочивающих норм; 2) закон нередко предусматривает договорные условия в диспозитивном виде, что предполагает возможность выработки сторонами любой формулировки такого условия, в противном случае будет действовать условие, содержащееся в диспозитивной норме; 3) правовые нормы нередко предусматривают альтернативные варианты условий договора или рассчитаны на конкретизацию их содержания самими сторонами.

Названные положения использованы в качестве базовых при определении содержания условий по охране конфиденциальности КЗИ, которые имеют определенную специфику по сравнению с другими договорными условиями.

Как уже отмечалось ранее, в сфере обращения КЗИ могут быть заключены различные виды договоров. Поэтому имеет смысл проанализировать процесс формирования условия о конфиденциальности информации применительно к различным группам договоров, заключаемых при обращении КЗИ. При этом речь пойдет о прямых (вырабатываемых самими сторонами) условиях, их содержания и порядке согласования. Тем более что результаты обобщения и анализа практики реализации правового усмотрения лежат в основе изменений, которые так необходимы для науки частного права.

Процесс правового регулирования договоров включает различные этапы, характеризующие порядок заключения и исполнения сторонами принятых на себя обязательств, а также ответственность за неисполнение таких обязательств. Договоры, заключаемые в сфере обращения КЗИ, имеют в этом плане определенные особенности, которые необходимо учитывать при формулировании условий охраны конфиденциальности такой информации.

<sup>1</sup> Пугинский Б.И. Коммерческое право России: Учебник. 2-е изд. М., 2006. С. 179.

<sup>2</sup> Там же. С. 179.

<sup>3</sup> См.: Там же. С. 178–181.

Во-первых, при формировании условий любого договора в сфере обращения КЗИ важно учитывать основные виды отношений по передаче информации, которые принято делить на две группы: 1) «отношения по передаче информации, опосредуемые специальными договорами, в которых передача информации является их предметом; 2) отношения по передаче информации, возникающие в процессе возникновения и развития договорных отношений, направленных на регулирование передачи вещей, выполнения работ и оказания услуг»<sup>1</sup>.

Каждая из этих групп, как подчеркивает А.Е. Шерстобитов, регулируется соответствующей группой гражданско-правовых обязательств: первая — договорами на передачу информации (*такими применительно к сфере обращения КЗИ являются непоименованные в ГК РФ договоры на передачу коммерческой информации и др.* — Прим. авт.), вторая — обязательствами по передаче информации в гражданско-правовых договорах (*все остальные договоры в сфере обращения КЗИ.* — Прим. авт.)<sup>2</sup>. Применительно к названным группам договоров критериями, лежащими в основе общих требований, предельными к формированию содержания условия о конфиденциальности, являются следующие:

стороны берут на себя обязательство принимать необходимые предупредительные меры, исключающие разглашение (утечку) КЗИ в процессе ее использования при производстве и реализации товаров (работ, услуг);

полученные по договору документы и изделия, содержащие КЗИ, будут рассматриваться сторонами как строго конфиденциальные; стороны обязуются не передавать без предварительного согласия другой стороны оригиналы (копии) документов или изделий третьей стороне;

стороны обязуются обеспечить ознакомление с КЗИ ограниченного числа работников, путем заключения с ними соглашения в рамках трудовых отношений о неразглашении такой информации.

По соглашению сторон нарушение таких требований может явиться основанием для расторжения договора (п. 1 ст. 450 ГК РФ). В договоре стороны определяют конкретные нарушения сохранения

<sup>1</sup> См.: Шерстобитов А.Е. Гражданско-правовое регулирование обязательств по передаче информации: Дисс. канд. юрид. наук. М., 1980. С. 18.

<sup>2</sup> См.: Там же. С. 41.

сти КЗИ, процедуру их документального подтверждения и порядок принятия решения о расторжении договора.

*Во-вторых, заключению любого договора предшествуют преддоговорные контакты сторон*<sup>1</sup>. Это начальный и самый важный этап, требующий повышенного внимания к охране конфиденциальности информации. На этом этапе, как свидетельствуют данные анализа, отдельные организации заключают с партнерами договоры о неразглашении конфиденциальной информации. В рамках этого договора осуществляется регулирование всех последующих взаимоотношений партнеров. Особенно это важно в случаях намерения сторон об установлении долгосрочных договорных отношений. Дополнительно к этому договору стороны могут разработать и согласовать Положение об обеспечении конфиденциальности информации, регулирующее их отношения на весь период действия договора.

*В-третьих, на этапе согласования и заключения договоров стороны выработывают общие критерии, определяющие порядок обеспечения конфиденциальности информации при выполнении совместных работ (НИОКР, маркетинговые исследования); передаче информации (КИ), новых продуктов (передача ноу-хау, коммерческой информации (КИ), передача информации, содержащейся в базе данных, переработка КИ); оказании возмездных информационных услуг (консультационное и техническое содействие, юридический консалтинг и др.).* Определенная специфика присуща формированию условий охраны КЗИ для договора коммерческой концессии. В данном случае нужен комплексный подход, учитывающий, что по этому договору одновременно осуществляется передача КЗИ, выполняются работы и оказываются услуги с использованием такой информации, и предоставляются услуги от формы КЗИ (техническая, технологическая и коммерческая информация) различать производственный, торговый и иные виды франчайзинга<sup>2</sup>.

Каждая из названных групп договоров в сфере обращения КЗИ имеет свою специфику в части обеспечения конфиденциальности информации. Наиболее сложный порядок, отличающийся объемом мер обеспечения конфиденциальности информации, устанавли-

<sup>1</sup> См.: Соловьев Э.Я. Искусство проведения переговоров. М., 2006. С. 6–88, и др.

<sup>2</sup> См.: Авшилов Г.Е. Коммерческая концессия // Гражданский кодекс Российской Федерации. Ч. 2 / Под ред. О.М. Козырь, А.Л. Маковского, С.А. Хохлова. М., 1996. С. 551, и др.

ливается при выполнении НИОКР. Стороны в соответствии с п. 1 ст. 771 ГК РФ, если иное не предусмотрено договором, обязаны обеспечить конфиденциальность сведений, касающихся предмета договора, хода его исполнения и полученных результатов. Стороны до заключения договора на этапе согласования технического задания определяют объем сведений, признаваемых конфиденциальными, разрабатывают и согласовывают меры по охране конфиденциальности информации. Это могут быть самые различные по названию и содержанию документы, которые после подписания договора являются его неотъемлемой частью. Чаще всего на практике стороны используют такие документы, как: совместное заключение организации о наличии условий обеспечения конфиденциальности информации при проведении контрагентских работ, план мероприятий или единый план (в случаях, когда несколько контрагентов) и другие документы по охране КЗИ.

Кроме того, стороны составляют, как правило, протокол проверки наличия у контрагента условий по охране КЗИ.

Названные документы, выработанные правовой практикой, могут быть использованы по усмотрению сторон в том или ином виде для обеспечения конфиденциальности любой группы договоров, заключаемых в сфере обращения КЗИ. Содержание этих документов, точно так же, как и их использование, зависит от специфики предмета конкретного вида договора.

*В-четвертых, на этапе исполнения обязательств стороны могут разработать совместные методические документы о проверке соблюдения условия конфиденциальности при выполнении НИОКР, использования переданной по договору КЗИ; определить процедуру разрешения споров в случаях разглашения (утечки) КЗИ и возможности их рассмотрения помимо арбитражного суда, в третейском суде при наличии третейской оговорки в договоре и заключении соглашения о передаче дела в такой суд; согласовать методику расчета возмещения убытков и процедуру их доказывания.*

Формирование условий о конфиденциальности применительно к различным группам договоров, регулирующих сферу обращения КЗИ, имеет определенные особенности.

*Первая группа — это договоры на выполнение НИОКР и проведение маркетинговых исследований.* В литературе, посвященной правовому регулированию договоров на выполнение научно-исследовательских, опытно-конструкторских и технологических работ в советский пери-

од<sup>1</sup> и в настоящее время<sup>2</sup>, не уделяется должного внимания раскрытию конфиденциальности, которая, по мнению М.И. Брагинского, «внутренне присуща рассматриваемым договорам»<sup>3</sup>.

Как правильно подчеркивает Л.А. Трахтенгерц: «Обязанности сторон по обеспечению конфиденциальности относятся на практике к одним из основных договорных обязательств. Результаты НИОКР не могут быть иначе защищены от незаконного использования третьими лицами»<sup>4</sup>.

Нужно отметить, что в советский период защита результатов НИОКР, ход их выполнения обеспечивались с помощью государственной системы режима секретности. Ученые-экономисты<sup>5</sup> отмечают, что НИОКР были ориентированы преимущественно на военнотехнический комплекс и связанные с ним отрасли. Вследствие этого гражданские отрасли, связанные с насыщением рынка высокотехнологичными товарами, существенно отставали от требований мирового рынка и выпускали неконкурентоспособные товары.

С началом экономических реформ система планирования и финансирования НИОКР в России прекратила свое существование. Государство оказалось определять политику в этой сфере. Обязанности инновационного развития были возложены на бизнес. Однако предприниматели занимались делом государственной собственности<sup>6</sup>. По данным на 2001 г., финансово-промышленные олигархические группы контролировали шестую часть внутренних активов страны<sup>7</sup>. Надежды государства, что коммерческие организации сами

будут вести НИОКР за счет своих средств, не оправдались. Бизнес перестал заниматься не только базисными, но и улучшающими инновациями. Причинами этого были инфляция, неплатежи, налоговый пресс, давление мафиозных структур<sup>1</sup>.

В настоящее время положение несколько улучшилось. Постановлением Правительства РФ от 21 августа 2001 г. № 605 (в ред. от 12 октября 2004 г. № 540) была принята Федеральная целевая научно-техническая программа «Исследования и разработки по приоритетным направлениям развития науки и техники» на 2002—2008 г. и до 2020 г. В рамках этой программы организациями России независимо от их организационно-правовых форм выполняются открытые НИОКР. Государственные заказы размещаются на конкурсной основе в соответствии с действующим порядком организации закупки товаров, работ и услуг для государственных нужд. Решение о выполнении НИОКР в инициативном порядке принимается коммерческими организациями с учетом условий рынка сбыта. Финансирование инвестиционных проектов осуществляется Российской Федерацией и ее субъектами за счет бюджетных средств. Создана сеть венчурных фондов. Работы ведутся в научно-промышленных центрах, наукоградах с участием государственных предприятий и коммерческих организаций при обязательном учете их специфики и потенциала. При выполнении НИОКР по госзаказу и заказу конкретного потребителя заключается государственный контракт (договор) и разрабатывается техническое задание на выполняемые работы. Заказчиком НИОКР, выполняемых в рамках названной Программы, является Министерство образования и науки РФ.

Государством в последние годы увеличено количество заказов на вооружение и военную технику, создание которых требует проведения фундаментальных и прикладных НИР. Правовое регулирование порядка формирования, размещения и исполнения на контрактной основе заказов на выполнение НИОКР для федеральных государственных нужд осуществляется на основании ФЗ от 13 декабря 1994 г. № 60-ФЗ «О поставках продукции для федеральных государственных нужд»<sup>2</sup> и ФЗ от 6 мая 1999 г. № 97-ФЗ «О конкурсах на размещение заказов на поставки товаров, выполнение работ, оказание услуг

<sup>1</sup> См.: *Барабаш Я.Б.* Договоры на выполнение научно-исследовательских и конструкторских работ. М., 1962; *Ринг М.П.* Договоры на научно-исследовательские и конструкторские работы. М., 1967; *Азиев Ч.Н.* Договоры на научно-исследовательские и опытно-конструкторские работы. Харьков, 1976, и др.

<sup>2</sup> См.: Гражданское право: Учебник. В 2 т. Т. II. Полуптом 1/ Отв ред. проф. Е.А. Суханов. 2-е изд., М., 2000. С. 611—622; *Брагинский М.И., Витрянский В.В.* Договорное право. Книга третья: Договоры о выполнении работ и оказании услуг. М., 2005. С. 203—204, и др.

<sup>3</sup> См.: *Брагинский М.И., Витрянский В.В.* Указ. соч. С. 203.

<sup>4</sup> См.: Комментарий к ГК РФ, части второй (постатейный). М., 1996. С. 340.

<sup>5</sup> См.: *Кузык Б.Н., Яковец Ю.В.* Россия — 2050. Стратегия инновационного прорыва. М., 2005. С. 438—440.

<sup>6</sup> См.: *Меньшиков С.М.* Анатомия российского капитализма. М., 2004. С. 138—142.

<sup>7</sup> См.: Там же. С. 160.

<sup>1</sup> См.: *Кузык Б.Н., Яковец Ю.В.* Указ. соч. С. 439.

<sup>2</sup> СЗ РФ. 1994. № 34. Ст. 3540; 1995. № 26. Ст. 2397; 1997. № 12. Ст. 1381; 1999. № 19. Ст. 2302.

для государственных нужд»<sup>1</sup>. Причем ФЗ от 27 декабря 1995 г. № 213-ФЗ «О государственном оборонном заказе»<sup>2</sup> устанавливает определенные особенности поставки продукции для федеральных государственных нужд в целях поддержания необходимого уровня обороноспособности и безопасности РФ, включая и выполнение НИОКР. По оборонному заказу заказчиком может быть только федеральный орган исполнительной власти, имеющий в своем составе войска и вооруженные формирования (Министерство обороны РФ, Министерство внутренних дел РФ, Федеральная служба безопасности РФ и др.).

Поставщиками продукции по оборонному заказу являются предприятия — государственные, смешанные и частные. Заказчиками НИОКР являются соответствующие оборонные агентства (Авиационно-космическое «Авиакосмос», Агентство по системам управления, Агентство по обычным вооружениям, Агентство по судостроению и Агентство по боеприпасам)<sup>3</sup>. НИОКР военного назначения финансирует главным образом МО РФ. Оно же определяет его исполнителей и процедуры проведения закрытого конкурса в соответствии с Законом РФ от 21 июля 1993 г. № 5485-1 «О государственной тайне»<sup>4</sup>, Указом Президента РФ от 30 ноября 1995 г. № 1203 «Об утверждении перечня сведений, отнесенных к государственной тайне»<sup>5</sup>. В данном случае приглашение принять участие в конкурсе направляется каждому потенциальному поставщику без опубликования в печати. В остальной части к закрытым конкурсам применяются нормы об открытых конкурсах. Организатор торгов определяет поставщика, профессионализм и надежность которого проверены с учетом установленных требований, с которым не позднее двадцати дней со дня проведения конкурса должен быть заключен государственный контракт.

Согласно п. 4 ст. 3 Закона об оборонном заказе такой заказ является обязательным для принятия государственными унитарными предприятиями, а также иными организациями, если они занимают

<sup>1</sup> СЗ РФ. 1999. № 19. Ст. 2302.

<sup>2</sup> СЗ РФ. 1996. № 1. Ст. 6; 1997. № 9. Ст. 1012; 1999. № 19. Ст. 2302.

<sup>3</sup> См.: Меньшиков С.М. Указ. соч. С. 132–138.

<sup>4</sup> СЗ РФ. 1997. № 41. Ст. 4673; 1997. № 41. Ст. 8220.

<sup>5</sup> СЗ РФ. 1995. № 49. Ст. 4775; 2001. № 24. Ст. 2418; № 38. Ст. 3725; 2002. № 22. Ст. 2074.

доминирующее положение на товарном рынке или обладают монополией на производство продукции по оборонному заказу.

Предварительное проведение переговоров с поставщиками (исполнителями) НИОКР и согласование с ними конкурсной документации (тактико-технические требования (ТТТ), тактико-технические характеристики (ТТХ) продукции, техническое задание (ТЗ), объем конфиденциальных сведений и методы их защиты, планы по охране конфиденциальности информации и т.д.) позволяют говорить о существовании отдельных этапов проведения конкурса, инициируемых по усмотрению его организатора. Контроль за проведением конкурсов на размещение заказов на поставку продукции (НИОКР) возложен постановлением Правительства РФ от 13 октября 1999 г. № 1160<sup>1</sup> на Министерство экономического развития и торговли РФ<sup>2</sup>. Предприятия, выполняющие работы по оборонному заказу, должны в установленном порядке получить лицензию на право доступа к сведениям, составляющим государственную тайну. В противном случае их участие в конкурсе исключается по решению организатора.

Условия государственного контракта на поставку товаров для государственных нужд в отношении оборонной продукции должны предусматривать защиту сведений, составляющих государственную тайну, доступ к которым ограничен на основании закона; требования по сохранности документов и продукции, содержащих такие сведения. Особенности технического и организационного регулирования в отношении оборонной продукции, составляющей государственную тайну, учтены в ст. 5 ФЗ от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании»<sup>3</sup>. Оборонный заказ на всех этапах разрабатывается и реализуется в соответствии с требованиями заказчика по обеспечению режима государственной тайны.

Конфиденциальность остальных НИОКР определяется заказчиком и разработчиком в техническом задании. Их защита осуществляется с использованием режима коммерческой тайны. Действующий в стране порядок предусматривает единые требования

<sup>1</sup> См.: Постановление Правительства РФ от 13 октября 1999 г. № 116 «О контроле за проведением конкурсов на размещение заказов на поставку товаров (работ, услуг) для государственных нужд и координации их проведения» // СЗ РФ. 1999. № 42. Ст. 5062; 2000. № 46. Ст. 4563.

<sup>2</sup> См.: Приказ Минэкономразвития РФ от 29 декабря 2000 г. № 130. Зарегистрирован в Минюсте РФ от 14 февраля 2001 г. Рег. № 2575 // БНА. 2001. № 9.

<sup>3</sup> См.: СЗ РФ. 2002. № 52 (ч. 1). Ст. 5140.

государственной регистрации открытых НИОКР и доставки обязательного бесплатного экземпляра отчета о них во Всероссийский научно-технический информационный центр (ВНТИЦ)<sup>1</sup>. Документы, направляемые во ВНТИЦ и накапливаемые в его фондах, не относятся к информации с ограниченным доступом. Исключением являются НИОКР, содержащие сведения, составляющие государственную и коммерческую тайну. При их выполнении стороны определяют условия конфиденциальности.

**Процесс разработки и внедрения новой техники представляет собой ряд этапов, регулируемых стандартами на выполнение НИР и ОКР<sup>2</sup>.** Э.Я. Вольнец-Руссет выделяет: проблемные научно-исследовательские работы (НИР), которые направлены на установление неизвестных ранее закономерностей, свойств и явлений материального мира и возможностей их практического применения (1-й этап); прикладные НИР, которые направлены на создание конкретных объектов новой техники (2-й этап); опытно-конструкторские работы (ОКР), изготовление, испытание опытного образца, корректировка чертежей (3-й этап); изготовление, испытание промышленного образца и окончательная обработка технической документации (4-й этап); освоение и промышленное производство новой техники (5-й этап); освоение промышленной эксплуатации новой техники у потребителя (6-й этап)<sup>3</sup>.

При разработке и внедрении новой техники следует учитывать ряд факторов, влияющих на процесс формирования условий конфиденциальности НИОКР. **Постоянно ведущаяся разведывательная деятельность по сбору, анализу, хранению и использованию ценной конфиденциальной информации, которая осуществляется иностранными государственными спецслужбами, конкурирующими частными зарубежными и отечественными фирмами.** Для получения конфиден-

<sup>1</sup> См.: Приказ Министерства науки и технологий РФ от 17 ноября 1997 г. № 125 «Об утверждении положения о государственной регистрации и учете открытых научно-исследовательских и опытно-конструкторских работ». Зарегистрирован в Минюсте РФ от 29 января 1998 г. № 1459, получено СПС «Консультант Плюс».

<sup>2</sup> См.: ГОСТ 15.101-80 «Порядок проведения НИР. Основные положения»; ГОСТ 7.32-91 «Отчет о НИР. Структура и правила оформления»; ГОСТ 2.103-68 «Стандии разработки конструкторской документации»; ГОСТ 2.119-73 «Эскизный проект»; ГОСТ 2.120-73 «Технический проект»; ГОСТ РФ Р15.201-2000 «Система разработки и поставки продукции на производство», и др. Получены в СПС «Консультант Плюс».

<sup>3</sup> См.: Вольнец-Руссет Э.Я. Международный технологический обмен и его роль в экономическом развитии России: Дисс. в виде научн. доклада на соис. уч. ст. д.э.н. М., 2005. С. 50–52.

циальной информации используется агентурная и техническая разведка, осуществляемая с легальных и нелегальных позиций. Данные, опубликованные в печати, позволяют судить об усилении тенденции незаконного получения информации о результатах НИОКР, планах их внедрения по разработке вооружения и военной техники, а также коммерческом их использовании. Такая деятельность направлена на причинение вреда обладателю такой информации. В зависимости от того, кто является заказчиком НИОКР, ущерб на уровне государства может выражаться в угрозах государственной независимости, военной мощи, на уровне коммерческой организации это финансовые и иные потери, которые могут стать причиной ее банкротства.

**Информационная революция и происходящий на ее базе постиндустриальный этап развития** («третья волна перемен в жизни человечества») и глобализации мировых процессов существенным образом влияют на международный обмен научно-технической и технологической информацией. Происходит процесс стремительного формирования единого общемирового финансово-экономического пространства с использованием новых информационных технологий. Государства, совершающие переход от индустриального к индустриальному обществу, преимущественно производят и продают информацию (нововведения). Поэтому они крайне заинтересованы в их постоянном пополнении за счет других стран. В мире отмечается тенденция перетекания интеллектуальных ресурсов в наиболее развитые страны с постепенной концентрацией информационно-коммуникационного потенциала в корпорациях и государствах постиндустриального типа<sup>2</sup>.

**Нужно учитывать существующие каналы возможной утечки охраняемой информации в деятельности организаций** (технические, организационные и иные), а также наличие информации, которая является объектом устремлений со стороны спецслужб иностранных государств и конкурирующих фирм, ведущих промышленный шпионаж. Их деятельность направлена на добычу информации о ведущихся фундаментальных и прикладных НИР, о планируемых и выполняемых ОКР, о сделанных в РФ открытиях и изобретениях, исполь-

<sup>1</sup> См.: Гофлер Э., Гофлер Х. Создание новой волны цивилизации. Политика третьей волны / Пер. с англ. М., 1995. С. 20–36.

<sup>2</sup> См.: Рубанов В.А. Информационная безопасность России / Под ред. проф. В.И. Добрынькова. М., 2001. С. 56–78.

зование которых может привести к значительному повышению эффективности создаваемой новой техники и снижению ее стоимости. Учитывая направленность разведывательной деятельности, сокрытию и защите подлежат:

- а) основные направления разработки совершенно новых образцов техники, знаменующих собой «технологический и технологический прорыв» и их обоснование; перечни перспективных НИР и ОКР по сферам общественного производства;
- б) сравнительная оценка прогнозируемых уровней развития новой техники и технологии с аналогичными новшествами за рубежом;
- в) сроки начала и окончания НИР и ОКР по разработке систем и комплексов; наименование и профиль организаций, участвующих в этих работах;
- г) рекомендуемые по результатам НИР и ОКР важнейшие характеристики новой техники: тактико-технические характеристики комплексов, их экономические характеристики на этапах разработки и серийного производства, особенности технических, технологических и конструкторских решений, результаты испытаний и др. характеристики.

Охрана сведений при разработке и внедрении новой техники осуществляется с использованием различных систем режима секретности или режима конфиденциальности информации (государство или частная компания). Это связано не только с различными источниками финансирования, но и с порядком согласования и утверждения документов, обеспечивающих режим секретности (конфиденциальности) при выполнении НИОКР.

Анализ ряда организаций, выполняющих НИОКР, показывает, что, независимо от формы собственности заказчика, можно говорить об одних и тех же типовых формах правовых документов, разработываемых для обеспечения режима секретности (конфиденциальности) НИОКР. Поскольку большинство НИОКР финансируется за счет федерального бюджета<sup>1</sup>, рассмотрим механизм их формирования с участием государства. При этом нужно иметь в виду, что названные выше этапы разработки и внедрения новой техники характерны и для частных организаций, выполняющих НИОКР, за исключением некоторых особенностей, которые присущи только госзаказчику.

<sup>1</sup> См.: Кузык Б.Н., Яковец Ю.В. Россия — 2050. Стратегия инновационного прорыва. М., 2005. С. 417–440.

**Начальная стадия разработки НИР и ОКР состоит в проработке технических заданий, технического обоснования и исходных технических требований.** Эта работа выполняется в несколько этапов путем рассмотрения предложений и окончательного формирования НИР и ОКР.

Основанием и исходными документами для выполнения НИР и ОКР являются: годовой план министерства или частной организации по разработке и внедрению новой техники; техническое задание (ТЗ) на выполнение НИР и ОКР; государственный контракт (договор) между заказчиком и исполнителем НИР и ОКР.

*ТЗ является обязательным документом, определяющим цель, содержание, порядок проведения работ, способы реализации результатов НИР и ОКР.* ТЗ на НИР разрабатывается на основе научного прогнозирования, анализа достижений отечественной и зарубежной науки и техники, результатов поисковых НИР, изучения патентной документации и требований заказчика. Результаты НИР являются исходными данными для разработки ТЗ на проведение ОКР с целью создания новой и модернизированной продукции.

В зависимости от характера, сложности и объема работ в выполнении НИР и ОКР могут принимать участие по согласованию с заказчиком несколько организаций. В этом случае определяется головной исполнитель, который координирует работу организаций-соисполнителей. По отношению к ним он выступает заказчиком и отвечает в целом за научно-технический уровень работы и создание образца системы (комплекса).

Служба безопасности заказчика, принимающая участие в подготовке ТЗ на НИР и ОКР, разрабатывает меры в виде *Единого плана мероприятий по обеспечению режима конфиденциальности работ* (далее — Единый план). Единый план согласовывается с головным исполнителем и, в зависимости от важности работ, утверждается руководством министерства или советом директоров либо генеральным директором общества (если частный заказ).

Основной задачей Единого плана является координация усилий сторон по сохранению в тайне работ, выполняемых в кооперации, их научного замысла и основных ГТХ, раскрывающих направления разработки и внедрения продукции. Единый план включает такие вопросы, как: основное назначение НИР и ОКР, степень их конфиденциальности, состав организаций и круг выполняемых ими заданий, порядок пользования документами, содержащих ГТХ, объ-

ем сведений, предоставляемых исполнителям, меры по обеспечению режима работ.

Порядок построения, изложения и оформления ТЗ на НИР и ОКР регламентирован соответствующими ГОСТами<sup>1</sup>. ТЗ на НИР состоит из следующих разделов: основание для проведения работ; цель и исходные данные для проведения работ; этапы НИР; основные требования к выполнению НИР; способ реализации результатов НИР; перечень технической документации, предоставляемой по окончании работ; порядок рассмотрения и приемки НИР и ее этапов; технико-экономическое обоснование.

ТЗ на ОКР включает разделы: наименование и шифр разработки; основание для разработки; цель разработки и назначение изделия; технические требования, в том числе эксплуатационные; требования к стандартизации и унификации; технико-экономические показатели; эргономические требования; порядок разработки испытаний, приемки изделий и окончания работ.

В соответствии с требованиями ГОСТов допускается уточнение и введение новых разделов, определяемых заказчиком по согласованию с исполнителем.

Изучение практики организаций в сфере обращения КЗИ показывает, что *требования по обеспечению конфиденциальности работ могут быть дополнительно внесены в соответствующие разделы ТЗ на НИР и ОКР либо сформулированы в виде нового раздела ТЗ*. В отдельных случаях эти требования были приложены к ТЗ в виде отдельного документа, имевшего название: «*Дополнение к разделу ТЗ о конфиденциальности выполнения НИР и ОКР*» (далее — Дополнение к ТЗ). В разделе ТЗ указываются требования ГОСТов по обеспечению конфиденциальности работ, требования заказчика, вытекающие из Единого плана, подготовки плана мероприятий на основе методических рекомендаций заказчика по выявлению возможных каналов утечки информации и предупреждению правонарушений в сфере обращения охраняемых сведений. Например, такие требования для НИР содержатся в ГОСТе В15.101-79 и ОКР в ГОСТе В15.201-83. В разделе ТЗ содержится также требование к исполнителю о представлении им отчета о выполненной работе по охране конфиденциальности информации.

<sup>1</sup> См.: ГОСТ 7.32-2001 «Отчет о научно-исследовательской работе. Структура и правила оформления»; ГОСТ 315.201-2000 «Система разработки и постановки продукции на производство», и др.

В дополнение к ТЗ на НИР и ОКР заказчик указывает следующие требования.

Обязанность исполнителя по защите выделенных сведений с учетом степени их конфиденциальности. К числу этих сведений относятся: направление исследований, программа создания и внедрения новой техники, ТТХ систем и комплексов. Речь идет о сведениях, характеризующих эффективность исследования, продолжительность и стоимость работы, использование материалов и специальных видов оборудования, результаты лабораторных экспериментов, перспективность разработки изделия и его конструктивные особенности и другие.

Обеспечение необходимого уровня конфиденциальности при выполнении работ с другими организациями. Указывается, с какими организациями, в каком объеме и какие вопросы исследований и технических решений должны быть согласованы с соблюдением условия конфиденциальности. При этом заказчиком может быть предложено использование условного, а не действительного наименования НИР и ОКР для открытой переписки, передачи информации по защищенным каналам связи. В связи с важностью проводимых работ могут быть использованы легендирование и дезинформация. Имея общую цель, они различаются по направленности действия. Если легендирование используется для искажения видимости действий, характера работ, назначения скрываемого объекта, то дезинформация технической направленности используется для искажения реальных характеристик скрываемых объектов. Безусловно, нужно уделять внимание проведению мероприятий, подтверждающих легенду прикрытия и дезинформацию НИР и ОКР. Таким работам присваивается условное наименование и шифр темы, которые включаются в ТЗ для использования во взаимоотношении с соисполнителями.

Осуществление необходимых мер охраны конфиденциальности при выполнении НИР и ОКР, определяемых заказчиком. Речь идет о требованиях, предъявляемых к помещениям, где ведутся НИР и ОКР. Они должны быть оборудованы техническими средствами охраны, обеспечивать звукоизоляцию, условия хранения и использования документов и изделий. Выделенные помещения должны быть аттестованы с учетом рекомендаций по противодействию иностранным техническим разведкам и промышленному шпионажу. Заказчик определяет перечень сведений по теме, которые не могут быть опубликованы в печати, а также те, публикация которых возможна по его письменному разрешению. Указываются требования, которые

необходимо соблюдать при обработке, хранении и передаче информации с использованием ЭВМ.

В государственном контракте (договоре) в разделе «Технические условия» указывается, что предусмотренная договором работа выполняется в соответствии с ТЗ и другими утвержденными в установленном порядке документами. Эти документы устанавливают режим ограничения доступа к работам и документам, степень конфиденциальности сведений и другие обязательные условия. В разделе договора «Дополнительные условия» могут быть кратко сформулированы требования по обеспечению конфиденциальности работ, вытекающие из Единого плана, ТЗ или дополнения к нему.

В некоторых организациях разрабатывается Положение по обеспечению режима конфиденциальности выполняемых работ (далее — Положение). Это основной документ, регулирующий отношения заказчика и исполнителя в сфере обращения КЗИ. Положение содержит перечень наиболее важных охраняемых сведений и меры по их охране. Организация-исполнитель на основании Положения разрабатывает свои внутренние *Планы мероприятий по обеспечению конфиденциальности работ* (далее — План), которые детализируются с учетом этапов НИР и ОКР, а также состояния оперативной обстановки.

Головные организации — исполнители НИР и ОКР разрабатывают ТЗ (частные ТЗ) исполнителям работ, в которых указываются выделенные охраняемые характеристики (параметры) создаваемой системы и требования по обеспечению их охраны. Размещение заказов производится после проведения необходимых мероприятий по обеспечению режима, подтвержденных *Совместным заключением головной организации (заказчика) и исполнителя работ* (далее — Совместное заключение). Отдельные организации составляют Совместное заключение вместе с Планом, что в большей степени может обеспечить заказчика в установлении исполнителем необходимых мер по охране конфиденциальности информации и готовности приступить к выполнению заказа.

В Совместном заключении стороны подтверждают гриф конфиденциальности темы, определяют ответственных лиц за обеспечение устанавливаемого режима работ (научный руководитель НИР и главный конструктор ОКР); формы и способы контроля за реализацией мер режима; указывают наиболее важные сведения по теме, степень конфиденциальности отдельных этапов работ; сведения, которые могут быть опубликованы в печати; подразделение, выполняющие

работы по теме, и характеристика помещений, выделенных для этих целей. Особо оговариваются требования к персоналу и средствам, которые потребуются для обеспечения режима работ. Затраты, по согласованию сторон, должны быть отражены в условиях договора (прием на работу дополнительного числа работников, приобретение оборудования и др.). Стороны могут согласовывать вопросы организации проверки лиц, допускаемых к охраняемым сведениям, о проверке знаний ими правил работы с конфиденциальными документами и изделиями, о порядке допуска командированных лиц к работам по совместным темам.

В ходе согласования Совместного заключения заказчик может обязать исполнителя провести ряд дополнительных мероприятий по обеспечению режима размещаемого заказа, что может задержать начало работ. Поэтому следует заблаговременно разработать и согласовать с заказчиком План мероприятий по обеспечению режима конфиденциальности НИР и ОКР и провести первоочередные мероприятия до подписания Совместного заключения. Такой план может включать следующие мероприятия:

— порядок подбора и проверки работников, привлекаемых к работам по НИР и ОКР, оформление их доступа к охраняемым сведениям, инструктаж по вопросам сохранения в тайне информации, передаваемой по работе; разъяснение требований при работе с документами и иными носителями, использовании сведений на совещаниях и конференциях, приеме командированных лиц, а также предупреждение об ответственности за разглашение охраняемых сведений, имеющихся отношении к НИР и ОКР;

— определение подразделений, участвующих в работах (объем выдаваемых сведений, порядок подготовки и хранения документов и др.), и производственных участков, на которых вводится легенда прикрытия работ;

— аттестация помещений, выделенных для проведения конфиденциальных работ, совещаний, оформление списка работников, имеющих доступ в такие помещения;

— определение мер защиты и маскировки от технических средств разведки;

— организация конфиденциального делопроизводства, обеспечения режима накопления, хранения и выдачи документов по НИР и ОКР (инвентарный учет ТЗ, сосредоточение документов по теме в отдельных делах и др.);



анализ отечественных и зарубежных источников с целью определения осведомленности конкурирующих фирм по конкретным НИР и ОКР;

учет осведомленности работников организации по НИР и ОКР, сведения о которых охраняются в установленном сторонами порядке;

изучение и анализ хозяйственной ситуации с целью определения дополнительных мероприятий по выявлению возможных каналов утечки охраняемой информации на различных этапах выполнения НИР и ОКР, а также предупреждению правонарушений в сфере обращения КЗИ;

подготовка отчета о выполнении требований ТЗ в части обеспечения охраны конфиденциальности информации при выполнении НИР и ОКР.

Особенности работ, выполняемых на различных этапах НИР и ОКР, определяют специфику формирования требований заказчика по обеспечению конфиденциальности информации и действий исполнителя по планированию мер обеспечения ее защиты. *На этапе НИР «Теоретические и экспериментальные исследования»* могут быть получены новые теоретические обоснования предлагаемого решения по объекту исследования, которые не были отнесены заказчиком к числу конфиденциальных сведений. В процессе засекречивания важно не только правильно определить степень конфиденциальности сведений, содержащихся в новом направлении работы, но и своевременно разработать дополнительные меры по их защите. В процессе разработки перечня сведений специалисты пользуются ранее разработанными перечнями по аналогичным темам, учитывая существующую преемственность создаваемых изделий и используя опыт. В массиве сведений важным является учет тех, которые относятся «облик создаваемого изделия». Выделяются сведения, которые отражают достигнутый уровень, новизну и оригинальность применяемых в новой разработке научно-технических решений, раскрывают особенности и ТТХ создаваемого образца новой техники. Такие сведения иногда называют на практике выделенными охраняемыми сведениями или наиболее важными сведениями по НИР и ОКР (комплексу, системе).

Межгосударственный стандарт ГОСТ 7.32-2001 «Отчет о научно-исследовательской работе. Структура и правила оформления» введен в действие с 1 июля 2002 г. в качестве стандарта России. Однако он не предусматривает обязанности по включению в отчет раздела о вы-

полнении требований ТЗ по обеспечению охраны конфиденциальности информации. Эти данные могут быть предоставлены заказчику, по его усмотрению, на основании договора.

*Этапы ОКР тесно взаимосвязаны со стадиями разработки конструкторской документации* по ГОСТ 2.103-68, что находит отражение в ТЗ.

*Начальным этапом является разработка тактико-технического задания (ТТЗ), ТЗ на ОКР.* Выполнение этого этапа не предусмотрено ГОСТом. Однако именно с этого этапа начинается формирование ОКР. На этом этапе происходит: 1) согласование тактико-технических требований (ТТТ) к системам и комплексам и включение их в планы министерств; 2) доведение до исполнителей требований заказчика в части, их касающейся; 3) предварительное обсуждение возможностей реализации ТТТ в головной организации; 4) составление, согласование и утверждение ТТЗ (ТЗ) на ОКР. Названные подэтапы включают различные меры режима. При формировании проекта ТТЗ в него включается перечень первичных режимных мероприятий по защите темы. Важнейшими из них могут быть легендирование и маскировка работ.

На этапах согласования ТЗ и заключения договоров с организациями-исполнителями составляется на основании требований заказчика план предварительных мероприятий по обеспечению конфиденциальности работ. По результатам экспертизы технического предложения, как отдельного этапа ОКР, могут быть предложены дополнительные меры защиты. После рассмотрения ТТЗ на научно-техническом совете (НТС) головного исполнителя ОКР с участием заказчика оформляется уточненный план предварительных мероприятий по обеспечению режима.

*Этапы разработки эскизного и технического проекта* предусмотрены соответственно ГОСТ 2.119-73 и ГОСТ 2.120-73. В зависимости от характера и сложности ОКР, степени предварительной проработки темы допускается исключение названных этапов, если это предусмотрено в ТЗ. Эскизный проект (ЭП) разрабатывается для установления конструктивных, схемных и др. решений образца, дающих общее представление о принципе его работы и устройства.

Технический проект (ТП) ОКР разрабатывается для выявления окончательных технических решений, дающих полное представление о конструкции образца системы (комплекса).

На этапах эскизного и технического проекта могут выполняться НИР, происходит разработка конструкторской документации на

макеты, их изготовление и испытание, рассмотрение и утверждение результатов работы на НТС. На этих этапах происходит расширение круга работников, осведомленных в охраняемых секретах о создаваемой системе (комплекса), резкое увеличение объема проектной и технической документации по изделию, расширение работ в опытно-производстве (завод) и связей с организациями-соисполнителями (рост числа командированных лиц).

На основании ТТЗ заказчик разрабатывает *Положение по обеспечению режима конфиденциальности работ* (далее — Положение), формирует требования по режиму в ТЗ на разработку ЭП и ТП, согласовывает с исполнителем договорные условия о конфиденциальности в договорах на выполнение НИР, ЭП и ТП. Соисполнители на основании договора, ТЗ и Положения составляют и согласовывают с заказчиком свои планы по обеспечению режима конфиденциальности темы (далее — План). После рассмотрения ЭП и ТП на НТС могут быть приняты дополнительные меры по защите темы.

Следующим этапом ОКР является *разработка рабочей конструкторской документации (РКД) для изготовления опытного образца*. РКД разрабатывает головной исполнитель в соответствии с требованиями ТЗ на ОКР на основании ТП или ЭП. После разработки РКД она утверждается головным исполнителем в соответствии с требованиями ГОСТ 2.104-68 и передается по акту изготовителю опытного образца. На этом этапе в части обеспечения конфиденциальности работают действующее Положение, утвержденное заказчиком на начальном этапе ОКР, а также План, который разработан исполнителем с учетом особенностей работы по разработке РКД.

*Изготовление опытного образца, проведение предварительных (заводских) испытаний и приемочных испытаний опытного образца* являются отдельными самостоятельными этапами ОКР, которые выполняются с учетом требований ГОСТ 2.106-96, ГОСТ 15.001-88. По результатам изготовления и предварительных (заводских) испытаний опытного образца производится корректировка РКД с присвоением ей литеры «О». На этапе приемочных испытаний может быть проведена корректировка РКД и доработка опытного образца. После проведения опытной оперативной эксплуатации опытного образца, завершения корректировки РКД ей по результатам испытания присваивается литера «О1». Эти работы проводятся в соответствии с требованиями ГОСТ 2.902-68, ГОСТ 2.503-90. ОКР считается завершенной, если проведены приемочные испытания, опытная оперативная эксплуатация и РКД присвоена литера «О1».

На этапах изготовления опытного образца и его наземных и летных испытаний резко возрастает объем переписки с организациями, испытательными центрами (полигонами), увеличивается число лиц, допускаемых к изделиям и осведомленных с результатами испытаний (параметрами) изделий. На период проведения испытаний заказчик устанавливает специальные требования по противодействию иностранным техническим разведкам, выделяя при этом охраняемые параметры, подлежащие защите.

*Постановка продукции на производство* включает подготовку и освоение производства, регулируемые в соответствии с требованиями ГОСТ Р15.201-2000 «Система разработки и постановки продукции на производство. Продукция производственно-технического назначения. Порядок разработки и постановки продукции на производство».

Основанием для постановки на производство является заключенный с заказчиком договор (контракт) по закупке у поставщика (изготовителя) продукции. Подготовка производства включает передачу разработчиком изготовителю комплекта конструкторских (КД) и технологических документов (ТД), специальных средств контроля и испытаний, опытного образца, заключений эксперта, акта приемочного испытания. Подготовка производства считается законченной, когда изготовителем отлажены средства технологического обеспечения и технологические процессы, подготовлен персонал и установлена готовность к освоению производства продукции. В этот период изготовитель проводит работы для обязательной последующей сертификации продукции.

*На этапе освоения производства* выполняется изготовление установленного договором количества единиц продукции установочной серии, проводятся квалификационные ее испытания, при необходимости отработка конструкции на технологичность и утверждение КД и ТД с присвоением литеры «А».

При формировании договорного условия о конфиденциальности ОКР следует учитывать «фактор рассеивания» конфиденциальной информации о создаваемом образце продукции. Его действие выражается через различные носители: люди, документы, различные технологические процессы, испытания, отдельные элементы системы, само изделие. Как было показано выше, на этапе разработки ТТЗ (ТЗ) к охраняемым сведениям имеет доступ ограниченное число лиц. По мере перехода к этапам создания опытных образцов, их испытаний, серийного производства значительно расширяется круг

лиц, имеющих доступ к охраняемым сведениям. Растет количество материальных носителей, на которых зафиксирована такая информация. Одновременно возрастают возможности конкурентов по получению информации о защищаемых изделиях с помощью технических средств разведки. На этих этапах становится значительно сложнее защищать сведения с необходимой степенью надежности, а порой и невозможно. Это обстоятельство необходимо, во-первых, учитывать при формировании условий о конфиденциальности НИР и ОКР, а во-вторых, при переходе к следующим этапам НИОКР целесообразно проводить корректировку перечня охраняемых сведений для исключения необоснованного засекречивания информации и уменьшения затрат на ее охрану.

*К первой группе договоров на выполнение НИОКР, предметом которых является получение (создание, производство) КЗИ технического и технологического характера, тесно примыкает договор на выполнение маркетинговых исследований.* Главной особенностью этого договора является получение в ходе исследований КЗИ делового характера, которая нуждается в охране. Такую информацию заказчик может получить на основании программы работ, осуществляемых исполнителем, и задания на проведение маркетингового исследования, отражающих коммерческие интересы. Эти сведения позволяют правильно организовать работу с поставщиками и покупателями; объективно оценить конкурентов, совершающих аналогичные торговые операции, правильно выбрать «нишу» на рынке и решать другие вопросы, связанные с продвижением товара и заключением договоров купли-продажи.

По договору на выполнение маркетинговых исследований исполнитель обязуется провести исследование в соответствии с заданием, утвержденным заказчиком, и передать ему результат в виде документированной информации (отчет), а заказчик обязуется принять его и оплатить выполненную работу. В ГК РФ и иных актах отсутствуют нормы, регулирующие отношения сторон в связи с выполнением этого договора. Потребность в маркетинговой информации заставляет организации заключать такие договоры. При этом стороны руководствуются общими нормами гражданского законодательства о заключении и исполнении договора, и нормами, регулирующими аналогичные правоотношения, содержащимися в главах 37, 38 и 39 ГК РФ. Анализ показывает, что при разработке такого соглашения стороны используют различные элементы других договоров, что не противоречит ГК. К такому смешанному договору маркетинга

применяются в соответствующих частях правила, например, регулирующие договоры подряда, выполнения НИР, возмездного оказания услуг и т.д., включая охрану конфиденциальности информации. Такая правовая конструкция договора на выполнение маркетинговых исследований хотя и не предусмотрена законом, но имеет право на существование (ст. 421 ГК РФ).

Общие условия договора о выполнении маркетинговых исследований определяются по усмотрению сторон. Особо оговариваются условия о конфиденциальности, меры по установлению и обеспечению режима коммерческой тайны, сроки их действия и ответственность сторон.

Предмет договора позволяет определить территорию проведения (район, регион, отрасль хозяйства, вид деятельности и т.д.) и направления исследований, касающиеся объема получения КЗИ, интересующей заказчика, и сформулировать условия по ее охране. При определении направлений исследования в договоре важно закрепить положение о том, что получение маркетинговой информации не должно нарушать право потенциальных конкурентов на защиту своей коммерческой тайны. В противном случае, если задание заказчика предусматривает сбор информации, на которую установлена монополия другой организации, то такие действия будут рассматриваться как промышленный шпионаж.

Заказчик вправе рассчитывать на получение конкретного результата исследования, качество которого зависит от использования научно обоснованных методик, которые могут представлять интерес для конкурентов. Поэтому стороны должны предусмотреть условия конфиденциальности при разработке и использовании таких методик. Заказчик может принять на себя обязательство не разглашать третьим лицам методику проведения исследований и другие неопубликованные сведения, которые, по мнению исполнителя, составляют секретную особенность его деятельности (ноу-хау).

Заказчик должен определить основные требования к разделу отчета о соблюдении условий конфиденциальности при получении результатов исследования. Реализация исполнителем мероприятий по охране конфиденциальности КЗИ должна убедить заказчика в том, что информация, содержащаяся в отчете, не является общедоступной и ее использование принесет ожидаемый эффект. Представляется, что отчет должен иметь высший гриф «Коммерческая тайна», поскольку содержит совокунные данные о результатах исследования; о методах, которые применялись для сбора, анализа и обработки све-

дений; о величине возможных погрешностей, влияющих на степень достоверности информации и др. сведения, представляющие интерес для конкурентов. Претензии, связанные с несоблюдением условия конфиденциальности при проведении исследований могут быть предъявлены исполнителю лишь до подписания заказчиком акта сдачи-приемки работы. В последующем невозможность использования результатов маркетинговых исследований по причине их разглашения (утечки) не может связываться с эффективностью применения последних в конкурентной стратегии, поскольку исполнитель не отвечает за их содержание после сдачи работы и подписания акта.

Результаты маркетинговых исследований являются собственностью заказчика, и исполнитель не вправе разглашать эти данные третьим лицам, в том числе информацию о том, кто являлся инициатором проведения данных исследований. В этих целях по инициативе заказчика стороны могут предусмотреть конкретный срок после сдачи работы, в период которого исполнитель обязан будет соблюдать условия конфиденциальности и осуществлять мероприятия по охране информации, используя для этого свои силы и средства. Заметим, что речь не идет о бесплатном выполнении исполнителем работы по режимному сопровождению данных, полученных им в ходе маркетингового исследования. Учитывая продолжительность такой работы, она может быть оформлена по усмотрению сторон договором о возмездном оказании услуг.

Рассмотрим **вторую группу договоров на передачу информационных продуктов**, в которые, по усмотрению сторон, включается условие о конфиденциальности КЗИ. К этой группе относятся договоры на передачу секрета производства (ноу-хау) или технологии либо предоставлении права использования секрета производства или технологии; передачу коммерческой информации и ее переработку.

**Договоры о передаче ноу-хау и о предоставлении права его использования** начали использоваться в нашей стране в 60-е годы XX в. в связи с продажей за рубеж лицензий на технологии (ноу-хау). В гражданском законодательстве длительное время отсутствовало правовое регулирование этих договоров. Принятие части четвертой ГК РФ, способствовало закреплению договора об отчуждении исключительного права на секрет производства (ст. 1468) и лицензионного договора о предоставлении права использования секрета производства (ст. 1469), а также договорному регулированию прав на результаты интеллектуальной деятельности в составе единой технологии (гл. 77 ГК РФ). Законодатель обязывает обладателя секрета производ-

ства (ноу-хау) и технологии вводить режим коммерческой тайны (ст. 1465, 1554 ГК РФ) для сохранения конфиденциальности сведений.

Нужно сказать, что конфиденциальность вытекает из правовой природы этих договоров, поэтому относится к числу существенных условий, обычно согласовываемых сторонами. Хотя договоры о передаче ноу-хау и технологии урегулированы теперь законом, но в них не совсем четко раскрывается содержание условий конфиденциальности. В литературе имеются разработки по этому вопросу, которые давно используются на практике. Наиболее удачно условия конфиденциальности, включаемые в договор ноу-хау, были сформулированы И.А. Зениным<sup>1</sup>. Вместе с тем ряд положений, на наш взгляд, необходимо уточнить и дополнить.

В предмете договора, а при необходимости и в приложении к нему, должна быть дана исчерпывающая характеристика передаваемого ноу-хау или технологии. Из технического описания должно быть очевидным, что именно передается по договору. Обычно речь идет о технических знаниях, которые могут включать предметы, например, опытные незарегистрированные образцы изделий, техническую документацию, содержащую расчеты, формулы, чертежи, планы; инструкции о регулировании процессов изготовления и использования продукции, о применении различных способов создания приспособлений для оснастки производства; технические рецепты, рекомендации по расположению машинного оборудования; предписания персоналу для работы на испытательных стендах; технологии, выраженные в объективной форме, которые могут служить технологической основой определенной практической деятельности. При этом нужно учитывать суть и назначение ноу-хау и технологии.

По мнению Э.Я. Вольнец-Руссет, «...знания, опыт и навыки, связанные с разработкой, освоением, производством, реализацией, эксплуатацией, обслуживанием, ремонтом, совершенствованием и утилизацией новой техники, технологии и материалов»<sup>2</sup> являются важнейшими критериями признания технических решений ноу-хау. В предмете договора следует обязательно указать, что передаваемые ноу-хау и технологии охраняются в соответствии с требованиями

<sup>1</sup> См.: Гражданское право: Учебник. Т. II. Полутом I / Отв. ред. проф. Е.А. Суханов. 2-е изд. М., 2000. С. 618–622.

<sup>2</sup> См.: Вольнец-Руссет Э.Я. Международный технологический обмен и его роль в экономическом развитии России: Дисс. в виде науч. доклада на соиск. уч. ст. д.э.н. М., 2005. С. 34.

ГК РФ, Закона о коммерческой тайне. Исходя из этого, стороны согласовывают свои права и обязанности по поводу соблюдения условия конфиденциальности. Причем их объем и содержание мер охраны конфиденциальности могут быть различными, в зависимости от распоряжения исключительным правом путем его отчуждения либо предоставления другому лицу права использования ноу-хау и технологии. Вид лицензионного договора (неисключительная лицензия либо исключительная лицензия), обуславливает круг лиц, ознакомившихся с охраняемой информацией и объем мероприятий по обеспечению ее конфиденциальности. В любом случае стороны принимают на себя обязательство по охране конфиденциальности ноу-хау или технологии в течение срока действия договора, а также обеспечивают такой режим после передачи либо предоставления исключительного права третьим лицам.

Стороны согласовывают в договоре взаимную ответственность за несоблюдение обязательств по сохранению конфиденциальности ноу-хау или технологии с определением размеров и методики возмещения убытков, а также использования иных способов защиты гражданских прав, указанных в ст. 12 ГК РФ. В договоре может быть предусмотрена ответственность приобретателя за неумышленное разглашение информации, составляющей ноу-хау или технологии, если он не предпринимал в разумных пределах мер по охране конфиденциальности полученных результатов интеллектуальной деятельности.

Практически слабым местом в охране конфиденциальности при распоряжении исключительным правом на ноу-хау или технологии являются преддоговорные контакты, когда происходит демонстрация возможностей применения ноу-хау и технологии в производстве. Опасность разглашения (утечки) информации о ноу-хау и технологии существует в случае конфликта интересов правообладателя (лицензиара) и приобретателя (лицензиата), что, как правило, приводит к досрочному расторжению договора. Важным средством, позволяющим защитить интересы заинтересованных лиц, может быть договор о защите коммерческой тайны (о конфиденциальности). На практике этот договор может предшествовать заключению основного договора о передаче ноу-хау или технологии либо заключаться в момент его подписания. В предмете такого договора раскрывающая сторона отражает содержание передаваемой информации, являющейся коммерческой тайной фирмы, а получающая сторона берет на себя обязательство не разглашать полученную информацию третьим лицам и соблюдать достаточную степень конфиденциальности, позволяющую

шую избежать утечки информации по различным каналам. Стороны определяют особые условия, при которых информация не будет являться коммерческой тайной. Это могут быть случаи, когда полученная информация уже известна получающей стороне или раскрыта по мотивированному запросу государственного органа, и иное. Такой договор носит долгосрочный характер и позволяет надежно защищать коммерческие интересы сторон. Сам факт его заключения между сторонами не разглашается.

В отличие от договора о передаче ноу-хау или технологии, методом которых является техническая и технологическая информация, в торговом обороте все чаще используются **договоры на передачу и на переработку коммерческой информации**, включая ту ее часть, которая защищается в режиме коммерческой тайны. В науке коммерческого права сформулированы подходы к определению понятия договора на передачу информации<sup>1</sup> и его содержания. По мнению Б.И. Пугинского, «передача деловой информации, используемой в торгово-предпринимательской деятельности, опосредуется договором купли-продажи»<sup>2</sup>. Такого же мнения придерживается и автор настоящей работы, а также с некоторой оговоркой Е.В. Измайлова, которая отмечает, что договор на передачу информации «...по своему основному характеристикам находится все-таки ближе к договору купли-продажи, чем к договору возмездного оказания услуг»<sup>3</sup>.

Договор купли-продажи информации в ГК РФ не упоминается. Вместе с тем ст. 421 ГК РФ предполагает свободу в заключении договоров, которые не предусмотрены законом. Причем стороны могут заключить смешанный договор, в котором содержатся элементы различных договоров. Общие положения о купле-продаже (§ 1 гл. 30 ГК РФ) на основании п. 4 ст. 454 ГК РФ могут применяться к купле-продаже различных информационных продуктов.

Содержание договора купли-продажи информационных продуктов включает в себя следующие условия. Прежде всего, это условие о предмете договора. Оно должно быть четко сформулировано сторонами и касаться вида целевого назначения, полноты передаваемой

<sup>1</sup> См.: *Северин В.А.* Правовое регулирование информационных отношений // Вестн. Моск. ун-та. 2001. № 6. С. 68–70; *Измайлова Е.В.* Информация в коммерческих отношениях // Вестн. Моск. ун-та. Сер. 11 «Право». 2005. № 1. С. 70–71, и др.

<sup>2</sup> См.: *Пугинский Б.И.* Коммерческое право России. 2-е изд. М., 2006. С. 247.

<sup>3</sup> См.: *Измайлова Е.В.* Указ. соч. С. 76.

информации, содержащейся на материальных носителях, и ее грифа конфиденциальности. Требования к содержанию и полноте информации, обеспечению охраны ее конфиденциальности могут быть сформулированы в приложениях к договору в виде перечня критериев оценки ее достоверности, мероприятий по обеспечению охраны конфиденциальности, и др.

Определяя предмет договора, стороны должны учитывать императивные нормы, запрещающие передачу информации, составляющей коммерческую тайну, третьим лицам без ведома ее обладателя.

Условие о качестве передаваемой информации, критериями которого являются ее достоверность и точность, представляет согласованные сторонами гарантии того, что информация отражает факты действительности и способствует потребности покупателя. Проблемным является вопрос подтверждения достоверности сведений, составляющих коммерческую тайну продавца, содержащихся в передаваемом информационном продукте. Для его решения стороны могут согласовывать круг источников информации, не вызывающих у них сомнения, которые должны быть раскрыты по требованию покупателя. В противном случае достоверность может быть установлена экспертизой, условие о проведении которой также согласовывается сторонами. Но в этом случае произойдет расширение круга лиц, имеющих доступ к ценной деловой информации.

Условие об определенных сроках передачи информационного продукта является существенным для покупателя, поскольку информация подвергается моральному старению и может со временем не представлять для него коммерческой ценности. При нарушении срока исполнения договора покупатель утрачивает интерес к договору, вправе отказаться от принятия исполнения и требовать возмещения убытков (ст. 457 ГК РФ).

Важным условием договора является определение сторонами объема передаваемых покупателем сведений. Что касается передачи информации третьим лицам, то продавец может устанавливать запрет на ее передачу либо ограничения, которые оговаривает особыми условиями, вытекающими из конфиденциальности КЗИ, охраняемой в режиме коммерческой тайны.

Способ передачи информации, в каком виде (письменном, электронном) она должна быть оформлена и в каком порядке передана, также оговаривается сторонами в договоре. Названные выше условия договора должны учитываться при планировании и реализации мер по защите охраняемой информации от ее разглашения (утечки).

Условие о конфиденциальности стороны согласовывают на этапе коммерческих переговоров о заключении договора купли-продажи информации. Уже на этом этапе стороны могут передать друг другу информацию, являющуюся коммерческой тайной. Поэтому следует заключить отдельный договор о защите коммерческой информации. В предмете такого договора раскрывающая сторона сообщает содержание передаваемой информации, являющейся коммерческой тайной фирмы, а получающая сторона указывает цель получения информации и правовые основания (договор купли-продажи и т.д.). Права и обязанности сторон по этому договору аналогичны тем, которые изложены применительно к договору на передачу ноу-хау.

С договором на передачу информации тесно связан **договор на переработку информации**, хотя правовая природа у них различна. Договор на переработку информации упоминается в литературе как договор на выполнение информационных работ<sup>1</sup>. Этот договор давно и широко используется в деловой практике.

*Договор на выполнение информационных работ (переработку информации)* специально не регулируется ГК РФ. К нему применяются общие нормы, предусмотренные § 1 главы 37 ГК РФ («Подряд»). Этот вид договора во многом схож с договором возмездного оказания услуг. Разница между ними состоит в том, что работа, выполняемая по договору подряда, имеет овеществленный результат, который передается заказчику в виде, например, отчета о результатах маркетинговых исследований, информационного продукта, полученного в результате обработки информации на ЭВМ. Определенную специфическую работу имеет договор подряда типа на создание информационного ресурса (базы данных<sup>2</sup> и сайта<sup>3</sup>). Их правовая охрана осуществляется в соответствии с Законом РФ от 23 сентября 1992 г. № 3523-1 «О правовой охране программ для ЭВМ и баз данных»<sup>4</sup>. Однако обеспечение конфиденциальности передаваемых сведений, необходимых для формирования совокупности систематизирован-

<sup>1</sup> См.: Шерстобитов А.Е. Правовое регулирование договорных отношений в сфере информатики // Право и информатика / Под ред. Е.А. Суханова. М., 1990. С. 32–35, и др.

<sup>2</sup> См.: Потяркин Д. Передача информации, содержащейся в базе данных // Хозяйство и право. 1996. № 6. С. 94–101, и др.

<sup>3</sup> См.: Петровский С.В. Специфика договоров на создание гипертекстовых документов (Интернет-страниц). См. по адресу: <http://www.russianlaw.net/law/doc/a108.htm>.

<sup>4</sup> См.: Ведомости Верховного Совета РСФСР. 1992. № 42. Ст. 2325

ных данных для обработки с помощью ЭВМ и создания гипертекстовых документов для веб-сайта, должно осуществляться на общих основаниях с учетом существующих проблем несанкционированного доступа в сети в Интернет. ГК РФ предусматривает обязанность подрядчика по сохранению конфиденциальности переданных ему сведений и устанавливает ответственность за ненадлежащее качество работы.

Результатом выполнения договора на переработку коммерческой информации является создание нового информационного продукта. Содержание договора на переработку информации зависит от согласованного сторонами предмета договора. Чаще всего подрядчиком выступает специализированное информационное агентство, которое может предоставить заказчику интересующую его информацию для последующей ее переработки. Стороны могут в этом случае заключить договор на передачу и переработку информации. Стоимость предоставляемой заказчику информации будет определяться степенью ее конфиденциальности. Переработка информации может производиться путем предоставления информации, которая имелась у заказчика. Ответственность за достоверность информации в этом случае лежит на стороне, предоставившей ее для переработки.

Полученные в результате переработки сведения совместным решением заказчика и подрядчика могут быть признаны коммерческой тайной. Меры по охране конфиденциальности такой информации должны обеспечиваться самостоятельными действиями сторон. В договоре стороны должны предусмотреть условие конфиденциальности информации, переданной на переработку. То же самое касается и полученного нового информационного продукта. Стороны должны установить запрет на его передачу третьим лицам без согласия другой стороны. В договоре или в отдельном соглашении к нему стороны должны определить общие меры по обеспечению охраны конфиденциальности такой информации. Как правильно отмечает М.И. Брагинский: «Отсутствие соглашения, о котором идет речь, не освобождает сторону от указанных обязанностей, если она предоставит доказательства того, что сообщила контрагенту о конфиденциальности соответствующей информации»<sup>1</sup>. Этот вывод подтверж-

<sup>1</sup> Брагинский М.И., Витрянский В.В. Договорное право. Книга третья: Договоры о выполнении работ и оказании услуг. М., 2005. С. 69.

дается императивным действием нормы, содержащейся в ст. 727 ГК РФ, но при условии наличия договорных отношений.

**Третью самостоятельную группу составляет договор на оказание возмездных информационных услуг.** Правовая природа и содержание этого договора достаточно подробно исследованы в юридической науке.

Понятие информационной услуги было дано в ныне утратившем силу ФЗ от 4 июля 1996 г. № 85-ФЗ «Об участии в международном информационном обмене»<sup>1</sup> и определялось как действия субъектов, связанные с обеспечением пользователей информационных продуктами. ГК РФ отдельно не регулирует договор на оказание информационных услуг, хотя в п. 2 ст. 779 ГК РФ упоминается, что правила, содержащиеся в главе 39 ГК РФ («Возмездное оказание услуг»), применяются к данному виду договора. Такое обобщение и урегулирование в одной главе ГК РФ широкого круга отношений, имеющих различную правовую природу (например, медицинские, аудиторские услуги и др.), при отсутствии общих положений о договоре этого типа, приводит на практике к произвольному толкованию норм по поводу урегулирования КЗИ. Поэтому к данному договору должны применяться общие положения о договоре и специальные нормы гл. 39 ГК РФ.

Потребитель информации (заказчик) заключает с соответствующим субъектом (исполнителем) договор об оказании услуг, связанных с консультативным и техническим содействием, например, при оборудовании технологической линии производства, проведением юридического консалтинга, использованием банком данных, размещением в Интернете рекламы на сайтах и в электронных изданиях, подготовкой и передачей письменных консультаций и заключений по электронной почте. В предмете договора указывается, что при оказании исполнителем услуг будет использована информация, составляющая его коммерческую тайну. Поэтому определяется условие о конфиденциальности.

Отдельно может быть оговорено условие о конфиденциальности при передаче информации на носителях и оказании консультационных услуг. Определенные особенности имеет договор с информационными посредниками — сервис-провайдерами, что выражается в присоединении пользователя к разработанным исполнителем

<sup>1</sup> СЗ РФ. 1996. № 28. Ст. 3347.

условиям договора с одновременным приобретением специальных пластиковых карт, содержащих уникальные коды доступа и идентифицирующие пользователя. Такая информация носит конфиденциальный характер.

Обязанностями исполнителя, осуществляющего информационное обслуживание, могут быть, например, ежемесячное предоставление анализа состояния рынка судных капиталов; публикация рейтинговых таблиц, отражающих конкретные параметры предприятий-конкурентов (уставный капитал, баланс, прибыль и др.); предоставление реkvизитов и балансовых показателей банков, выступающих гарантами в международной купле-продаже; анализ состава ценных бумаг предприятий-конкурентов на биржах. Специальная подборка для организации информации, с учетом специфики ее деятельности, несомненно, представляет интерес для конкурентов. Поэтому должны быть предприняты меры по ее защите.

Стороны должны включать в договор положение, запрещающее заказчику передавать информацию, полученную от исполнителя, третьим лицам. В свою очередь, исполнитель обязуется не разглашать данные коммерческого характера, полученные им от заказчика, составляющие его коммерческую тайну. Стоимость услуг и расчеты за них согласовываются сторонами с учетом важности информации и порядка, установленного ГК РФ.

Контрагенты могут предусмотреть ответственность за невыполнение или ненадлежащее выполнение обязательств, в том числе связанных с охраной КЗИ. В случае несвоевременного предоставления информации исполнитель возвращает заказчику деньги за тот период, в течение которого информация не представлялась, а заказчик приостанавливает перечисление денежных средств на расчетный счет исполнителя. Исполнитель в случае несвоевременного перечисления заказчиком денежных средств может приостановить информационное обслуживание. Сдача и прием выполненных работ в виде информационных услуг производится сторонами по акту, как правило, в месте нахождения заказчика.

Заключение договора об информационном обслуживании с использованием баз данных на ЭВМ имеет некоторые особенности. В предмете договора указывается конкретная база данных (например, банковское законодательство, формы правовых документов и др.). Особо оговаривается ответственность сторон в случаях, когда компьютер заражен каким-либо вирусом либо система не работает в свя-

зи с неисправностью компьютера; определяется порядок передачи права на пользование базой данных другой организации.

Обязанности сторон в зависимости от вида обслуживания и способа передачи информации (телефонная, телеграфная и факсимильная связь, др.) могут видоизменяться, но правовое существо договора возмездного оказания информационных услуг останется прежним. Оказание этих услуг оценивается заказчиком как положительная для него деятельность, независимо от результата использования полученной информации.

**Четвертая группа договоров в сфере обращения КЗИ может быть условно представлена договором коммерческой концессии**, который является в соответствии с ГК РФ самостоятельным видом гражданско-правовых договоров (Е.А. Суханов)<sup>1</sup>?. Условность отнесения его к этой группе объясняется тем, что одна сторона (правообладатель) обязуется предоставить другой стороне (пользователю) право использовать в предпринимательской деятельности пользователя комплекс принадлежащих правообладателю исключительных прав, включая и право на секрет производства (ноу-хау). В цивилистической науке выделяются обязательные (право на коммерческое обозначение правообладателя, секрет производства (ноу-хау)<sup>3</sup> и факультативные (право на товарный знак, знак обслуживания или иное средство индивидуализации) объекты договора коммерческой концессии.

Цель и экономическая сущность договора коммерческой концессии, его содержание неоднократно рассматривались в юридической литературе<sup>4</sup>. Данный договор носит долгосрочный характер. Правообладателем может быть только коммерческая организация, имеющая фирменное наименование. Пользователем может выступать юридическое лицо, занимающееся предпринимательской деятельностью, и индивидуальный предприниматель. Предметом договора

<sup>1</sup> См.: Гражданское право: Учебник. В 2 т. Т. II. Полутом 1 / Отв. ред. проф. Е.А. Суханов. М., 2000. С. 623 — 636.

<sup>2</sup> И.А. Зенин предлагает договор о коммерческой концессии относить к особому классу договоров об использовании исключительных прав и ноу-хау, см.: Гражданское право. В 2 т. Т. II. Полутом 1. С. 581.

<sup>3</sup> См.: Гражданское право. В 2 т. Т. II. Полутом 1. С. 577, 582—583, 585.

<sup>4</sup> См.: *Авилов Г.Е.* Коммерческая концессия (глава 54) // Гражданский кодекс РФ. Ч. 2 / Под ред. О.М. Козырь, А.Л. Маковского, С.А. Хохлова. М., 1996; *Брагинский М.И., Витрянский В.В.* Договорное право. Книга третья: Договоры о выполнении работ и оказании услуг. М., 2005. С. 977—1049; *Лугинский Б.И.* Коммерческое право России. Учебник. 2-е изд. М., 2006. С. 257—262, и др.



является не только предоставление пользователю права использования в своей деятельности комплекса исключительных прав, включая передачу технической и коммерческой документации, иной информации, необходимой ему для осуществления исключительных прав, и защита пользователем такой информации в режиме коммерческой тайны. ГК РФ содержит императивные нормы, обязывающие правообладателя производить инструктаж пользователя и его работников по вопросам, связанным с осуществлением исключительных прав (п. 1 ст. 1031 ГК РФ), включая и охрану конфиденциальности КЗИ. Пользователь обязан соблюдать устоявшийся режим коммерческой тайны и не разглашать секреты производства правообладателя и другую полученную от него конфиденциальную информацию (ст. 1032 ГК РФ).

Названные положения должны учитываться сторонами при определении условий конфиденциальности, и могут содержать не посредственно в самом договоре о коммерческой концессии или в отдельном договоре о защите коммерческой информации. Учитывая долгосрочный характер договора и привлечение других лиц (коммерческая субконцессия) с передачей им комплекса или части прав правообладателя, представляется необходимым, по аналогии с охраной конфиденциальности информации по НИОКР, использовать Совместное заключение, Единый план (при заключении договоров субконцессии) и план мероприятий по обеспечению конфиденциальности информации. Основными условиями договора о защите коммерческой информации, которые могут быть предметом обсуждения сторон, являются следующие положения.

В предмете договора раскрывающая сторона отражает содержание передаваемой информации, составляющей ее коммерческую тайну, а получающая сторона указывает цель получения такой информации и правовые основания передачи (договор коммерческой концессии и др.) Получающая сторона берет на себя обязательство не разглашать полученную информацию третьим лицам и соблюдать достаточную степень секретности, позволяющую предупредить возможную утечку информации.

С момента заключения договора получающая сторона не будет разглашать информацию, полученную от раскрывающей стороны, являющуюся коммерческой тайной, другим лицам и не будет использовать эту информацию для своей собственной выгоды, за исключением целей, названных в договоре. В договоре может быть указан срок, в течение которого запрещается разглашать информацию,

а также ответственность в случаях разглашения (утечки) такой информации.

Получающая сторона будет соблюдать столь же высокую степень конфиденциальности во избежание разглашения этой информации, какую получающая сторона соблюдала бы в разумной степени в отношении своей собственной конфиденциальной информации такой же степени важности. В этих целях назначается конкретное лицо, ответственное за обеспечение режима коммерческой тайны.

Любая информация, передача которой оформлена в письменном виде и отнесена обеими сторонами к договору, считается конфиденциальной и подлежит защите в режиме коммерческой тайны. Конкретная информация, содержащая коммерческую тайну, может быть передана в приложении к договору. Стороны прилагают все усилия по сохранности документов, материалов и изделий, имеющих гриф «Коммерческая тайна», и реализуют в полном объеме меры по обеспечению режима конфиденциальности информации.

Информация не будет считаться конфиденциальной, и получающая сторона не будет иметь никаких обязательств в отношении данной информации, если информация стала известной получающей стороне из открытых источников, получена на законных основаниях от третьей стороны без ограничения и нарушения договора, самостоятельно получена в процессе производственной деятельности, раскрыта по мотивированному требованию государственных органов или органов местного самоуправления.

Перечисленные обязательства сторон могут быть примерными и использоваться при формировании условия о конфиденциальности применительно к любой группе договоров с учетом особенностей регулирования ими сферы обращения КЗИ.

защитности имущественных и иных интересов организации в информационной сфере от внутренних и внешних угроз, реализация которых может причинить ей ущерб. Доктрина информационной безопасности России Российской Федерации отделила не выделяет угрозы интересам организаций и меры по их предупреждению, а формулирует лишь общие положения по обеспечению информационной безопасности интересов личности, общества и государства<sup>1</sup>. Поэтому организации с учетом особенностей своей деятельности вынуждены формировать собственную систему обеспечения информационной безопасности. Важное место в этой системе занимает деятельность по охране конфиденциальности информации, которая включает организационное, правовое и научно-методическое ее обеспечение и, по существу, образует систему обеспечения безопасности организации.

В литературе<sup>2</sup> содержатся различные предложения по решению проблем создания системы обеспечения безопасности организации. Большинство авторов<sup>3</sup> при определении понятия такой системы справедливо включают в нее три взаимосвязанных элемента: «интересы — угрозы — защита», отмечая при этом их основополагающую роль в механизме этого процесса. Безусловно, этот вывод имеет прямое отношение к построению системы обеспечения ИБ организаций, но нуждается в пояснении применительно к целям настоящего исследования. Построение системы безопасности организации требует учета существующих угроз ее интересам. Под *интересами* в данном случае понимаются частные интересы организаций и индивидуальных предпринимателей, динамично связанные с их экономическими целями и задачами. *Угрозы* (внутренние и внешние) обычно проявляются в негативных проявлениях, реально или потенциально препятствующих организации по достижению своих целей и созданию

<sup>1</sup> См.: Доктрина информационной безопасности РФ от 9 сентября 2000 г. // Российская газета. 2000. 28 сент.

<sup>2</sup> См.: Шиверский А.А. Защита информации: проблемы теории и практики. М., 1996. С. 97–109; Ярошкин В.И. Безопасность информационных систем. М., 1996. С. 205–290; Герасименко В.А., Малюк А.А. Основы защиты информации. М., 1997. С. 357–417; Панкратов Ф.Г., Серегина Т.К. Коммерческая деятельность. М., 1997. С. 55–61; Фатыхов А.А. Правовое обеспечение безопасности информации в Российской Федерации. М., 2001. С. 199–207, и др.

<sup>3</sup> См.: Стрельцов А.А. Обеспечение информационной безопасности России. Теоретические и методологические основы / Под ред. В.А. Саловниченко и В.П. Шерстюка. М., 2002. С. 41–117; Экономическая безопасность России: Общий курс: Учебник / Под ред. В.К. Сенчагова. М., 2005. С. 106–126, и др.

## ГЛАВА 3

### Организационное обеспечение деятельности по охране конфиденциальности информации

#### § 1. Угрозы интересам коммерческой организации и основные параметры построения системы ее безопасности

**Сущность обеспечения деятельности по охране конфиденциальности информации.** Обеспечение национальных интересов страны тесно связано с деятельностью коммерческих организаций, занимающих доминирующее положение в рыночной экономике. В ст. 1 Закона РФ от 5 марта 1992 г. № 2446-1 «О безопасности»<sup>1</sup> дается общее определение безопасности как состояния защищенности жизненно важных интересов личности, общества и государства от внутренних и внешних угроз. Под жизненно важными интересами организаций понимается совокупность потребностей, удовлетворение которых надежно обеспечивает их существование и создает возможности для прогрессивного развития.

Информационная безопасность (ИБ) организаций является важнейшим звеном общей системы национальной безопасности Российской Федерации. В общих чертах ее можно определить как *состояние*

<sup>1</sup> См.: Ведомости Съезда народных депутатов РФ и Верховного Совета РФ. 1992. № 15. Ст. 769; 1993. № 2. Ст. 77; Собрание актов Президента и Правительства РФ. 1993. № 2. Ст. 5086.

щих опасность ее жизненно важным частным интересам. Под защитой информации имеются в виду меры организационного, правового и научно-методического характера, реализация которых позволяет защищать КЗИ от непреднамеренного воздействия, несанкционированного доступа, от разглашения и утечки информации<sup>1</sup>, включая деятельность по предотвращению получения информации конкурентной разведкой с целью обеспечения стабильного и устойчивого экономического развития организации.

Названные общие положения определяют условия формирования системы безопасности любой организации. В концептуальном плане для решения задачи, связанной с созданием надежной системы безопасности, важно иметь точное представление о *понятии, целях и принципах обеспечения ИБ организации*. Понятия «обеспечить», «обеспечение», в широком смысле слова, определяются в русском языке как один из видов деятельности и как средство деятельности. Как вид деятельности, «обеспечение» означает совокупность действий, предпринимаемых для того, чтобы сделать нечто «вполне возможным, действительным, реально выполнимым», а как средство деятельности — «то, чем обеспечивают кого-нибудь или что-нибудь». Нужно согласиться с мнением А.А. Стрельцова<sup>2</sup>, что в первом случае речь идет об одном из видов деятельности, связанном с действиями, предпринимаемыми для того, чтобы сделать нечто «вполне возможным, действительным, реально выполнимым», а во втором — как средство деятельности. По мнению А.А. Стрельцова, структура понятия «обеспечение» включает «деятельность по обеспечению — оказание помощи субъектам в достижении поставленных ими целей», «средства обеспечения — совокупность материальных, духовных, финансовых, правовых, организационных и технических средств...» и «субъекты обеспечения — индивиды, организации, органы государства, осуществляющие деятельность по обеспечению»<sup>3</sup>.

*Деятельность по обеспечению охраны конфиденциальности информации в гражданском обороте* может быть представлена в виде совокупности продолжающихся в течение длительного времени действий, направленных на увеличение доходов организации, исклю-

<sup>1</sup> См.: ГОСТ Р 50922-96 «Защита информации. Основные термины и определения».

<sup>2</sup> См.: Стрельцов А.А. Указ. соч. С. 41.

<sup>3</sup> См.: Там же. С. 45.

чение неоправданных расходов, сохранение положения на рынке производства и реализации товаров или получение иной коммерческой выгоды. Постоянный характер этих действий можно объяснить тем, что информация, обращаемая в организациях, охватывается во всех факторах общественного производства и составляет начальный, «нулевой» цикл по отношению к любому производимому товару, выполняемой работе и оказываемой услуге. Субъектами такого рода деятельности выступают лица, относимые доктриной частного права к различным видам субъектов гражданского и коммерческого права. Они реализуют свои коммерческие цели в условиях оборотоспособности товаров (работ, услуг), являющихся объектами гражданского права. Деятельность по обеспечению охраны коммерческой тайны заключается в оказании помощи субъектам гражданского и коммерческого права в решении стоящих перед ними задач.

*Обеспечение как средство деятельности*, то есть «то, чем обеспечивают кого-нибудь или что-нибудь», представляет собой совокупность материальных, финансовых, правовых, организационных и иных средств, которые повышают эффективность деятельности по достижению целей. При определении *целей обеспечения ИБ организации* следует учитывать, что любой хозяйствующий субъект представляет собой сложную информационную систему. Конкуренция обуславливает обновление ассортимента и улучшение качества выпускаемых товаров, достижение которых возможно за счет введения в оборот новой технической, технологической и деловой информации. В этой связи КЗИ постоянно подвергается различным внутренним и внешним угрозам со стороны конкурентов и других лиц. Меры по обеспечению ИБ организацией направлены на исключение факторов разглашения (утечки) КЗИ и несанкционированного доступа к ней. Реализация мер должна обеспечивать не только собственно безопасность статуса КЗИ, но и способствовать стабильному развитию организации, увеличению ее доходов и получению иной коммерческой выгоды.

*Целями обеспечения ИБ организацией* является защита их законных прав и интересов во взаимоотношениях с органами государственной власти и местного самоуправления, партнерами и конкурентами, поддержание внутреннего порядка управления, повышения конкурентоспособности производимых товаров, развитие кооперированных связей и недопущение зависимости от недобросовестных конкурентов и партнеров, ориентация развития техники и технологий на мировые стандарты по профилю деятельности организации,

создание благоприятной рыночной конъюнктуры и рост прибылей за счет эффективного использования КЗИ. Достижение указанных целей предполагает решение *задач* по своевременному выявлению угроз жизненно важным интересам, оперативному использованию правовых средств предупреждения причин и обстоятельств, способствующих правонарушениям и ведущим к открытию возможных каналов утечки (ВКУ) КЗИ, пресечению неправомерных действий лиц и возмещению убытков.

*Реализация задач требует от организаций соблюдения принципов законности при осуществлении мер ИБ с учетом разрешенных законом методов выявления, предупреждения и пресечения правонарушений в сфере обращения КЗИ; экономической целесообразности мероприятий по обеспечению ИБ, которые не должны снижать экономические показатели деятельности организации и ее прибыль; взаимодействия и координации мер по защите КЗИ с партнерами; профессионализма и ответственности работников, специализирующихся по конкретным направлениям ИБ организаций, их ответственности за результаты своей деятельности.*

**Характеристика угроз безопасности коммерческих организаций.** Построение системы безопасности организации требует учета существующих угроз ее интересам. Коммерческая организация в процессе своего функционирования выступает объектом безопасности. Поэтому она сама определяет содержание, понятие и пределы своей безопасности, учитывая при этом возникающие возможные угрозы ее существованию и развитию. Безопасность организации проявляется через ее состояние, которое позволяет увеличивать доходы (получать прибыль), избежать неоправданных расходов, сохранить стабильное и прогрессивное положение на рынке товаров (работ, услуг) или получить иную коммерческую выгоду.

Понятие информационной безопасности организаций нельзя сводить только к понятию безопасности информации. Как отмечал А.И. Алексеев, «потеря носителя информации, хищения носителя информации или отображенной в нем информации, несанкционированного уничтожения носителя информации... искажения информации, блокирования информации, разглашения информации»<sup>1</sup> представляет нарушения целостности безопасности информации.

<sup>1</sup> См.: Алексеев А.И. Понятие и структура угроз защищаемой информации // Безопасность информационных технологий. 2000. № 3. С. 79–80.

Очевидно, что понятие информационной безопасности организации значительно шире и включает в себя не только нарушение статуса КЗИ, но и множество других угроз внутреннему и внешнему характеру, оказывающих негативное воздействие на экономическую деятельность и определяющих в конечном итоге ее безопасность.

Отсюда важно проанализировать общие и конкретные угрозы, оказывающие влияние на защиту имущественных интересов организаций с использованием института коммерческой тайны.

*Общие угрозы* национальным интересам России, действующие в информационной сфере, могут привести к дестабилизации устойчивого экономического положения организации. Сравнительно распространяющую их разновидность составляют угрозы имущественным интересам организаций, в основе которых лежит принятие<sup>1</sup> правовых актов, ущемляющих интересы организаций, их многообразие и противоречивость; неспровоцированные претензии различных контролирующих федеральных органов (по ценным бумагам, налогам и сборам и др.); невыполнение партнерами, заказчиками, поставщиками своих обязательств по поставке товаров и их оплате; получение криминальными структурами доступа к КЗИ финансового характера; проведение целенаправленных спекуляций на рынке ценных бумаг; вытеснение отечественного производства импортом<sup>2</sup>. Кроме названных, исследователи отмечают другие явления и процессы, отрицательно влияющие на деятельность организаций, которые особо проявляются в период мирового финансового кризиса. В их числе: широкое распространение неплатежей, резкое снижение выпуска качественной продукции, низкая эффективность и конкурентоспособность товаров по сравнению с дореформенным уровнем, недостаточная занятость работников на предприятиях и задержки выплаты заработной платы в отдельных регионах страны, перевод денежных ресурсов за рубеж, хроническая убыточность примерно одной трети промышленных предприятий, превращение российской экономики в объект политического противоборства политических элит, партий и движений.

Отдельные общие угрозы могут носить конкретный характер для организации с учетом сложившейся хозяйственной ситуации. Наи-

<sup>1</sup> См.: Ващенко Н.П., Дзалиев М.И., Урсул А.Д. Безопасность предпринимательской деятельности. М., 2002. С. 237–239.

<sup>2</sup> См.: Информационное право: Учебник / Под ред. Б.Н. Топорнина. СПб., 2001. С. 438–446. и др.

более типичными, на наш взгляд, внешними угрозами безопасности организации являются следующие явления, которые достаточно широко распространены в предпринимательской практике.

*Во-первых*, как отмечает Н.П. Ващенко, угрозы могут исходить от нормативных актов, издаваемых различными ведомствами<sup>1</sup>. С такой оценкой трудно согласиться, но, тем не менее, необходимо отметить наличие отдельных правовых актов, которые порой носят противоречивый характер. Их применение на практике представляет значительные сложности в сфере малого предпринимательства и вызывает справедливые нарекания со стороны работников этих организаций. К этому следует добавить и имеющиеся место неспровоцированные претензии со стороны различных контролирующих органов (налоговая инспекция, пожарная служба, санитарный надзор и др.). Иногда, в результате непродуманных действий, они существенно затрудняют работу путем проведения многочисленных, беспорядочных проверок и запрашивают такую КЗИ, которая не нужна им для выполнения возложенных на них функций.

*Во-вторых*, угрозы могут возникнуть вследствие невыполнения или ненадлежащего выполнения контрагентами своих обязательств, например, по оплате отгруженной продукции, своевременной ее поставки.

*В-третьих*, угрозы могут исходить от криминальных структур, которые пытаются получить доступ к КЗИ, и, прежде всего, к данным о финансовом состоянии организации. Следует особо подчеркнуть существующую опасность сращивания государственных и криминальных структур, что способствует снижению степени защищенности законных интересов и прав организаций.

Итак, внешние угрозы безопасности нормальной деятельности организаций могут проявляться в результате правотворческой и правоприменительной деятельности государственных органов и органов местного самоуправления, недостаточно учитывающих частные интересы организаций при формировании «правил поведения» на рынке, а также нарушений договорной дисциплины со стороны контрагентов.

*Состояние внутренней безопасности организаций* существенно отражается на их финансовых результатах в сфере бизнеса. По статистике, более ¾ убытков фирма несет из-за прямого участия своих ра-

<sup>1</sup> См.: Ващенко Н.П., Дзюев М.И., Урсул А.Д. Указ. соч. С. 242–244.

ботников в тех и иных незаконных деяниях<sup>1</sup>. В литературе описаны различные способы классификации угроз информационной безопасности. Так, компания Digital Security предлагает различать угрозы технологического (физические и программные) и организационного (физическое и психологическое воздействие на персонал и действия персонала) характера<sup>2</sup>. В центре этой классификации находится работник фирмы, от которого может исходить угроза безопасности информации. К числу наиболее распространенных *внутренних угроз*, по нашему мнению, следует отнести: внутренние конфликты в коллективе или среди руководства организаций, порой контролируемые конкурентами либо преступными группировками; противоправные и иные негативные действия работников организаций; нарушение установленного порядка сохранения продукции и документов; несоблюдение установленного режима работ, при выполнении технических и иных средств защиты КЗИ; нарушения порядка использования технических и иных средств информации, к несанкционированному доступу к которой, ее тиражированию и модификации. Поэтому внутренние угрозы напрямую связаны с «человеческим фактором» и представляют наибольшую опасность для организаций.

Существенное значение для понимания угроз безопасности организации имеет **учет дестабилизирующих факторов, обуславливающих угрозы безопасности обращения КЗИ**. Система обеспечения безопасности организации представляет собой взаимодействие различных служб и подразделений, которым предоставлены определенные полномочия по защите интересов организации. Специально создаваемое в рамках организации подразделение — *служба безопасности* — обеспечивает слаженное функционирование всей системы обеспечения безопасности. Нормальная хозяйственная деятельность организации может быть нарушена вследствие воздействия на нее неблагоприятных внешних и внутренних факторов, реализация которых может причинить ущерб ее частным интересам. В литературе<sup>3</sup> эти факторы получили название «**дестабилизирующих факторов**», то есть условий, ведущих к *дестабилизации*, в результате чего происходит снижение уровня хозяйственной деятельности организации, и возникают угро-

<sup>1</sup> См.: Ващенко Н.П., Дзюев М.И., Урсул А.Д. Указ. соч. С. 242–250.

<sup>2</sup> См.: Сайт компании Digital Security: <http://www.dssec.ru/>

<sup>3</sup> См.: Алексеев А.И. Указ. соч. С. 79–85, и др.

зы для ее безопасности. Дестабилизация работы организации означает нарушение привычного, делового ритма ее хозяйственной деятельности.

Причинами возникновения и развития хозяйственных кризисных ситуаций, угрожающих безопасности организации, могут быть различные объективные и субъективные факторы дестабилизации, которые способствуют формированию причины и помогают ее действию. Речь идет о детерминации, которая «...означает связь основания и производного, зависимость свойств вещей, событий, процессов, состояний в их осуществлении и изменении от любых факторов»<sup>1</sup>. Как отмечает Н. Ф. Кузнецова: «Специфика социальной детерминации состоит в том, что сами поступки членов общества и их последствия происходят мотивированно и целенаправленно»<sup>2</sup>. Их можно рассматривать как совокупность взаимосвязанных *determinants* (в переводе с лат. означает «*опредетитель*»), позволяющих охарактеризовать объект как *основной фактор*, и связанными с ним *производных факторов*: субъект, объективную (внешнюю) и субъективную (внутреннюю) стороны, образующих *состав дестабилизации*, и раскрыть его содержание.

*Под объектом дестабилизации*, создающей угрозу безопасности организации, следует понимать нарушение ее жизненно важных интересов путем неправомерного изъятия в конкурентных целях КЗИ, касающейся управления, финансово-кредитной и маркетинговой деятельности, полученных результатов НИОКР, освоения промышленного производства и реализации товаров, выполнения других работ (услуг). В данном случае происходит нарушение нормального цикла деятельности организации, которая уже не способна в прежнем режиме решать задачи, связанные с увеличением доходов; предпринимем неоправданных расходов; сохранением лидирующего положения на рынке товаров (работ, услуг); получением иной коммерческой выгоды. Нарушение конфиденциальности информации в силу действия дестабилизирующих факторов, ведет к ее утрате, разглашению (утечке) и, таким образом, способно причинить ущерб организации.

<sup>1</sup> Кузнецова Н. Ф. Детерминация в уголовном праве и криминологии // Теоретико-методологические проблемы права / Под ред. проф. М. Н. Марченко. Вып. 2. М., 2007. С. 319.

<sup>2</sup> Там же.

*Субъектом дестабилизации* является физическое или юридическое лицо, которое может причинить вред жизненно важным интересам организации. *Объективная сторона дестабилизации* формируется в результате внешних по отношению к организации действий субъектов и зависит от степени влияния на хозяйственную ситуацию дестабилизирующих явлений и процессов, происходящих в обществе и государстве. Это может проявляться в результате действий государственных органов и органов местного самоуправления по изданию правовых актов, ущемляющих частные интересы организаций, ис требованию не нужной им для работы информации, составляющей коммерческую тайну; действий контрагентов, не выполняющих договорные условия о конфиденциальности информации, а также конкурентов, неправомерно осуществляющих сбор и использование КЗИ. *Субъективная сторона дестабилизации* проявляется в тех целях, которые преследует субъект дестабилизации, находящийся внутри организации. Речь идет о неисполнении или ненадлежащем исполнении сторонами условий трудового договора по охране конфиденциальности КЗИ, что связано с причинением вреда интересам организации.

Определенное выше **понятие состава дестабилизирующих факторов (ДФ) положено в основу типизации дестабилизирующих факторов (ДФ)**, обуславливающих существование угроз безопасности организации. Как представляется, типизация ДФ имеет значение для принятия решения о направлении защиты КЗИ в конкретной хозяйственной ситуации, сложившейся в организации. Ее разработка нужна для составления примерного перечня угроз интересам организации. Угрозам должны адекватно противостоять конкретные меры, составляющие содержание системы обеспечения безопасности. Реализация этих мер осуществляется различными подразделениями, на которые возложены соответствующие обязанности по обеспечению безопасности организации.

Определение примерного перечня ДФ необходимо для нахождения более эффективных способов противодействия возможным угрозам безопасности. Их типизация может быть проведена на основе учета взаимодействия элементов, образующих содержательную сторону дестабилизирующих явлений и процессов. Такой способ применяется во многих организациях<sup>1</sup>. Он представляется достаточно

<sup>1</sup> О фактах дестабилизации при нейтрализации угроз экономической безопасности см.: Экономическая безопасность России. М., 2005. С. 643–647, и др.

наглядным и позволяет определить основные направления деятельности организации по обеспечению ее безопасности.

*Объект дестабилизации* занимает в типизации ДФ базисное, практически неизменное положение. Его место определяется основными жизненно важными интересами организации, связанными с получением прибыли. Этой цели подчинены все другие интересы. Остальные элементы состава дестабилизации в типизации ДФ выстраиваются в такой последовательности и взаимозависимости, которая позволяет им находиться в прямой связи с объектом дестабилизации.

Ключевое место в типизации ДФ отводится *субъекту дестабилизации*, действия либо бездействие которого определяют характер и содержание угроз организации. Субъектами дестабилизации могут выступать: конкуренты (конкурирующая организация), в лице своих представителей; персонал организации (администрация, руководители структурных подразделений, менеджеры и другие работники); партнеры, в том числе дочерние и зависимые общества, клиенты, посредники и другие лица, ведущие предпринимательскую деятельность; эркет и иные формы организованной преступности; государственные органы и органы местного самоуправления в лице их служащих; сторонние юридические и физические лица, действующие в своих интересах, противоречащих интересам данной организации.

Важным этапом типизации ДФ является определение наиболее характерных дестабилизирующих явлений и процессов, составляющих содержание объективной и субъективной стороны дестабилизации организации. Эта работа представляет собой трудность для любой организации. Приведенные выборочные данные о дестабилизирующих явлениях и процессах, создающих угрозы безопасности организации, являются результатом многолетних опросов работников ряда предприятий, и личных наблюдений автора.

*Дестабилизирующие факторы, определяющие содержание объективной стороны дестабилизации*, проявляются в виде следующих действий субъектов: принятие отдельных правовых актов, ущемляющих имущественные интересы организаций (налогообложение, кредитование, инвестирование и др.); целенаправленное вытеснение с определенного рынка товаров (работ, услуг) путем использования недобросовестных форм конкуренции; невыполнение или ненадлежащее выполнение контрагентами обязательств по охране конфиденциальности информации; вмешательство криминальных структур в управление организацией (заключение невыгодных сделок, слияние компаний, доведение до банкротства и др.); неправомерный доступ кри-

минальных структур к КЗИ о финансовом состоянии организации; использование приемов недобросовестной конкуренции для получения КЗИ о деятельности организации за счет сращивания государственных и криминальных структур; ведение промышленного шпионажа по сбору КЗИ конкурентами; совершение иных неправомерных действий в отношении организации, запрещенные законом.

*Дестабилизирующие факторы, определяющие содержание субъективной стороны дестабилизации*, могут проявляться в следующих действиях организации и ее персонала: неправомерное получение информации о деятельности партнеров и конкурентов, что может быть связано с исками в суд; отсутствие материальных и иных условий, обеспечивающих функционирование системы безопасности организации; пренебрежительное отношение руководства к вопросам сохранения КЗИ; отсутствие корпоративных требований к персоналу по обеспечению охраны КЗИ; несоблюдение работниками правил собственной безопасности при работе с КЗИ; получение личной выгоды за счет использования КЗИ в ущерб интересам организации.

Перечень внешних и внутренних ДФ не является исчерпывающим. Их взаимосвязь и взаимодействие с другими элементами состава дестабилизации позволяет выявить угрозы объекту, т.е. судить о возможности возникновения реальных и потенциальных угроз безопасности организации. На этой основе можно моделировать различные изменения хозяйственной ситуации, ведущие к дестабилизации безопасности организации.

Использование данного способа типизации ДФ на практике состоит в построении графических конструкций взаимосвязи объективной стороны, субъекта и субъективной стороны дестабилизации, обловливающих изменение хозяйственной ситуации по отношению к исследуемому объекту дестабилизации. Полученные конструкции взаимодействия элементов дестабилизации позволяют понять, какие действия либо бездействие субъектов представляют угрозы безопасности организации и могут причинить вред ее жизненно важным интересам. Выявленные таким образом угрозы безопасности организации необходимо учитывать при разработке и реализации адекватных мер противодействия.

На основе полученных данных **разработан концептуальный подход к созданию системы мониторинга угроз информационной безопасности**, применительно к крупным коммерческим организациям. При формулировании предложений был использован опыт разработки аналогичных по структуре систем в советский период. В литературу-

ре давно обсуждается проблема автоматизации функций работников юридической службы и подразделения безопасности. Однако во многих публикациях не учитываются особенности организационно-правового обеспечения создания такой системы<sup>1</sup>. Вопрос о том, каким образом выявлять угрозы ИБ, которые в общем виде сформулированы в Доктрине информационной безопасности РФ, и, главное, как предупредить возникновение этих угроз, приобретает особую актуальность. Большая часть источников угроз интересам личности, общества и государства, которые названы в Доктрине, давно известны. Их противодействию в бывшем СССР уделялось серьезное внимание. Особенно, когда речь шла о защите государственных интересов. Однако с образованием Российской Федерации, переходом ее к рыночной экономике и вхождением в мировое информационное общество количественный и качественный состав угроз ИБ многократно возрос. Появились новые опасности как внутри страны, так и исходящие извне. Особенно это характерно для коммерческих организаций, которые вынуждены с использованием собственных сил и средств осуществлять противодействие угрозам их бизнесу.

В этих условиях важно определить на уровне организации алгоритм разработки системы сбора и анализа данных об источниках угроз ее безопасности, что позволит эффективно осуществлять меры предупреждения угроз на ранних стадиях их возникновения. Задача состоит в проведении постоянной работы, связанной с выявлением и предупреждением угроз. Это объясняется тем, что в короткий промежуток времени в различных звеньях организации возникают угрозы ИБ. Реакция органов управления на угрозы зачастую проявляется в действиях по ликвидации их последствий. Вместе с тем задача состоит, образно говоря, не в «тушении очагов пожара», явившихся источником угроз, а в выявлении их причин и разработке мер по их предупреждению. Поэтому должна постоянно действовать система, позволяющая решать задачи оперативного выявления угроз ИБ, оценки и прогнозирования ситуаций в наиболее важных сферах деятельности организаций, на конкретных участках, где сосредоточена КЗИ, и выдачи рекомендаций субъектам. Решение этой задачи

<sup>1</sup> См.: Ретин А.А., Кравченко С.В. Концепция автоматизации функций сотрудников режимно-секретных органов и контроль эффективности режимных мер на предприятиях России // Вопросы защиты информации. 1999. № 3; Ефрекина О.В. Информационное обеспечение договорно-правовых отношений: Опыт и перспективы применения автоматизированных информационно-поисковых систем: Автореф. дисс. канд. юрид. наук. М., 1997, и др.

может быть достигнуто путем разработки комплексно-целевой программы создания и внедрения автоматизированной системы управления мониторингом угроз (АСУ МУ) информационной безопасности коммерческих организаций. Кратко охарактеризуем основные параметры предлагаемой системы.

Проектирование и разработка системы должны осуществляться с соблюдением определенных принципов. К числу основных положений следует отнести:

- функционально-организационный и территориальный принцип создания АСУ МУ, позволяющий учитывать сферу интересов коммерческих организаций;
- комплексный охват информационной сферы с учетом имущественных интересов организаций и анализа их взаимоотношений с государственными органами, органами местного самоуправления, партнерами, клиентами, заказчиками и т.д.;
- единство организационного, правового, информационного, математического и технического обеспечения АСУ МУ;
- принцип последовательности разработки и внедрения отдельных составных звеньев системы (информационно-справочная система, оперативного контроля по выявлению и анализу возможных угроз ИБ, прогнозирования событий на объектах контроля и моделирования мер по предупреждению причин и условий, способствующих возникновению угроз ИБ и закрытию ВКУ информации);
- принцип типизации технических элементов АСУ МУ, методов преобразования информации и алгоритмов решения задач, связанных с возникновением угроз и их предупреждением; возможность адаптации и развития системы применением к любому уровню коммерческой организации;
- принцип непрерывного развития системы.

Названные принципы лежат в основе разработки *комплексно-целевой программы создания АСУ МУ*, которая может включать, на наш взгляд, три самостоятельные подпрограммы:

- быстрого выхода на автоматизацию основных функций, связанных с установлением режима коммерческой тайны в организации (сбор и анализ информации для включения в перечень сведений, составляющих коммерческую тайну, формирование и обеспечение функционирования допускной и разрешительной системы и др.);



- достижения основного результата автоматизации функций, связанных с обеспечением установленного в организации режима обращения КЗИ (выявление, оценка и прогноз возможных угроз ИБ, ВКУ КЗИ применительно к условиям конкретной хозяйственной ситуации с использованием различных форм и методов);
- моделирование мер по предупреждению угроз и закрытию ВКУ КЗИ, позволяющим в автоматизированном виде осуществлять выдачу рекомендаций субъектам (служба безопасности, руководители подразделений и др.) по использованию правовых и иных средств в целях предупреждения нарушений установленных режима коммерческой тайны и пресечению выявленных правонарушений.

При проектировании системы должны быть учтены существующая в крупных организациях специфика иерархической структуры управления (ассоциация, холдинг, корпорация и т.п.) и распределение функций между основным и дочерним акционерными обществами и их структурными подразделениями. Заказчиком системы может выступить основное общество, которое по договору о совместной деятельности с дочерним обществом выполняет функции головной организации — заказчика, разрабатывает и согласовывает техническое задание на разработку системы АСУ МУ, заключает договоры и обеспечивает выполнение обязательств.

Проектируемая система может включать различные *технологические режимы* ее работы. В частности, она может выполнять функции справочно-информационного обслуживания и управления системой защиты КЗИ.

*В-первых*, справочно-информационное обслуживание состоит в обеспечении необходимой информацией собственных подразделений и контрагентов в режиме «запрос — ответ» по вопросам обеспечения ИБ. Поэтому с контрагентами дополнительно заключается договор на оказание информационных услуг.

*Во-вторых*, АСУ МУ выполняет обеспечительную функцию управления системой безопасности. Режим управления системой состоит из ряда детерминированных операций. В частности, информационные потоки регламентируются по времени и кругу пользователей; соответствующие данные об угрозах выдаются оперативно в объеме поставленных задач; поступающие к субъектам данные используются в целях предупреждения возможных угроз безопасности; корректируются действия субъектов по нейтрализации и устранению

нию причин, способствующих возникновению угроз, которые могут привести к утечке КЗИ; осуществляется оперативное оповещение субъектов о появлении угроз, при этом их действия контролируются системой с помощью ЭВМ. Полученные таким образом результаты позволяют оперативно оценивать хозяйственную ситуацию и эффективность принимаемых мер по охране конфиденциальности КЗИ.

*Решение задач, связанных с разработкой и функционированием систем, предполагает соблюдение ряда условий:* обеспечение организационного единства выполняемых научно-исследовательских и проектных работ со стороны головного разработчика системы; согласование частных технических заданий исполнителям на разработку опытного образца системы; формирование заказчиком условий рамочного (основного) договора и их согласование с головной организацией — разработчиком; определение сроков выполнения работы и ее отдельных этапов; заключение договоров с исполнителями на выполнение отдельных частей НИОКР, включая и опытный образец АСУ МУ; привлечение к этой работе специалистов различного профиля (юристов, социологов, экономистов, математиков, программистов и др.); обеспечение гибких форм управления трудовым коллективом с учетом специализации разработчиков и аналитиков на различных этапах создания и эксплуатации системы.

*Работа по созданию АСУ МУ выполняется в несколько этапов. Для первого этапа характерным является развертывание головным разработчиком научно-исследовательских, проектных и макетных работ, практическое решение задач справочного, учетного, аналитического и контрольного характера с учетом типизации угроз организации заказчика. Второй этап связан с автоматизацией процессов подготовки, сбора, обработки и выдачи информации о возможных угрозах безопасности организации, причинах и условиях, способствующих разглашению (утечке) КЗИ, выполняемых на основании договора с заказчиком, в котором учтены особенности его хозяйственной деятельности, а также согласованы условия по охране конфиденциальности информации. Окончание работ на этом этапе позволит обеспечить организацию оперативной информацией о причинах и условиях возникновения возможных угроз ИБ, об открытии ВКУ КЗИ; совмещение функций управления и оперативного контроля за развитием хозяйственной ситуации на конкретных направлениях деятельности организации; получение необходимой информации для моделирования ситуаций, ведущих к угрозам. Третий этап автоматизации процессов в сфере обращения КЗИ посвящен созданию*

экспертной системы, обеспечивающей оперативное представление субъекту, в соответствии с его требованиями, набора автоматически проанализированных альтернатив решения задач, связанных с реализацией мер по предупреждению причин и условий, способствующих возникновению угроз ИИБ организации, ее партнерам и контрагентам.

Таким образом, разработка и внедрение АСУ МУ в организациях позволит более качественно решать задачи выявления и предупреждения угроз, возникающих в процессе ее деятельности с использованием ЭВМ и средств коммуникации.

## § 2. Опыт защиты секретной информации в советский период

*Деятельность органов государственной власти и управления в области защиты государственных секретов.* Существенное значение для понимания современного механизма регулирования защиты коммерчески значимой информации, организационного, правового и научно-методического обеспечения информационной безопасности коммерческих организаций имеет изучение советского опыта деятельности субъектов, осуществлявших защиту государственных секретов (далее — секретов), включавших информацию технического и технологического характера. Для современного этапа развития нашей страны в условиях смешанной рыночной экономики отдельные элементы советской системы защиты секретов обнаруживают тесную связь с практикой охраны конфиденциальности информации, прежде всего крупных коммерческих организаций.

В советский период действовал хорошо отлаженный механизм обеспечения режима секретности и охраны государственной тайны, в рамках которого осуществлялась защита сведений технического и технологического характера. Функционирование государственного механизма позволяло обеспечить на ранней стадии предотвращение разглашения (утечки) охраняемой информации. Обеспечение режима секретности (ОРС) проводимых работ представляло собой в тот период специфическую область государственного управления, имело многоуровневый характер и осуществлялось в процессе решения как общих задач производственной, научно-технической и хозяйственной деятельности, так и специализированных задач. ОРС работ не сводилось только к деятельности режимно-секретных органов

(РСО), а включало в себя широкий круг мер, которые осуществлялись государственными органами, администрацией и общественными организациями предприятий.

В зависимости от возложенных на них функций они осуществляли планирование мероприятий по ОРС работ и контроль за их выполнением и несли в этой связи ответственность в соответствии с законодательством. Деятельность субъектов по ОРС работ была объединена внутренним единством и обусловлена производственной, научной и хозяйственной деятельностью предприятий. Основными субъектами ОРС работ являлись государственные органы, администрация и общественные организации предприятий. Их деятельность осуществлялась при поддержке работников предприятий, которые по своей инициативе в целях оказания им помощи создавали органы общественной самодеятельности. Деятельность названных выше субъектов, независимо от выполнения ими тех или иных функций в области охраны секретов, осуществлялась под руководством партийных органов (КПСС), которые направляли и контролировали работу в этой области на различных уровнях управления. Рассмотрим более подробно роль каждой группы и входящих в нее органов и организаций.

**Первая группа субъектов — это высшие органы партийной (Центральный Комитет КПСС) и государственной власти (Верховный Совет СССР, Президиум СССР),** которые определяли политику в области защиты государственных секретов. Они принимали в установленном порядке законодательные акты по вопросам охраны государственной тайны, устанавливали уголовную ответственность за преступления, посягающие на сохранность секретов, порядок взаимодействия советских органов с иностранными учреждениями, определяли подсудность уголовных дел о государственной тайне и правовой статус органов хозяйственного управления в этой сфере.

Политика регулирования общественных отношений в области защиты технических и технологических секретов определялась объективными условиями исторического развития страны с учетом влияния факторов научно-технической революции и международной обстановки. Политические решения, принятые в тот период, находили отражение в законодательской и правоприменительной деятельности. Внимание высших органов власти было обращено, судя по принятым в то время постановлениям ЦК КПСС и законам, на повышение бдительности советских людей, усиление режима секретности, повышение мер уголовной ответственности и исключение преступ-

ных проявлений в области охраны секретов, определение компетенции органов государственного и хозяйственного управления, а также исключение фактов параллелизма и дублирования в их работе. Меры, принимаемые высшим эшелонном власти, поддерживали тотальный уровень секретности в стране. Достаточно сказать, что примерно 70 процентов действовавших в СССР нормативных правовых актов носили закрытый характер<sup>1</sup>. В этих условиях отсутствие закона о государственных секретах было естественным состоянием общества, когда само упоминание «режима секретности» уже было тайной.

Основной объем работы по охране государственных секретов выполняли **органы государственного управления общей (Правительство СССР), специальной (КГБ СССР, ГТК СССР, ГУОГ СССР) и отраслевой (министерства и ведомства СССР) компетенции**. Этими органами устанавливался административно-правовой режим защиты государственных секретов, представлявший совокупность административно-правовых норм, регулировавших порядок деятельности государственных органов и общественных организаций, предприятий, учреждений и организаций (далее — предприятия) в этой сфере.

Важная роль в формировании административно-правового режима принадлежала *Правительству СССР* как высшему органу государственного управления. Оно определяло с учетом состояния внутренней и внешней обстановки страны перечни главнейших сведений, составлявших государственную тайну, устанавливало единый на всей территории Союза ССР порядок обеспечения сохранения государственной тайны и режима секретности проводимых работ, принимало различные постановления по совершенствованию системы защиты секретов. Направления работы Правительства РФ, его полномочия применительно к защите государственных секретов, урегулированы в настоящее время ФЗ «О государственной тайне»<sup>2</sup> и не касаются правового регулирования КЗИ.

*Комитет государственной безопасности (КГБ) СССР* в пределах предоставленной ему компетенции осуществлял издание обязательных для всех министерств, ведомств и предприятий нормативных правовых актов в области защиты государственных секретов; толко-

вание порядка применения Инструкции № 0126-87 и других общесоюзных актов, регламентирующих режим секретности проводимых работ; контроль за состоянием обеспечения сохранности секретов и режима секретности. Инструкция № 0126-87 устанавливала обязательное согласование с органами КГБ вопросов создания или ликвидации РСО на предприятиях; издания ведомственных перечней сведений, подлежащих засекречиванию, и иных актов, регламентирующих порядок защиты секретов; оформления на допуск лиц к секретным, совершенно секретным и особой важности работам и документам; организации приема иностранцев в советских учреждениях и другие. Органам КГБ были предоставлены исключительные полномочия, связанные с запрещением производства секретных работ, если они проводились в помещениях и условиях, не гарантировавших режим их сохранности и секретности. Названные направления деятельности КГБ распределены в настоящее время на основании ФЗ «О государственной тайне» между различными органами государственной власти и местного самоуправления и не включают функцию защиты КЗИ. Полномочия государственных органов распространяются на коммерческие организации в том случае, если организации имеют допуск к проведению работ, связанных с использованием сведений, составляющих государственную тайну, и в установленном порядке получили лицензию и право использования сертифицированных средств защиты информации. Требования, предъявляемые к порядку работы со сведениями, составляющими государственную тайну, не распространяются на КЗИ, обрабатываемую в рыночной экономике.

Специальной компетенцией по защите государственных секретов, кроме КГБ СССР, были наделены и другие государственные органы. *Государственной технической комиссией СССР (ГТК СССР)* были предоставлены весьма обширные властные полномочия: она занималась общей организацией противодействия иностранным техническим разведкам (ПД ИТР). ГТК СССР была создана по постановлению ЦК КПСС и Совета Министров СССР от 18 декабря 1973 г. № 933-303 и являлась общесоюзным органом по организации в стране комплексных работ по ПД ИТР, проводимых всеми министерствами, ведомствами и предприятиями, выполнявшими работы по оборонной тематике. ГТК СССР и ее органы на местах определяли охраняемые сведения технического и технологического характера и осуществляли организационно-правовые и технические мероприятия по сокрытию демаскирующих признаков, раскрывающих

<sup>1</sup> См.: Социалистическая законность. 1988. № 9. С. 7.

<sup>2</sup> См.: Закон РФ от 21 июля 1993 г. № 5485-1 с изм. и доп. от 6 октября 1997 г. № 131-ФЗ // СЗ РФ. 1997. № 41. Ст. 4673.

эти сведения; оценивали и прогнозировали реальную опасность до-  
бывания охраняемых сведений с помощью технических средств раз-  
ведки; разрабатывали экономически обоснованные меры ПД ИТР и  
осуществляли контроль за эффективностью их реализации. Деятель-  
ность подразделений ПД ИТР на предприятиях была направлена на  
исключение или существенное затруднение действий иностранной  
технической разведки по добыванию охраняемых сведений о разра-  
батываемых образцах вооружения (В) и военной техники (ВТ) либо  
на создание у противника ложных представлений об этих объектах  
(легендирование). На территории страны был установлен единый  
порядок ПД ИТР, который регулировался Положением по противо-  
действию иностранным техническим разведкам, утвержденным пос-  
тановлением Совета Министров СССР от 10 июля 1984 г. № 733/162.  
В настоящее время действует аналогичный орган и в России. Зада-  
чей Государственной технической комиссии при Президенте Рос-  
сийской Федерации<sup>1</sup> является техническая защита информации, со-  
держашей сведения, составляющие государственную тайну, а так-  
же служебной тайны с пометкой «Для служебного пользования», в  
отношении которой установлен специальный порядок обращения  
в федеральных органах исполнительной власти, на подведомствен-  
ных предприятиях<sup>2</sup>. Полномочия Гостехкомиссии России по защи-  
те КЗИ технического и технологического характера правовыми ак-  
тами не установлены. Поэтому работа по противодействию конку-  
рентным техническим разведкам осуществляется коммерческими  
организациями самостоятельно.

К числу государственных органов, наделенных специальной  
компетенцией, относилось и *Главное управление по охране государ-  
ственных тайн в печати и других средствах массовой информации при  
Совете Министров СССР (ГУОТ СССР)*. Правовой статус этого орга-  
на определялся Правительством СССР (последнее постановление от  
24 августа 1990 г. № 843). В 1990 г. на основании решения Комитета  
конституционного надзора СССР орган государственной цензуры,  
известный под названием «Главлит», был упразднен. Основными за-  
дачами ГУОТ СССР являлись организация единой в стране систе-

<sup>1</sup> См.: Положение о Гостехкомиссии, утв. Указом Президента РФ от 19 февраля 1999 г. № 212 (с изм. от 6 марта 2002 г., 5 октября 2002 г., 4 марта 2003 г.).

<sup>2</sup> См.: Положение о порядке обращения со служебной информацией ограничен-  
ного распространения в федеральных органах исполнительной власти, утв. пост. Пра-  
вительства РФ от 3 ноября 1994 г. № 1233.

мы охраны государственных тайн в печати и других средствах массо-  
вой информации; координация деятельности министерств, ведомств  
и предприятий при осуществлении мер защиты от разглашения го-  
сударственных тайн и оказание методической помощи экспертным  
комиссиям.

Нужно отметить, что предприятия самостоятельно проводили  
экспертизу материалов НИОКР с целью определения возможности  
их открытого опубликования или издания с грифом «Для служеб-  
но пользования». Экспертизе подлежали любые материалы, которые  
содержали результаты научных исследований по естественным и тех-  
ническим наукам, а также раскрывали технологии производства про-  
дукции. Преждевременное опубликование таких материалов могло  
причинить ущерб оборонным и иным интересам государства. Эк-  
перты предприятий, рассматривая материалы для открытого опубли-  
кования, руководствовались специальными перечнями сведений,  
составленных ГУОТ СССР, министерствами и ведомствами. ГУОТ  
и его органам на местах были предоставлены обширные полномо-  
чия по ОРС и охране государственных секретов, которые носили в  
основном запретительный или ограничительный характер.

В состав экспертных комиссий включались представители ин-  
формационного и патентного подразделений, РСО, а также юри-  
консульты и специалисты по профильным отраслям научных зна-  
ний. В современный период коммерческие организации самостоя-  
тельно ведут аналогичную экспертную работу в целях исключения  
несанкционированного открытого опубликования КЗИ.

**Основные направления деятельности министерств и ведомств  
в сфере защиты государственных секретов (вторая группа субъектов).**  
Особая роль в обеспечении охраны государственных секретов была  
отведена министерствам и ведомствам СССР. Они в рамках своей от-  
раслевой компетенции объединяли усилия подчиненных им объеди-  
нений и предприятий по ОРС, создавали необходимые финансовые,  
трудовые и производственные условия для сохранения секретов.

Организационная деятельность министерств и ведомств по  
ОРС и защиты секретов в отраслях народного хозяйства была уре-  
гулирована общесоюзными и ведомственными актами. Функция  
организационно-методической работы в области защиты секретов  
была возложена на главные управления по режиму министерств.  
Деятельность министерств способствовала формированию на пред-  
приятиях единообразного понимания содержания основных направ-  
лений организационной защиты охраняемой информации и вносила

определенную стабильность в обеспечении правопорядка в сфере защиты секретов. Основными направлениями деятельности министерств по защите охраняемой информации являются: подбор, расстановка и воспитание кадров, планирование мероприятий, обеспечивающих сохранность секретов; разработка для предприятий показателей отчетности о защите секретов; осуществление мер по повышению ответственности руководителей предприятий за ОРС работ.

Названные направления деятельности министерств были взаимосвязаны между собой и представляли собой единую общесоюзную систему, обеспечивавшую процесс защиты охраняемой информации на уровне отдельной отрасли и конкретного предприятия. Уровень организации режима секретности конкретного предприятия определялся важностью и объемом выполняемых оборонных НИОКР, производством В и ВТ, а также количеством лиц, допущенных к той или иной степени секретности работ. Такой подход лежал в основе выделения трех групп предприятий, которые в соответствии с Перечнем Правительства СССР относились к категории «особо режимные объекты», «особо важные объекты» и «режимные объекты». Категория режимности предприятия определяла порядок и размеры финансирования по ОРС, а также характер использования сил и средств по защите государственных секретов. Наибольшее число таких предприятий было сосредоточено в оборонных отраслях промышленности.

Рассмотрим основные направления деятельности министерств по защите секретов.

**Во-первых, это организация работы по подбору, расстановке и воспитанию кадров на подведомственных предприятиях.** Суть этой работы состояла в согласовании кандидатур на замещение вакантных должностей руководящего состава предприятий (директор, его заместители, начальники подразделений РСО и их заместители). Серьезное внимание в кадровой работе уделялось подбору работников, обладавших организаторскими способностями и аналитическим мышлением, умением отстаивания государственных интересов в практической деятельности по защите секретов. Назначение и освобождение от должности заместителей (помощников) руководителей предприятий по режиму, начальников подразделений РСО осуществлялось по письменному согласованию с органами КГБ и РСО министерств, главных управлений по подчиненности. Значительный объем работы по организации защиты секретов на предприятиях являлся основанием для назначения на должности руководящего состава РСО офи-

церов действующего резерва КГБ СССР. Министерствами разрабатывались квалификационные характеристики на работников РСО, в которых были изложены общие личные и профессиональные требования к руководящим и инженерно-техническим работникам РСО. Лица, назначенные на должности начальников РСО, обязаны были до приема дел пройти инструктаж в РСО министерства. Лица, вновь принятые на работу в РСО, допускались к самостоятельной работе после сдачи зачетов по знанию нормативно-правовых актов и методики защиты секретов.

РСО министерств и предприятий использовали различные формы воспитательно-профилактической работы (ВПР) среди исполнителей секретных работ и документов. Основными формами ВПР являлись: инструктаж по вопросам соблюдения требований режима секретности, лекции и беседы по повышению бдительности, доведение до исполнителей секретных работ и документов требований норм законодательства в области охраны секретов, аттестация работников с учетом выполнения ими работ по ОРС. Наибольшее воспитательное значение имели собрания трудовых коллективов, на которых обсуждались вопросы ОРС проводимых работ.

**Во-вторых, это планирование мероприятий по обеспечению режима секретности в отрасли.** В министерствах весьма распространеной была практика годового планирования мероприятий по ОРС. В отдельных министерствах наряду с годовым планированием велось и перспективное, рассчитанное на более длительный период, например на пятилетие. Но такие планы были малоэффективными и требовали их ежегодной корректировки. Годовые планы утверждались министром с предварительным их рассмотрением, как правило, на коллегии министерства. Квартальные планы главных управлений министерства носили более конкретный характер и утверждались начальниками РСО министерства. Создание сложных технических систем и комплексов с участием различных министерств и ведомств было связано с межотраслевым планированием ОРС работ. Наприммер, имелись совместные планы ряда министерств с Академией наук СССР, Министерством высшего и среднего специального образования СССР по отдельным работам, имевшим важное народнохозяйственное и оборонное значение. На предприятиях разрабатывались годовые и квартальные планы по ОРС работ.

Структурно планы различных уровней управления состояли из мероприятий, направленных на совершенствование системы защиты секретов при формировании и выполнении НИОКР; обеспече-

ние режима секретности на каналах внешних связей и внутренней кооперации предприятий, выполнявших оборонный заказ; осуществление аналитической работы и контроль за эффективностью мер по ПД ИТР и другие. Важное внимание при планировании работы уделялось совершенствованию нормативно-правовой базы защиты секретов, организации и проведению ВПР в трудовых коллективах. Разработка планов и контроль за их исполнением осуществлялись на основании ведомственных методических рекомендаций, которые имелись на предприятиях.

**В-третьих, введение единой отчетности в работе по обеспечению режима секретности в отрасли.** Ежегодно РСО предприятий представляли в министерства отчеты о выполненной работе и статистическую отчетность о состоянии режима секретности на объекте. Содержание структуры отчетов определялось методическими рекомендациями министерств с учетом специфики задач, решаемых предприятиями. Структурно отчет состоял из пояснительной записки и статистических сведений. Одновременно, как правило, предприятия вместе с отчетом представляли в министерство план мероприятий по ОРС на следующий год.

Анализ результатов годовой работы предприятий позволял министерству выявлять характерные причины нарушений режима секретности и предлагать рекомендации по их предупреждению, а также предпринимать необходимые меры по совершенствованию защиты секретов в отрасли. Кроме того, анализ позволял обобщать имеющийся положительный опыт в сфере защиты секретов и распространять его на подведомственных предприятиях отрасли.

В годовых отчетах предприятий находили отражение сведения о выполнении приказов и указаний министерств по ОРС, о мерах по сохранности документов и изделий с различными степенями секретности, об оперативной обстановке (категория режимности объекта, устремления вероятного противника к секретам по материалам изучения зарубежной печати, экономическое и научно-техническое сотрудничество с зарубежными странами и др.), о комплексном противодействии иностранным техническим разведкам (легендирование, маскировка, зашифровка объектов и работ), о результатах проведенных аналитических исследований с изложением причин разглашения (утечки) секретной информации по конкретным направлениям научной, производственной, хозяйственной деятельности предприятий и мерах по их предупреждению; о мерах по совершенствованию ведения секретного делопроизводства, внедрению в работу РСО

средств оргтехники и ЭВМ, об эффективности ВПР по повышению ответственности лиц, работающих с секретными документами и издательствами, об организации учебы по повышению квалификации работников РСО.

В практике отдельных министерств использовались формы формализованных бланков отчетности по отдельным направлениям работы предприятий. Статистические данные представлялись, например, о структуре и кадрах РСО, выполнении мероприятий, предусмотренных отраслевым планом за отчетный период, об участии в научно-техническом сотрудничестве с зарубежными странами, о правонарушениях в сфере защиты секретов и по другим вопросам. Использование указанных бланков и обработка их в автоматизированном режиме способствовали повышению уровня предупредительной работы на предприятиях.

**В-четвертых, осуществление мероприятий по повышению ответственности руководителей предприятий и их структурных подразделений за обеспечение режима секретности.**

*Общесоюзные и ведомственные акты устанавливали ответственность руководителей министерств, ведомств и предприятий за обеспечение надлежащего режима секретности работ, своевременную разработку и осуществление необходимых мероприятий по защите секретов от разглашения и технических средств разведки противника. Такая же ответственность была возложена и на руководителей подразделений предприятия.*

Государством была установлена персональная ответственность Генеральных (главных) конструкторов и руководителей министерств за ОРС в отраслях народного хозяйства. В Положении о Генеральном конструкторе по важнейшим видам и системам вооружения и военной техники, утвержденном постановлением Совета Министров СССР от 6 июня 1985 г. № 551-168, подчеркивалось, что Генеральный конструктор несет перед Правительством СССР ответственность за соблюдение установленного режима секретности и осуществление мероприятий по ПД ИТР при выполнении НИОКР. Положениями о министерствах предусматривалась ответственность руководителей центрального аппарата за ОРС на участках их работы. На руководителях министерств оборонных отраслей промышленности дополнительно были возложены более строгие меры ответственности, предусмотренные Положением о Государственной комиссии Совета Министров СССР по военно-промышленным вопросам, ут-

верженным постановлением ЦК КПСС и СМ СССР от 7 февраля 1986 г. № 200-72.

*В министерствах использовались различные формы повышения ответственности руководителей предприятий и подразделений.* Обязанности по ОРС содержались в ведомственных нормативных актах, в частности, в правилах внутреннего трудового распорядка для работников центрального аппарата и подразделений большинства министерств и подчиненных им предприятий, в отраслевых стандартах, предусматривавших ответственность руководителей и работников предприятий за своевременность, полноту и достоверность представления документов и соблюдение режима секретности. В ряде отраслей оборонного комплекса действовало типовое положение о РСО предприятий, определявшее должностные права и обязанности в сфере защиты секретов и ответственность директора и его заместителей, руководителей РСО и подразделений за обеспечение надлежащего режима секретности проводимых работ, своевременную разработку и проведение мер по ПД ИТР. В отдельных министерствах существовала практика проведения обязательного инструктажа в РСО министерств при назначении на должность руководителей предприятий. Выполнение работниками трудовых обязанностей по защите секретов рассматривалось руководством как важная составляющая часть их основной производственной деятельности, хотя об этом в трудовом договоре и не упоминалось.

Существенное влияние на процесс усиления режима секретности в отраслях и повышение ответственности руководителей предприятий оказывала практика рассмотрения этих вопросов на коллегиях министерств. На заседаниях коллегий примерно 1–2 раза в год обсуждались проблемы совершенствования работы в сфере защиты секретов. Решения коллегии министерства с планами мероприятий направлялись на предприятия. По инициативе министерств ежегодно проводились отраслевые совещания по различным вопросам ОРС.

В министерствах распространенной была практика заслушивания с отчетом руководителей предприятий о состоянии охраны государственных секретов и ОРС с анализом выявленных недостатков и упущений. По результатам этой работы отдельные из них привлекались к дисциплинарной ответственности за совершение нарушений режима секретности, выразившихся в отсутствии контроля за процессом защиты секретов. Министерством предлагались меры по устранению имевших место нарушений. Реализация этих мер находилась на контроле у руководства министерства. Аналогичную дея-

тельность в отношении заместителей руководителей предприятий по режиму осуществляли управления по режиму министерств. Такая же работа проводилась и на предприятиях. Руководители предприятий регулярно заслушивали по этим вопросам руководителей среднего звена.

Широко использовались и другие формы работы с руководителями составом предприятий под руководством партийных комитетов. Вопросы ОРС рассматривались на советах директоров предприятий, балансовых комиссиях, в работе которых участвовали руководители министерства. При подведении итогов работы предприятий и его отраслевых структурных звеньев учитывались такие показатели в сфере защиты секретов, как: полнота и качество выполнения в установленном сроки приказов министерства по вопросам ОРС; создание условий, обеспечивающих сохранность охраняемой продукции и документов; реализация мер по предупреждению правонарушений и др. По этим же показателям оценивалась работа предприятия в системе отрасли.

Важной формой воздействия министерств на деятельность предприятий являлся контроль за реализацией мероприятий по ОРС. В частности, получила распространение практика выдачи предприятиям предписаний по результатам проверок, проводимых министерством, в котором отражался характер нарушения, и предлагались меры по закрытию ВКУ информации. Исполнение требований предписания находилось на контроле министерства.

Проведение министерством такой работы способствовало созданию в трудовых коллективах атмосферы ответственности работников за сохранение секретов.

В отдельных отраслях по решению министерств были созданы межведомственные Советы по проведению единой политики в области ОРС разрабатываемых систем вооружения (В) и военной техники (ВТ). В состав Совета входили заместители руководителей предприятий по режиму, начальники производственных подразделений и работники РСО. Руководство работой Совета осуществлял, как правило, заместитель директора предприятия по режиму головной организации — разработчика. В заседаниях Совета принимали участие представители министерств, органов КГБ, заказывающего управления МО СССР и другие. Эффективность работы Совета определялась важностью задач, решаемых предприятиями-исполнителями, участвующими в операции по созданию специальной техники. Функциями Совета были разработка единых планов по ОРС, ана-

лиз причин, снижающих надежность сохранения секретов при создании систем и комплексов В и ВТ, заслушивание представителей РСО предприятий-соисполнителей о состоянии работы по ОРС и другие. Властными полномочиями такие Советы не обладали. Принятые ими решения носили рекомендательный характер, что отражалось на эффективности их работы. Тем не менее осуществление Советом функций координации деятельности по защите секретов способствовало слаженности работы предприятий-соисполнителей. При необходимости решения Совета подкреплялись приказами соответствующих министерств.

Таким образом, в министерствах хотя и были свои особенности, вместе с тем существовала примерно одинаковая практика повышения ответственности руководителей предприятий и их структурных подразделений за ОРС. Это объясняется действием единого административно-правового режима, который был установлен в сфере защиты государственных секретов на всей территории страны.

**Третья группа субъектов включает деятельность местных органов власти и правоохранительных органов по сохранению государственных секретов.**

Местные партийные и советские органы власти, на территории которых находились предприятия союзного значения, проводили значительную работу по укреплению законности и правопорядка. Их взаимоотношения с предприятиями по поводу охраны государственного секретов были определены нормами действующего законодательства. Доступ к новейшей производственной и научно-технической информации о деятельности режимных предприятий был ограничен. Отношения в основном строились в рамках партийной и хозяйственной работы предприятий и не касались сферы защиты секретов.

Деятельность правоохранительных органов на режимных предприятиях регулировалась в тот период Указом Президиума Верховного Совета СССР от 1 июня 1979 г. № 214-к «О судах, прокуратуре, адвокатура, нотариате и органах внутренних дел, действующих на особом режимных объектах»<sup>1</sup> и иными правовыми актами. В соответствии с Указом обслуживание таких предприятий осуществлялось специально выделенными подразделениями правоохранительных органов, работники которых должны были иметь соответствующую форму до-

<sup>1</sup> См.: Бюллетень Верховного Суда СССР. 1991. № 6.

пуска к секретным работам, документам и изделиям, согласованную с органами КГБ. Указ обязывал правоохранительные органы осуществлять взаимодействие и координацию работы с органами КГБ. В рассматриваемый нами период главная ставка делалась на органы государственной безопасности. Как отмечает Ю.Д. Северин, в административно-управленческих кругах сложились «представления о второстепенном месте и роли правосудия в области государственной, хозяйственной деятельности, социальной сферы, обеспечения демократии», что в определенной мере отражалось на работе судов, рассматривавших дела на работников режимных предприятий. Органы прокуратуры осуществляли общий надзор за исполнением законов на режимных предприятиях. В ходе прокурорских проверок выявлялись причины и условия, способствовавшие совершению правонарушений, и предпринимались меры по их устранению. Лица, совершившие правонарушения, привлекались к различным видам юридической ответственности.

**Четвертая группа субъектов характеризует деятельность администрации предприятий и общественных организаций по обеспечению режима секретности.** Эта группа субъектов занимает особое место в деятельности по ОРС, поскольку непосредственно занималась организацией защиты секретов в процессе производства продукции.

Руководители предприятий и структурных подразделений в силу своего служебного положения устанавливают порядок работы с документами и изделиями с учетом специфики производственной деятельности и требований режима секретности. В частности, они занимаются подбором, расстановкой и воспитанием кадров, организацией контроля за выполнением требований режима секретности, разработкой и применением системы материальных и моральных стимулов в работе по ОРС, что является характерным для современных коммерческих структур. Важным направлением работы в рассматриваемый нами период было проведение ВПР среди работников по разъяснению им требований режима секретности.

Решение задач, связанных с ОРС, осуществлялось администрацией в рамках общих полномочий, предоставленных ей государством. Речь идет о мерах по сокращению текущей численности кадров, о возможности применения премирования, о повышении профессионального уровня работников и другие. Руководителю предприятия по согласованию с органами КГБ было предоставлено право отстранения от се-

<sup>1</sup> См.: Северин Ю.Д. Организационные основы правосудия. М., 2003. С. 6.



кретных работ лиц, допустивших грубые нарушения по ОРС, и привлечение виновных к ответственности в соответствии с нормами законодательства.

Важная роль в ОРС принадлежала *юридическому отделу (юрисконсульту) предприятия*. Выполняя свои прямые функции, связанные с визированием проектов локальных актов и различных организационно-распорядительных документов, с проверкой финансово-хозяйственной деятельности подразделений и др., юридическая служба вскрывала недостатки в работе и способствовала установлению нарушений в сфере охраны секретов и разрабатывала в этой связи меры правового характера по выявлению, пресечению и предупреждению правонарушений в области защиты секретов.

На большинстве предприятий действовали *постоянно действующие технические комиссии*. В их работе участвовали руководители подразделений, ученые и специалисты, работники РСО и подразделений ПД ИТР. Комиссией проводился анализ защиты секретов на конкретных производственных участках и жизненного цикла создания В и ВТ. Рекомендации комиссии утверждались приказами по предприятию и были обязательны для исполнения.

На предприятиях действовали различные *общественные организации*, которые, в зависимости от представленных им законом полномочий, оказывали предупредительное воздействие на ситуацию, возникавшие на каналах утечки охраняемой информации, выявляли причины, их обуславливающие, и применяли по согласованию с администрацией соответствующие меры общественного воздействия. В числе таких организаций следует назвать *партийную организацию предприятия (партком)*, которая действовала в рамках Конституции СССР и являлась политическим ядром трудового коллектива. Нужно отметить значительное влияние парткомов на повседневную жизнь предприятий, в том числе и в сфере защиты секретов. Это объясняется тем обстоятельством, что подавляющее большинство руководителей предприятий и подразделений, начальников РСО являлись коммунистами и поэтому обязаны были отчитываться о своей работе в партийной организации. Партийный контроль был самым строгим и действенным средством, обеспечивавшим выполнение плановых заданий по защите секретной информации. В настоящее время таких рычагов воздействия ввиду действия принципа плюрализма и многопартийности у коммерческих организаций не имеется.

*Профсоюзные организации* в силу предоставленных им полномочий обладали широкими возможностями по предупреждению пра-

вонарушений, в том числе связанных с защитой секретов. Такими рычагами воздействия на должностных лиц являлись контроль за их премированием по итогам социалистического соревнования, где в числе других показателей учитывались состояние ОРС, согласование кандидатур работников, рекомендации для выдвигения на высшую должность, допустивших нарушения режима секретности, включая и увольнение их по этим основаниям.

Нельзя не учитывать роль народных контролеров и членов добровольных народных дружин, действовавших в то время на предприятиях. Их общественная деятельность на режимных предприятиях отмечалась определенной спецификой, связанной с производством специальной продукции, хранением изделий и секретных документов. В процессе своей деятельности они способствовали выявлению нарушений внутриобъектового режима, установлению причин и условий, способствовавших возникновению ВКУ информации, и вносили предложения по нейтрализации их действия. Кроме того, на предприятиях действовали товарищеские суды, советы профилактики правонарушений и другие органы общественной самодеятельности, которые, выполняя свои прямые обязанности, определенные законодательством, вносили определенный вклад в ОРС и тем самым обеспечивали участие в ней значительного числа работников предприятия.

***Пятая группа субъектов, действовавших на предприятиях, представляла собой специализированные подразделения, которые профессионально занимались защитой секретов.*** К их числу следует отнести *режимно-секретные органы (РСО)*, созданные в нашей стране в 1959 г. на основании постановления Совета Министров СССР от 9 февраля 1959 г. № 126-52. Нужно отметить, что в министерствах и на предприятиях не было единого подхода к определению структуры РСО. Практически на большинстве предприятий в структуру РСО входили подразделения секретного делопроизводства, отдела режима, шифровальные органы и архивы. Аналитические подразделения, отделы ПД ИТР и ведомственной охраны не всегда и не везде включались в структуру РСО.

РСО принимали непосредственное участие в производственной, научно-исследовательской, хозяйственной и иной деятельности предприятий, т.е. на всех тех участках, где был установлен режим секретности проводимых работ. В 90-е годы РСО были преобразованы в службы безопасности коммерческих организаций.

### § 3. Осуществление организационных прав на установление режима коммерческой тайны

**Концептуальные основы установления режима коммерческой тайны в организациях.** Право коммерческих организаций на установление режима коммерческой тайны в общих чертах закреплено в Законе о коммерческой тайне и иных правовых актах. Более детально процедуры установления режима коммерческой тайны регламентированы в корпоративных актах, регулирующих деятельность организаций в сфере обращения КЗИ. Содержание права организации на установление режима коммерческой тайны обусловлено фактической монополией ее на КЗИ, обращение которой осуществляется по инициативе обладателя с использованием собственных сил и средств. Анализ литературных источников и практики хозяйствующих субъектов показывает, что установление режима коммерческой тайны и его правовое обеспечение напрямую связаны с достижением организацией стратегических целей. При этом учитываются приоритетные направления развития бизнеса, исходя из общей стратегии экономической безопасности. *Основными целями, стоящими перед организациями и определяющими характер и направления установления режима коммерческой тайны и его правового обеспечения, являются:*

— защита законных прав организаций и их работников во взаимоотношениях с государственными органами власти, местными органами самоуправления, партнерами и конкурентами, поддержание стабильного внутреннего порядка управления;

— сохранение и защита частной собственности учредителей (акционеров), рациональное и эффективное использование ее в их интересах;

— повышение конкурентоспособности производимых товаров, работ и услуг, создание благоприятной рыночной конъюнктуры для их реализации на внутреннем и внешнем рынке; рост прибылей организации и доходов работников;

— достижение стабильности в коммерческой и иной деятельности, развитие кооперированных и иных связей и недопущение од-

<sup>1</sup> См.: Бачило И.Л. Право на информацию // Проблемы информатизации. 1995. № 1, и др.

носторонней зависимости от случайных и недобросовестных конкурентов и партнеров;

— выполнение плановых заданий в финансово-хозяйственной деятельности, достижение требуемого качества выпускаемой продукции, развитие производства и реализации товаров на передовой научно-технической основе;

— укрепление дисциплины труда, формирование материальных стимулов в целях повышения творческой активности и производительности труда работников;

— ориентация развития техники и технологий на мировые стандарты и лидерство в разработке и освоении производства продукции по профилю деятельности организации;

— получение преимуществ на приоритетных направлениях научных исследований, ускорение производственно-технологического освоения новейших научных достижений, укрепление интеллектуального потенциала организации;

— информационное обеспечение финансово-экономической, производственной, научно-технической и иной деятельности, защита коммерческих секретов и прав на интеллектуальную собственность, повышение эффективности использования имеющейся информации для укрепления имиджа организации при взаимоотношениях с отечественными и зарубежными партнерами и др.

Выбор организацией конкретных целей правового обеспечения своей безопасности зависит от финансового состояния и изменения хозяйственной ситуации (изменение спроса и налогов, появление новых технологических решений производства товаров, угрожающих конкурентоспособности продукции, недобросовестность партнеров, воздействие факторов, определяющих внутренние и внешние угрозы и др.<sup>1</sup>).

Достижение целей, стоящих перед организацией, требует *определения задач* по своевременному выявлению угроз ее жизненно важным интересам, способных причинить реальный ущерб и внести элементы дестабилизации; оперативному использованию правовых средств реагирования на различного рода угрозы и негативные тенденции в развитии процессов разработки и реализации товаров; формированию надежных гарантий поддержания внутреннего порядка в организации, договорной дисциплины контрагентов, взаимовыгод-

<sup>1</sup> См.: Экономическая безопасность России. С. 738–748.

ного сотрудничества, организационной стабильности хозяйственных связей; максимально полному возмещению ущерба, причиняемого неправомерными действиями физических и юридических лиц; ослаблению иных негативных факторов, влияющих на достижение стоящих перед организацией целей.

Реализация задач в области безопасности, связанной с установлением режима коммерческой тайны и его правового обеспечения, требует от организаций соблюдения определенных *принципов*, вытекающих из основных положений Конституции РФ, ГК РФ, законов и иных правовых актов, регулирующих предпринимательскую деятельность и обращение КЗИ. Важнейшими из них являются следующие.

1) *Законность* принимаемых мер по установлению режима коммерческой тайны и его правовому обеспечению, учитывающих возможность применения норм законодательства для выявления, предупреждения и пресечения правонарушений в сфере обращения КЗИ.

2) *Самостоятельность и ответственность* подразделений, специализирующихся на решении задач по обеспечению безопасности организации. Подразделения должны быть обеспечены необходимыми ресурсами, использование которых позволит достичь баланса производимых затрат и достигнутых результатов. Необходимо закрепить в корпоративных актах и трудовых договорах ответственность руководителей и исполнителей за своевременное установление режима коммерческой тайны и его обеспечение на конкретных участках их работы.

3) *Экономическая целесообразность* мероприятий по обеспечению безопасности не должна приводить к снижению экономических показателей деятельности организации. Стабильность получения прибыли является основным критерием оценки качества работы подразделений службы безопасности (СБ).

4) *Специализация и профессионализм* кадрового состава подразделений СБ, специализирующихся по отдельным направлениям обеспечения безопасности организации.

5) *Планирование* мероприятий по обеспечению безопасности организации.

6) *Взаимодействие и координация* деятельности по обеспечению безопасности организаций, осуществляемая путем установления связей с органами государственной власти и местного самоуправления.

ния, правоохранительными органами, негосударственными организациями (партнерами, контрагентами и др.) и их СБ.

7) *Гласность в сочетании с необходимой конспиративностью обеспечения безопасности организации* предусматривает регулярное информирование трудового коллектива о результатах этой деятельности. В определенных ситуациях меры по обеспечению безопасности могут носить скрытый характер при условии контроля со стороны руководящих органов организации за их применением с соблюдением необходимых процедур и осуществлением прокурорского надзора за исполнением законов в этой сфере деятельности. Например, проверка поступающих на работу лиц, оформление им допуска к КЗИ и другие. Запрещается сокрытие деяний, за совершение которых законом установлена юридическая ответственность.

Названные принципы должны в полной мере учитываться при *создании и функционировании организационных структур, профессионально обеспечивающих безопасность организации*. Установление режима коммерческой тайны и функционирование системы его правового обеспечения предполагает управление этими процессами внутри организации. Управление осуществляется на основе сочетания административных методов руководства со стороны администрации, учета фактора самоуправления трудовых коллективов, взаимного согласования их интересов и установления гражданско-правовых отношений с контрагентами по охране конфиденциальности информации в процессе совместной деятельности. *Объектом управления* в области обеспечения безопасности на уровне организации являются: разработка и принятие комплексно-целевых программ обеспечения безопасности, координация усилий своих подразделений, а также контрагентов, направленных на их выполнение; взаимодействие с контрагентами и иными лицами при подготовке и реализации долговременных и крупномасштабных мероприятий по защите КЗИ; упорядочение взаимоотношений организации с правоохранительными органами, органами местного самоуправления, иными государственными и негосударственными органами и организациями по поводу использования и защиты КЗИ; концентрация и распределение кадровых, материальных и иных ресурсов для выявления и устранения возможных угроз нормальному функционированию организации.

*Система безопасности организаций строится в основном по линейному принципу с наличием вертикальных и горизонтальных связей*. Анализ материалов ряда крупных акционерных обществ показывает, что

в большинстве из них созданы примерно аналогичные **организационные структуры управления в области безопасности**. Структурными звеньями этой системы являются: совет директоров общества, правление общества или генеральный директор и его заместитель по вопросам безопасности; совет безопасности общества, постоянно действующая техническая комиссия организации; служба безопасности организации; специализированные подразделения, функционально ориентированные на обеспечение отдельных направлений безопасности организации. Кратко охарактеризуем правомочия названных структурных звеньев.

Высшим распорядительным органом, отвечающим за политику обеспечения безопасности организации, является совет директоров общества, правление общества или генеральный директор. Общее руководство обеспечением безопасности организации осуществляет заместитель председателя совета директоров или правления общества либо заместитель генерального директора по вопросам безопасности. Для повышения уровня обоснованности принимаемых решений в области безопасности в организациях сложилась определенная практика, когда постоянно действующая техническая комиссия проводит экспертную оценку и проработку отдельных проблем безопасности, требующих повышенного внимания ученых и специалистов.

Организационно-распорядительные документы, устанавливающие правомочия подразделений и отдельных работников по вопросам безопасности, оформленные в виде решений совета директоров общества, правления или генерального директора, являются обязательными для исполнения. Речь идет о комплексной целевой программе (основных направлениях) обеспечения безопасности организации; отдельных программах (планах) обеспечения безопасности производства и реализации товаров (работ, услуг) в процессе которых используется КЗИ; планах совместных мероприятий с другими предприятиями по охране конфиденциальности информации и других документах. Названные субъекты принимают решения о содержании и характере взаимодействия по вопросам безопасности организации с правоохранительными органами, органами местного самоуправления; по организации и проведению работ, связанных с формированием перечней сведений, составляющих коммерческую тайну; об образовании, реорганизации и стратегии деятельности СБ, а также ее специализированных подразделений; другие решения, касающиеся деятельности организации в области обеспечения безопасности, требующие утверждения высшим распорядительным органом общества.

В отдельных крупных организациях создаются и действуют *советы безопасности*, образуемые при совете директоров (правлении) общества. Совет безопасности организации, как правило, возглавляет ее первый руководитель. Состав, права, обязанности и ответственность членов совета безопасности устанавливаются советом директоров общества или генеральным директором. Разрабатываемые советом организации или генеральными директорами документы оформляются решениями совета директоров общества или генеральным директором. Организационной формой деятельности совета являются заседания, на которых рассматриваются наиболее важные вопросы безопасности, требующие всестороннего обсуждения с участием экспертов.

*Служба безопасности организации является исполнительным органом*, реализующим решения председателя совета директоров (правления) или генерального директора по вопросам безопасности. Служба обеспечивает функциональное управление деятельностью специализированных подразделений, решающих конкретные задачи в сфере безопасности. Она осуществляет координацию усилий всех структурных звеньев, обеспечивающих в целом безопасность организации. Рассмотрим структуру и функции службы безопасности (СБ). Структура СБ определяется ее целями и обеспечивает комплексное решение поставленных перед ней задач на основе стратегии и взаимосвязи тактических приемов подготовки и проведения мероприятий по обеспечению безопасности организации. СБ состоит из подразделений, осуществляющих разработку процедур режима безопасности, установление и обеспечение этих режимов, а также контроль за их соблюдением. Структура СБ утверждается руководителем организации.

В составе СБ могут быть созданы информационно-аналитические подразделения, организационные звенья по направлениям обеспечения безопасности, а также временные структуры для решения конкретных задач. Временные структуры создаются с привлечением ведущих специалистов для решения сложных задач по комплексному обеспечению безопасности, определяемых конкретными целями и хозяйственной ситуацией.

Для решения поставленных задач **СБ выполняет ряд важных функций**. *Административно-распорядительная функция* реализуется службой путем подготовки решений по установлению и поддержанию режимов безопасности, определения правомочий подразделений, прав, обязанностей и ответственности работников по вопросам обеспече-

ния безопасности и по осуществлению представительских функций в конкретной области деятельности. Служба участвует в определении ресурсов, необходимых для решения задач безопасности, в подготовке и проведении мероприятий по обеспечению сохранности имущества и интеллектуальной собственности, рациональному их использованию, выполняя, таким образом, *хозяйственно-распределительную функцию*.

Важное место в деятельности СБ занимает реализация *учетно-контрольной функции*, что связано с выделением важных направлений финансово-коммерческой деятельности, обнаружением угроз финансовой стабильности и устойчивости организации, оценкой их источников, налаживанием контроля за ведением учета негативных факторов, влияющих на безопасность организации, а также накоплением информации о недобросовестных конкурентах, ненадежных партнерах, лицах и организациях, посягающих на интересы организации. Реализация *социально-кадровой функции* состоит в участии СБ в подборе и расстановке кадров, выявлении негативных тенденций в трудовых коллективах и возможных причин социальной напряженности, в предупреждении и локализации конфликтов, инструктаже работников по вопросам обеспечения безопасности, формировании у них «фирменного» чувства ответственности за соблюдение установленных режимов безопасности. Служба участвует в решении вопросов, связанных с командированием специалистов организации за рубеж и предупреждением в этой связи возможной утечки КЗИ.

Служба выполняет важную *организационно-управленческую функцию*, которая реализуется путем оказания управленческого воздействия на создание, поддержание и своевременную реорганизацию структуры управления процессом обеспечения безопасности организации, гибких временных структур по отдельным направлениям работы, организации взаимодействия и координации между их отдельными звеньями для достижения программных целей. Служба совместно с производственными и планово-финансовыми подразделениями непосредственно занимается разработкой комплексной программы и отдельных планов обеспечения безопасности организации, подготовкой и проведением мероприятий по их осуществлению, что позволяет говорить о выполнении СБ *планово-производственной функции*. С названной функцией тесно связана *организационно-техническая функция*, состоящая в определении СБ необходимого материально-технического и технологического обеспечения режимов безопасности в организации, приобретением и

§ 3. Осуществление организацией права на установление режима коммерческой тайны

освоением специальной техники в целях повышения уровня защиты КЗИ.

Особое значение для повышения уровня обеспечения безопасности организации имеет выполнение СБ *информационно-аналитической и научно-методической функций*. Служба осуществляет сбор, накопление и обработку информации, относящейся к сфере безопасности. Для этих целей она использует необходимые технические средства аналитической обработки информации. Полученная информация доводится до сведения заинтересованных подразделений и руководящего состава. Научно-методическая роль СБ проявляется в изучении опыта обеспечения безопасности и создании методической базы, организации обучения работников службы, научной проработки проблем обеспечения безопасности и методического сопровождения этой деятельности. Названные функции СБ реализуются ее подразделениями.

В организациях с большим объемом работы по защите коммерческих секретов в состав СБ могут включаться подразделения (отделы, сектора, группы) делопроизводства документов с грифом «Коммерческая тайна», режима, анализа, специальной связи, охраны.

*Подразделение делопроизводства*. В его задачи входят: организация и ведение делопроизводства документов с грифом «Коммерческая тайна», осуществление их учета, контроль за обеспечением установленного порядка обращения<sup>1</sup>. Основными формами работы является учет конфиденциальных документов и обеспечение их хранения, контроль за соблюдением порядка доступа к документам, содержанием коммерческую тайну, в процессе их обращения, проведение с работниками воспитательно-профилактической работы с целью исключения утраты документов и предупреждения разглашения (утечки) конфиденциальных сведений.

*Подразделение режима* решает несколько иные задачи. Оно разрабатывает и осуществляет совместно с производственными подразделениями мероприятия по обеспечению защиты коммерческих секретов при производстве товаров (работ, услуг); принимает участие в разработке, пересмотре и дополнении перечня сведений, составляющих коммерческую тайну организации; разрабатывает проекты инструкций, правил, положений и других корпоративных актов по защите коммерческой тайны. К числу важных направлений деятель-

<sup>1</sup> См.: Степанов Е.А., Корнеев И.К. Информационная безопасность и защита информации. М., 2001. С. 107–182, и др.

ности этого подразделения следует отнестись: принятие мер по выявлению и нейтрализации действия маскирующих признаков новых образцов продукции; обеспечение режима при разработке, хранении, транспортировке и уничтожении макетных и опытных образцов, содержащих КЗИ (эта работа выполняется совместно с подразделением по противодействию конкурентным разведкам (ПДКР); осуществление мероприятий по ограничению числа лиц, допускаемых к документам, изделиям и работам, содержащим коммерческие секреты; принятие мер по недопущению случаев разглашения КЗИ при выполнении совместных работ с другими предприятиями, проведении совещаний, конференций, выставок.

Кроме того, на подразделение режима могут быть возложены обязанности по обследованию и аттестации помещений, в которых ведутся работы, содержащие коммерческую тайну, и обеспечению в них внутриобъектового режима; разработке и осуществлению мероприятий по защите КЗИ от возможной утечки по техническим и иным каналам (совместно с подразделением ПДКР); разработке мероприятий по защите коммерческих секретов при посещении подразделений представителями иностранных фирм. Подразделением используются такие формы работы, как проведение инструктажа работников, допущенных к работам, содержащим коммерческую тайну, профилактическая работа по предупреждению случаев утраты конфиденциальных документов и изделий, разглашения (утечки) сведений, составляющих коммерческую тайну. В случаях выявления фактов грубого нарушения правил защиты коммерческой тайны подразделение режима вправе провести служебное расследование, результаты которого докладываются руководству для принятия мер, включая возможность передачи материалов в следственные органы МВД.

Деятельность *аналитического подразделения* в рамках СБ отличается определенной спецификой. В частности, за ним не закреплены конкретные участки обеспечения безопасности, связанные с учетом и хранением конфиденциальных документов и изделий, режимным сопровождением коммерческих сделок, работ (услуг), при выполнении которых используется КЗИ. Его назначение в системе безопасности организации несколько иное. Главной задачей этого подразделения является обеспечение руководства достоверной информацией об угрозах организации на конкурентоспособных направлениях ее деятельности и подготовка научно обоснованных мер по их предотвращению. Важное место занимает оценка эффективности планиру-

емых мер с точки зрения предупреждения нарушений, допускаемых в сфере обращения КЗИ, предложений по использованию правовых и иных средств для устранения или нейтрализации угроз, а также оценка стоимости предлагаемых мер по предупреждению угроз безопасности организации. Для решения этих задач подразделение изучает различные стороны производственно-технической, научно-исследовательской, опытно-конструкторской, коммерческой и иной деятельности в целях выявления ВКУ КЗИ и нарушений в процессе обращения такой информации; анализирует и обобщает данные об устремлениях конкурентов к работам организации, содержащей коммерческие секреты. Основной формой деятельности аналитических подразделений является выполнение научно-исследовательской и методической работы, связанной с разрешением проблем безопасности организации. Результаты аналитических исследований находят свое отражение в отчетах, методических рекомендациях, проектах корпоративных актов и распорядительных документов.

В обеспечении режима коммерческой тайны участвуют и другие подразделения СБ. Так, *подразделение специальной связи* обеспечивает при необходимости передачу КЗИ другим организациям с использованием закрытой автоматической связи и шифровальной техники, а также внедряет для защиты коммерческих секретов технические средства, предназначенные для их передачи по открытым каналам связи. *Подразделение охраны* осуществляет физическую защиту имущества организации, обеспечивает установившийся пропускной и внутриобъектовый режим, исключающий хищения, а также вынос, вывоз с территории документов, макетных и опытных образцов, содержащих коммерческую тайну, без соответствующих разрешений.

В отдельных крупных организациях действует *пресс-служба*, которая играет важную роль в общении с внешним миром. Она осуществляет связь со средствами массовой информации, государственными органами и общественными организациями, участвует в рекламных акциях организации; на нее возложен контроль за недопущением случаев преждевременной публикации материалов, содержащих коммерческую тайну, без разрешения руководства. СБ имеет тесные связи с пресс-службой и дозирует ее помощью информацию, имеющую коммерческую значимость для организации.

*Правовой статус подразделений СБ*, их структура и численность работников определяются первым руководителем организации по согласованию с начальником СБ, в зависимости от объема выполняемой работы на конкретных направлениях обеспечения безопасно-

сти организации. В случае отсутствия в структуре организации одного из названных специализированных подразделений выполнение соответствующей функции по защите КЗИ осуществляется другим подразделением или специально назначенным для этих целей работником.

Решение о создании и прекращении деятельности СБ принимается советом директоров общества либо правлением (генеральным директором) в соответствии с Законом «О частной детективной и охранной деятельности в РФ». Взаимоотношения СБ с производственными подразделениями определяются уставом организации и корпоративными актами, в которых подчеркивается необходимость оказания СБ содействия в подготовке и проведении мероприятий по обеспечению безопасности. Решение по этим вопросам должно быть оформляется соответствующими внутренними документами. Службе предоставляется возможность использования производственно-технического и финансового потенциала организации для решения проблем обеспечения безопасности в установленном порядке.

*Служба безопасности организации взаимодействует в своей деятельности с правоохранительными органами.* В частности, отношения строятся на основании норм действующего законодательства, регламентирующего правоохранительную деятельность в сфере государственной безопасности и безопасности коммерческих организаций. СБ обеспечивает соблюдение в организации законодательства и подзаконных актов, входящих в компетенцию органов ФСБ РФ, и оказывает им содействие в выявлении, предупреждении и пресечении государственных преступлений. С этой целью она представляет в органы ФСБ информацию о признаках преступной деятельности, входящей в их компетенцию, и оказывает помощь в расследовании возбужденных уголовных дел и проведении оперативно-розыскных мероприятий в отношении работников организации, а также в осуществлении таких мероприятий на своей территории. Кроме того, служба взаимодействует с органами ФСБ по вопросам защиты государственных секретов, связанных с обеспечением экономических интересов государства в процессе участия организации в международном разделении труда и поддержании иных связей с зарубежными партнерами.

Служба взаимодействует с органами МВД РФ. Их отношения касаются решения задач по охране собственности и физической защите имущества организации, поддержанию общественного порядка и

режимов, входящих в компетенцию органов МВД. Для решения этих задач органами МВД используются информационные возможности СБ по выявлению преступных нарушений, направленных против интересов организации.

Анализ материалов ряда предприятий показывает, что с учетом сложившихся взаимоотношений между СБ организации и правоохранительными органами, которые в соответствии с законом наделены правом на проведение оперативно-розыскной деятельности, допускается участие работников службы в подготовке и реализации отдельных оперативных мероприятий. В этих случаях правоохранительные органы могут предоставить необходимые полномочия работникам СБ для выполнения ими отдельных поручений. Обеспечение контроля за выполнением поручения возлагается на правоохранительный орган. Важно подчеркнуть, что пределы дозволительного поведения работника СБ, участвующего в проведении специальных мероприятий по поручению правоохранительного органа, определяются действующим законодательством.

Отношения СБ с органами прокуратуры, суда и арбитражного суда определяются решением задач поддержания законности и практического осуществления реализации правовых норм в сфере защиты частных интересов организации.

Реализация стратегии безопасности организации требует учета действующего в месте ее расположения законодательства в области ведения бизнеса в силу специфики местных условий. Это связано с мерами основного общества, которые предлагаются дочерним обществам, филиалам и представительствам, взаимодействующим с местными органами власти по вопросам выявления и устранения условий, способствующих совершению нарушений. Следует особо выделить отношения СБ с аналогичными структурами *внешних организаций*. При наличии договорных отношений СБ организует взаимодействие с аналогичными подразделениями контрагентов. Содержание и формы сотрудничества определяются общностью целей, необходимостью разрешения противоречий в сфере безопасности и оказания взаимопомощи при возникновении угроз, требующих совместного участия в их преодолении.

Выполнение СБ своих функций, связанных с установлением режима коммерческой тайны и его обеспечением, возможно при условии создания в организации необходимых *юридических, организационных и материальных гарантий*, позволяющих оперативно вести работу по выявлению, предупреждению и пресечению правонарушений.

Речь идет о посягательствах на нормальный порядок корпоративного управления и ущемление законных прав организации, незаконное изъятие ее имущества, присвоение результатов интеллектуальной деятельности, создание неблагоприятной финансово-коммерческой конъюнктуры, нарушение устойчивости хозяйственных связей, создание напряженной социально-психологической обстановки в трудовом коллективе, нарушение договорной дисциплины; утрату технологического лидерства, научные достижения которого определяются содержанием КЗИ.

*Юридические гарантии* установления режима коммерческой тайны и его обеспечения закреплены в нормах законодательства, улучшивших конкретизацию в корпоративных актах, в которых регламентирован порядок установления режима и его обеспечения, закреплены организационные и материальные условия, обеспечивающие реализацию прав и обязанностей при обращении КЗИ, а также критерии правомерного поведения работников по поводу охраны коммерческой тайны и использования мер государственного принуждения в этой области.

*Организационные гарантии* установления и обеспечения мер безопасности могут быть сформированы в процессе разработки и поддержания высокой работоспособности общей организационной структуры управления процессом выявления и предупреждения угроз организации, использования эффективного механизма стимулирования ее оптимального функционирования, соответствующей подготовки кадров, а также принятия мер по гармонизации интересов и консолидации усилий трудового коллектива организации на достижение целей обеспечения ее безопасности.

*Материальные гарантии* формируются за счет выделения и использования финансовых, трудовых, информационных и иных ресурсов организации, обеспечивающих выявление, ослабление и нейтрализацию источников угроз, предотвращение и локализацию возможного ущерба, создание благоприятных возможностей для эффективной деятельности. Названные гарантии находят свое практическое выражение в содержании правовых, организационных и иных мер безопасности, реализуемых в организации.

*Служба безопасности осуществляет свою деятельность на основании комплексного плана обеспечения и поддержания высокого уровня безопасности организации, включающего ряд целевых программ. Это могут быть программы обеспечения безопасности перспективных направлений деятельности, где чаще всего используется КЗИ.*

Отдельная программа может предусматривать координацию и взаимодействие с правоохранительными органами по безопасности персонала. Планирование деятельности в сфере обеспечения безопасности осуществляется с участием трудового коллектива при условиях рационального использования сил и средств. В крупных организациях основной формой планирования деятельности СБ является годовой план. Основные мероприятия этого плана включаются в общий годовой план развития организации. Содержание планов может быть скорректировано в соответствии с практикой, принятой в организации. Концепция перспективного планирования и прогнозирования развития событий в области безопасности деятельности рассматривается и обсуждается советом директоров общества или правлением с принятием конкретных решений.

*Оптимальный выбор организационной структуры безопасности коммерческой организации* обусловлен особенностями управления процессом установления режима коммерческой тайны и его обеспечения на малом, среднем и крупном предприятии. Определение наиболее оптимальных параметров СБ (ее структуры, задач и функций) зависит от направлений деятельности и участков, где обращается КЗИ, и тех угроз, которые объективно представляют опасность для деятельности организации.

С учетом полученных данных об угрозах безопасности организациям представляется, что реализация мероприятий по обеспечению безопасности статуса КЗИ не может быть возложена лишь на одну СБ организации. Достижение эффективности результатов этой работы возможно только при взаимодействии СБ со всеми производственными подразделениями и участии работников организации.

Типовых методик, позволяющих определить наиболее приемлемую структуру СБ для коммерческих организаций, не существует. В каждом конкретном случае она индивидуальна. Практически этот вопрос решается применительно к отдельной организации с учетом ее основных параметров производственной, научной и коммерческой деятельности. Объем обстоятельств, имеющих общий характер, влияющих на определение организационной структуры СБ, сравнительно невелик. К ним главным образом относятся особенности хозяйственной деятельности организации, виды и характер проявления основных угроз безопасности ее жизненно важным интересам, специфика причинного комплекса лежащих в основе свойственных конкретной организации правонарушений в информационной сфере. Существенным для решения указанных задач является учет требуемой совокуп-



ности мероприятий, связанных с использованием различных правовых средств, выполнение которых обеспечит надежную безопасность организации. И, наконец, ресурсный потенциал организации, определяющий возможность материально-технического, кадрового, информационного обеспечения выполнения мероприятий, связанных с созданием надежной защиты организации от несанкционированного проникновения в ее информационную систему. Особо нужно отметить, что при выборе оптимальной организационной структуры СБ в обязательном порядке учитывается специфика малых, средних и крупных коммерческих организаций.

В свете выказанных положений проанализируем деятельность различных видов предприятий по обеспечению их безопасности, начав с **малых предприятий**. Типичным примером малого предприятия, как показывает практика, является посредническая организация. Основными направлениями деятельности таких организаций является получение кредита в банке, приобретение на кредитные средства оптовых партий товаров, имеющих спрос у потребителей, реализация товара оптом и (или) розницу с использованием специализированных магазинов, в том числе и партнеров. Обычно такие предприятия арендуют офисные и складские помещения, имеют наемный штат работников, состоящий из директора, коммерческого директора, главного бухгалтера, экономиста-диспетчера, водителей, экспедиторов. Возможные угрозы безопасности такой наиболее распространенной в торговом обороте организации определяются, прежде всего, имущественными интересами организации, наличием сил и средств.

Анализ хозяйственной деятельности малых предприятий показывает, что их собственность, как правило, составляют лишь оборудование, транспорт и другое движимое имущество. Такие предприятия учреждаются в форме производственных кооперативов, хозяйственных товариществ и обществ. Общая классификация основных угроз организации в целом пригодна для определения угроз безопасности малых предприятий. Наиболее характерными являются следующие деяния, которые способны дестабилизировать работу малых предприятий, занимающихся торгово-посреднической деятельностью:

- хищение товаров со склада или при их транспортировке работниками предприятия и посторонними лицами;

- передача экспедитором товара на реализацию в магазины по завышенным ценам, превышающим установленные руководством предприятия, и сокрытие дополнительно полученных доходов;

уничтожение или повреждение товара по вине работников предприятия (например, нарушение правил пожарной безопасности на складе, дорожное движение при перевозке грузов и др.);

повреждение или хищение товара, предоставленного предприятием на реализацию, совершенное по вине работников магазина-партнера;

хищение денег и материальных ценностей, принадлежащих предприятию, совершенное работниками или посторонними лицами;

приобретение уполномоченными представителями предприятия товара, не пользующегося спросом, в корыстных целях;

разглашение работниками предприятия сведений, составляющих коммерческую тайну (о торговых и финансовых операциях, партнерах, клиентах, местах закупки товаров и т.д.);

утечка сведений, составляющих коммерческую тайну, произошедшая по вине работников организаций-контрагентов, государственных и муниципальных служащих, которым такие сведения были переданы по договору или по мотивированному запросу;

утрата документов, содержащих конфиденциальные сведения о деятельности предприятия;

риск со стороны криминальных структур и другие.

Перечисленные выше деяния, создающие угрозы предприятию, хотя и различны по своему содержанию, тем не менее, в большинстве случаев, совершаются штатными работниками, что следует учитывать при планировании и проведении воспитательно-профилактических мероприятий. Составленный перечень вероятных угроз безопасности позволяет определить наиболее характерные меры по защите интересов малого предприятия, которые включают: осуществление проверки лиц при их подборе и расстановке на конкретных участках работы; проведение воспитательно-профилактической работы (ВПР) в целях предупреждения совершения правонарушений; контроль за исполнением работниками трудовых обязанностей в период выполнения ими коммерческих поручений; определение порядка доступа работников к КЗИ, учета в конфиденциальном делопроизводстве; физическая охрана материальных ценностей; обеспечение конфиденциальности сведений, касающихся торгового оборота товаров, процедуры заключения договоров и исполнения обязательств, а также порядка финансирования коммерческих сделок.

Решение задач, связанных с реализацией названных мероприятий, требует создания специального подразделения в рамках малого предприятия. Однако финансовые возможности малого предприятия

не позволяют ему решить проблему таким образом. Передача функций обеспечения безопасности другой организации тоже в данном случае неприемлема. Поэтому в большинстве случаев малые предприятия решают задачу обеспечения своей безопасности исходя из собственных возможностей либо вообще не занимаются ее решением. *Руководитель малого предприятия* по согласованию с учредителем распределяет обязанности между работниками в части обеспечения безопасности, в зависимости от предоставленных им правомочий по занимаемой должности.

Самые важные вопросы решаются лично *директором предприятия*. Он осуществляет подбор, расстановку кадров и проводит их инструктаж. Периодически ведет в коллективе ВПР, позволяющую сформировать команду единомышленников. Директор осуществляет контроль за выполнением работниками обязанностей по сохранности коммерческой тайны при ведении ими коммерческих переговоров и заключении сделок. Важным направлением его работы является установление степени конфиденциальности сведений и возможности их использования при ведении коммерческих переговоров и заключении договоров; установление цены на товар; принятие мер по противодействию рэкету; организация физической охраны объектов и определение условий взаимодействия с органами внутренних дел; организация маркетинговых и аналитических исследований; определение процедуры допуска и доступа лиц к сведениям, составляющим коммерческую тайну предприятия.

*Главный бухгалтер малого предприятия* выполняет обязанности, связанные с ведением бухгалтерского учета и отчетности, в том числе учета нематериальных активов использования информационных ресурсов; осуществлением контроля за финансовой деятельностью и соблюдением законности при ведении коммерческой деятельности; за сохранностью коммерческой тайны в части, касающейся экономической деятельности, и обеспечивает в этой связи конфиденциальность работ, выполняемых работниками бухгалтерии. Главный бухгалтер готовит предложения по включению в перечень категорий сведений, составляющих коммерческую тайну (бухгалтерская отчетность, данные учетных регистров, сведения о кредиторской задолженности, рентабельности фирмы, размере заработной платы каждого работника и др.), и определяет степень конфиденциальности документов, находящихся в обороте бухгалтерии; участвует в проведении маркетинга путем определения сведений экономического характера, которые необходимы предприятию, а также определяет

круг сведений, характеризующих финансовое положение организации для использования их в рекламе.

Обязанности *экономиста-диспетчера* несколько иные. Он занимается определением надежности партнеров, систематизацией и обобщением сведений об изменении цен и конъюнктуры рынка. Ему поручается ведение делопроизводства. Он обеспечивает сохранность сведений, используемых в ходе коммерческих переговоров, составляющих коммерческую тайну, ведет договорную работу и учет конфиденциальных документов. *Заведующий складом* выполняет обязанности, связанные с сохранностью сведений о партнерах, клиентах, местах закупки товаров, составляющих коммерческую тайну. Он обеспечивает учет материальных ценностей, находящихся на складе, и осуществляет контроль за исправностью технических средств охраны. На *экспедиторов* возлагаются обязанности по учету изменения цен и конъюнктуры рынка товаров, закупаемых предприятием, а также контроль за сохранностью товаров в период их транспортировки и передачи на реализацию.

Названный подход к обеспечению безопасности организаций получил широкое распространение на практике и является типичным для малых предприятий.

Обеспечение безопасности **средних коммерческих организаций** связано с расширением направлений хозяйственной деятельности, увеличением численности работников организации и связей с контрагентами, что объективно обуславливает рост числа дестабилизирующих факторов. Эти факторы существенно влияют на определение оптимальной структуры управления и объем правомочий работников, а также на содержание мероприятий по обеспечению безопасности организации.

Определенные особенности имеет обеспечение безопасности организации, относящейся к категории средних предприятий, которая специализируется на закупке и реализации товаров широкого потребления, оказании транспортных услуг юридическим лицам и гражданам, оказании складских услуг, организации платных автостоянок и строительстве гаражей. Численность работников в таких организациях составляет примерно 100–150 человек. Права организации по обеспечению безопасности закреплены за работниками обычно в следующем порядке.

*Руководитель организации* на основании устава и иных корпоративных актов осуществляет общее руководство и управление предприятием в условиях рыночной экономики. С учетом специфики

деятельности организации к нему предъявляются обычные, стандартные требования, как к руководителю такого уровня. Наряду с выполнением задач по развитию предприятия и получению стабильной прибыли руководитель обязан организовать выполнение решений собственников (акционеров, учредителей) организации, в том числе и по вопросам обеспечения безопасности. В этих целях ему делегированы учредителем права по утверждению перечня категорий сведений, составляющих коммерческую тайну, установлению степени конфиденциальности информации; выдачи разрешений на допуск и доступ лиц к конфиденциальным документам, изделиям и работам и ряд других вопросов. В поле зрения директора находятся самые важные направления охраны конфиденциальности КЗИ.

*Коммерческий директор* определяет направления маркетинговых исследований рынка товаров (работ, услуг) с учетом специализации организации, готовит прогноз развития новых видов коммерческой деятельности. В его обязанности входит ведение коммерческих переговоров и заключение договоров, определение надежности партнеров, выявление угроз бизнесу и разработка рекомендаций по их предупреждению; установление неправомерного использования в торговом обороте фирменных знаков и наименований, принадлежащих организации; проведение служебного расследования по факту разглашения сведений, составляющих коммерческую тайну. В подчинении коммерческого директора могут находиться работники, которые выполняют часть названных выше обязанностей. Это могут быть *экономист, маркетолог, эксперт по безопасности* и другие.

Анализ материалов ряда организаций показывает, что эксперт по безопасности часто совмещает функции маркетолога или наоборот, и выполняет в этой связи обязанности, связанные с проверкой финансового положения партнеров, контрагентов и иных лиц при заключении договоров; анализом и обобщением информации об изменениях конъюнктуры рынка и цен; формированием заданий на проведение маркетинга по определенным сегментам рынка.

*Юридическая служба (юрисконсульт)* обеспечивает разработку проектов договоров, ведет учет и систематизацию правовых актов, имеющих отношение к хозяйственной деятельности организации. Обязанностями юриста является согласование проектов корпоративных актов на предмет их соответствия нормам законодательства; разработка рекомендаций по соблюдению законности в хозяйственной деятельности; представление интересов и защита прав организации в суде, правоохранительных и иных государственных орга-

нах; осуществление контроля за выполнением договорных обязательств, в том числе по соблюдению условий конфиденциальности. Анализ материалов показывает, что в отдельных организациях в штате юридической службы находится инспектор по кадровой работе (в ряде организаций, наоборот, юрисконсульт находится в штате отдела кадров), который ведет кадровый учет и личные дела работников, оформляет материалы на допуск лиц к сведениям, составляющим коммерческую тайну, и участвует в иных мероприятиях по обеспечению безопасности<sup>1</sup>.

*Главный бухгалтер (старший бухгалтер, бухгалтер)* обеспечивает в процессе своей основной деятельности конфиденциальность сведений, составляющих коммерческую тайну, относящихся к деятельности бухгалтерии. Нарушения могут быть выявлены при проверке подлинности платежных и иных финансовых документов, проведении инвентаризации материальных средств, включая изделия, соержащие КЗИ, анализе документального оформления процессов кредитования, инвестирования и решении других задач, стоящих перед этой службой. Кроме того, необходимо выделить роль *аудитора, работающего по гражданско-правовому договору с организацией*. Он несет ответственность за сохранность конфиденциальных сведений, которые ему доверены по работе, осуществляет контроль правильности ведения финансовых операций; готовит рекомендации по устранению выявленных нарушений в финансовой деятельности.

Обязанности других работников аппарата управления организации несколько иные. *Секретарь-референт* во многих организациях ведет конфиденциальное делопроизводство, а именно: учет, обработку и хранение документов с грифом «Коммерческая тайна», и несет в этой связи ответственность за сохранность таких документов, обеспечивает проведение служебных совещаний, на которых оглашаются сведения конфиденциального характера. *Бухгалтер-кассир* ведет кассовую книгу, оформляет ведомости на выплату заработной платы работникам; работает с денежными средствами и отвечает за их сохранность на основании договора о полной материальной ответственности; располагает в силу выполнения служебных обязанностей КЗИ о выручке денежных средств организации, сведениями о работниках, партнерах, клиентах, других лицах и обеспечивает их конфиденциальность. *Заведующий складом* ведет учет материальных

<sup>1</sup> См.: Эффективный юридический департамент: Сборник / Сост. О.А. Филимонова. М., 2007. С. 7–74, и др.

ценностей и обеспечивает их сохранность; обеспечивает эксплуатацию инженерно-технических средств охраны; несет ответственность за сохранность конфиденциальных сведений о продукции, содержащей КЗИ.

Весьма специфические обязанности выполняет *подразделение охраны*, которое осуществляет круглосуточное дежурство на объектах, принадлежащих организации, обеспечивает эксплуатацию и техническое обслуживание инженерно-технических средств охраны, внутриобъектовый и пропускной режим.

Значительные по объему правомочия предоставлены *руководителю структурного подразделения*. Он осуществляет подбор кадров для работы на конкретных участках производства и реализации товаров, где используется КЗИ, ведет контроль за деятельностью подчиненных работников в процессе обращения такой информации, несет ответственность за сохранность конфиденциальных документов и изданий, находящихся в подразделении, организует реализацию мероприятий по обеспечению установленного на конкретном участке режима коммерческой тайны.

При определении структуры службы безопасности нужно учитывать, что на среднем по размерам предприятии в отличие от малого возрастает объем хозяйственных связей, увеличивается число угроз, направленных против частных интересов; возрастает оборот конфиденциальных документов. Кроме того, требуется усиленная охрана материальных ценностей по сравнению с обычными условиями охраны на малых предприятиях. Нельзя не учитывать и возрастающее количество коммерческих договоров, заключаемых средним предприятием. Это обстоятельство требует учета появления новых объектов обеспечения безопасности, особенно при совершении крупных финансовых операций. В целом можно говорить о том, что с увеличением масштабов деятельности предприятия возникает необходимость принятия дополнительных мер по обеспечению его безопасности. Это связано не только с необходимостью привлечения дополнительных финансовых и трудовых ресурсов, но и с совершенствования форм и методов работы. При этом, как свидетельствуют результаты исследования, неизменными остаются основные направления обеспечения безопасности предприятия в рыночной экономике.

Следовательно, система безопасности предприятий, относящихся к категории среднего бизнеса, претерпевает в основном количественные изменения. Расширение круга хозяйственных интересов

предприятия, подверженных тем или иным угрозам, влечет за собой увеличение числа его работников, занятых обеспечением безопасности. Нужно отметить, что такая тенденция количественного роста работников РСО была характерна и для советского периода.

Аналогичная закономерность в обеспечении безопасности отмечается при переходе от среднего к **крупному предпринятию**, численность которого превышает 1000 человек. Обеспечение безопасности такого предприятия осуществляется по тем же направлениям, что и среднего предприятия, в зависимости от сфер занятия бизнесом, а также существования дочерних компаний, филиалов и представительств, требующих единого подхода к организации защиты КЗИ<sup>1</sup>. Различие, пожалуй, состоит только в количестве подразделений и работников, занятых разработкой и реализацией мероприятий по установлению режима коммерческой тайны, и его обеспечению.

Таким образом, существование угроз организации и необходимость адекватных мер по их предотвращению определяют структуру ее безопасности. Установление режима коммерческой тайны и его обеспечение может осуществляться различными производственными и иными подразделениями (звеньями, отдельными работниками) либо самостоятельной службой безопасности. Такой подход объясняется необходимостью противодействия угрозам, являющимся, как правило, общими для любых категорий предприятий. Следовательно, организационная структура безопасности формируется на всех предприятиях с соблюдением общих принципов. Существующие различия объясняются лишь количественными параметрами, и, прежде всего, численностью работников, занятых реализацией мер по обеспечению безопасности.

#### § 4. Методология и методика определения степени конфиденциальности коммерчески значимой информации

Методология обоснования критериев, лежащих в основе определения степени конфиденциальности коммерчески значимой информации, до сего времени в юридической науке не разработана. Боль-

<sup>1</sup> См.: *Могилевский С.Д.* Правовые основы деятельности акционерных обществ. М., 2004. С. 167–201, и др.

шинство ученых<sup>1</sup>, занимающихся проблемами правового регулирования коммерческой тайны, не выделяют признаки, по которым можно отнести информацию к такой тайне. По этому пути идет и действующее законодательство о коммерческой тайне, закрепляющее право на отнесение информации к коммерческой тайне за ее обладателем (ст. 4 Закона о коммерческой тайне). Поэтому имеется необходимость в разработке принципов отнесения информации к коммерческой тайне и методики определения перечня таких сведений.

Материалы проведенного исследования позволяют сделать вывод о том, что степень конфиденциальности информации, составляющей коммерческую тайну, определяется ее важностью и ценностью для организации, характером и размером ущерба, который может быть причинен ей в случае разглашения или незаконного использования третьими лицами. Для обоснования этого вывода обратимся к результатам анализа двух важнейших категорий: «фактора ущерба» и «фактора времени», оказывающих существенное влияние на определение и изменение степени конфиденциальности КЗИ.

**Ущерб как материальный признак отнесения информации к коммерческой тайне.** Гражданско-правовое понятие «материальный вред» (ущерб), разработанное в цивилистической науке<sup>2</sup>, имеет определенную специфику по отношению к предмету нашего исследования, сущность которого может быть раскрыта с учетом свойств информации как объекта гражданско-правового регулирования.

Очевидно, что для принятия обоснованного решения при составлении перечня сведений, составляющих коммерческую тайну организации, и изменении степени конфиденциальности сведений или снятия грифа «Коммерческая тайна», необходимо сформулировать подход к определению понятия ущерба, определить его качественные и количественные признаки по отношению к КЗИ.

Отсутствие научного определения понятия ущерба применительно к КЗИ вызывает определенные трудности при проведении экспертизы степени конфиденциальности информации в ходе расследования фактов разглашения сведений, составляющих коммерческую

<sup>1</sup> См.: Шиверский А.А. Защита информации: проблемы теории и практики. М., 1996. С. 32–34; Фатьянов А.А. Правовое обеспечение безопасности информации в Российской Федерации. М., 2001. С. 188–197; Зельцер М.С. Гражданско-правовой режим информации: Автореф. дисс. на соис. уч. ст. к.ю.н. М., 2004, и др.

<sup>2</sup> См.: Грибанов В.П. Осуществление и защита гражданских прав. 2-е. изд. М., 2001. С. 329–332, и др.

тайну, утраты документов и изделий, содержащих такие сведения, а также в случаях необходимости снятия грифа «Коммерческая тайна». Анализ показывает, что иногда сведениям различной степени конфиденциальности экспертным путем дается одинаковая оценка ущерба либо, наоборот, по-разному оценивается ущерб сведений одной и той же степени конфиденциальности в случаях их разглашения (утечки). Учитывая нематериальную природу КЗИ и то обстоятельство, что ее денежная оценка не отражается в бухгалтерском балансе, **материальный вред (ущерб) в случае разглашения (утечки) КЗИ может быть связан с имущественными потерями для организации, которые при необходимости можно оценить экспертным путем.** Поэтому, говоря об ущербе применительно к КЗИ, мы в данном случае имеем в виду имущественные потери, которые могут наступить вследствие неправомерного использования такой информации.

Изучение материалов организаций позволило сформулировать наиболее характерные виды материального вреда (ущерба), который связан с имущественными потерями и причинением организации убытков, выраженных в денежной форме. Имущественные потери организации могут наступить чаще всего вследствие неправомерных, а иногда и правомерных, но без учета хозяйственной ситуации, действий либо бездействия субъектов в гражданском обороте. К числу наиболее характерных обстоятельств следует отнести:

- разрыв деловых отношений с одним или несколькими партнерами организации;
- срыв переговоров и выгодного организации договора;
- снижение уровня сотрудничества организации с контрагентами по производственным, научно-техническим, коммерческим и другим вопросам;
- невыполнение или ненадлежащее выполнение договорных обязательств, включая поставки для государственных нужд;
- необходимость проведения дополнительных маркетинговых исследований и разработки новой конкурентной стратегии;
- отказ от организационных, научно-технических или коммерческих решений, ставших неэффективными в результате утечки сведений, и необходимость разработки новых средств конкурентной борьбы;
- использование конкурентами полученных сведений для разработки новой конкурентной стратегии;
- имущественная ответственность и экономические санкции государства против организации;

- создание «узких мест» в снабжении производства и реализации продукции;
- потеря приоритета в научных исследованиях и возможности патентования, продажи лицензий и ноу-хау;
- сокращение конкурентами затрат на проведение собственных НИОКР;
- потери, связанные с утратой лидерства в научных исследованиях;
- создание трудностей в приобретении оборудования или технологии, в том числе путем повышения цен на них;
- другие виды возможного материального вреда (ущерба) организации, в том числе связанные с выполнением задач, определенных ее уставом.

*При определении размеров возможного материального вреда, связанного с имущественными потерями, может быть произведена его оценка в стоимостном выражении.* Для решения этой задачи необходимо воспользоваться принятыми в планово-экономическом, научно-техническом, производственном и иных подразделениях, сходных по своему значению, такими показателями оценки, как:

- стоимость произведенной продукции вследствие невыполнения обязательств контрагентами по поставкам оборудования, сырья и материалов, в результате отказа партнеров от экономического и научно-технического сотрудничества и осуществления конкурентами недружественных действий, связанных с неправомерным использованием КЗИ;
- стоимость неправомерно используемых конкурентами отдельных результатов НИОКР (определяется экономия затрат конкурента на проведение собственных научных исследований);
- эффект от внедрения в производство неправомерно полученных конкурентами результатов НИОКР (определяется коммерческая выгода конкурентного преимущества в реализации товаров);
- стоимость приобретенного у конкурентов оборудования и технологий, которые изготовлены с использованием незаконно полученной КЗИ;
- возможные объемы продаж товаров на рынке с использованием незаконно полученной конкурентами КЗИ, другие показатели, характеризующие возможный материальный вред (ущерб) организации.

*Оценка размеров материального вреда (ущерба) производится специалистами как расчетным, так и экспертным способом.* Получение

количественной оценки материального вреда (ущерба) позволит на основании его размера варьировать значение степени конфиденциальности информации. Представляется, что *дополнительно гриф «Коммерческая тайна» может содержать пометку с указанием степени важности охраняемой информации.* Например, обладатель КЗИ может ввести дополнительные пометки к грифу «Коммерческая тайна» в виде *1-й категории (ущерб), 2-й категории (крупный ущерб) и 3-й категории (ущерб, ведущий к банкротству).* Установление степени категорий КЗИ необходимо для определения объема разумно достижимых мер по охране конфиденциальности информации. В силу деления организаций на крупные, средние и малые прогнозируемый ущерб, исчисляемый по названному выше трем категориям КЗИ, будет различным.

Среди факторов, влияющих на принятие решения о защите конкретной информации и внесении ее в перечень сведений, составляющих коммерческую тайну, необходимо выделить *ущерб, причиняемый организации в результате необоснованного отнесения информации к коммерческой тайне.* Отнесение информации к КЗИ может быть связано с наступлением определенных отрицательных последствий, причем как для самой организации, так и общества в целом. В их числе можно назвать, с одной стороны, отвлечение материальных, финансовых и трудовых ресурсов, направляемых на установление режима коммерческой тайны и его обеспечение, не вызываемых объективной необходимостью, которые могли быть использованы для повышения эффективности производства. С другой — потери общества от установленных ограничений использования информации, которая выведена из гражданского оборота. Проблема в данном случае заключается в том, как сделать отрицательные последствия минимальными.

До настоящего времени *вопрос об отрицательных последствиях засекречивания информации недостаточно изучен в юридической науке.* Конфиденциальность как атрибут производства и реализации товаров (работ, услуг) присутствует в деятельности любой фирмы. Она выступает как универсальное правовое средство предотвращения ущерба, который может быть причинен организации. Однако ограничение само по себе далеко не безвредно. Общеизвестно, что излишняя конфиденциальность мешает нормальному функционированию организаций, затрудняет внедрение научных достижений и технических идей в производство, ограничивает права и законные интересы граждан на получение и пользование информацией. Поэ-

тому организации всегда стоят перед сложной дилеммой, какая информация, прежде всего технического, технологического и делового характера, должна быть закрытой, а какую ее часть следует оставить открытой, т.е. доступной для всех на общих основаниях.

*Речь идет о необходимости учета не только возможного материального вреда при попадании сведений к конкуренту, но и наступления негативных последствий в случае введения организации необоснованных ограничений на распространение информации путем ее засекречивания.* В литературе отсутствует содержательный анализ отрицательных последствий засекречивания организациями информации, относящейся к коммерческой тайне. Законодательством не предусмотрены санкции в отношении хозяйствующих субъектов, злоупотребляющих своим правом на отнесение информации к коммерческой тайне. Такое положение дел отражается на практике, когда происходит необоснованное повсеместное засекречивание организациями сведений, чем причиняется ущерб не только отдельным предприятиям, отраслям экономики, но и в целом стране. В некоторых случаях, когда приходится оценивать степень конфиденциальности сведений, даже при первичной оценке видно, что ущерб в случае попадания сведений к конкуренту будет меньше затрат (ущерба) от их засекречивания. Безусловно, на практике могут встречаться такие случаи. Но чаще эта разница не настолько очевидна. В этих случаях необходимо сопоставление двух названных видов ущерба, после чего должен решаться вопрос о засекречивании информации.

Представляется, что ущерб от необоснованного засекречивания информации должен включать: а) непосредственные затраты на засекречивание КЗИ; б) ущерб обществу и государству в результате ограничения обладателем обращения КЗИ, и невозможности ее использования в рыночной экономике.

**Непосредственные затраты на засекречивание информации** складываются из материальных, трудовых и финансовых затрат, необходимых для организации и осуществления мероприятий по установлению и обеспечению режима конфиденциальности. При учете затрат нужно исходить из необходимости решения организацией комплекса задач. В числе первоочередных задач, требующих ресурсного обеспечения, следует назвать: создание службы безопасности и обеспечение финансирования ее деятельности; осуществление проверочных мероприятий, связанных с допуском к конфиденциальным работам и документам необходимого числа работников; разработка системы корпоративной конфиденциальной связи внутри организа-

ции; проведение необходимых инженерно-технических работ, связанных с обеспечением охраны конфиденциальности информации; организация физической охраны конфиденциальных документов и изделий, а при необходимости и персонала, выполняющего секретные работы; реализация других мероприятий, которые должны быть предварительно оценены в стоимостном выражении. В зависимости от общего объема предполагаемых работ по обеспечению охраны конфиденциальности информации учитываются непосредственные затраты, связанные с засекречиванием КЗИ, которые включаются в бюджет организации.

Проведение оценки затрат на засекречивание информации должно увязываться с возможностями получения ее конкурентной разведкой. Для этого необходимо предварительно определить принципиальную возможность защиты таких сведений с учетом имеющихся сил и средств.

**Ущерб обществу и государству в результате ограничения обладателем обращения КЗИ, и невозможности ее использования в рыночной экономике** в значительной мере связан с уровнем *эффективности использования КЗИ в отраслях экономики*. Официальные данные о масштабах ущерба, причиняемого экономике страны в результате засекречивания информации коммерческими организациями, отсутствуют. Эффективность использования закрытых сведений для развития экономики можно оценить путем анализа данных, опубликованных в западной печати. Так, использование научно-технических достижений НАСА, применяемых в военной области, оказывает значительное влияние на развитие экономики США<sup>1</sup>. Передача технологии из военно-космических корпораций в гражданские отрасли является в экономически развитых странах одним из главных источников обновления продукции. В 1996 г. в США был принят федеральный закон о порядке передачи технологий двойного применения<sup>2</sup>. Распространение полученных в ходе исследований технологий, нововведений и открытий, а также доступ фирм США к секретной научно-технической информации и ее обмен между подрядчиками НИОКР осуществляется на основе включения соответствующих условий в контракты. Поэтому, начиная с 80-х гг., между военны-

<sup>1</sup> См.: Индастриал Речес. 1998. 10. № 7. С. 50—53.

<sup>2</sup> См.: Кузык Б.Н., Яковец Ю.В. Россия — 2050. Стратегия инновационного профиля. 2-е изд. М., 2005. С. 197—204.

ми и гражданскими секторами экономики США не существует значительного «информационного барьера», что способствует быстрому развитию роста технологичности выпускаемых товаров<sup>1</sup>.

Для нашей страны еще в советское время потери от тотального засекречивания научно-технических разработок были весьма значительны. По оценке специалистов, в 90-е гг. государство практически перестало поддерживать изобретательскую деятельность. Россия имеет более низкую долю затрат на НИОКР (в 2,4 раза ниже среднемировой)<sup>2</sup>. Большая часть изобретений в СССР не была запатентована и до сих пор держится в секрете, с соблюдением режима ноу-хау. Их продажа за рубеж не всегда является выгодным делом для государства<sup>3</sup>, тем более что большая часть изобретений применяется в создании военной техники и поэтому является государственной тайной.

Негативные последствия ограничения оборота информации называют непосредственное влияние на *эффективность использования КЗИ для научно-технического прогресса*. Ограничение доступа специалистов к информации затрудняет ее использование в научных и технических разработках, что отражается на качестве и сроках исследований. Темпы научно-технического прогресса в отраслях экономики определяются в значительной мере НИОКР, результаты которых базируются на научных открытиях и фундаментальных работах, поэтому их засекречивание должно производиться в обоснованных случаях.

Засекречивание научных работ и разработок не всегда целесообразно. Оправданным является засекречивание планов и концепций лишь тогда, когда это позволяет обеспечить временные преимущества на ближайшие 2–3 года. Такой подход к решению вопроса о рассекречивании научных разработок представляется в значительной мере оправданным. Это позволяет широко использовать в экономике новейшие достижения науки и извлекать организациям прироста.

<sup>1</sup> См.: Кузык Б.И., Яковец Ю.В. Россия — 2050. Стратегия инновационного прорыва. 2-е изд. М., 2005. С. 197–198.

<sup>2</sup> См.: Там же. С. 174–175.

<sup>3</sup> См.: *Вольнец-Руссет Э.Я.* Международный технологический обмен и его роль в экономическом развитии России: Дисс. в виде науч. доклада на соис. уч. ст. д.э.н. М., 2005. С. 39–46.

*Оценивая последствия закрытия информации, нужно иметь в виду и воздействие этого процесса на эффективность использования КЗИ для успешного развития рыночной экономики в России.* Отдельные сведения, относимые к категории КЗИ, могут эффективно использоваться в экономической политике государства. Засекречивание таких сведений организацией косвенно причиняет вред государству. Однако, с другой стороны, публикация КЗИ может причинить ущерб частным интересам. Поэтому речь идет о компенсации государством ущерба в случаях раскрытия КЗИ по требованию его представителей.

Итак, при решении вопроса о засекречивании сведений необходимо учитывать его возможные отрицательные последствия.

*Анализ и сопоставление возможного ущерба при разглашении (утечке) сведений, с одной стороны, и отрицательных последствий защиты информации — с другой, позволяет определить целесообразность защиты той или иной информации. Однако для включения ее в соответствующий перечень этого недостаточно. Необходимо учитывать важность КЗИ, обуславливающей степень ее конфиденциальности.*

В Законе о коммерческой тайне отсутствует классификация сведений, составляющих коммерческую тайну, с учетом степени их конфиденциальности. Анализ показывает, что в большинстве крупных организаций применяется система классифицированной информации, составляющей коммерческую тайну. Критерием классификации является размер ущерба, который может быть причинен организации. В литературе не содержатся предложения по градации категорий ущерба. Безусловно, предельный размер ущерба определяется индивидуально каждой организацией. Вместе с тем, применительно к любой организации, экспертным путем могут быть условно, на наш взгляд, выделены три категории ущерба: *коммерческая тайна (КТ) первой категории (ущерб), КТ второй категории (крупный ущерб), КТ третьей категории (тяжкие последствия в виде банкротства организации)*. Повышение категории возможного ущерба от разглашения (утечки) КЗИ непосредственно влияет на уровень охраны конфиденциальности такой информации.

Изучение корпоративных документов, устанавливающих режим коммерческой тайны, показывает, что на практике не существует каких-либо различий, например, в правилах обращения с документами различной категории конфиденциальности. Поэтому кроме общих требований, предъявляемых к охране конфиденциальности информации, необходимо дополнительно закрепить правила, позво-



ляющие учитывать различный уровень защиты категоризированной КЗИ. Эти вопросы должны дифференцированно отражаться в системе безопасности организации.

**Анализ влияния фактора времени на степень охраны конфиденциальности КЗИ.** При оценке конфиденциальности информации следует учитывать ее актуальность. То, что вчера представляло коммерческий интерес, сегодня может потерять свое значение. В то же время появляются новые сведения, требующие защиты. Примером, подтверждающим учет влияния фактора времени на определение степени охраны информации, является история развития в советский период института перечня сведений, составляющих государственную тайну (далее — Перечень). Изучение содержания перечней подтверждает тенденцию расширения или сужения категорий сведений, составляющих государственную тайну, в зависимости от времени принятия Перечня<sup>1</sup>.

Так, в Перечень 1959 г., по сравнению с предыдущим, в котором военной тайной признавались сведения о мобилизационных планах и сводные данные в целом по стране, были включены аналогичные сведения по отдельным наиболее важным предприятиям, выпускающим специальные виды вооружения. Кроме того, был утвержден перечень «Особо режимных и наиболее важных предприятий, выпускающих специальные виды вооружения», который ранее не существовал. В Перечне 1966 г. названные сведения были конкретизированы с указанием видов вооружения, имевшихся в то время в Вооруженных Силах СССР.

Расширение или сужение категорий сведений, составляющих государственную тайну, представляет собой объективный процесс, участвующий изменения во внешней и внутренней политике нашего государства, развитие науки и техники и другие факторы. Перечень главнейших сведений, составляющих государственную тайну (ПГС), судя по времени внесения в него изменений, являлся более стабильным правовым актом. Этот вывод подтверждается результа-

тами анализа. Так, в СССР за период с 1918 по 1926 г. были приняты 4 перечня, с интервалом в среднем 2 года. Перечень 1926 г. действовал без изменений почти 21 год. Соответственно Перечень, утвержденный в 1947 г., — 9 лет, в 1956 г. — 10 лет, в 1966 г. — 14 лет и в 1980 г. — 11 лет. В министерствах и ведомствах действовали на основании ПГС свои перечни, в которые более оперативно вносились изменения и дополнения. Эта работа носила систематический характер и позволяла более гибко реагировать на происходящие изменения в науке и технике.

В общесоюзных правовых актах (Инструкция № 0126-87 и др.) содержалось требование о необходимости учета фактора времени и определении в ведомственном перечне контрольного срока перечисления степени секретности сведений. В Инструкции содержалось требование о том, что степень секретности категорий сведений изменяется в связи с появлением объективных факторов, вызывающих необходимость ее корректировки. Например, появление новых достижений в науке и технике, снятие изделия с вооружения и др. В современный период срок засекречивания сведений, составляющих государственную тайну, не должен превышать 30 лет. В отдельных случаях он может быть продлен в порядке, установленном законом<sup>1</sup>.

В период рыночной экономики коммерческие организации сами решают, какая информация представляет для них ценность в тот или иной период времени. Работа по установлению и изменению категорий сведений, составляющих КЗИ, ведется организацией без привлечения посторонних лиц. Корпоративные акты содержат правила и устанавливают порядок проведения этой работы. В частности, степень конфиденциальности сведений по НИР и ОКР определяется заказчиком и подрядчиком (исполнителем) непосредственно в техническом задании либо в отдельном прилагаемом к нему документе. Для учета фактора времени, влияющего на изменение степени конфиденциальности КЗИ, необходимо проанализировать особенности жизненного цикла разработки изделия. Это наглядно проявляется на различных этапах создания новых изделий.

На этапе научных исследований к защищенным сведениям имеет доступ ограниченное число исполнителей. Производственные процессы, связанные с различным рода излучениями, практически отсутствуют. В таких условиях организовать защиту сведений можно с

<sup>1</sup> См.: Ф3 от 6 октября 1997 г. № 131-ФЗ «О государственной тайне» // СЗ РФ. 1997. № 41. Ст. 4673.

<sup>1</sup> См.: Сборник законов СССР. М., 1926. № 32; Ведомости Верховного Совета СССР. 1947. № 20; Сборник документов по истории уголовного законодательства СССР и РСФСР 1917—1952 гг. М., 1953; Уголовное законодательство СССР и союзных республик. Т. 1. М., 1963; Справочник по законодательству для работников органов прокуратуры, суда и МВД. Т. 26. Ч. 1. М., 1971; Северин В.А. Правовое регулирование охраны государственных секретов в СССР // Советское государство и право. 1991. № 1, и др.

достаточной степенью надежности. По мере перехода от НИР к ОКР и созданию опытных образцов, их испытаниям, серийному производству и эксплуатации значительно увеличивается круг лиц, имеющих доступ к защищенным сведениям, и количество материальных носителей, содержащих такие сведения. Одновременно возрастают возможности конкурентов по получению защищаемой информации с помощью технических средств разведки. Становится значительно сложнее защищать сведения с необходимой степенью надежности, а порой практически невозможно это сделать. Поэтому необходимо проводить корректировку степени конфиденциальности сведений для предотвращения ущерба организации от необоснованного засекречивания информации. Такую корректировку целесообразно проводить и в том случае, когда на защиту КЗИ предполагается использовать значительные материальные и иные ресурсы, превышающие сумму возможного ущерба.

При принятии решения о рассекречивании информации следует учитывать осведомленность конкурента о введущихся работах. Такие данные СБ получают путем анализа материалов зарубежных публикаций, изучения докладов ученых и специалистов конкурирующих фирм на съездах, конференциях, симпозиумах. Причем осведомленность в КЗИ одного конкурента не означает отмену ее защиты по отношению к другим конкурирующим фирмам. Кроме того, необходимо учитывать решения Правительства РФ о продаже техники и технологии за рубеж, содержащих КЗИ. Организация в этом случае вынуждена рассекречивать передаваемые за рубеж изделия и технологии.

Вопрос о снятии грифа «Коммерческая тайна» с документов, изделий и работ полностью находится в ведении организации. Вмешательство государства в этот процесс не допускается, кроме случаев, установленных законом. Ассоциации и союзы организаций могут вырабатывать общие условия и правила отнесения сведений к информации, составляющей коммерческую тайну. Усилия заинтересованных организаций позволяют решить задачу разработки эффективного механизма установления степени конфиденциальности КЗИ, ее пересмотра, изменения и рассекречивания, что способствует формированию перечня сведений, составляющих коммерческую тайну конкретной организации.

**Концептуальные аспекты установления категорий сведений, составляющих коммерческую тайну.** Важное место в системе мер по охране конфиденциальности КЗИ занимает процедура установле-

ния на корпоративном уровне категорий сведений, составляющих коммерческую тайну, определения и изменения на их основе грифа «Коммерческая тайна» конкретных сведений, содержащихся в работах, документах и изделиях. В Законе о коммерческой тайне не упоминается и не раскрывается содержание этих процедур, за исключением обязанности организации по составлению перечня информации, составляющей коммерческую тайну (п. 1 ч. 1 ст. 10). Реализация названной меры по составлению Перечня связана с обменом научнотехнической и деловой информацией, с рациональным использованием организационной сил и средств, используемых для охраны конфиденциальности КЗИ.

Эта работа является достаточно сложной. Она представляет собой первоначальный этап в системе мер по установлению режима коммерческой тайны в организации. Ее сущность состоит в выделении из общего массива разнообразной информации категорий сведений, отражающих наиболее важные направления деятельности организации. *Под категорией сведений нужно понимать выраженную в обобщенном виде, без привязки к конкретному образцу изделия, создаваемой техники, коммерческой сделке и т.п., не подлежащую разглашению информацию, степень конфиденциальности которой устанавливается организацией в перечне сведений, составляющих коммерческую тайну.*

На основании установленных и утвержденных организацией категорий сведений исполнитель и его руководитель определяют степень конфиденциальности конкретных сведений, содержащихся в работах, документах и изделиях. Естественно, что с изменением хозяйственной ситуации возникает необходимость в пересмотре степени конфиденциальности КЗИ, т.е. в повышении или снижении грифа «Коммерческая тайна». Регулирование этих вопросов осуществляется на основании Перечня сведений, составляющих коммерческую тайну организации (далее — Перечень), и с учетом имеющегося опыта работы по защите КЗИ. В большинстве крупных организаций, где обращается КЗИ, составляется такой Перечень, который является руководством для определения категории важности информации. Составление Перечня требует кропотливого труда многих специалистов. Это объясняется тем, что если какие-либо сведения будут упущены из виду, то принимаемые меры охраны окажутся неэффективными. С другой стороны, неоправданное ограничение доступа к информации может осложнить работу организации и привести к материальным издержкам.

При составлении Перечня следует руководствоваться определенными критериями подхода. Во-первых, необходимо выделить те направления деятельности организации, которые приносят прибыль, во-вторых, исходя из рыночной конъюнктуры сбыта аналогичных товаров, оценить уровень прибыльности по сравнению с другими предприятиями, в-третьих, определить рентабельность организации на перспективу с учетом производства конкретных товаров. Данные о превышении уровня получаемой прибыли по сравнению с выпускном аналогичных товаров на других предприятиях свидетельствуют о необходимости уточнения круга сведений, составляющих коммерческую тайну.

Методически процесс установления категорий сведений, составляющих КЗИ, можно условно разделить на несколько этапов.

Первый этап включает составление списка сведений, подлежащих рассмотрению. Анализ практики защиты коммерческой тайны на ряде предприятий позволяет выделить устойчивые элементы организации и управления предприятием, включающие сведения о производстве, управлении, планах, финансах, состоянии рынка, партнерах, переговорах, заключаемых и выполняемых договорах, ценах и научно-технических достижениях. Структура Перечня зависит от особенностей деятельности организации, стратегии развития, заключения контрактов, интереса конкурентов к КЗИ, установления факта утечки и изменения условий защиты КЗИ. Первоочередной характер носит выделение таких сведений, использование которых позволит организации быть конкурентоспособной и стабильно получать прибыль.

Второй этап состоит в оценке ущерба организации при разглашении (утечке) КЗИ. Важной является оценка наступления отрицательных последствий в виде ущерба в случаях открытого использования сведений, включенных в Перечень. В их числе могут быть:

- прекращение или снижение уровня деловых отношений с партнерами;
- срыв переговоров и выгодного контракта;
- невыполнение договорных обязательств;
- необходимость проведения маркетинговых исследований и разработки новой рыночной стратегии;
- отказ от ранее принятых решений, ставших неэффективными в результате утечки сведений;
- экономические санкции в отношении организации;

- возникновение сложных ситуаций в снабжении, производстве и сбыте продукции и другие.

Для определения ущерба в стоимостном выражении используют-ся показатели, применяемые в планово-экономическом и финансовом подразделении. Показателями ущерба могут быть:

- потери вследствие прекращения финансовых инвестиций;
- экономический эффект от внедрения предприятия-конкурентом результатов НИОКР и полученных при этом преимуществ;
- стоимость оборудования и технологий, незаконно использованных конкурентом в производстве аналогичных товаров, и другие.

Сложность расчетов предполагает проведение оценки ущерба экспертным путем.

Третий этап должен быть посвящен проверке сведений, включенных в Перечень, не являются ли они общедоступными и общедоступными на законных основаниях. Оценка сведений по данному критерию заключается в поиске и установлении законных источников информации. В частности, сведения статистического характера не могут составлять коммерческую тайну, сведения о деловых партнерах содержатся в справочной литературе, сведения научно-технического характера после их открытого опубликования не являются коммерческой тайной.

Четвертый этап посвящен проверке возможностей организации осуществлять меры по защите сведений, доступ к которым ограничен. Ограничение на доступ к информации связано с отрицательными последствиями для организации. Во-первых, это затраты на защиту информации, а во-вторых, потери других предприятий, связанные с неиспользованием информации, доступ к которой ограничен.

- Для обеспечения защиты выделенных сведений организацией:
- закрепляют функцию защиты коммерческой тайны за конкретными подразделениями и работниками;
  - проводят необходимые организационные, инженерно-технические и иные работы;
  - устанавливают режим охраны конфиденциальности технологий, материалов, порядок работы с документами, и другие меры.

При оценке затрат необходимо установить:

- категории и численность лиц, допускаемых к КЗИ;

- затраты на заработную плату, стоимость оборудования, технических средств и материалов, необходимых для организации охраны конфиденциальности КЗИ;
- затраты, связанные с оборудованием контрольно-пропускных пунктов, систем охраны и сигнализации, обеспечением безопасности связи;
- затраты на подготовку и переподготовку кадров в сфере информационной безопасности и другие.

Ограничение на доступ к КЗИ является вынужденной мерой. Поэтому сопоставление данных об отрицательных последствиях задерживания сведений с ущербом при их открытом использовании, анализ возможности финансирования организацией защитных мер позволит определить экономическую целесообразность отнесения сведений к коммерческой тайне.

*Пятый этап заключается в проверке того, что рассматриваемые сведения не могут составлять коммерческую тайну.* Законодательством предусмотрено, что сведения, содержащие государственную, служебную и иную тайну, учредительные документы, годовые отчеты, бухгалтерские балансы, документы, связанные с уплатой налогов, и иные не могут составлять коммерческую тайну.

*Шестой этап состоит в проверке того, что относимые к коммерческой тайне сведения не касаются негативной деятельности организации, способной причинить ущерб личности, обществу и государству.* Речь идет о сведениях, касающихся: загрязнения окружающей среды; нарушения законов; сокрытия информации, якобы подрывающей имидж организации; злоупотреблений в коммерческих интересах; уклонения от выполнения договорных обязательств либо уплаты налогов; недобросовестной конкуренции и другие.

Таким образом, категории сведений, включаемые в Перечень, должны удовлетворять следующим критериям: открытое использование выделенных сведений связано с ущербом для организации; сведения не являются общеизвестными или общедоступными на законных основаниях; организация имеет возможность осуществлять надлежащие меры по охране их конфиденциальности, руководствуясь соображениями экономической выгоды; выделенные сведения нуждаются в охране, так как не являются государственной тайной, не защищены авторским и патентным правом, к ним нет ограничений на отнесение их к коммерческой тайне; сокрытие этих сведений не может причинить ущерб личности, обществу и государству.

**Методика определения степени конфиденциальности сведений, содержащихся в работах, документах и изделиях.** Разработка и утверждение Перечня создает нормативную основу для руководства по определению степени конфиденциальности конкретных сведений, содержащихся в работах, документах и изделиях. Степень конфиденциальности конкретных сведений определяется непосредственно исполнителем работ на основании соответствующих категорий сведений, предусмотренных в Перечне, и лицом, которому направлен документ на утверждение. Следует подчеркнуть, что от того, насколько верно определена степень конфиденциальности сведений и присвоена категория важности с указанием грифа «Коммерческая тайна», зависит уровень установления режима охраны, порядок работы с документами и изделиями, их учет, хранение, обращение и уничтожение, а также защита в суде прав обладателя КЗИ.

В Законе о коммерческой тайне не упоминается обязанность исполнителя по определению конфиденциальности сведений с учетом их новизны и степени осведомленности конкурентов. Работники, кроме Перечня, в своей практической деятельности учитывают и иные факторы. В их числе:

- 1) наличие уязвимых мест в разработке изделия, знание которых потенциальным конкурентом может ослабить эффективность их использования и продажи;
- 2) тактико-технические характеристики изделия, обеспечивающие преимущества по сравнению с аналогичными изделиями конкурентов;
- 3) уникальные характеристики изделия, присущие только данному классу изделий;
- 4) состав элементов системы, обеспечивающий изделие высокие эксплуатационные характеристики и технические возможности;
- 5) уникальность проекта модернизации или создания нового класса изделий или необычность применения технологических процессов.

Перечень названных факторов не является исчерпывающим. Их наличие определяется спецификой деятельности организации и учитывается работниками при определении степени конфиденциальности КЗИ.

*Изучение опыта работы по определению степени конфиденциальности информации позволяет предложить введение системы разрядов, в зависимости от важности КЗИ.* Сведения, разглашение которых может оказать отрицательное воздействие на финансовое состояние

организации и даже поставить под угрозу сам факт ее существования, должны относиться к наивысшему разряду конфиденциальности КЗИ (третья категория ущерба). Иным сведениям, отнесенным к коммерческой тайне, устанавливается средний и низший разряды конфиденциальности (соответственно вторая и третья категории ущерба). Технически процедура установления разрядов, в зависимости от степени конфиденциальности, состоит в том, что рядом с грифом «Коммерческая тайна» проставляется соответствующий разряд (высший, средний, низший), который соответствует размеру возможного ущерба (третья, вторая и первая категории ущерба).

Установленный в Перечне разряд указывает на важность охраны сведений. Однако в Перечне сведений, составляющих коммерческую тайну, как правило, не выделяется КЗИ по степени ее конфиденциальности и не устанавливаются разряды в зависимости от возможного ущерба при ее разглашении. Более того, на практике до сих пор не выработано единого понимания категорий сведений, включаемых в Перечень.

Это приводит к неоднозначной оценке степени конфиденциальности одних и тех же сведений. В отдельных случаях отмечается снижение степени конфиденциальности защищаемых сведений или полное их расекречивание. Часто в силу действия «перестраховочного» фактора происходит завышение степени конфиденциальности КЗИ. Такая практика порождает ненужное отвлечение сил и средств на защиту менее важных сведений и увеличивает объем работ по обеспечению безопасности организации.

Изучение практики определения степени конфиденциальности сведений свидетельствует о несколько приниженной роли представителей организации-заказчика в этом процессе. Она сводится в основном к согласованию документов, включая и те, которые содержат коммерческую тайну. Например, действия заказчика ограничиваются выдачей подрядчику перечня охраняемых сведений, на основании которого исполнитель работ определяет степень их конфиденциальности. Однако сведения, указанные в Перечне, не всегда отражают перспективы развития науки и техники, особенности коммерческого оборота. Представители заказчика должны принимать непосредственное участие в определении степени конфиденциальности конкретных работ, и вносить изменения в техническое задание. Совместная работа подрядчика и заказчика по определению степени конфиденциальности КЗИ позволит, с одной стороны, учитывать изменения хозяйственной ситуации и вносить коррективы

в процесс обеспечения охраны параметров создаваемого изделия, с другой стороны, согласовывать коммерческие интересы по использованию (продаже) новых технологий.

В процессе засекречивания КЗИ важно не только правильно определить степень конфиденциальности сведений, содержащихся в новой работе, но и определиться с необходимостью применения дополнительных мер защиты.

Основным документом, которым обязан руководствоваться подрядчик, является техническое задание (ТЗ), разрабатываемое заказчиком. Руководствуясь нормами ФЗ «О техническом регулировании»<sup>1</sup>, ГОСТ Р52069.0-2003 «Защита информации. Система стандартов. Основные положения», ГОСТ Р50922-96 «Защита информации. Основные термины и определения», ГОСТ Р51275-99 «Защита информации. Объект информатизации. Факторы, воздействующие на информатизацию. Общие положения» и др., подрядчик может использовать любые правовые конструкции, определяющие требования по обеспечению секретности разработок, испытаний, производства и эксплуатации изделий и разработке перечня охраняемых характеристик (параметров) создаваемого конкретного изделия. Весьма полезным в этом плане является советский опыт обеспечения режима секретности, который может быть использован в работе коммерческих организаций. В частности, в разработке перечня охраняемых сведений принимал участие генеральный (главный) конструктор темы или его заместитель, руководитель РСО, начальники отдела режима и аналитического подразделения. Перечень согласовывался с заказчиком, представителем министерства и утверждался руководителями предприятий заказчика и подрядчика.

Сегодня в процессе разработки перечня специалисты используют ранее разработанные перечни по аналогичным темам и применяют опыт в сфере защиты КЗИ. При этом учитывается главный критерий — это новизна создаваемого изделия. Эти данные могут быть получены путем сравнительного анализа отечественных и зарубежных разработок, которые определяют облик вновь создаваемого изделия. Вместе с тем специалисты руководствуются не только Перечнем, но и используют личный опыт, методологии, учитывают важность сведений, возможный ущерб, который может быть причинен организации, новизну изделия, стоимость работы и др. критерии.

<sup>1</sup> См.: Собрание законодательства РФ. 2002. № 52. Ст. 5140.

Опрос работников организаций по вопросам улучшения порядка определения степени конфиденциальности КЗИ показывает, что решение этой проблемы видится им не только в конкретизации, расширении, сужении или отказе от Перечня или регулярности его просмотра, но и в **создании единой методики определения степени конфиденциальности КЗИ**. В этом плане *предлагается примерная система критериев и признаков, которые в совокупности составляют методику определения степени конфиденциальности сведений, содержащихся в работах, документах и изделиях*. Как представляется, структурно ее содержание состоит, во-первых, из учета **общего критерия**, это ущерб коммерческой организации при попадании сведений в конкурирующую организацию. **Во-вторых**, из учета **частных критериев**, которые включают характер сведений и их относимость к защищаемым сферам деятельности организации; важность сведений; возможность защиты сведений и материальные затраты на их защиту. Содержание частных критериев может быть охарактеризовано отдельными признаками.

*Характер сведений, составляющих КЗИ*, зависит от направленности деятельности организации. Методически нами учитывается информация, циркулирующая в сфере управления, производства (технические и технологические сведения) и коммерческой деятельности (деловые сведения). *Критерий важности сведений, составляющих КЗИ*, характеризуется актуальностью, новизной, объемом и степенью обобщенности сведений, эффективностью и др. *Критерий защиты сведений с использованием соответствующих материальных затрат* раскрывается при помощи изучения таких **признаков**, как: уязвимость КЗИ от конкурентной разведки, осведомленность и устремления конкурентов к защищаемой КЗИ, опасность разглашения (утечки) КЗИ со стороны работников, осведомленных в таких сведениях. Выделенные критерии и признаки составляют содержание примерного варианта методики, использование которой позволяет обобщенно подходить к процессу определения степени конфиденциальности КЗИ.

Рассмотрим характеристику отдельных выделенных критериев. *Общим критерием оценки является ущерб коммерческой организации при попадании сведений к конкуренту*. Размер ущерба зависит от масштабов деятельности организации (крупное, среднее и малое предприятия). Размер ущерба может быть выражен такими понятиями, как «стратегический» (организация на грани банкротства) или «тактический» (потеря управляемости и доходности одного из подразде-

лений) материальный вред. Показателем ущерба может быть его характер имущественной потери для организации вследствие разглашения (утечки) КЗИ. Например, распространение ложных сведений о деятельности организации, связанных с выпуском некачественных товаров, и т.п. Также учитывается размер убытков, превышающих, например, размер уставного капитала или балансовую стоимость имущества, и т.п.

Существенное значение имеет *учет вероятности и быстроты причинения конкурентом ущерба в случае получения им сведений, составляющих КЗИ*. Оценка этих показателей необходима организации для установления соответствующего уровня режима коммерческой тайны и реализации предупредительных мер. Эти меры могут быть связаны с изменением структуры управления и технологии изготовления изделия или отдельных его частей (узлов), выпуском более совершенных по своим техническим характеристикам товаров и другие. Представляется, что эти показатели могут быть определены в количественном и качественном отношении. Это позволит организации предметно оценивать возможный ущерб от попадания КЗИ к конкурентам. Если вероятность нанесения ущерба условно принять в интервале от 0 до 1, то повышение этого значения до 1 будет означать необходимость определения высшего разряда конфиденциальности КЗИ. *Вероятность (быстрота) причинения ущерба* может исчисляться при этом днями, месяцами, годами. Соответственно оценка *фактора быстроты* причинения ущерба зависит от возможности принятия организацией адекватных мер противодействия усилиям конкурентов с целью уменьшения размера ущерба.

*Характер сведений и их относимость к основным направлениям деятельности организации определяется такими показателями, как актуальность, новизна и эффективность использования КЗИ в рыночной экономике*. Можно с уверенностью сказать, что такие совокупные сведения, которые носят научно-технический, технологический и коммерческий характер, имеют значимость для организации. Показатель новизны работы организации в плане создания (модернизации) изделия определяется исходя из существующих аналогов в РФ и других странах. Если имеются аналогичные изделия или ведутся аналогичные работы, то новизна в данном случае отсутствует. Актуальность КЗИ оценивается с учетом возможного теоретического и практического использования полученных сведений. Следует учитывать показатель, характеризующий эффективность использования технической, технологической и деловой информации. Если отмеча-

ется высокая эффективность использования полученных сведений, например, при заключении коммерческой сделки или модернизации элементов конечного изделия, то следует отнести такие сведения к КЗИ. Важно различать класс сведений по степени их обобщенности и объему. Речь идет о сведениях, содержащихся в отдельном элементе (узле) изделия или о работе (изделии) в целом. В данном случае степень конфиденциальности будет различной.

*Осведомленность конкурентов и их устремления к получению технической, технологической и деловой КЗИ* должны оцениваться с позиций степени их осведомленности и с учетом вероятности такой осведомленности. Оценка этих показателей может быть получена путем изучения обстоятельств появления публикаций в СМИ, анализа выступлений участников на конференциях и симпозиумах, раскрывающих данные о тактико-технических характеристиках и конструктивных особенностях опытных образцов изделий, оригинальных методах управления, о ведущихся коммерческих переговорах по поводу инвестирования крупных проектов. Конкурирующей организацией могут быть получены сведения в результате утраты или хищения документов, изделий либо разглашения КЗИ путем попадания образцов изделий и технической документации (чертежи и др.) с использованием методов промышленного шпионажа. Специалистами изучается не только возможная осведомленность конкурентов, но и их устремления к конкретным защищаемым сведениям.

При оценке названных выше частных критериев (характер сведений, важность сведений и возможность защиты сведений) и их признаков необходимо учитывать этапы работ, выполняемые организацией. Полученные результаты исследования указывают на существующую зависимость степени конфиденциальности КЗИ от этапов работ. Если мы возьмем, например, начальный цикл работ, связанный с постановкой проблемы и ее теоретическим решением, что является характерным для НИОКР, то эта часть работы содержит наиболее ценную информацию, которая должна охраняться по высшему разряду. Такая же степень конфиденциальности сохраняется на этапах изготовления и испытаний опытного образца. Принятие заказчиком изделия и передача его в серийное производство несколько снижают степень конфиденциальности. Снятие изделия с производства, в зависимости от возможности использования научно-технических решений при модернизации и изготовлении новых образцов, требует решения вопроса об изменении степени конфиденциальности.

На основании выделенных нами критериев и признаков представляется возможным произвести оценку степени конфиденциальности технической, технологической и деловой информации, имеющей коммерческую значимость.

Оценка степени конфиденциальности информации, циркулирующей в организации, производится (Оску) путем суммирования значения  $i$ -критерия (признака) в баллах и коэффициента значимости  $i$ -го признака (может быть использована шкала качественной оценки, выраженная в виде разрядов «низкий» (категория «В»), «средний» (категория «Б») и «высший» (категория «А»), означающая степень конфиденциальности информации с грифом «Коммерческая тайна».

$$\text{Оску} = \sum_{i=1}^n 3Ni \cdot K_{3n},$$

где Оску — означает оценку степени конфиденциальности информации;  $3Ni$  — значение  $i$ -го признака (в баллах);  $K_{3n}$  — коэффициент значимости  $i$ -го признака (шкала качественной оценки, по разрядам (категориям) коммерчески значимой информации), причем Формула 2;  $n$  — число критериев (признаков).

**Во-первых, предлагаемая методика позволяет учитывать значение следующих критериев (признаков):**

*Первый критерий (3n1) — характер и относимость технической, технологической и деловой информации в зависимости от доступа работников к защищаемым сферам деятельности организации, имеет следующую балльную оценку (значения).*

Таблица 3.4.1

№ п/п	Признаки относимости (характера) информации к защищаемым сферам деятельности организации	Баллы
1	Управление: подготовка и принятие решений по производственным, коммерческим и иным вопросам; планы, совещания, финансы, безопасность и др.	10
2	Научно-исследовательские и опытно-конструкторские работы, разработка технологий и др.	8
3	Производство: структура, производственные мощности, запасы сырья, комплектующих и т.д., изготовление изделий, применение технологий и др.	6
4	Коммерческая деятельность: рыночная стратегия организации, изучение рынка, партнеры, переговоры, контракты (договоры), цены, торги и др.	5
5	Иные признаки	

**Второй критерий (Зн2)** — степень важности технической, технологической и деловой информации, имеет следующие значения.

Таблица 3.4.2

№ п/п	Признаки важности сведений	Баллы
1	Актуальность сведений	10
2	Новизна сведений	9
3	Обобщенность сведений	7
4	Эффективность технического, технологического и коммерческого решения, оригинальность методов управления	5
5	Иные признаки	

**Третий критерий (Зн3)** — степень возможности охраны и защиты сведений, составляющих КЗИ, имеет следующие значения.

Таблица 3.4.3

№ п/п	Признаки возможности защиты сведений, составляющих КЗИ	Баллы
1	Уязвимость КЗИ от конкурентной разведки	10
2	Осведомленность конкурентов в КЗИ	9
3	Устремления конкурентов с целью получения КЗИ	8
4	Опасность разглашения (утечки) КЗИ работниками организации	7
5	Иные признаки	

Из таблиц 3.4.1, 3.4.2 и 3.4.3 видно, в какой степени (в баллах) те или иные признаки, характеризующие критерии относимости (характера), важности и возможности защиты сведений, определяют их «весовую» значимость при принятии решения об отнесении информации к коммерческой тайне.

**Во-вторых, методика позволяет вычислить коэффициент значимости (Кзн)** перечисленных выше признаков. При этом следует учитывать, что

$$\sum_{i=1}^n \text{Кзн} = 1.$$

Таблица 3.4.4

**Коэффициент значимости критериев (признаков), определенных опытным путем**

№ п/п	Кзн	Кзн 1	Кзн 2	Кзн 3
	Предлагаемые значения	0,1	0,2	0,3

*В-третьих, суммируются значения каждого признака и коэффициент его значимости, и находится соответствующая сумма шкала качественной оценки степени конфиденциальности КЗИ (Оску).*

Таблица 3.4.5

**Оценка степени конфиденциальности КЗИ**

№ п/п	Степень конфиденциальности КЗИ Гриф (разряд, категория)	Примерные значения Оску
1	Открытая информация (доступ не ограничен)	Менее 5
2	Гриф «Коммерческая тайна», разряд низший, категория «В»	5÷7
3	Гриф «Коммерческая тайна», разряд «средний», категория «Б»	7÷9
4	Гриф «Коммерческая тайна», разряд «высший» категория «А»	9÷10

Определение коммерческой тайны в области НИОКР (оценка конфиденциальности) имеет ряд особенностей, которые необходимо учитывать в практической деятельности. К числу важнейших признаков следует отнести:

1) Определение конфиденциальности НИОКР, а также составных ее этапов и частей, на которые выдаются задания, осуществляются совместно заказчиком и исполнителем. Если в работе участвуют несколько организаций, то конфиденциальность определяется головной организацией-исполнителем.

2) Степень конфиденциальности определяется на стадии планирования НИОКР и уточняется по окончании работы (этапов, частей). Определение степени конфиденциальности работ осуществляется руководителем НИОКР (ответственным исполнителем, главным конструктором). Выполнение работ по определению степени конфиденциальности осуществляется с участием патентного, информационного, планово-экономического, финансового и других подразделений организации.



3) В соответствии с результатами определения степени конфиденциальности руководитель НИОКР по согласованию с представителем заказчика выделяет конкретные подлежащие охране сведения, составляющие коммерческую тайну. Без этих сведений невозможно воспроизвести результаты работ. К ним относятся ключевые идеи, аналитические и графические зависимости, отражающие найденные закономерности и взаимосвязи, данные об условиях экспериментов и оборудовании, на котором они проводились, точное значение конструктивных характеристик создаваемых изделий и оптимальных параметров разрабатываемых технологических процессов (размеры, объемы, конфигурация, процентное содержание компонентов, температура, давление, время и т.д.), сведения о материалах, из которых изготовлены отдельные детали, и др.

4) В публикациях, направленных на закрепление приоритета и поддержание престижа российской науки и техники, рекламы экспорта товаров и создание условий для выгодной продажи технологий, подлежащие охране сведения не указываются. До официальной регистрации изобретения любые сведения о нем должны сохраняться в тайне. После опубликования формулы и описания изобретения защищается лишь неопубликованная информация, составляющая предмет ноу-хау, охраняемого в режиме коммерческой тайны.

5) Результаты определения степени конфиденциальности НИОКР, в том числе конкретные сведения, выделенные для охраны, отражаются в самостоятельном разделе технического задания на работу. Охрана выделенных сведений по НИОКР осуществляется в соответствии с порядком, установленным в организации. Учитывая, что результаты НИОКР в виде технологии представляют собой товар организации-исполнителя, заказчик может не устанавливать степень конфиденциальности работы по экономическим соображениям. В этом случае в техническом задании должно быть обоснование о целесообразности охраны конфиденциальности сведений.

Перед началом серийного производства продукции, изготовляемой по результатам НИОКР, при снятии ее с производства и эксплутации, передаче (продаже) за границу продукции и (или) документации и при наступлении других обстоятельств, влияющих на степень конфиденциальности, заказчик совместно с разработчиком документации и изготовителем продукции пересматривает ранее установленную степень конфиденциальности НИОКР и обеспечивает внесение необходимых изменений в документацию. Решение об

изменении степени конфиденциальности выделенных сведений отражается в техническом задании на проведение работ.

Итак, использование организациями названных критериев и признаков оценки степени конфиденциальности сведений позволит обоснованно подходить к решению задач отнесения информации к коммерческой тайне. При этом могут быть использованы сводные результаты работы по определению степени конфиденциальности сведений, составляющих коммерческую тайну организации, которые включают: содержание сведений, представляющих коммерческую значимость для организации, возможный материальный вред (ущерб), затраты на защиту (финансовые, трудовые и иные ресурсы), а также другие, влияющие на сроки пересмотра и снятия грифа «Коммерческая тайна» (разряда, категории). Полученные данные определяют границы устанавливаемого режима коммерческой тайны и характер мероприятий, которые необходимо осуществить в целях обеспечения безопасности организации.

## § 5. Система мер по установлению режима коммерческой тайны

Меры по охране конфиденциальности информации составляют одно из обязательных условий достижения необходимого уровня защищенности коммерческой тайны. Их содержание и объем определяются организацией исходя из правомочия на собственные действия (неюрисдикционная форма защиты). Меры воздействия на нарушителя реализуются управомоченным лицом самостоятельно (самозащита гражданских прав)<sup>1</sup>. Речь идет об использовании организацией самостоятельных действий (сил и средств) по охране конфиденциальности информации без обращения к государственным и иным уполномоченным органам. Самозащита сводится к мерам правового, организационного, технического и иного характера, которые реализуются по усмотрению организации на основе корпоративных актов в соответствии с Законом о коммерческой тайне. В настоящей книге анализируются меры правового, организационного и иного характера.

<sup>1</sup> См.: Грибанов В. П. Осуществление и защита гражданских прав. 2-е изд. М., 2001. С. 104–132; Рожкова М.А. Средства и способы правовой защиты сторон коммерческого спора. М., 2006. С. 19–29, 235–249, 363–372, и др.

Меры по охране конфиденциальности информации нельзя смешивать со способами защиты гражданских прав на коммерческую тайну, осуществляемых в юрисдикционной форме в судебном или административном порядке. Используя различные способы гражданских прав, перечень которых указан в ст. 12 ГК РФ, организация имеет правомочие требования определенного поведения от обязанных лиц, нарушивших ее право на коммерческую тайну, путем обращения в компетентные государственные органы.

Закон о коммерческой тайне не раскрывает понятие «мера по охране конфиденциальности информации», а лишь перечисляет меры, которые, по мнению законодателя, образуют *режим коммерческой тайны* (п. 1 ст. 10 Закона). Большинство авторов, труды которых посвящены исследованию проблем коммерческой тайны, как правило, широко используют это понятие, но при этом лишь перечисляют различные меры, не раскрывая их сущности<sup>1</sup>. В русском языке слово «мера» определяется как «средство для осуществления чего-нибудь, мероприятия» и «предел, в котором осуществляется, проявляется что-нибудь». Понятия «мера» и «мероприятие», используемые в сфере обеспечения безопасности организации, различны по своему содержанию. На практике эти понятия часто смешиваются. Понятие «*мероприятие*», используемое в книге, означает организованное действие или совокупность действий, имеющих целью решение отдельных, частных задач по установлению и обеспечению режима коммерческой тайны.

Понятие «*мера*» применительно к режиму коммерческой тайны означает способ воздействия на участников процесса обращения КЗИ путем определения границ (пределов) дозволительного и разрешительного порядка ее использования и охраны конфиденциальности в гражданском обороте и характеризуется:

адекватными активными действиями администрации на возникающие угрозы безопасности организации с использованием различных правовых, организационных, технических и иных средств по установлению режима коммерческой тайны;

реализацией мероприятий по обеспечению соблюдения режима конфиденциальности информации, направленных на выявление каналов возможной утечки КЗИ, установлению причин и обстоя-

тельств, способствующих совершению правонарушений и их предупреждению в сфере обращения такой информации.

Такой подход позволяет выделить специфику мер по установлению режима коммерческой тайны и его обеспечению в процессе обращения КЗИ, и отличить их от иных мер хозяйственной деятельности организации.

Порядок, обеспечивающий режим коммерческой тайны, устанавливается во всех организациях, в которых ведется разработка и использование продукции, выполняются НИОКР и оказываются услуги, содержащая КЗИ. В организациях, с учетом особенностей и масштабов их деятельности, разработаны и осуществляются различные мероприятия по установлению и обеспечению режима коммерческой тайны. Анализ функционирования систем охраны конфиденциальности информации ряда организаций показывает, что, несмотря на разнообразие и различную степень использования правовых средств, их объединяют цель и принципы работы, связанные с достижением частных интересов. Элементы системы охраны конфиденциальности КЗИ составляют основное содержание понятия установления и обеспечения режима коммерческой тайны.

*Сущность установления режима коммерческой тайны* состоит в разработке и реализации правовых, организационных, технических и иных мер, направленных на поддержание порядка при производстве товаров (работ, услуг) в сфере обращения КЗИ с целью сохранения в тайне конфиденциальной информации. Установленный порядок обращения со сведениями, составляющими КЗИ, должен обеспечивать надежную охрану таких сведений и исключать либо затруднять их утечку к конкурентам. Эти условия формируются в результате разработки и осуществления различных по своему характеру и назначению мер.

Традиционно выделяются три группы мер правового, организационного и технического характера, которые используются при установлении режима коммерческой тайны. Их характеристика достаточно подробно раскрывается в литературе. Отдельные авторы рассматривают меры технического характера несколько шире, включая в них инженерно-технические, программно-аппаратные и криптографические элементы. Такой подход не вызывает возражений. В свою очередь, меры правового и организационного характера можно дробить по отдельным отраслям и институтам права, а также направлениям хозяйственной деятельности организации.

<sup>1</sup> См.: Панкратов Ф.Г., Сергина Т.К. Коммерческая деятельность: Учебник. М., 1996. С. 55–61; Степанов Е.А., Корнеев И.К. Информационная безопасность и защита информации. М., 2001. С. 41–47, и др.

При установлении режима коммерческой тайны определяющее значение имеют *правовые меры*, которые проявляются в нормотворческой деятельности организаций по разработке и принятию корпоративных актов, регулирующих процессы обращения КЗИ в гражданском обороте и устанавливающих порядок в этой сфере; закрепляющих полномочия лиц по охране конфиденциальности информации, определяющие возможность использования правовых и иных средств в сфере обеспечения безопасности.

Роль *организационных мер* состоит в том, что они направлены на создание таких форм, которые с максимальной эффективностью способствовали бы реализации задачи по предотвращению разглашения (утечки) КЗИ. Речь идет об определении организационной структуры, которая будет осуществлять функцию обеспечения безопасности организации, о координации этой работы с дочерними обществами, филиалами и др. обособленными подразделениями, о формах взаимодействия с правоохранительными органами и иными государственными и негосударственными структурами, об установлении эффективного контроля за сохранением коммерческих секретов и соблюдением требований по обеспечению режима коммерческой тайны, и др. В пределах правовой регламентации обеспечения режима коммерческой тайны значительное место занимают вопросы организации непосредственной работы с конфиденциальными документами и изделиями, обеспечения режимными мерами защиты КЗИ при осуществлении коммерческих переговоров, служебных совещаний, конференций и др. мероприятий, а также реализация мер ответственности за нарушение режимных требований, разглашение (утечку) коммерческой тайны.

К организационным мерам тесно примыкают *воспитательные меры*. Они обращены к лицам, имеющим доступ к КЗИ. Роль этих мер определяется тем фактом, что указанные лица, являясь осведомленными в коммерческой тайне, представляют наиболее вероятный канал разглашения (утечки) КЗИ, в случаях несоблюдения ими установленных правил режима. Поэтому приоритетной в данном направлении мерой должна быть хорошо организованная индивидуально-воспитательная работа в сочетании с проведением общих воспитательных мер, которые хотя и выходят за рамки обеспечения безопасности, однако способствуют укреплению трудовой и договорной дисциплины.

Существенное значение имеют *технические меры*. Они служат материальным обеспечением реализации названных выше мер и

включают технические устройства (комплексы, системы), выполняющие функции защиты. Речь идет об использовании технических средств охранной сигнализации, оповещения и связи, телевидения (видеонаблюдения), обнаружения подслушивающих и передающих устройств, с помощью которых ведется техническая разведка, и др. Оборудование технических средствами охраны мест проведения работ, связанных с исследованием, разработкой, изготовлением и испытанием опытных образцов, хранением конфиденциальных документов, позволяет решать задачи по своевременному обнаружению угроз и их предупреждению. Самостоятельное значение в рамках этой группы мер имеют программные и криптографические средства защиты. К *программным средствам защиты* относятся специальные программы, которые включаются в состав программного обеспечения ЭВМ и используются для решения задач защиты информации, обрабатываемой в компьютерах и хранящейся в рабочих станциях локальных сетей и информационной системе организации. *Криптографические средства защиты* представляют собой специфический способ защиты информации и имеют многовековую историю развития и применения. Разработаны различные методы шифрования, созданы теоретические и практические основы их применения. Они могут применяться для защиты информации, обрабатываемой в ЭВМ и локальных сетях, а также для закрытия информации, передаваемой по незащищенным линиям телеграфной, телетайпной, факсимильной и электронной связи.

Структура, состав и содержание мер, направленных на установление режима коммерческой тайны, обусловлены объемом охраняемой КЗИ и уровнем противодействия реальным и потенциальным угрозам, а также наличием материальных и иных ресурсов, используемых для обеспечения безопасности. Эти обстоятельства определяют выбор мер и их комплексное применение в рамках единой системы обеспечения безопасности организации.

При всем многообразии мер, используемых для установления и обеспечения режима коммерческой тайны, имеется определенная специфика, связанная с их применением, что позволяет выделить в структуре хозяйственной деятельности «режимные меры». Под термином *«режимные меры»* понимается порядок, устанавливаемый организацией с помощью правовых и иных средств, обеспечивающий сохранность КЗИ при производстве и реализации товаров (работ, услуг).

Разработка и пределы осуществления режимных мер определяются нормами Закона о коммерческой тайне и иных правовых актов, корпоративных актов, их назначением и целевой направленностью, степенью конфиденциальности информации, обусловленных особенностями производственной, научно-технической, коммерческой и иной деятельности организаций. Содержание режимных мер в значительной степени зависит от устремления конкурентов, методов их разведывательной деятельности и иных факторов, определяющих оперативную обстановку внутри организации. В зависимости от действия названных факторов режимные меры могут охватывать деятельность одного или нескольких направлений организации или ограничиваться обеспечением охраны конфиденциальности информации, например, при выполнении НИОКР.

Сложившаяся в организациях система мер, устанавливающая и обеспечивающая режим конфиденциальности КЗИ, получила в теории и на практике название «система режимных мер». В любой организации, где обращается КЗИ, действует своя система режимных мер. Она состоит из двух основных групп мер, *устанавливающих режим коммерческой тайны до начала производства и реализации товаров, выполнения работ и оказания услуг, и мер, обеспечивающих режим коммерческой тайны в процессе обращения такой информации в гражданском обороте.*

В основу классификации положен принцип учета разделения деятельности в области конфиденциальности информации, определяющий необходимость первоначального установления режима коммерческой тайны в организации, где обращается КЗИ, а затем режимного обеспечения работ с использованием правовых и иных средств. Поэтому первая группа режимных мер, по сути, образует режим конфиденциальности КЗИ, определяемый в Законе о коммерческой тайне (в ред. ФЗ от 18 декабря 2006 г. № 231-ФЗ) как *коммерческая тайна*, со всеми составляющими его элементами, о которых в общих чертах говорится ст. 10 названного Закона. Эффективность режимных мер этой группы определяется условиями, широко используемыми на практике и закрепленными в Законе. Речь идет о признании мер разумно достаточными в том случае, если исключается доступ к информации любых лиц без согласия обладателя и обеспечивается возможность ее использования работниками и контрагентами без нарушения режима конфиденциальности КЗИ. Установленный режим, с одной стороны, должен гарантировать сохранность коммерческих секретов, а с другой — может ограничивать права работников и вза-

имоотношения с партнерами по поводу передачи им КЗИ. Поэтому при выборе режимных мер следует учитывать возможные отрицательные последствия их применения с учетом задач, стоящих перед организацией.

По своему содержанию эта группа режимных мер включает *мероприятия подготовительного характера*, направленные на реальное обеспечение защиты КЗИ. К их числу следует отнести: изучение особенностей обстановки организации в целях выявления угроз ее безопасности, определение перечня сведений, составляющих КЗИ, закрепление в корпоративных актах требований к лицам, допускаемым к коммерческим секретам, а также порядка установления, изменения и снятия грифа «Коммерческая тайна», определение порядка учета, хранения и обращения конфиденциальных документов и изданий, содержащих такие сведения, разработку мер организационно-технического характера по противодействию разведывательной деятельности конкурирующих фирм (легендирование, маскировка и защита объекта и работ), осуществление мероприятий, связанных с защитой КЗИ в рамках трудовых и гражданско-правовых отношений.

*Вторая группа режимных мер включает мероприятия по выявлению угроз и возможных каналов утечки КЗИ, установлению причин и обстоятельств, способствующих совершению правонарушений в сфере обращения такой информации, осуществлению контроля за выполнением требований режима конфиденциальности КЗИ.* Содержанием мер данной группы являются *мероприятия обеспечения легального характера*, которые включают: 1) методики по выявлению правонарушений при обращении КЗИ путем контроля за состоянием режима конфиденциальности на всех стадиях научной, производственной и коммерческой деятельности; по проведению воспитательно-профилактической работы в трудовых коллективах с учетом трудовой и договорной дисциплины; моделирования ВКУ КЗИ на основе результатов аналитических и маркетинговых исследований; 2) принятие мер по предупреждению нарушений режима конфиденциальности в процессе производства товаров (работ, услуг); 3) пресечение незаконных действий лиц в при обращении КЗИ путем передачи материалов о выявленных нарушениях в следственные и административные органы, а также направления исков в суд о возмещении убытков и др.

В соответствии с принятой структурой изложения первая группа мер анализируется в настоящей главе, а вторая — в 4 и 5 главах.

*Установление режима коммерческой тайны* требует создания определенного механизма реализации режимных мер, включающего определенное сочетание принципов защиты, организационной структуры и основных направлений деятельности при обращении КЗИ с учетом специфики конкретной организации. Эта работа осуществляется на основе таких *принципов*, как, в частности: комплексный подход к решению задач охраны коммерческой тайны; координация действий внутренних подразделений и контрагентов; ресурсное обеспечение режима коммерческой тайны; систематический контроль за эффективностью установленных мер; ответственность работников за нарушения сохранности КЗИ. Названные принципы тесно взаимосвязаны и пронизывают всю систему мер по установлению режима коммерческой тайны организации.

Подчеркивая важность мер установления режима коммерческой тайны организации, связанных с созданием соответствующей *организационной структуры*, типа службы безопасности, нужно отметить, что в начале 90-х годов в России эти службы создавались по примеру зарубежных фирм. Затем их деятельность была урегулирована Законом РФ «О частной детективной и охранной деятельности в Российской Федерации» от 11 марта 1992 г. Тем не менее процесс упорядочения деятельности СБ, определения их структуры, призванной обеспечивать интересы организации в условиях коммерческого риска и конкурентной борьбы по реализации товаров, пока еще не завершен<sup>1</sup>. Нужно сказать, что именно перед СБ ставятся конкретные задачи по установлению режима коммерческой тайны, которые не должны противоречить ст. 3 Закона о частной детективной и охранной деятельности в РФ. Речь идет о подготовке и реализации мер, связанных с обеспечением физической сохранности носителей информации, содержащих коммерческую тайну; предотвращением утечки КЗИ в процессе деятельности организации; доведением до работников сведений, которые им необходимы для выполнения обязанностей, с учетом действия системы доступа к конфиденциальным документам; получением информации о конкурентах, в части принимаемых ими действий по недобросовестной конкуренции, и разработкой мер по их нейтрализации.

Анализ практики показывает, что при установлении режима коммерческой тайны *отмечается определенная закономерность в раз-*

*работке и реализации системы примерно одинаковых мер*, к числу характерных можно отнести: предварительное изучение различных направлений деятельности организации с целью выявления реальных и потенциальных угроз и разработка мер по их предупреждению или нейтрализации; разработка перечня сведений, составляющих коммерческую тайну, и его последующая корректировка; определение порядка контроля за правильностью установления грифа «Коммерческая тайна» документам, изделиям и работам, а также за соблюдением работниками и контрагентами установленных ограничений при обращении КЗИ; установление порядка доступа в помещения, где ведутся работы с использованием КЗИ и хранятся носители с грифом «Коммерческая тайна»; проектирование разрешительной системы доступа работников и контрагентов к КЗИ и определение порядка ее функционирования; определение порядка ведения конфиденциального делопроизводства, обращения документов и изделий, содержащих коммерческую тайну, организация их учета, хранения и уничтожения. Характер и содержание мер по установлению режима коммерческой тайны определяют необходимость предоставления по усмотрению администрации соответствующего объема правомочий службе безопасности и производственным подразделениям.

При подготовке и реализации мер по установлению режима коммерческой тайны исходным должно быть положение о том, что *главным действующим лицом в процессе обращения КЗИ является работник*. В отношении него, на основании норм законодательства и корпоративных актов, устанавливается ряд ограничений и запретов. Причем речь идет не только о своих работниках, но и — организации-контрагента, которые непосредственно связаны с использованием и охраной такой информации. Определенная часть ценной информации не отражается в документах и остается в памяти работника, что может быть использовано в конкурентных целях. Привлечение работника к закрытым работам, например, участие в коммерческих переговорах и заключение договоров, обязывает руководителя передать ему для выполнения поручения необходимую информацию, составляющую коммерческую тайну. В этой связи следует учитывать проблемы, связанные с проверкой лиц при найме на работу, которые будут допущены к КЗИ; предупреждением текучести кадров, осведомленных в коммерческой тайне. Решение этих вопросов связано с формированием допускной системы и осуществлением профилактической работы, использованием различных правовых средств и стимулирования. Действия администрации, составляющие

<sup>1</sup> См.: Экономическая безопасность России: Общий курс: Учебник / Под ред. В.К. Сенчагова. 2-е изд. М., 2005. С. 739.

содержание разнообразных мер, в центре которых находится работник, должны осуществляться в рамках действующего законодательства на основании порядка, установленного в организации. При таком подходе имеется возможность создания эффективно работающего механизма защиты коммерческой тайны.

Важное место в деятельности по установлению режима коммерческой тайны и его обеспечению должно уделяться *планированию* этой работы, которая включает определение целей и способов их достижения, приспособление имеющихся ресурсов к изменениям внешних и внутренних условий хозяйствования. Планы по обеспечению охраны коммерческой тайны утверждаются руководителем организации. Различают годовые и квартальные планы. Мероприятия по обеспечению безопасности, с учетом их характера и направленности, систематизируются в отдельных разделах плана. Структурно, как показывает анализ материалов ряда организаций, *план включает чаще всего разделы, раскрывающие содержание мероприятий, связанных с организационно-методической, контрольно-проверочной и воспитательно-профилактической работой*. Отдельно, как правило, выделяется *работа с кадрами*, занятиями в сфере обращения КЗИ, что подтверждает практическую значимость этой меры.

*Вводная часть плана*, как правило, содержит данные анализа и оценки хозяйственной ситуации, влияющей на определение задач по установлению режима коммерческой тайны и его обеспечению. Эти сведения являются исходной базой для определения содержания разделов плана. *Организационно-методическая деятельность* включает в себя разработку проектов корпоративных актов, инструкций, методик, а также предложений о внесении в них изменений и дополнений с учетом изменившихся условий хозяйствования; внедрение новых методов защиты КЗИ и др. мероприятий.

*Контрольно-проверочная работа* состоит в организации контроля за выполнением требований корпоративных норм; проверке соблюдения режима при проведении коммерческих переговоров, обращении с носителями коммерческой тайны и др. В разделе *воспитательно-профилактических мероприятий* планируются действия администрации, направленные на формирование мотивации правомерного поведения работников, побуждающих к соблюдению режима коммерческой тайны. Раздел *работы с кадрами* включает мероприятия по обучению работников приемам защиты КЗИ.

Содержание планируемых мероприятий включает программу действий работников-исполнителей, возможность использования

ими правовых и иных средств, сроки исполнения и прогнозируемый результат. С планом мероприятий должны быть ознакомлены руководители подразделений и работники в части, касающейся выполнения обязанностей, что является основанием для применения мер юридического воздействия.

Изучение практики работы коммерческих организаций показывает, что **основными направлениями деятельности по установлению режима коммерческой тайны** являются: определение порядка допуска лиц к коммерческой тайне; закрепление условий по охране конфиденциальности информации в трудовых и гражданско-правовых договорах; разработка перечня сведений, составляющих коммерческую тайну, иных корпоративных актов, определяющих требования по сохранению КЗИ, и ознакомление с ними работников и контрагентов в части, их касающейся; физическая охрана носителей, содержащих такие сведения; организация конфиденциального делопроизводства; защита конфиденциальной информации при ведении служебных сообщений и коммерческих переговоров; закрепление функции контроля за соблюдением требований по охране коммерческой тайны в должностных инструкциях и положениях о подразделениях. Особое место в этой системе мер занимает «разрешительная система» доступа работников к КЗИ. Учитывая тот факт, что многие из названных направлений уже рассматривались, проанализируем отдельные из них, которые непосредственно связаны с обращением материальных носителей, содержащих КЗИ.

**Физическая охрана материальных носителей, содержащих КЗИ.** Решение этой задачи предполагает введение пропускного и внутриобъектового режима, который установлен в большинстве организаций. Содержанием *пропускного режима* являются правила, регламентирующие порядок входа (выхода) лиц, въезда (выезда) транспортных средств на территорию организации, вноса (выноса) документов и изделий. Пропускной режим предназначен для того, чтобы исключить проникновение посторонних лиц на территорию организации (режимные помещения); внос (вывоз) на территорию организации (режимные помещения) и вынос (вывоз) с территории организации документов и изделий без разрешения; хищение документов и изделий. Для решения этих задач в организации могут быть созданы бюро пропусков, контрольно-пропускные пункты и посты, реализующие пропускные функции на входах (выходах) в режимные помещения и здания. Организацией вводится система постоянных, временных и разовых пропусков, а также материальных пропусков;

применяются специальные шифры и вкладыши к пропускам, дающие право прохода (проезда) на определенные режимные территории и помещения; устанавливается охрана режимных территорий, зданий, помещений, хранилищ документов и изделий.

Охрана помещений, где хранятся носители, содержащие КЗИ, решается в комплексе общих охранных мер, предпринимаемых организацией по сохранности своего имущества. Виды охраны зданий, помещений достаточно подробно описаны в литературе. Охрана может осуществляться с помощью технических средств с подключением на пульт централизованного наблюдения либо с установкой автономной сигнализации, что позволяет обнаружить возникновение пожара в помещении, проникновение постороннего лица; путем выставления постов введомственной охраной либо своими силами. В последнем случае организация на свой страх и риск решает задачи по охране имущества<sup>1</sup>. При наличии финансовых средств лучшим вариантом будет заключение договора на охранное обслуживание с делом введомственной охраны МВД. Предварительно согласовываются вопросы, связанные с подготовкой здания и помещений для передачи под охрану, оборудованием технических и иных средств охраны. К договору прилагается акт о состоянии принимаемых под охрану объектов, средств охраны и пожаротушения, в котором может быть указана дополнительная потребность в этих средствах, а также сроки их внедрения.

Установление *внутриобъектового режима* в организации происходит, прежде всего, в ограничениях, которые вводятся с целью предупреждения разглашения (утечки) КЗИ. Внутриобъектовый режим включает установление порядка подбора, изучения и оформления лиц для работы в подразделениях, где ведутся конфиденциальные работы; ограничение круга лиц, допускаемых к работам, документам и изделиям; определение лиц, имеющих право разрешать ознакомление исполнителей с той или иной категорией документов и сведений; проведение воспитательно-профилактической работы с исполнителями по разъяснению требований режима коммерческой тайны, установление порядка передвижения и производства работ на территории организации в целях исключения проявления демаскирующих признаков разработки новой продукции; установление порядка пользования конфиденциальными документами и изделиями,

<sup>1</sup> См.: ФЭЗ от 14 мая 1999 г. № 77-ФЗ «О ведомственной охране» // СЗ РФ. 1999. № 16. Ст. 1935.

а также процедуры их транспортировки; введение контроля за применением технических средств, используемых для передачи, приема, обработки и копирования КЗИ.

Определенные особенности имеет установление режима при **ведении делопроизводства с конфиденциальными документами, содержащими коммерческую тайну**<sup>1</sup>. Технологии защиты, обработки и хранения бумажных, машиночитаемых и электронных документов, применительно к системе секретного делопроизводства, давно применяются на практике. Их содержание раскрывается в литературе. Многие элементы этой системы используются и в конфиденциальном делопроизводстве. Это обстоятельство должно учитываться при установлении режима коммерческой тайны на участках документооборота, выполняющего функцию информационного обеспечения деятельности организации. Целями установления режима документооборота, как объекта защиты КЗИ, является: исключение несанкционированного доступа посторонних лиц к документам; разглашения КЗИ; утраты, подмены или хищения документов либо случайно или умышленного их уничтожения.

Решение задач по сохранности коммерческой тайны требует установления единого порядка работы с документами, содержащими такие сведения, обязательного для выполнения всеми работниками, получившими к ним доступ; определения ограничений на доступ работников к документам и их ответственности; нанесения отличительной отметки (грифа) на чистый машинный носитель или документ, содержащий КЗИ; формирования изолированных потоков конфиденциальных документов; использования автономной системы их обработки и хранения; создания подразделения конфиденциальной документации.

Установленный порядок должен соблюдаться на всех этапах обращения (учет, хранение, копирование, передача, уничтожение) документов, содержащих коммерческую тайну. Такие документы, в зависимости от их важности, могут иметь дополнительные пометки, указывающие на их разряд (низший, средний, высший) конфиденциальности. После регистрации документы передаются на рассмотрение руководителю организации, а затем, в соответствии с разрядной системой, с ними знакомятся руководители подразделений и исполнители. В организации должен быть установлен порядок

<sup>1</sup> См.: Степанов Е.А., Корнеев И.К. Указ. соч. С. 107–177, и др.

работы с документами на рабочих местах. При направлении документов контрагентам следует соблюдать меры предосторожности, исключающие их утрату. Поскольку у коммерческих структур отсутствует возможность использования услуг фельдъегерской связи, доставка осуществляется силами самой организации либо путем заключения договора с фирмой, оказывающей такие услуги.

Важным направлением, требующим установление режима коммерческой тайны, является **проведение служебных совещаний и коммерческих переговоров с использованием КЗИ**. Практикой выработаны определенные процедуры подготовки, проведения и документирования совещаний, которые не всегда регламентированы в корпоративных актах и иных документах. В большинстве случаев порядок проведения таких мероприятий поддерживается в силу обычая, в соответствии с которым принято соблюдать определенные требования, обеспечивающие конфиденциальность информации. Совещания и переговоры, в процессе которых участникам может быть передана КЗИ, проводятся, как правило, с разрешения руководителя, в специально отведенных для этих целей помещениях. Участники должны иметь доступ к КЗИ на основании трудового или гражданско-правового договора. Для проведения совещания предвзительно составляется список его участников, который визируется службой безопасности и утверждается руководителем организации. Участники допускаются на совещание по спискам или пропускам при предъявлении документов, удостоверяющих их личность. Важную роль в соблюдении работниками требований режима играет организатор совещания. По его инициативе может быть разработан план мероприятий по обеспечению режима, которым предусмотрен порядок допуска участников к КЗИ, демонстрации иллюстрированных материалов с использованием технических средств воспроизведения информации, пользования аппаратурой звукозаписи и мобильными телефонами, копирования, тиражирования и направления материалов совещания его участникам.

Служба безопасности осуществляет проверку и обследование помещений, в которых будут проводиться совещания с целью исключения возможности установки и несанкционированного подключения технических средств разведки. Принимаются меры, затрудняющие визуальное наблюдение и фотографирование объектов с помощью оптическоеlectronных средств, а также прослушивание ведущихся разговоров с использованием акустической аппаратуры разведки.

При проведении *коммерческих переговоров* следует соблюдать определенные меры предосторожности. Факты проведения переговоров и условия заключения договоров должны являться коммерческой тайной. Конкуренты, располагая такой информацией, могут предложить более выгодные условия партнерам, с которыми у них налажены доверительные отношения. В ходе подготовки к переговорам определяется ограниченный круг лиц, имеющих отношение к этой работе и знающих условия переговоров по коммерческой сделке. На стадии предварительных переговоров, когда контракт еще не заключен, используется лишь открытая информация, содержащая, как правило, сведения рекламного характера. В последующем перечень сведений по предмету переговоров может быть расширен, но при условии перспективы сотрудничества. Такие сведения могут быть предоставлены в том случае, если с партнером по переговорам будет подписан договор о неразглашении сведений, составляющих коммерческую тайну. В организации должны быть созданы условия для хранения договоров как документов, содержащих коммерческую тайну высшей степени конфиденциальности. Доступ к ним должен быть ограничен узким кругом лиц, определяемым руководителем организации.

**Разработка системы доступа лиц к информации, составляющей коммерческую тайну организации**, получившей в 80-е гг. название «разрешительной системы» применительно к обеспечению охраны государственной тайны, является и сегодня важнейшей частью мер по установлению режима коммерческой тайны в коммерческой организации. Актуальность использования разрешительной системы доступа к информации объясняется значением информационной составляющей любого хозяйственного процесса, сопровождающейся разработкой новых документов, макетов, опытных образцов и т.д., содержащих КЗИ, неправомочный доступ к которой может причинить ущерб организации. Функционирование разрешительной системы позволяет решить задачи, связанные с обеспечением производственной деятельности путем предоставления работникам необходимого объема конфиденциальных сведений, и исключения доступа посторонних лиц.

В литературе под *доступом лиц к коммерческой тайне* понимается *совокупность норм и правил, устанавливаемых руководством организации с целью правомерного ознакомления и использования работниками конфиденциальных сведений, необходимых им для выполнения трудовых обязанностей*. При этом должны быть соблюдены условия, выпол-



нение которых свидетельствует о правомерном доступе лица к КЗИ, а именно: подписание работником обязательства о неразглашении сведений, составляющих коммерческую тайну, наличие допуска к таким сведениям и работам; разрешение руководителя подразделения на ознакомление с конкретными документами и работами.

Практикой выработаны определенные процедуры правовой регламентации доступа лиц к сведениям, документам и базам данных. Речь идет об оптимальном распределении информации различного характера между исполнителями соответствующих работ. Процедура доступа работника к КЗИ состоит в издании приказа о назначении на должность, письменном обосновании руководителем подразделения необходимости доступа работника к такой информации и согласование этого вопроса со службой безопасности; принятии решения о доступе работника к КЗИ.

*Определенные особенности присущи порядку доступа к сведениям (акционером), членом ревизионной комиссии общества к сведениям, составляющим КЗИ. Он определен ГК РФ, законодательством о хозяйственных обществах и товариществах, уставом и иными корпоративными актами. Учредители (акционеры) имеют право знакомиться с любой информацией, содержащейся в отчетных документах общества за определенный период. С согласия руководителя НИОКР в отчеты, представляемые по запросу учредителя (акционера), могут включаться сведения научно-технического и производственного характера, содержащие КЗИ. Эти сведения и документы представляются учредителям (акционерам) с согласия руководителя организации. Члены ревизионной комиссии в пределах своих полномочий, определенных уставом, могут быть ознакомлены с любой информацией, необходимой им для выполнения своих обязанностей. Допуск членом ревизионной комиссии к работам, документам и изделиям, содержащим конфиденциальные сведения, осуществляется на основании предписания, подписанного председателем совета директоров общества и согласованного с руководителем организации, о возможности ознакомления определенных лиц со сведениями, составляющими КЗИ. В предписании указываются состав ревизионной комиссии, цель и объект проверки.*

Руководство организации, включая генерального директора, коммерческого директора, главного инженера, руководителя службы безопасности и их заместителей, имеют право доступа к любой информации, необходимой им для выполнения служебных обязанностей. Руководители среднего и низшего звена управления имеют до-

ступ к конфиденциальным сведениям, которые необходимы им для решения задач, стоящих перед подразделением.

*Доступ других работников к КЗИ осуществляется в объеме, необходимом для выполнения ими своих прямых обязанностей. Работники производственных и научно-технических подразделений допускаются к КЗИ по решению руководителя подразделения, согласованному с начальником участка, мастером и руководителем НИОКР. Необходимость доступа определяется руководителем соответствующего подразделения сведениями бухгалтерии, финансово-экономического отдела, юридической и коммерческой служб и др.)*

Оформление документов на доступ лиц к коммерческой тайне осуществляется в соответствии с положением о разрешительной системе. На малых предприятиях с ограниченным объемом работ руководитель имеет возможность лично распределять КЗИ между работниками, независимо от занимаемых ими должностей. В крупных организациях такое распределение становится достаточно трудоемким. Поэтому первый руководитель часть своих прав делегирует руководителям нижестоящих уровней, оставляя за собой право распоряжения наиболее ценными сведениями, составляющими коммерческую тайну. На практике используются различные варианты разрешений, оформляющих право на доступ к конфиденциальной информации. Широкое распространение имеет такой традиционный вид разрешения, как резолюция руководителя на самом документе. Такое разрешение содержит перечень фамилий работников, обязанных ознакомиться с документами или их исполнить, срок исполнения, другие указания, подпись руководителя и дату. Право работников на доступ к КЗИ может содержаться в распорядительных документах организации. В документах персонально указаны работники, которым предоставлено право доступа в силу занимаемой должности и выполнения обязанностей. При значительных объемах технической документации используются пофамильные списки лиц, имеющих право доступа к такой информации (с указанием отдела, фамилии и должности исполнителя, категории документа).

Система доступа исполнителей к конфиденциальным документам и изделиям должна быть предельно простой и без излишних ограничений. Любые непродуманные ограничительные меры снижают ее эффективность, увеличивают затраты рабочего времени исполнителей, связанные с оформлением разрешений на право доступа к необходимой информации. Разрешительная система доступа лиц к

КЗИ должна адекватно реагировать на изменения в хозяйственной ситуации при проведении конфиденциальных работ.

Названные факторы должны учитываться при разработке *полосения о разрешительной системе доступа лиц к КЗИ в организации* (далее — Положение). Положение является специальным корпоративным актом, регулирующим доступ работников к КЗИ. Разработка такого Положения поручается, как правило, комиссии, назначаемой приказом руководителя организации. Членами комиссии являются работники основных производственных подразделений и службы безопасности (СБ), хорошо знающие тематику и специфику деятельности организации, требования, предъявляемые к обеспечению режима коммерческой тайны. Разработка Положения требует предварительного проведения *аналитической работы* с целью выявления информационных потоков КЗИ, используемой в научной, производственной и коммерческой деятельности; определения объема охраняемой информации и возможности ее использования работниками организации и контрагентами. Изучаются структура и направления деятельности организации, подчиненность и взаимодействие структурных звеньев, их связь с контрагентами. Анализируются различные этапы выполнения НИОКР и участки, где могут быть сосредоточены коммерческие секреты. Выясняется необходимость доступа к КЗИ представителей обслуживающих подразделений организации (например, пожарной охраны, медсанчасти, административно-хозяйственных служб и др.). По результатам обследования выделяются уязвимые участки, где обрабатывается КЗИ, на которых устанавливается более строгий порядок доступа к документам и изделиям, а также составляется перечень «режимных помещений» с учетом характера проводимых в них работ и степени их конфиденциальности.

Подготовительный этап работы завершается составлением проекта Положения, который обсуждается комиссией и утверждается руководителем организации либо общим собранием учредителей (акционеров). Положение включает правила доступа работников к КЗИ, имеющей различную степень конфиденциальности; государственных органов и органов местного самоуправления, командированных лиц и др. вопросы.

С Положением должны быть ознакомлены работники в части, их касающейся. Мероприятия по внедрению Положения предусматривают, во-первых, изучение документа с руководящим составом и исполнителями, прием зачетов по знанию ими режимных требований. Во-вторых, знание работниками информационных потоков на своем

участке работы. В-третьих, проведение работы по заполнению разрешительных документов, представлению классификационных рядов (категорий) грифа «Коммерческая тайна» на материальных носителях. В-четвертых, определяется состав работников, осуществляющих контроль за выполнением требований разрешительной системы.

В структуре управления организацией важное место занимает *деятельность руководителей среднего звена*, которым предоставляются полномочия, связанные с определением доступа работников к КЗИ. В этой связи к ним предъявляются такие требования, как, в частности: знание уязвимых участков производства, где сосредоточены коммерческие секреты и степень их конфиденциальности, обязанности подчиненных им работников, использующих в работе КЗИ; предупреждение неправомερных действий работников, нарушающих конфиденциальность КЗИ; сообщение в СБ сведений об изменении характера работ и обязанностей работников, а также об имевших место нарушениях, связанных с соблюдением режима коммерческой тайны.

Результаты проведенного исследования позволили выделить ряд направлений по *совершенствованию работы, связанной с установлением режима коммерческой тайны. Во-первых*, это оценка экономических факторов (угроз) в сфере обращения КЗИ, влияющих на изменение структуры организации, штатной численности работников. *Во-вторых*, появление новой технической и технологической информации в результате выполнения НИОКР, обработка на ЭВМ, не исключающая ее утечки. *В-третьих*, изменение системы внутрифирменного планирования и отчетности, порядка расчетов и транспортировки продукции, способов передачи по договору КЗИ; повышение (понижение) степени конфиденциальности работ. *В-четвертых*, проблемы, связанные с приемом командированных лиц, в том числе представителей иностранных фирм с использованием КЗИ. Выезд работников, осведомленных в КЗИ, за границу, участие в международных конференциях. *В-пятых*, увеличение или сокращение числа организаций-контрагентов, изменение объема и характера выдаваемых им конфиденциальных материалов. *В-шестых*, анализ опубликованных работ, содержащих КЗИ, для оценки осведомленности конкурентов. *В-седьмых*, изменение условий деятельности, связанных с возникновением или упряднением технологических операций движения продукции, содержащей КЗИ, объема и характера документации с грифом «Коммерческая тайна». *В-восьмых*,

изменение перечня сведений, составляющих коммерческую тайну; пропускного и внутриобъектового режима в связи с повышением (понижением) степени конфиденциальности работ. *В-девятых*, анализ практики введения новых форм доступа, например, разработчика классификатора, позволяющего учитывать различные категории конфиденциальности КЗИ.

Приоритетным, на наш взгляд, должно быть изучение практики взаимоотношений с контрагентами по вопросам конфиденциальности и анализ происходящих в этой связи изменений в оперативной обстановке, оказывающих влияние на стабильность «разрешительной системы», с которой тесно связаны другие режимные меры.

Итак, первоначально установленный в организации режим коммерческой тайны требует постоянного правового обеспечения деятельности по его поддержанию с целью охраны конфиденциальности информации в процессе ее обращения с применением научных методов и методик.

## ГЛАВА 4

# Правовое обеспечение деятельности по охране конфиденциальности информации

## § 1. Характеристика нарушений режима конфиденциальности информации и каналов ее возможной утечки

*Понятие характеристики нарушений режима коммерческой тайны относится к числу важнейших элементов понятийного аппарата механизма правового регулирования обращения коммерчески значимой информации и охраны ее конфиденциальности.* Ее назначение состоит в раскрытии определенной системы признаков, использование которых необходимо для решения задач выявления и предупреждения правонарушений, совершаемых в сфере обращения КЗИ.

Введение понятия «правовое обеспечение деятельности по охране конфиденциальности информации» в цивилистической науке берет свое начало с концепции правового режима ноу-хау, сформулированной И.А. Зениным, а затем получившей дальнейшее развитие в работах В.В. Погуляева, З.Ф. Гайнуллиной, М.С. Зельцер и др. Это понятие можно рассматривать в широком и узком смысле слова применительно к целям настоящего исследования. В широком смысле «под правовым обеспечением имущественных интересов по поводу ноу-хау следует понимать **комплекс правовых средств**, способствующих ограждению имущественной сферы обладателя ноу-хау от тре-

тых лиц, включая контрагента по договору о передаче ноу-хау»<sup>1</sup> и работника, с которым заключен трудовой договор. В узком смысле слова «так называемая защита ноу-хау сводится к обеспечению на основе норм гражданского, трудового и даже уголовного права имущественных интересов обладателя ноу-хау... В законодательстве предусматривается имущественная и иная ответственность: за незаконные действия по приобретению промышленной и коммерческой информации; за нарушение работниками правил внутренней трудового распорядка, устанавливающих ответственность рабочих и служащих за разглашение сведений, способных составить тайну нанимателя»<sup>2</sup>. Такой подход к защите частных интересов организации требует, по нашему мнению, исследования нарушений установленного режима коммерческой тайны и их связи с возможными каналами утечки (ВКУ) КЗИ, причин и обстоятельств, им способствующих, и мер по их предупреждению. Первоочередной задачей является определение понятия характеристики нарушений режима коммерческой тайны (далее — нарушения режима КЗИ), что позволит осмыслить суть правового обеспечения деятельности по охране конфиденциальности информации в коммерческих организациях.

*Выявление отличительных признаков, характеризующих процесс совершения нарушений режима КЗИ, и установление их связи с ВКУ информации представляет собой сложную теоретическую задачу.* Ее решение видится, во-первых, в раскрытии признаков понятия характеристики нарушений режима КЗИ. Во-вторых, в классификации ВКУ КЗИ и установлении их связи с нарушениями режима КЗИ. Несмотря на важность данного понятия, оно практически не нашло широкого применения в исследовательской практике, до сих пор нет четкости в определении его содержания. Ряд авторов<sup>3</sup> включают в понятие характеристики нарушений режима КЗИ примерно одинаковый круг признаков, характеризующих состояние режима коммерческой тайны на объекте (оперативную обстановку, структуру и динамику правонарушений, их причины, каналы утечки КЗИ, меры

<sup>1</sup> Зелин И. А. Гражданское и торговое право капиталистических стран. М., 1992. С. 157.

<sup>2</sup> Там же.

<sup>3</sup> См.: Гордов О. А. Комментарий к ФЗ «Об информации, информатизации и защите информации». СПб.: Питер, 2003. С. 167–168; Фатьянов А. А. Правовое обеспечение безопасности информации в Российской Федерации. М., 2001. С. 199–207, и др.

предупреждения). Подход к определению совокупности признаков, их показателей при рассмотрении различных аспектов характеристики нарушений режима КЗИ в рамках конкретных исследований, как правило, во многом зависит от субъективного усмотрения исследователя и поэтому отличается известной произвольностью их выделения. Но в любом случае критерием неправомерного поведения является анализ действия запрещающих, обязывающих и управомочивающих норм, неисполнение или ненадлежащее исполнение или выход за границы которых (дозволения) и свидетельствует о правонарушении.

Это происходит потому, что, как отмечает В. Н. Кудрявцев, теория правонарушений развита в юридической науке недостаточно, нет даже дисциплины, которая изучала бы совокупность этих явлений. Если применительно к анализу преступности такая дисциплина существует — это криминология, то весь массив правонарушений не изучается какой-либо единой отраслью науки или учебной дисциплиной<sup>1</sup>. Это в полной мере относится и к цивилистической науке, предметом исследования которой с недавних пор является информация как новый объект гражданско-правового регулирования. Отсутствие методологического аппарата, пригодного для изучения особенностей нарушений режима КЗИ, заставляет обратиться за помощью к другим наукам. «Цивилистика, — как подчеркивает Е. А. Суханов, — тесно взаимодействует с рядом отраслевых правовых наук, в том числе изучающих публично-правовую сферу... Цивилистическая проблематика в определенных случаях не может быть удовлетворительно разрешена без обращения к выводам и данным названных наук»<sup>2</sup>. Поэтому при раскрытии характеристики нарушений режима КЗИ в основном были использованы теоретические знания и методология криминологической науки.

Произвольность подхода к интерпретации понятия характеристики нарушений режима КЗИ не может не повлечь серьезных отрицательных последствий (несопоставимости результатов отдельных исследований, невозможности их использования как материала при подготовке обобщающих документов и т. п.). Поэтому предпринята попытка восполнить имеющийся пробел в теоретическом обоснова-

<sup>1</sup> См.: Социальные отклонения. 2-е изд. М.: Юрид. лит., 1989. С. 6–19, 93–108, 244–256.

<sup>2</sup> См.: Гражданское право: Учебник. Т. 1 / Под ред. проф. Е. А. Суханова. М., 2000. С. 52.

нии содержания характеристики нарушений режима КЗИ. Наш поиск мы начали с того, что попытались наметить тот круг признаков, который, по нашему мнению, достаточен для выявления основных свойств изучаемых нарушений.

Практика показывает, что ощущается настоятельная необходимость выяснения принципиальных основных позиций относительно взглядов на характеристику нарушений режима КЗИ. Это, во-первых, решение вопроса о том, каков круг признаков, которые охватываются понятием характеристики нарушений режима КЗИ, во-вторых, достижение договоренности об унификации показателей, которые используются для раскрытия содержания того или иного признака.

Учитывая направленность раскрытия основных проблем настоящего исследования, основное внимание уделено рассмотрению первой группы вопросов и освещению на их основе содержания характеристики нарушений режима КЗИ.

При определении совокупности признаков, отражающих различные аспекты характеристики нарушений режима КЗИ, в качестве исходных были использованы теоретические положения, сформулированные В.Б. Ястребовым<sup>1</sup>. Смысл этих положений заключается в выделении в качестве элементов криминологической характеристики преступлений трех групп признаков, представляющих: 1) пространственно-временные параметры преступных проявлений; 2) особенности, имеющие значение для понимания их детерминант; 3) особенности, имеющие значение для организации предупредительной деятельности.

Будучи в целом приемлемыми, названные положения применительно к рассматриваемым целям настоящего исследования нуждаются в уточнении, что объясняется особенностями предупреждения правонарушений в сфере обращения КЗИ, их связью с производственной, научной, коммерческой и иной деятельностью, выявления и раскрытия ВКУ КЗИ, накопления и анализа данных об устремлениях и осведомленности конкурентов, ведущих промышленный шпионаж. Как представляется, при раскрытии характеристики нарушений режима КЗИ должны быть отражены свойства рассматриваемых правонарушений. Они определяются принадлежностью данных де-

<sup>1</sup> См.: Ястребов В.Б. К вопросу о понятии криминологической характеристики преступлений // Сб.: Вопросы борьбы с преступностью. Вып. 37. М., Юрид. лит., 1982. С. 14–20.

ятий при наличии состава преступления, предусмотренного нормами УК РФ, к преступным нарушениям или к дисциплинарным проступкам, значительной ситуационной обусловленностью совершения нарушений режима КЗИ при исполнении гражданско-правовых обязательств и трудовых обязанностей, зависимостью решения задач предупреждения правонарушений при обращении КЗИ от мероприятий по правовому регулированию рыночной экономики, доминирующим развитием частной собственности и предпринимательства. Исходя из названных соображений, характеристику нарушений режима КЗИ можно определить как совокупность признаков:

1) Раскрывающих распространенность, структуру нарушений режима КЗИ в организациях, в которой наряду с традиционными структурными элементами представлено распределение нарушений и особенности их проявления на каналах возможной утечки информации. Эта группа признаков представляет информационную базу для оценки степени актуальности борьбы с нарушениями режима КЗИ и учета их связи с ВКУ информации в организациях, определены основных направлений этой деятельности и достижения наиболее оптимального использования сил и средств профилактического воздействия.

2) Характеризующих сферы профессиональной деятельности исполнителей конфиденциальных документов, изделий и работ, в которых наблюдаются проявления нарушений в сфере обращения КЗИ; показывающих внутреннюю и внешнюю среду, в рамках которой могут быть совершены нарушения режима КЗИ, что имеет значение для реализации практических действий по предупреждению нарушений в этой сфере.

3) Отражающих личностные особенности лиц, допускающих нарушения режима КЗИ, которые базируются на наличии неразрывной связи между деянием и его исполнителем. Такой подход позволяет знать и учитывать при решении задач борьбы с нарушениями режима КЗИ особенности проявления этих нарушений, обусловленные личностными качествами тех, кто совершает такого рода нарушения, и учитывать их в профилактической деятельности.

4) Имеющих значение для понимания причин нарушений режима КЗИ и осуществления предупредительной деятельности; отражающих социальные явления и процессы, обуславливающие нарушения режима КЗИ, единство объективных и субъективных элементов в характеристике нарушения режима КЗИ, показывающих

необходимость учета такого рода данных в предупредительной деятельности.

Названные группы признаков находятся между собой в тесной взаимосвязи и взаимно дополняют друг друга. Их выделение преследует цель — связать работу по анализу различных аспектов характеристики нарушений режима КЗИ с решением задач осуществления целенаправленной борьбы с данным явлением в организации. В книге раскрываются признаки правонарушений в сфере обращения КЗИ, за совершение которых в соответствии с законодательством предусмотрены различные виды ответственности, однако юридическая оценка деяний и механизм привлечения лиц к ответственности за совершение правонарушений не рассматриваются, поскольку являются задачей отдельного исследования.

**Структура и распространённость нарушений КЗИ в организациях.** Анализ дисциплинарной практики в организациях промышленности, транспорта, связи и торговли за пятилетний период показывает, что были допущены такие нарушения режима КЗИ, которые выразились в фактическом невыполнении или ненадлежащем выполнении обязанностей, закрепленных в корпоративных актах, трудовом договоре, а также связанных с исполнением гражданско-правовых обязательств. Выборочные данные изучения личных дел работников, допустивших нарушения режима КЗИ, материалов служебных расследований фактов нарушения трудовой и договорной дисциплины показывают, что наибольшее число работников были подвергнуты дисциплинарным взысканиям за совершение следующих нарушений:

— за утрату удостоверений, пропусков, ключей от режимных помещений, хранилищ, сейфов (металлических шкафов), личных печатей — 12%;

— за пронос без разрешения работников службы безопасности (СБ) на территорию организации видео- и фотосъемочной, звукозаписывающей и множительно-копировальной аппаратуры личного пользования; за недонесение о фактах утечки конфиденциальных сведений руководству подразделения и СБ; за вынос документов и изданий, содержащих коммерческую тайну, без разрешения администрации — 4%;

— за неправильное определение грифа «Коммерческая тайна» документа; за оставление открытыми и не опечатанными после окончания работы помещений (хранилищ) — по 3% случаев;

— в 2% случаев работники были наказаны за оставление грифованных документов на рабочих столах при выходе из помещения, за нарушение установленного порядка ознакомления прикомандированных лиц с такими документами и изделиями, за перевозку таких документов и изделий без санкции руководства обществственным транспортом и перемещение с ними в места, не связанные с выполнением заданий;

— по 1% случаев — за неправильное оформление грифованных документов и передачу их контрагентам; за несвоевременное сообщение в кадровую службу об изменениях автобиографических данных; за ведение переговоров с использованием КЗИ по незащищенным линиям связи; за снятие копий с грифованных документов без разрешения начальника СБ; за передачу и взятие без расписки документов и изделий, содержащих коммерческую тайну.

**Борьба с названными нарушениями, совершение которых характерно для многих организаций, не полностью обеспечивает закрытие или нейтрализацию действия ВКУ КЗИ.** Результаты проведенного исследования подтверждают вывод о том, что администрация и СБ оперируют существенно суженным представлением о разновидностях проявления нарушений режима КЗИ, ведущих к образованию ВКУ КЗИ.

Сложился определенный стереотип, при котором реагирование администрации связывается лишь с нарушениями внутриобъектового и пропускного режима, а другие нарушения режима КЗИ, которые прямо ведут (или могут привести) к утечке информации, не выявляются, меры предупреждения по таким нарушениям проводятся недостаточно. К числу таких нарушений следует отнести: ознакомление лиц с конфиденциальными документами, изделиями и работами, не входящими в круг их служебных обязанностей; направление адресатам конфиденциальных документов, к которым они не имеют отношения; подготовка конфиденциальных документов, записей, зарисовок, расчетов на неучтенных листах бумаги, личных блокнотах; нарушение порядка работы с конфиденциальными документами и изделиями, связанного с обзором их посторонними лицами; посещение без служебной необходимости конкурирующих отечественных и иностранных компаний и фирм; использование конфиденциальных сведений в открытой служебной переписке, технических заданиях, статьях, докладах и выступлениях; преждевременная публикация результатов научных исследований, выполнявшихся в порядке служебного задания, которые могут быть оформлены как изобретения или открытия, и другие. Как показывают данные выборочного исследо-

вания, перечисленные выше нарушения в организациях не устанавливались и лица за их совершение не привлекались к ответственности. Нарушения режима КЗИ в зависимости от характера и частоты их совершения в сферах профессиональной деятельности работников — исполнителей конфиденциальных работ образуют определенные объективные возможности для образования различных каналов утечки информации и обуславливают их существование.

**Классификация возможных каналов утечки информации** может быть проведена в зависимости от проявления характерных, часто повторяемых, нарушений, совершаемых работниками организаций, контрагентами и иными лицами при обращении КЗИ.

Для раскрытия особенностей образования ВКУ КЗИ необходимо рассмотреть формы их проявления на основе такой классификации, которая с наибольшей полнотой отражала бы специфику факторов, определяющих характер поведения лиц, допускающих нарушения режима КЗИ. Представляется продуктивным в этом отношении подход, в соответствии с которым любая организация может быть представлена как сложная организационно-техническая и информационная система. Системное представление о коммерческой организации в информационной среде позволяет рассматривать ее во взаимодействии с другими субъектами (организации-контрагенты, государственные органы и органы местного самоуправления и др.), связанными с созданием, преобразованием и потреблением КЗИ при внешних возмущающих воздействиях в информационной инфраструктуре и с учетом внутренней оперативной обстановки.

Учет взаимодействия факторов внешней и внутренней среды позволяет выделить и сгруппировать ВКУ КЗИ, изучить особенности процесса их образования и функционирования сквозь призму нарушений режима КЗИ. Функционирование ВКУ КЗИ происходит в силу неконтролируемого распространения защищаемой информации в результате ее разглашения, несанкционированного доступа к КЗИ и получения конкурентной разведкой в рамках информационно-ных потоков с учетом сложившихся внутренних и внешних связей организации

Рассмотрим особенности проявления типичных, характерных для многих хозяйствующих субъектов, нарушений режима КЗИ на ВКУ информации, их распространенность на уязвимых участках деятельности организации, где чаще всего совершаются такие нарушения.

**Первая группа ВКУ КЗИ включает каналы оперативной связи, существующие в организации.**

Наряду с использованием новейших информационных технологий, каждая организация имеет традиционные телефонные сети общего пользования (по данным С.В. Сафронова, на эти линии приходится более 60% объема услуг коммуникационного рынка страны)<sup>1</sup>. Кроме того, организация использует различные технологические системы сети электросвязи, обеспечивающие один или несколько видов передач: телеграфную, факсимильную, передачу данных и других видов документальных сообщений, включая обмен информацией между ЭВМ, телевизионное, звуковое и иные виды радиопроводного вещания. Конечные технические устройства коммуникации устанавливаются в режимных подразделениях (помещениях), где циркулирует КЗИ. Линии связи имеют выход за охраняемый периметр организации и подвержены технической возможности несанкционированного снятия КЗИ. Нужно отметить общемировую тенденцию, когда конкурирующие фирмы, ведущие промышленный шпионаж, широко используют технические средства для перехвата охраняемой информации, передаваемой по незащищенным каналам связи, используя для этих целей радио- и радиотехническую аппаратуру, установленную, например, на автомобилях и других средствах, а также портативные радиоэлектронные средства, переносимые их агентами. Это позволяет осуществлять несанкционированное прослушивание линий связи, связывающих организацию с деловым внешним миром. Для обработки полученной информации конкурентами используются современные ЭВМ, методы системного анализа, математической логики и искусственного интеллекта. С помощью технических средств вводная информация преобразуется в качественно новую выводную информацию. Из сопоставления множества разрозненных сведений аналитическим путем конкурирующим фирмам удается раскрыть охраняемую информацию.

В условиях кооперации и специализации производства любая организация имеет множество деловых связей, соединяющих ее с контрагентами. Ежегодно растет число служебных междугородных и международных телефонных переговоров (СМТП). С введением мобильной телефонной связи их число увеличивается в геометрической прогрессии. Опрос работников организаций показал, что 47% из них

<sup>1</sup> См.: Сафронов С.В. Вопросы информационной поддержки предпринимательства в ФЦП «Электронная Россия» // В сб.: Информационное обеспечение предпринимательства. М., 2001. С. 36.



считают ведение СМТП без соблюдения правил режима конфиденциальности крайне опасным ВКУ КЗИ. В организациях установлен порядок ведения СМТП. В частности, еще с советских времен существует практика определения телефонов, разрешенных для ведения СМТП. Ведутся списки лиц, допущенных к ведению переговоров. Работотаны и периодически пересматриваются корпоративные акты, регулирующие ведение СМТП. Уточняются перечни несекретных технических терминов и других косвенных признаков, раскрывающих охраняемую в организации информацию. Ежегодно уточняются списки лиц, допущенных к ведению СМТП.

Контроль за соблюдением требований режима конфиденциальности при ведении СМТП возлагается на руководителей подразделений. Ежемесячно сверяются лицевые счета, поступающие из городской телефонной станции на оплату, с перечнем телефонов, с которых разрешено ведение СМТП. В случаях, когда телефонный разговор велся с неразрешенного аппарата, проводится служебное расследование с целью установления лиц, нарушивших установленный порядок. Используются различные технические устройства, ограничивающие выход на междугородную линию связи при наборе определенной цифры. Отдельные организации используют аппаратуру внутреннего контроля за ведением СМТП, позволяющую автоматически проинвестить отключение телефонного аппарата при упоминании сведений, составляющих коммерческую тайну.

Фиксация результатов контроля СМТП осуществляется работниками СБ с использованием технических средств и ЭВМ. В основу используемых методик контроля положен системный подход к оценке информативности сведений, передаваемых по телефону. Выбор периодов контроля и их длительность обуславливаются особенностями оперативной обстановки, сложившейся в организации, и периодами интенсивного обмена информацией с другими предприятиями. Это, как правило, начало и окончание НИР и ОКР, проведение испытаний опытного образца изделия, коммерческая деятельность, связанная с заключением договоров. Важным звеном этой работы является оценка информативности сведений и отнесение их к КЗИ. Суммарный контроль, составляющий примерно 15—20% от общего числа СМТП за год, является оптимальным для оценки действительной информативности сведений, передаваемых по телефонной линии связи.

Нарушения режима КЗИ при ведении СМТП проявляются в том, что при употреблении определенных слов и терминов могут быть

определены: принадлежность перехваченной информации к важным работам (например, сведения, раскрывающие демаскирующие признаки предприятия, технические и технологические характеристики новых изделий, и др.); характер и направление работ, принцип действия разрабатываемых систем (при этом называются технические термины, общепринятые устройства, системы). Анализ этих сведений и привязка их к направлениям деятельности организации и ее контрагентов дает возможность конкурентам получить данные о ведущихся работах, сведения о которых составляют коммерческую тайну.

**Вторая группа ВКУ КЗИ связана с перепишкой по служебным вопросам, которая ведется в организациях с использованием открытого и конфиденциального делопроизводства.** При ведении открытой и конфиденциальной переписки существуют различные каналы возможной утечки КЗИ. Выборочный опрос исполнителей конфиденциальных работ показал, что наиболее характерными каналами утечки КЗИ могут быть следующие: публикация материалов, содержащих КЗИ в открытой печати, оглашение ее в передачах по радио и на телевидении — 15%; отнесение информации к КЗИ и включение ее в открытые документы — 11%; переписка с другими организациями и ведение междугородных телефонных переговоров — 9%; подготовка и защита диссертационных материалов — 7%; осуществление государственной регистрации НИОКР — 6%; ведение конфиденциального делопроизводства — 6%; внедрение изобретений, открытий и результатов НИОКР — 4% и другие.

**Публикация материалов в открытой печати, оглашение в передачах по радио и на телевидении.** Любая публикация требует, с одной стороны, включение в нее максимума полезных данных, а с другой — ограничение информации с учетом коммерческих интересов. В последнем случае могут допускаться нарушения, поэтому необходим *авторский самоконтроль и заключение экспертной комиссии* организации о возможности публикации материалов. Авторский самоконтроль предполагает знание автором документов, в которых изложены режимные ограничения. Так, опрос работников ряда организаций показал, что 25% от числа опрошенных не ознакомились с перечнями сведений, составляющих коммерческую тайну, 46% — ознакомились в общих чертах, и только 29% — ознакомились в части, их касающейся. Такое положение дел, когда работники слабо представляют, какие сведения составляют КЗИ, может привести к раскрытию в открытых публикациях сведений конфиденциального характера.

При определении конфиденциальности сведений, содержащихся в работах, документах и изделиях, опрошенные работники заявили, что в 41% случаев они руководствуются возможным ущербом, который может быть причинен организации при попадании сведений к конкурентам, в 31% случаев — личным опытом, в 15% случаев — перечнем сведений, составляющих коммерческую тайну, в 14% случаев — новизной изделия (работы), в 2% — вредом, который может наступить вследствие излишнего отнесения информации к коммерческой тайне. Как видно, критерии, которыми руководствуются работники при определении степени конфиденциальности сведений, сформулированы недостаточно четко и в корпоративных актах, как правило, не закреплены, что отрицательно сказывается на защите КЗИ и может привести к ее утечке.

Анализ работы *экспертных комиссий* по рассмотрению ими материалов для открытого опубликования показывает, что имеется ряд недостатков, связанных с проведением экспертизы, которые могут привести к утечке сведений конфиденциального характера. Экспертиза материалов иногда поручается самому автору, который одновременно является членом экспертной комиссии, либо некомпетентному работнику, плохо знающему специфику организации и требования конфиденциальности КЗИ. Имеются нарушения процедурного характера при рассмотрении материалов и оформлении акта экспертизы.

Опрос исполнителей, выполняющих конфиденциальные работы, показывает, что **нарушение установленных правил государственной регистрации НИОКР** может стать одной из причин утечки КЗИ. Государственная регистрация и учет НИОКР осуществляется в соответствии с требованиями законов, ГОСТов и стандартов организаций, которые являются обязательными для руководителей и ответственных исполнителей НИОКР. Работники отделов научно-технической информации организаций отвечают за своевременное представление регистрационных, информационных карт (РК, ИК) и отчетной научно-технической документации (ОНТД) в федеральные государственные органы. Нарушения режима КЗИ могут проявляться, во-первых, в подготовке и оформлении РК и ИК на НИОКР, содержащих КЗИ, лицами, не допущенными к этой работе; во-вторых, в неправильном оформлении РК, ИК и ОНТД вследствие незнания исполнителями нормативно-технических документов или недобросовестного отношения к данной работе; в-третьих, во внесении исполнителями конфиденциальных сведений в аннотации, рефераты и

другие графы РК и ИК на открытые части работ, выделяемых из НИОКР с грифом «Коммерческая тайна».

**Ведение конфиденциального делопроизводства** с нарушением требований, установленных в организации, может стать одним из каналов утечки КЗИ. Нарушения режима КЗИ выражаются в невыполнении или ненадлежащем выполнении работниками этих подразделений обязанностей по созданию, учету, хранению и обращению грифованных документов. Изучение приемов и способов охраны документов, применяемых в конфиденциальном делопроизводстве, позволяет выделить ряд упущений, допускаемых работниками в этой деятельности. К числу основных, чаще всего повторяющихся, недостатков относятся: отсутствие должного контроля со стороны руководства за созданием, оформлением, учетом и хранением документов; нерегулярное проведение проверок наличия документов на рабочих местах исполнителей и в местах их хранения; несвоевременное составление номенклатуры дел и неправильное оформление первичных документов; нарушение порядка размножения и копирования документов; неправильное ведение информационно-справочной работы; нарушение требований, предъявляемых к порядку уничтожения грифованных документов.

**Третья группа ВКУ КЗИ включает нарушения, которые возникают в процессе хозяйственной деятельности организации.** Условно эту группу можно обозначить как «**материальные потоки**» объекта, обеспечивающие оборот готовых изделий, комплектующих деталей и иных материальных ценностей от изготовителя к потребителю, что связано с передачей, в том числе изделий и документов, содержащих конфиденциальные сведения, для доставки которых используются различные виды транспорта и связи. Опрос работников ряда организаций показывает, что 3% из числа опрошенных считают нарушения, допускаемые при транспортировке грузов и почты, возможными каналами утечки КЗИ. Обязанностью администрации является сопровождение и охрана изделий, содержащих КЗИ, при их транспортировке за пределами территории организации. Закон о коммерческой тайне не регулирует порядок охраны изделий и документов, в период их транспортировки. Поэтому организации руководствуются общими нормами ГК РФ, регулирующими перевозку и хранение с учетом особенностей охраны КЗИ в период транспортировки изделий и документов, которые согласовываются сторонами в договоре. Реализация мер, связанных с транспортировкой изделий и документов, осуществляется в соответствии с принятым в организациях порядком

ком. Как показывают данные опроса, работники, обеспечивающие движение материальных ценностей и документов, содержащих КЗИ, только в 52% случаев были ознакомлены с этим порядком. Это ведет к нарушениям, которые проявляются в доставке работниками документов на личном транспорте, без сопровождения охраны, в несогласовании со СБ маршрутов движения транспорта, на котором осуществляется доставка материальных ценностей.

**Четвертая группа ВКУ КЗИ — это технические каналы, обслуживающие возможность утечки такой информации.** Различают пассивные и активные способы несанкционированного доступа (НСД) к КЗИ, которые обуславливают структуру (визуально-оптические, акустические, электромагнитные и др.) и особенности образования каналов утечки информации через технические средства информационных систем организаций. К числу распространенных активных способов НСД относятся незаконное подключение к линиям связи, установка в технические средства микрофонов и телефонных радиозакладок, НСД к информации, обрабатываемой на ЭВМ, ее копирование, модификация, хищение, визуальное наблюдение экранов.

Наибольшую опасность представляют каналы, возникающие вследствие использования конкурентами портиваемых технических средств, которые могут устанавливаться в служебных помещениях или вблизи расположения объектов организации. Такие средства позволяют комплексно решать задачу НСД к КЗИ. Это достигается, во-первых, путем фиксации на магнитный или иной носитель разговоров по каналам телефонной связи; во-вторых, путем визуального наблюдения и фотографирования из соседних зданий передвигания контролируемых грузов, а также документов, содержащих КЗИ, с которыми работают исполнители в рабочих комнатах. Судя по опубликованным в печати данным, можно судить о достаточно высоких тактико-технических характеристиках таких средств, используемых конкурентной разведкой<sup>1</sup>. Они обладают высокой чувствительностью и разрешающей способностью, обеспечивают ведение конкурентной разведки на значительных расстояниях от разведываемых объектов. Важно отметить и возможность скрытого использования порти-

<sup>1</sup> См.: Сб. материалов 2-й Всероссийской конференции «Информационная безопасность России в условиях глобального информационного общества» / Под ред. А.В. Жукова. М., 2001. С. 148–216, и др.

ных средств разведки, которые могут камуфлироваться под различные предметы повседневного обихода. В частности, могут быть замаскированы в автомашинах, в одежде и на переносимых человеком предметах. Утечка информации по техническим каналам чаще всего происходит в силу действия субъективного фактора, а именно: невыполнения или ненадлежащего выполнения работниками требований организационно-технического характера по обеспечению режима КЗИ.

**Пятая группа ВКУ КЗИ, которую мы условно обозначаем как «внешние окна».** Это особая группа информационных каналов о деятельности организаций, позволяющих производить извне обзор внутренней территории или какого-либо помещения визуальными или с помощью оптических и иных средств. Опрос работников ряда организаций показал, что 6% опрошенных указали на наличие *дема-скирующих признаков* объекта как возможный канал утечки охраняемой информации. Под демаскирующими признаками понимаются следы производственной и иной деятельности, по которым можно определить использование организацией специально охраняемой ею информации. Об этом могут свидетельствовать такие признаки, как, в частности, дозирование информации о деятельности организаций для средств массовой информации в целях уменьшения степени осведомленности конкурентных разведок; специфика территориальной дислокации объектов и их удаленность от воздушных трасс, железнодорожных линий и автодорог для затруднения ведения агентурной и технической разведки; наличие уникальных технических сооружений, запретных зон на подступах к объекту, специальных рубежей войсковой охраны периметра предприятия, пропускного режима. Характерными нарушениями режима КЗИ является несоблюдение мер комплексной защиты объекта с использованием правовых, организационных, технических и иных средств.

**Шестая группа ВКУ КЗИ обозначена условно нами как «людские потоки»,** объединяющая возможности утечки КЗИ, образующейся вследствие действия «человеческого фактора» (работников и командированных лиц). Эта группа ВКУ КЗИ распределена по числу опрошенных лиц следующим образом: 32% опрошенных заявили, что ВКУ информации является прием и увольнение работников; 28% — посещение предприятия командированными лицами; 15% — проведение совещаний по конфиденциальным вопросам; 15% — ведение конфиденциальных работ в помещениях, не обеспечивающих их надежную охрану; 14% — допуск и доступ к КЗИ; 10% — выезд

работников за границу; 8% — недостатки пропускного и внутреннего режима; 7% — прохождение практики студентами и стажировки аспирантами; 7% — посещение международных выставок; 5% — обучение на курсах повышения квалификации; 4% — подготовка приказов и иных внутренних документов. С учетом данных опроса охарактеризуем отдельные, наиболее распространённые, кадры этой группы.

**Прием и увольнение работников организации** — наиболее характерный канал утечки КЗИ. Его функционирование обусловлено частой сменой персонала в организациях (утечка кадров) и нарушениями, которые имеют место при оформлении допуска и доступа лиц к КЗИ. Опрос руководителей ряда предприятий показывает, что в среднем ежегодно утечка кадров составляет от 10 до 20% от общего количества работающих. В отдельные годы, в связи с ростом инфляции и спадом производства, каждый третий работающий вынужден был увольняться в поисках более высокого заработка. Почти половина работников, уволившись с предприятия, по оценке администрации, были ознакомлены с КЗИ. Недостатки в допускной работе, отсутствие в Законе о коммерческой тайне нормы, регулирующей порядок оформления допуска лиц к КЗИ, приводят к тому, что к КЗИ допускаются лица, которые по своим деловым и иным качествам не способны надежно охранять доверенные им секреты. Существенное значение имеет инструктаж лиц, допущенных к КЗИ, обучение, воспитание и контроль уровня знаний. Причем подход должен быть дифференцированным, в зависимости от категории (разряда) КЗИ, к которой лицо имеет доступ. Опрос показал, что всесторонне ознакомлены с *правилами внутреннего трудового распорядка*, в которых имелись нормы об охране КЗИ, 79% работников, с *инструкцией по обеспечению режима коммерческой тайны* были ознакомлены 33%, с *положением о разрешительной системе доступа к КЗИ* были ознакомлены в части, их касающейся, 36% работников, ознакомлены в общих чертах — 35%, не ознакомлены — 17%; с *памяткой об ответственности за разглашение коммерческой тайны* всесторонне были ознакомлены 58% работников, ознакомлены в общих чертах — 30%, не ознакомлены — 12%. Эти данные свидетельствуют о неудовлетворительной работе администрации по воспитанию и обучению работников, занятых в сфере обращения КЗИ, когда большинство опрошенных лиц не знают или плохо знают требования корпоративных норм, что создает условия для их невыполнения и образования канала утечки КЗИ.

**Посещение организаций командированными лицами** становится реальным каналом утечки КЗИ в случае нарушения корпоративных требований внутриобъектового и пропускного режима. Характерными нарушениями режима КЗИ при приеме командированных лиц являются, *во-первых*, допуск лиц к КЗИ без оформления разрешения при отсутствии командировочного удостоверения, предписания на выполнение служебного задания и договора с организацией. *Во-вторых*, невыполнение принимающей стороной требований по сопровождению прибывших в подразделение командированных лиц. *В-третьих*, отсутствие в подписаниях на выполнение служебного задания отметок о решении конкретных производственных вопросов и передачи необходимого объема КЗИ. *В-четвертых*, отсутствие в предписании на выполнение служебного задания основания для совместной деятельности (номер и дата договора, технического задания и др.). *В-пятых*, допуск командированных лиц к новым сведениям, степень конфиденциальности которых еще не определена в организации.

Решение производственных задач не обходится без **служебных совещаний**, на которых обсуждаются вопросы, содержащие КЗИ. Порядок их проведения, который регламентирован внутренними документами, может быть нарушен, о чем указали 15% опрошенных лиц ряда организаций. Распространенными являются такие нарушения, как, в частности: проведение совещаний в не аттестованных СБ помещениях; допуск на совещание лиц, не имеющих отношения к обсуждаемому вопросу; несоблюдение очередности рассмотрения вопросов конфиденциального характера; нарушения внутриобъектового режима, создающие условия для визуального осмотра помещений, в которых проводятся совещания; фотографирование экзоплатов и документов, представляемых на совещании; звукозапись и видеозапись выступлений участников совещания на носителях, не учтенных в СБ.

Предоставление информации, составляющей коммерческую тайну, по **мотивированному требованию органа государственной власти, органа местного самоуправления** создает в отдельных случаях предпосылки для ее возможной утечки. Это возможно вследствие допущенных служащими нарушений сохранности полученной КЗИ. Характерными нарушениями являются включение полученных от организаций конфиденциальных сведений в ведомственные открытые документы; ознакомление с конфиденциальными работами и документами работников госучреждений, не входящими в круг их обя-

занностей; направление в органы местного самоуправления конфиденциальных документов, к которым они не имеют отношения в соответствии с их правовым статусом.

Изучение проявлений нарушений режима КЗИ на каналах ее возможной утечки позволяет сделать вывод о том, что борьба ведется в основном с традиционными нарушениями пропускного и внутри-объектового режима, тогда как другие нарушения, прямо ведущие к утечке охраняемой информации, остаются вне поля зрения администрации. Внимание должно быть обращено к неградиционным формам ВКУ информации, в которых проявляются нарушения, которые слабо или практически не выявляются, к принятию мер по установлению лиц, допускающих такие нарушения, что будет иметь значение для повышения эффективности предупреждения правонарушений в сфере обращения КЗИ.

## § 2. Причины и обстоятельства, способствующие нарушениям режима конфиденциальности информации

**Понятие и классификация причин нарушений режима КЗИ.** Знание причин нарушений режима коммерчески значимой информации имеет определяющее значение для познания такого явления, как утечка КЗИ, и организации эффективного предупреждения правонарушений, совершаемых в этой области. Учитывая направленность данного исследования, представляется важным сформулировать теоретические положения о понятии причин нарушений режима КЗИ, дать классификацию общих и конкретных причин и охарактеризовать систему обстоятельств, ведущих к нарушениям режима КЗИ.

Определяя утечку охраняемой информации, следует отметить, что это явление представляет собой следствие каких-то предшествующих ей по времени событий. Если исследовать эти события, то можно выделить такие их совокупности, которые всегда (или почти всегда) прямо или непосредственно приводят к утечке КЗИ. Такие совокупности событий объективного и субъективного характера, которые всегда (или почти всегда) приводят прямо и непосредственно к утечке коммерческих секретов, называются **причинами утечки КЗИ**. **Причинная связь (или причинность)** определяется как объективная связь между двумя явлениями (ситуациями, событиями), одно из которых (причина) производит, порождает другое (следствие), т.е.

утечку КЗИ. Для того чтобы выявить утечку КЗИ в организации, нужно в целом иметь представление о системе причинности явлений и процессов, обуславливающих изменения в хозяйственной деятельности.

Будучи частью общей проблемы причин правонарушений, совершаемых в обществе, проблема причин правонарушений режима КЗИ требует учета ее основных положений, характеризующих понятие причинности, признаки которого наиболее полно исследованы в криминологической науке. Нужно сказать, что за последние 50 лет учеными-юристами проделана значительная работа по разработке теории причин правонарушений. В юридической науке общепризнанной является дифференциация причин и условий совершения правонарушений, предложенная В.Н. Кудрявцевым<sup>1</sup>. Он различает объективные и субъективные причины и условия совершения правонарушений. При этом к объективным причинам, по мнению В.Н. Кудрявцева, относятся конкретные противоречия в общественном бытии, в экономических и социальных отношениях людей, а к объективным условиям — недостатки организационного и технического порядка, поддерживающие и оживляющие действие объективных и субъективных причин правонарушений. Субъективными причинами правонарушений В.Н. Кудрявцев считает определенные элементы социальной психологии, находящие проявление в искаженных потребностях, мотивах, правосознании, нравственных ценностях лиц, совершающих правонарушения, а субъективными условиями — демографические и социально-психологические особенности населения. Поэтому при раскрытии предмета настоящего исследования мы будем опираться на основные теоретические положения этой концепции с целью выявления особенностей причинного комплекса, обуславливающего нарушения режима КЗИ, приводящие к возможной утечке такого рода информации.

Причинное объяснение правонарушений основывается на философской концепции причинности как объективной формы всеобщего взаимодействия явлений. Такой подход позволяет строить объяснения причин правонарушений на базе анализа объективно существующих явлений, определяющих негативное формирование личности, в данном случае работника организации, связанные с на-

<sup>1</sup> См.: Кудрявцев В.Н. Причины правонарушений. М.: Наука, 1976. С. 126–205.

рушением им норм, прежде всего, гражданского и трудового законодательства, регулирующих вопросы охраны КЗИ.

Ученые, занимающиеся проблемами правонарушений, рассматривают их как сложное социальное и исторически обусловленное явление, возникшее на определенном этапе развития общества и существующее в нем.

В число основных положений, характеризующих концепцию причин правонарушений, входит объяснение *правонарушения* как продукта сложного взаимодействия личности и среды при решающем исходном влиянии последней, выделение среди факторов, воздействующих на правонарушение, явлений и процессов, относящихся к различным сферам и уровням общественной жизни. Роль субъективных факторов нельзя не учитывать. Объективные экономические и социальные факторы отнюдь не фатально влияют на поведение человека. Их воздействие проходит через сознание человека. В основе антиобщественного, а точнее, антикорпоративного поведения лежит *индивидуалистическая позиция*, порождающая конфликт работника с администрацией организации по поводу соблюдения корпоративных норм охраны конфиденциальности КЗИ.

В науке криминологии проблема причин правонарушений рассматривается комплексно на трех основных направлениях (уровнях): *общества в целом, социальных групп и индивидуума*<sup>1</sup>. Причины правонарушений режима КЗИ следует рассматривать на уровне общества в целом (в сфере промышленности, торговли и др.), на уровне отдельной организации и индивида (работника).

Рассмотрение *причин правонарушений на уровне общества в целом* (в частности, в промышленности и торговле) связано с установлением явлений и процессов, образующих общие причины антиобщественных явлений, которые могут привести к утечке КЗИ. *Общая причина нарушений режима КЗИ обусловлена тем, что допускаются ошибки в ходе преодоления имеющих место в обществе противоречий*. Общая причина нарушений режима конфиденциальности (НРК) КЗИ объясняется существованием противоречий<sup>2</sup> в социально-экономическом развитии страны в условиях рыночной экономики с несвоевременностью и неправомерностью их разрешения на уровне

не государственного регулирования и отдельно взятой организации. Противоречия перерастают в открытое противостояние различных уровней властей, что отрицательно сказывается на эффективности управления процессом охраны конфиденциальности КЗИ.

*Причины, относящиеся к уровню социальных групп* (отдельная коммерческая организация), являются промежуточным звеном между высшим и индивидуальным уровнем, передающим влияние обстоятельств более высокого уровня на более низкий. Охватываемые им явления и процессы достаточно разнообразны. Их проявления наблюдаются в сфере охраны коммерческих секретов в экономической и правоохранительной деятельности. С помощью причин данного уровня происходит конкретизация общей и конкретных причин, создаются предпосылки объективного и субъективного характера, необходимые для проявления обстоятельств индивидуального уровня.

К *причинам индивидуального антикорпоративного поведения* относятся взгляды определенного круга работников, обуславливающих направленность личности против частных интересов организации (отдельных ее представителей), внешние обстоятельства, сформировавшие эти взгляды, различные жизненные ситуации, которые во взаимодействии с позицией личности вызывают антикорпоративное поведение, связанное с несоблюдением требований обеспечения режима КЗИ.

Характеризуя в целом причины правонарушений режима КЗИ, следует отметить следующее: у лиц, совершивших такие правонарушения, отмечается скорее не наличие отрицательных свойств личности, а отсутствие положительных качеств, которые обуславливают направленность личности против интересов организации, которые связаны с получением отдельными ее руководителями более высокого денежного вознаграждения. Они являются следствием дефектов корпоративно-ценностной сферы личности, проявляющихся в отсутствии правильного понимания работником истинного значения охраняемых организацией ценностей, в виде коммерческих секретов, охрана которых предусмотрена законодательством.

В сфере деятельности по сохранению коммерческих секретов дефекты корпоративно-ценностной сферы личности проявляются в невыполнении или в ненадлежащем выполнении работниками обязанностей по сохранению КЗИ, безответственном отношении к делу, в силу отсутствия материальных и иных стимулов к труду, равнодушии к освоению новых товаров и продвижению их на рынок, что указывает на специфику жизненной ситуации при совершении

<sup>1</sup> См.: Криминология. М., 2004. С. 122–149, 178–196.

<sup>2</sup> См.: Горбач В.И. Проблемы диалектических противоречий. М., 1972. С. 34–98, и др.

нарушений режима КЗИ. В соответствии с названной выше схемой изложения применительно к различным уровням проанализируем причины нарушений режима КЗИ, ведущие к утечке такой информации в организации.

Обращение к анализу противоречий в связи с исследованием причин нарушений режима КЗИ должно сочетаться, во-первых, с оценкой не всех явлений, а только имеющих консервативное начало в системе образующих противоречия обстоятельств; во-вторых, с учетом специфики противоречий, связанных с невыполнением или ненадлежащим выполнением работниками обязанностей по сохранению коммерческих секретов, обусловленных различными экономическими, социальными и правовыми факторами.

Концептуальные положения, раскрывающие связь противоречий и причин нарушений режима КЗИ, определяют важнейшую часть комплекса теоретических положений, лежащих в основе объяснения механизма детерминации рассматриваемых правонарушений.

Связь противоречий и причин нарушений режима КЗИ не следует представлять упрощенно. Она носит достаточно сложный характер, причем значение имеет правильная оценка процессов, связанных с разрешением противоречий, возникающих не только по поводу частной собственности. На наш взгляд, нужно последовательно исходить из того, что сами по себе противоречия, касающиеся частных интересов организаций, в условиях рыночной экономики, когда продолжает осуществляться государственное регулирование процесса преодоления противоречий в экономическом развитии, далеко не всегда и отнюдь не автоматически способны вызвать отрицательные последствия в деятельности коммерческих организаций. Такие последствия становятся возможными чаще всего тогда, когда допускаются ошибки, просчеты в ходе преодоления противоречий на различных уровнях регулирования рыночной экономики и, прежде всего, на уровне микроэкономики (отдельной организации).

На основе анализа факторов, влияющих на совершение нарушений режима КЗИ, ведущих к утечке охраняемой в организации информации, были **выделены четыре группы противоречий**:

1) *Сложности, наблюдающиеся при решении задач по защите коммерческих секретов, требующие оперативного реагирования со стороны администрации и служб безопасности (СБ) на изменения в хозяйственной практике работы организаций*. Задачи, которые решает трудовой коллектив, постоянно изменяются. Динамично меняется и оперативная обстановка, которую следует учитывать при организации и

осуществлении мер по охране конфиденциальности КЗИ. Служба безопасности не всегда отслеживает происходящие изменения в хозяйственной деятельности. Это приводит к тому, что на отдельных участках, где выполняются конфиденциальные работы, не устанавливается режим КЗИ, отсутствует контроль за обеспечением режимных мер, что увеличивает вероятность совершения правонарушений и возможность утечки охраняемых сведений.

2) *Противоречия между требованиями, предъявляемыми к подбору и расстановке кадров в подразделениях, работники которых подлежат оформлению на допуск к КЗИ, включая и работников служб безопасности, и состоянием современной практики их выполнения*.

Полученные результаты исследования показывают, что нарушения режима КЗИ, ведущие к утечке охраняемой информации, связаны чаще всего с занятием должностей лицами, не подготовленными к этой работе, не знающими требований норм корпоративных актов и законодательства по защите коммерческой тайны, работающими по старинке, не овладевающими новыми формами и методами работы по предупреждению утечки КЗИ.

В организациях не налажена работа по обучению и воспитанию лиц, допускаемых к КЗИ. Это происходит потому, что работники СБ, которые должны повседневно заниматься этой работой, сами оказываются к ней не подготовлены в силу отсутствия знаний по выявлению каналов утечки информации и их закрытию с использованием научных методов и методик.

3) *Противоречия между содержанием функций отдельных категорий работников СБ и объективными возможностями их выполнения*. Вследствие того, что нет точности в определении функций работников отдела конфиденциального делопроизводства, отдела по обеспечению режима при ведении работ и других подразделений, входящих в состав СБ в корпоративных актах, определяющих их правовой статус, некоторая часть работников может уклоняться от выполнения своих обязанностей. По отдельным направлениям охраны КЗИ некоторые корпоративные нормы дублируются, что порождает путаницу в работе по обеспечению режима КЗИ, создает условия для «оголенности» отдельных участков, где обращается КЗИ, с учетом требований их охраны. Анализ показывает, что на отдельные подразделения СБ и их работников возложен порой такой круг задач и обязанностей, которые для них не всегда являются реально выполнимыми. По причине этого какая-то часть обязанностей ими может хронически не выполняться. Здесь необходимо учитывать и противоречия между

практикой возложения обязанностей на работников по охране конфиденциальности КЗИ и возможностями финансирования этой работы. Анализ показывает, что в различные периоды времени растет количество заданий, исходящих от администрации по охране КЗИ, не подкрепленных финансовыми и трудовыми ресурсами.

Нельзя не учитывать противоречия между числом принятых административных решений по обеспечению безопасности организации и возможностями контроля за их выполнением. Анализ показывает, что в приказах организаций, относящихся к вопросам охраны коммерческих секретов, контроль за их выполнением возлагается на службы безопасности, которые зачастую в силу своей малочисленности не в состоянии проконтролировать все направления обеспечения режима КЗИ, и поэтому важнейшие решения остаются порой нереализованными.

На этой основе способен формироваться стереотип общего отношения работников к вопросам защиты коммерческих секретов, при котором ненадлежащее отношение к исполнению обязанностей по охране конфиденциальности КЗИ и реализации намеченных мер подчас выглядит своего рода нормой их трудового поведения. Это чревато открытием возможностей для утечки КЗИ.

4) *Противоречия, относящиеся к системе реализации юридической ответственности за невыполнение или ненадлежащее выполнение служебных обязанностей, связанных с охраной коммерческих секретов.*

Они проявляются, прежде всего, в несоблюдении отделными организациями принципа неотвратимости ответственности за совершение нарушений режима КЗИ. Этому способствует, во-первых, несовершенство норм действующего законодательства, определяющих порядок и процедуру возбуждения уголовных дел в случаях умышленного или неосторожного разглашения работником сведений, составляющих коммерческую тайну. Во-вторых, сложности доказывания в суде обстоятельств нарушения режимных требований с целью возмещения убытков. В-третьих, трудности привлечения работника к дисциплинарной ответственности в случаях нарушения работодателем обязанностей по созданию условий для охраны КЗИ.

Анализ практики организаций по борьбе с этой категорией нарушений показывает, что со многими нарушениями руководители свыклились и не обращают на них внимания, слабо ведут воспитательно-профилактическую работу с подчиненными работниками, недостаточно применяются меры материального воздействия к правонарушителям. Практически не применяются меры мо-

рального воздействия на нарушителей. Многие руководители неправомерно считают, что эти меры потеряли свое практическое значение в условиях рыночной экономики. Жизненная позиция лиц, допускающих нарушения режима КЗИ, является отрицательным примером для остальных работников, которые убеждаются в безнаказанности за действия, связанные с невыполнением требований конфиденциальности КЗИ.

Указанными противоречиями не исчерпывается совокупность явлений, способствующих утечке охраняемой в организации информации. Однако они дают достаточно полное представление о тех явлениях и процессах, которые тесно связаны с нарушениями режима КЗИ. В дальнейшем их характеристика будет дополнена при рассмотрении причин и обстоятельств, способствующих утечке КЗИ.

Важным звеном в системе причин нарушений режима КЗИ выступают явления и процессы, действующие на уровне социальных групп (ассоциаций, холдингов и т.д.), которые представляют собой систему обстоятельств, относящихся к различным сферам социальной действительности.

Выступая в качестве самостоятельного звена в системе причин нарушений режима КЗИ, они вместе с тем являются базой причин и условий индивидуального антикорпоративного поведения. Такого рода обстоятельства в значительной мере определяют наличие факторов, под влиянием которых формируется личность правонарушителя режима КЗИ. Возникают благоприятные ситуации для утечки охраняемой в организации информации. На этом фоне происходит взаимодействие личности и ситуации.

Полученные данные исследования позволили на концептуальном уровне сформулировать и раскрыть систему признаков, характеризующих конкретные причины, ведущие к утечке охраняемой информации, и обстоятельства, приводящие к нарушениям режима КЗИ. Анализ явлений и процессов, действующих на уровне организации, показывает, что конкретными причинами утечки охраняемой информации являются:

— неоправданный доступ работников и командированных лиц к конфиденциальным работам, документам и изделиям;

— необоснованная рассылка документов с грифом «Коммерческая тайна» в другие организации и передача (транспортировка) изделий, содержащих такие сведения;



— разглашение конфиденциальных сведений на совещаниях, собраниях и в открытых публикациях, частных беседах и в личных письмах;

— включение конфиденциальных сведений в открытые документы, доступ к которым ограничен;

— открытая публикация результатов научных исследований, которые в совокупности с ранее опубликованными материалами раскрывают конфиденциальные сведения;

— нарушение режима КЗИ при использовании средств связи, при транспортировке и испытании изделий, содержащих КЗИ;

— хищение и потеря документов, изделий с грифом «Коммерческая тайна»;

— несовершенство используемых средств противодействия фирмам, ведущим конкурентную техническую разведку (КТР);

— необоснованное снятие грифа «Коммерческая тайна» с документов и изделий;

— возможное наличие на объекте агентуры конкурирующих фирм, а также в местах, посещаемых работниками организации.

Названный перечень причин, ведущих к утечке КЗИ, не является исчерпывающим. В дальнейшем они будут конкретизированы обстоятельствами, способствующими утечке охраняемой информации.

Рассматривая причины нарушений режима КЗИ, ведущие к утечке охраняемой информации, следует отметить, что главной из них на индивидуальном уровне является *деформация личности*. Она проявляется в недооценке значения точного соблюдения трудовых обязанностей по сохранению коммерческих секретов, легкомысленном отношении к режимным требованиям; недисциплинированности и безответственном отношении к делу. Поскольку утечка охраняемой информации является следствием нарушений режима КЗИ, а нарушения совершаются в результате взаимодействия личности и ситуации, то роль последних нельзя недооценивать. Имеются в виду особенности личности правонарушителей и наличие конкретной *хозяйственной ситуации*, в которых происходит нарушение требований законодательства и корпоративных актов в сфере обращения КЗИ.

Опрос показал, что 35% опрошенных оправдывают совершение нарушений режима КЗИ незнанием норм, регулирующих охрану КЗИ, 59% — непредвиденностью некоторых обстоятельств производственного и финансового характера, повлиявших на невыполнение режимных требований, 61% — неопытностью и неумением работать с грифованными документами и изделиями. Нужно отметить,

что на хозяйственную ситуацию оказывают влияние факторы как позитивного, так и негативного характера, вследствие чего ситуация отличается подвижностью и динамизмом. Под хозяйственной ситуацией понимается оперативная обстановка, которая складывается в организации на различных направлениях ее деятельности, в определенном отрезок времени.

Явления и процессы, действующие на уровне общества в целом (промышленности, торговли и др. сфер), служат основой возникновения негативного явления, встречающегося на уровне федеральных министерств и агентств, субъектов Федерации, отдельных организаций и индивидов. Взаимосвязь между ними отличается значительной сложностью. Ее объяснение должно исходить из диалектики общего, особенного, единичного.

Имея в виду, что в реальной действительности обстоятельства, в которых находят отражение общие и конкретные причины нарушений режима КЗИ, ведущие к утечке охраняемой информации, односторонны по своему содержанию и то, что устранение этих обстоятельств составляет одну из главных задач деятельности организации по предупреждению утечки КЗИ, их рассмотрению уделено специальное внимание.

**Классификация обстоятельств, ведущих к нарушениям режима КЗИ.** Изучение проявлений нарушений режима КЗИ на канале возможной ее утечки, проведенное в ряде организаций, показывает, что обстоятельства, приводящие к нарушениям режима КЗИ вследствие которых происходит ее утечка, различны и весьма многочисленны. Вместе с тем, несмотря на их множество, они взаимосвязаны и взаимобусловлены.

Интересы углубленного рассмотрения данных обстоятельств выдвигают необходимость их классификации. Для этой цели могут быть плодотворно использованы классификационные схемы, разработанные в юридической науке, в частности, в криминологии<sup>1</sup>, прошедшие проверку временем и используемые в организациях.

Исходя из задач исследования, характеристика обстоятельств дается на базе классификации, используемой в качестве критерия распределения явления и процессы, выступающие в роли причин и условий, способствующих совершению нарушений режима КЗИ,

<sup>1</sup> См.: Теоретические основы предупреждения преступности. М., 1977. С. 78—92, 178—211, и др.

в зависимости от социальной среды, в которой они себя проявляют. В соответствии с данной классификацией были выделены *обстоятельства организационно-управленческого, воспитательного и правового характера*.

Изучение признаков, образующих указанные группы обстоятельств, дает возможность выявить определенную специфику причин нарушений режима КЗИ в различных организациях, имеющих общее значение. Следует отметить условность предложенной классификации. При характеристике обстоятельств нельзя не отдавать отчета в том, что порой одно и то же явление носит сложный характер и его признаки могут быть охарактеризованы не в одной, а в нескольких классификационных группах.

Рассмотрим *типичные проявления обстоятельств, способствующих утечке КЗИ*, относящихся к каждой из названных групп.

**Группа обстоятельств организационно-управленческого характера.** Их понятием объединяются конкретные недостатки в управлении процессом обеспечения режима конфиденциальности КЗИ, в которых используется охраняемая информация, обуславливающие отсутствие должного порядка и дисциплины в трудовых коллективах организаций, связанных с сохранением коммерческих секретов. Полученные результаты исследований позволили выделить в отдельные подгруппы явления, способствующие совершению нарушений режима КЗИ и утечке охраняемой информации.

**Во-первых, это несовершенство структуры управления режимным обеспечением работ в организациях.** Это одна из причин нарушений оптимального режима функционирования корпоративного механизма, обеспечивающего сохранность коммерческих секретов. Несвершенство этого механизма порождает нечеткое определение функций подразделений, использующих КЗИ, и компетенции СБ. Вследствие действия этого фактора около 14% опрошенных работников, нарушивших требования режима КЗИ, объяснили факт нарушения своей чрезмерной служебной загруженностью. Неукomплектованность подразделений СБ кадрами или, наоборот, штатные излишества отражаются на состоянии исполнительской дисциплины, что может проявиться в неполном и неточном выполнении обязанностей.

В организациях издается значительное число приказов и инструкций, противоречащих по содержанию друг другу, а порой и не соответствующих нормам законодательства. Рассогласование в руководящих документах направлений деятельности позволяет отдельным руководителям и исполнителям халатно относиться к этой работе.

Поэтому ориентиром должно быть действующее законодательство по вопросам охраны КЗИ, а корпоративные акты призваны расширить сферу дозволенного и возможного поведения работников.

**Во-вторых, это недостатки в подборе, расстановке и обучении кадров в сфере обращения КЗИ.**

Нарушение общеизвестных принципов в подборе и расстановке кадров, и, прежде всего, по деловым качествам является обстоятельством, которое может повлечь утечку КЗИ. Это происходит в прямой связи с назначением на должности лиц, не отвечающих предъявленным требованиям. Речь идет о приеме на работу лиц, у которых отсутствует опыт и квалификация, что не позволяет им успешно выполнять обязанности при обращении КЗИ и может стать каналом утечки информации. Недостатки в подборе и расстановке кадров могут проявляться в частой смене руководителей и работников СБ, что ведет к нестабильности в управлении системой защиты коммерческих секретов.

Общим принципом подбора и расстановки кадров в сфере обращения КЗИ является прием на работу лиц, которые по своим профессиональным качествам могут выполнять конфиденциальные работы. Вместе с тем Закон о коммерческой тайне не устанавливает требования к лицам, допускаемым к КЗИ, и не содержит ограничения по их допуску, отдавая, мягко говоря, «все на откуп» руководителям организаций. Невнимательность и небрежность работников отдела кадров и СБ при изучении деловых и моральных качеств лиц, поступающих на работу, особенно в связи с тем, что допуск к КЗИ оформляется непосредственно в организациях, чреват серьезными последствиями в виде возможной утечки КЗИ.

Упущения работников СБ, юридической службы и производственных подразделений связаны с отсутствием у первых — базовой профессиональной подготовки в области экономической и информационной безопасности, а у вторых — элементарных знаний и навыков по выявлению и предупреждению утечки КЗИ. Об этом заявили 16% выборочно опрошенных на предприятиях лиц, работающих в этих службах. Специалисты в области защиты секретов готовят в основном факультет защиты информации Российского государственного гуманитарного университета и факультет информационной безопасности Московского государственного инженерно-физического института (университета), ряд других вузов. Количество специалистов, ежегодно выпускаемых названными факультетами, не удовлетворяет потребности организаций.

Действующие кафедры (курсы), специализирующиеся по вопросам информационной безопасности в институтах повышения квалификации (ИПК), созданные в некоторых федеральных министерствах, ограничены в своих учебно-методических возможностях. В крупных организациях со значительным объемом КЗИ, где трудится большое количество работников — исполнителей конфиденциальных работ, имеются учебные классы, в которых ведется обучение работников. В советский период такая подготовка работников, имевших отношение к сохранности государственных секретов, являлась составной частью воспитательно-профилактической работы, которая велась под контролем парткомов с использованием методов убеждения и принуждения.

**В-третьих, несовершенство организации обеспечения режима конфиденциальности проводимых работ по охране КЗИ.**

Это проявляется в недостаточном внимании к вопросам обеспечения режима КЗИ со стороны отдельных руководителей, которые не занимаются обучением работников в области защиты КЗИ с учетом ежегодного обновления трудовых коллективов. В течение трех лет коллектив обновляется примерно на одну треть, о чем заявили 25% из числа опрошенных работников отделов кадров. Некоторые руководители, в частности члены правления общества, акционеры, входящие в состав совета директоров, считают сохранение коммерческих секретов второстепенным делом, что выражается в недостаточном финансировании работ в области безопасности.

Изучение показывает, что ряд руководителей среднего звена с молчаливого согласия вышестоящего руководства не заботятся о создании нормальных условий для обеспечения конфиденциальности работ. Речь идет об отсутствии условий для ознакомления работников-исполнителей с грифованными документами, в специально выделенном помещении отдела, занимающегося конфиденциальным делопроизводством. Практика ознакомления работников с документами на рабочих местах подтверждает возможность несанкционированного ознакомления с ними посторонних лиц. В частности, при выполнении НИОКР в рабочих помещениях могут находиться работники других подразделений, не имеющих отношения к данной тематике, об этом заявили 20% опрошенных лиц.

Недостатки в организации труда в 37% случаев являются причиной нарушений режима КЗИ. Это может быть неправильная комплектация документов в номенклатурные дела. По каждой НИР и ОКР должно быть заведено отдельное дело. Невнимательность ру-

ководителей подразделений и слабый контроль СБ являются причиной накопления в одном деле документов по разным темам, что ведет к расширению круга лиц, ознакомившихся с КЗИ, к которой они не имеют отношения по службе. Следующее обстоятельство — это расширенный доступ лиц к документам, содержащим тактико-технические характеристики разрабатываемых изделий. Имеется в виду процедура согласования технического задания, когда с документом знакомятся в полном объеме представители различных служб и подразделений, а не в части, их касающейся.

Несовершенство организации обеспечения режима КЗИ состоит также в приеме командированных лиц с неправильными оформленными служебными заданиями и предписаниями на выполнение работ. Нарушения проявляются в том, что в названных документах не указывается конкретная тема (шифр) и в какой части командированное лицо должно быть ознакомлено с КЗИ. Принимающая сторона не осуществляет сверку содержания предписания с условиями договора, в котором указан объем возможного использования КЗИ. Отсутствие контроля со стороны подразделений и СБ способствует расширительному толкованию и доступу к любым документам, содержащим КЗИ. Командированное лицо по собственному усмотрению определяет объем информации, который ему необходим для выполнения задания, что и рассматривается в данном случае как возможный канал утечки КЗИ.

Отдельные организации используют мероприятия по легендированию содержания введущихся НИОКР с целью введения в заблуждение конкурентов до начала выпуска качественно новых товаров. Легенда должна быть правдоподобной с технической и технологической стороны разрабатываемого изделия. Она должна быть доведена до исполнителей и включена в план мероприятий по охране конфиденциальности КЗИ. В противном случае недостаточно продуманные меры по легендированию могут явиться “внешними окнами” возможной утечки охраняемой информации.

Важно отметить отрицательное влияние нарушений трудовой и договорной дисциплины на формирование обстановки безответственности, на фоне которой происходит нарушение в сфере обращения КЗИ. Анкетирование дел на работников, допустивших нарушения режима КЗИ, показывает, что в 19% случаев этой категорией нарушителей были совершены дисциплинарные проступки (опоздания, прогулы и т.д.). В 16% случаев — имели место с их стороны срыв

графиков работы с контрагентами, невыполнение договорных обязательств.

**В-четвертых, неудовлетворительная постановка учета и отчетности, отсутствие регулярных проверок и инвентаризаций** конфиденциального делопроизводства и товарных складов, где хранятся изделия, содержащие КЗИ, может быть, как показал опрос, причиной утечки охраняемой информации в 21% случаев. Недостатки учета и отчетности часто ведут к созданию обстановки, в которой могут процветать безынициативность и нераспорядительность, отрицательно влияющие на отношение работников к исполнению своих служебных обязанностей по охране КЗИ. Отмечается слабый контроль со стороны руководителей подразделений и СБ за выполнением работниками правил, регламентирующих порядок обеспечения режима КЗИ. Речь идет о снижающем отношении к нарушителям дисциплины. Об этом заявили 28% опрошенных законопослушных работников.

**В-пятых, недостатки корпоративного планирования**, ведущие к неравномерному распределению работ, связанных с невозможностью заранее обеспечить организацию заказами путем заключения договоров с контрагентами. Отсюда наблюдается: во-первых, поспешность в определении сведений, составляющих КЗИ, которые предполагается передать контрагенту после подписания договора; во-вторых, отсутствие возможности в короткие сроки качественно обработать и поставить на учет документы и изделия, содержащие КЗИ. Отсюда данная работа ведется с большими отступлениями от правил, регулирующих охрану КЗИ. Работники допускают невнимательность и ненадлежащим образом выполняют свои обязанности, объясняя это чрезмерной загруженностью в работе, что может явиться одной из причин утраты грифованных документов и изделий.

Установленный порядок планирования в организациях не всегда соблюдается. Проводятся частые изменения планов, что влечет за собой установление дополнительных заданий, не подкрепленных материальными, трудовыми и финансовыми ресурсами, в том числе охраны КЗИ.

**В-шестых, недостатки финансирования работ по обеспечению режима конфиденциальности КЗИ.** Они связаны с невыполнением решений высшего органа управления в части обеспечения безопасности организации. Выделяемые средства порой изымаются по решению правления или директора на другие нужды. Это происходит потому, что отсутствует корпоративный акт, определяющий порядок финансирования работ по охране КЗИ. Выделение средств на охра-

ну КЗИ зависит от субъективного усмотрения руководства. При этом доводы научного руководителя НИР и главного конструктора, коммерческого директора о необходимости финансирования деятельности по охране КЗИ учитываются не во всех случаях.

**В-седьмых, недостаточная организация аналитической работы** в сфере обращения КЗИ может привести к тому, что своевременно не будут выявляться причины и обстоятельства, способствующие образованию каналов утечки охраняемой информации, не будут предлагаться производственным подразделениям и СБ рекомендации по предупреждению утечки КЗИ.

**В-восьмых, недостатки в стимулировании работников** ведут к повышенной текучести кадров на предприятиях, в том числе и лиц, озабоченных с КЗИ. Как уже отмечалось, текучесть кадров наблюдается в основном в период спада производства и обусловлена уменьшением объемов выполняемых работ при хронической невыплате заработной платы. Ежегодно, в течение последних пяти лет, как показывают данные опроса, примерно третья часть работников от числа штатного состава увольнялись с предприятия по собственному желанию и переходили на работу в другие организации, в основном в поисках более высокого заработка. Нужно отметить, что около 10% уволившихся работников были осведомлены в коммерческих секретах.

Существующие недостатки в системе материального поощрения являются, по мнению опрошенных, основной причиной недобровольного отношения работников к исполнению своих обязанностей, в том числе связанных с охраной коммерческих секретов. Более 24% опрошенных лиц заявили, что отсутствует надбавок к зарплате за «секретность» в работе не способствует повышению ответственности работников-исполнителей за сохранность КЗИ и является причиной невыполнения установленных требований по охране КЗИ. Причиной ненадлежащего выполнения работниками СБ своих обязанностей большинство из них считает отсутствие надбавок за трудовой стаж работы в СБ. Нужно отметить, что порой низкие должностные оклады работников СБ влияют на уровень активности в проведении ими аналитической и контрольно-проверочной работы. При этом особенно к охране государственных секретов действуют нормы, устанавливающие дифференцированные надбавки к должностному окладу за трудовой стаж работы в режимно-секретных органах.

**Группа обстоятельств воспитательного характера.** Эти обстоятельства связаны с недостатками в работе по формированию созна-

тельного отношения работников к исполнению своих трудовых обязанностей по сохранению коммерческих секретов. В условиях рыночной экономики воспитанию работника уделяется недостаточное внимание. Некоторые руководители организаций ошибочно полагают, что не стоит всерьез заниматься воспитательной работой, поскольку она якобы потеряла свое значение в новых экономических условиях. С такой оценкой трудно согласиться. Воспитание оказывает непосредственное влияние на качество выполняемых работниками обязанностей, в том числе и в сфере охраны КЗИ. Поэтому при определении причин, обуславливающих нарушения режима КЗИ, необходимо учитывать обстоятельства воспитательного характера, способствующие формированию антикорпоративных взглядов работников. *Во-первых*, это недостаточное внимание к проведению воспитательной работы в трудовом коллективе в связи с переходом к рыночной экономике и закреплением в Конституции права на частную собственность; недостаточное раскрытие экономических возможностей, открывающихся перед наемным работником. *Во-вторых*, недостаточное использование форм и методов воспитательной работы по привитию работникам чувства «фирменного патриотизма», признанию и уважению ими частных интересов собственника; отсутствие дифференцированного воспитательного подхода к различным категориям работников. *В-третьих*, отрыв воспитательной работы от решения организацией производственных задач в конкретно сложившейся хозяйственной ситуации. *В-четвертых*, недостаточная увязка воспитательной работы по формированию ответственного отношения работников к сохранности имущества собственника, включающая правовую охрану КЗИ, с материальным стимулированием этой работы, с проявлением заботы о работнике и уважением его личных интересов.

Изучение личных дел на нарушителей режима КЗИ за пятилетие показывает, что 78% из них указали в своих объяснениях в качестве причины — это незнание или непонимание требований администрации по этим вопросам вследствие недостаточного проведения воспитательной работы. Это проявилось в отсутствии занятий по изучению корпоративных актов и разъяснению требований по охране КЗИ. Этой работой практически не занимались руководители подразделений и работники СБ.

Существенное значение для сохранения коммерческих секретов имеет обстановка, сложившаяся в подразделениях. Как показал опрос работников — исполнителей конфиденциальных работ, 27%

из них отметили существующую связь между состоянием неблагоприятного социально-психологического климата в трудовом коллективе и частотой совершения правонарушений, в том числе и нарушениями режима КЗИ. Показательным в этом плане являются данные опроса об отношении исполнителей конфиденциальных работ к своим непосредственным руководителям. Из числа опрошенных отметили как вполне хорошие отношения — 52% работников, сносные отношения — 20%, плохие — 23%, трудно сказать — 3%.

Что касается отношений с руководством службы безопасности, то данные опроса распределились следующим образом. Отношения с руководителем отдела конфиденциального делопроизводства отмечаются как вполне хорошие — 35% работников, удовлетворительные — 33%, плохие — 8%, трудно сказать — 17%, с начальником службы безопасности отмечают как вполне хорошие — 43% работников, удовлетворительные — 19%, плохие — 0,7%, трудно сказать — 21%; с начальником охраны предприятия (ВОХР) отмечают как вполне хорошие — 22% работников, удовлетворительные — 10%, плохие — 0,7%, трудно сказать — 46%.

Сравнительный анализ этих данных с данными о социально-психологическом климате в трудовом коллективе позволяет сделать вывод о том, что плохие отношения исполнителей конфиденциальных работ с руководством подразделений и СБ оказывают неблагоприятное влияние на формирование у них отрицательной позиции по поводу исполнения обязанностей в сфере обращения КЗИ. Это происходит при отсутствии должной воспитательной работы и наличии отрицательных черт у руководителей, в силу которых у них не складываются нормальные отношения с подчиненными.

Беспринципная позиция отдельных руководителей подразделений по отношению к лицам, нарушившим порядок обеспечения режима КЗИ, с одной стороны, и недостаточное внимание к моральному стимулированию за добросовестный труд, связанный с охраной КЗИ, с другой стороны, в 30% случаев может быть условием, способствующим совершению нарушений. Важно учитывать, что если порицание или поощрение объявлены работнику незаслуженно, то утрачивается их воспитательное воздействие. Более того, оно начинает играть отрицательную роль в дальнейшей трудовой деятельности и может выступать в качестве одного из факторов, способствующих утечке информации. Между тем, как показало проведенное исследование, дисциплинарные взыскания подчас объявляются незаконно, причем в отсутствие гласности. Это способствует формиро-

ванию ценностно-корпоративной ориентации работников в направлении ненадлежащего исполнения обязанностей. Сюда же следует отнести и нечуткое отношение отдельных руководителей к бытовым нуждам работников, о чем заявили 18% из числа опрошенных лиц.

**Группа обстоятельстве правового характера.** Это понятие объединяет недостатки в правовом регулировании на законодательном уровне и использовании правовых средств обращения КЗИ на корпоративном уровне. Связь этих обстоятельств с утечкой КЗИ состоит в том, что в результате их действия происходит нарушение принципа неотвратимости ответственности лиц, допустивших неисполнение обязанностей в данной сфере, принижается общеправовая роль Закона о коммерческой тайне и иных актов, регулирующих обращение КЗИ, вследствие чего оказывается отрицательное влияние на правосознание работников, формируется определенная «нерадивая среда» в трудовом коллективе, допускающая недобросовестное отношение отдельных работников к исполнению своих обязанностей. Рассмотрим более подробно обстоятельства правового характера.

**Во-первых, это несовершенство законодательного регулирования правовой охраны конфиденциальности КЗИ, в частности:**

а) не решены вопросы, имеющие общетеоретический характер, что не позволяет сформулировать единый подход к пониманию механизма правового регулирования обращения КЗИ и охраны ее конфиденциальности (в Законе о коммерческой тайне упущен частноправовой подход к определению понятия коммерческой тайны; институт коммерческой тайны призван защищать, прежде всего, частные интересы предпринимателей; закон не содержит положений, закрепляющих право организации на документированную информацию, содержащую коммерческую тайну, что связано с возможной ее утратой, например, при реорганизации или ликвидации юридического лица и др.);

б) в Законе о коммерческой тайне не учтены сложившейся на корпоративном уровне отношения в этой области, которые не противоречат Конституции РФ и федеральным законам (разработка печатной информации, составляющих коммерческую тайну; оформление допуска граждан к коммерческим секретам и проведение проверочных мероприятий и др.);

в) имеются пробелы в регулировании трудовых правоотношений по поводу защиты КЗИ (в законе недостаточно закреплены материальные отношения сторон по трудовому договору, в частности, не установлены обязанности работодателя по выплате вознагражде-

ния работнику, создавшему документированную информацию, имеющую коммерческую значимость, а также надбавки к должностному окладу за выполнение обязанностей по сохранности коммерческой тайны; не урегулированы гражданско-правовые отношения после прекращения действия трудового договора и др.);

г) недостаточно урегулированы взаимоотношения организаций с государственными органами и органами местного самоуправления (достаточно широкий круг государственных органов, имеющих право истребования информации, содержащей коммерческую тайну, при этом законом не установлены гарантии сохранения в тайне государственных служащими таких сведений, которые им стали известны по службе, и др.);

д) в законе не закреплена правовая статус подразделений по защите коммерческой тайны (служб безопасности) с определением основных направлений их работы, которые детализируются организацией с учетом ее специфики, порядка и объема мероприятий, связанных с допуском работников к сведениям, содержащим коммерческую тайну; не названы законные основания для отказа гражданину в допуске к таким сведениям; не определены направления прокурорского надзора за соблюдением законодательства в этой области и др.).

**Во-вторых, это несовершенство корпоративного регулирования и практики реализации корпоративных норм, в частности:**

а) корпоративное регулирование обращения КЗИ остается чрезмерно громоздким и противоречивым, несмотря на наличие Закона о коммерческой тайне, и поэтому нуждается в упорядочении допуска и доступа лиц к КЗИ, отнесения сведений к коммерческой тайне и др.;

б) недостатки, связанные с ознакомлением работников с внутренними документами об обязанностях по охране конфиденциальности КЗИ, с процедурой получения подписки о неразглашении сведений, составляющих коммерческую тайну, и др.;

в) недостатки в деятельности службы безопасности, связанные с выявлением ВКУ КЗИ, изучением причин и обстоятельств, способствующих совершению правонарушений в данной сфере, и осуществлением предупредительных мер, направленных на обеспечение безопасности.

**В-третьих, недостатки в практике применения санкций за нарушение требований режима конфиденциальности КЗИ, которые непосредственно влияют на обеспечение принципа неотвратимости наказания, создание обстановки нетерпимости к лицам, не выполняю-**

щим обязанностями по сохранению коммерческих секретов. Речь идет о работниках, состоящих в трудовых отношениях, и лицах, которым эти сведения были переданы по гражданско-правовому договору или в силу закона на основании запроса государственного органа.

Опрос лиц, нарушивших требования законодательства о коммерческой тайне, показывает, что 61% считают недостатки применения санкций, установленных правовыми нормами, регулируемыми борьбой с нарушителями режима КЗИ, обстоятельством, способствующим утечке охраняемой информации. Недостатки проявляются и в том, что неудовлетворительно ведется контрольно-проверочная работа по фиксации нарушений режима КЗИ. Лица, осуществляющие проверки, не обладают достаточными знаниями по выявлению ВКУ КЗИ, установлению лиц, допустивших нарушения. Анализируя эти недостатки, важно учитывать мнение опрошенных работников, которые отмечают, что борьба с нарушениями в сфере обращения КЗИ (наряду с нарушениями трудовой и договорной дисциплины) ведется администрацией хорошо — 41%, удовлетворительно — 42%, плохо — 3%. Недостаточное реагирование администрации на совершаемые нарушения режима КЗИ, как показывает опрос, в 52% случаев является обстоятельством, которое может привести к утечке охраняемой информации. Речь идет о неполноте использования правовых средств в пресечении правонарушений.

Рассмотренные обстоятельства не исчерпывают всей совокупности явлений, ведущих к нарушениям режима КЗИ и утечке охраняемой информации. Были рассмотрены лишь те из них, которые с наибольшей полнотой отражают специфику причин утечки охраняемой информации. Акцентирование на них внимания диктовалось не только теоретическими, но и практическими соображениями по вышению результативности аналитической работы по выявлению и предупреждению утечки КЗИ.

### § 3. Характеристика лиц, допускающих нарушения в сфере обращения коммерчески значимой информации

**Понятие личности правонарушителя режима конфиденциальности КЗИ.** Объяснение причин нарушений режима конфиденциальности КЗИ (далее — режима КЗИ) не ограничивается только названными

выше обстоятельствами организационно-управленческого, воспитательного и правового характера, содержание которых принято относить в юридической науке к социологическому аспекту проблемы<sup>1</sup>. Важным представляется рассмотрение этой проблемы и на индивидуальном (психологическом) уровне, имея в виду, что причинами таких нарушений может быть «...рассогласование поведения человека с социальной средой»<sup>2</sup>. Речь идет о работниках, имеющих доступ к КЗИ, поведение которых противоречит интересам собственника и трудового коллектива. В юридической науке изучению особенностей формирования личности правонарушителей в сфере обращения КЗИ и проявления их личностных свойств, которые имеют значение для понимания причин «отклоняющегося от социальной нормы»<sup>3</sup> поведения и организации предупредительной работы, уделяется недостаточное внимание.

Проблема личности правонарушителя режима КЗИ является частью общей проблемы изучения отклоняющегося поведения, разработка которой особенно интенсивно осуществлялась отечественными учеными в 80-х гг. XX в. (В.Н. Кудрявцев, С.В. Бородин, В.С. Нерсисян, Ю.В. Кудрявцев). В связи с этим при исследовании личности правонарушителя режима КЗИ учитывались положения, характеризующие понятие и признаки социального отклонения, их причины и механизмы поведения, отклоняющегося от нормы. Без знания этих положений, имеющих междисциплинарный комплексный подход, выявление особенностей личности правонарушителей режима КЗИ, на наш взгляд, не может быть плодотворным.

Исследования, проведенные отечественными учеными в различных областях науки, связанных с изучением поведения, отклоняющегося от нормы, позволили получить представление о специфике поведения, отклоняющегося от правовой нормы. Важное значение имело изучение образа жизни различных профессиональных групп населения, занятых в сфере экономики. Опираясь на данные многочисленных социологических и криминологических исследований, В.Н. Кудрявцев и С.В. Бородин научно обосновали, что «образ жизни человека формирует основные черты его жизненной позиции,

<sup>1</sup> См.: Общая теория государства и права: Академический курс в 3-х томах. 2-е изд., перераб. и доп. / Отв. ред. проф. М.Н. Марченко. Т. 3. М., 2001. С. 464.

<sup>2</sup> См.: Там же. С. 462.

<sup>3</sup> См.: Социальные отклонения. Введение в общую теорию. М., 1984. С. 99–121.

определяет объективные условия его существования». Именно здесь, как считают ученые, проявляются социальные позиции (статусы), конкретные интересы и возможности людей<sup>1</sup>. Полученные результаты исследований способствовали укреплению методологической базы, на которой основывается изучение механизма поведения, отклоняющегося от корпоративных норм, регулирующих сферу обращения КЗИ.

Исследование характеристики личности правонарушителей режима КЗИ имеет значение для определения конкретных практических мер и использования правовых средств борьбы с такого рода нарушениями. Знание специфических признаков (черт) этой категории правонарушителей важно для правильного выбора мер по предупреждению противоправного поведения, выявлению и устранению причин и условий, его обуславливающих.

В литературе под механизмом поведения, отклоняющегося от нормы, понимается «...взаимодействие всех тех внутренних и внешних факторов (явлений, процессов), которые определяют возникновение целей, мотивов и решимости совершить антинормативный поступок, способствуют ему, делают его практически осуществимым»<sup>2</sup>. Это определение, по существу, является общим по отношению к механизмам социальных отклонений, которые достаточно давно являются объектом исследования применительно к преступности и иным правонарушениям, включая и попытки изучения особенностей личности правонарушителей в сфере обращения КЗИ. Исходя из общего понятия «поведения, отклоняющегося от социальной нормы», *характеристика правонарушителей режима КЗИ представляет собой определенную совокупность признаков, свойств, отношений, характеризующих лицо, выполняющее конфиденциальные работы, виновно нарушающее требования законодательства и корпоративных актов, влияющих на его антиобщественное (антикорпоративное) поведение, выражающееся в невыполнении или ненадлежащем выполнении трудовых обязанностей*.

Получение характеристики на правонарушителей режима КЗИ представляет большую сложность. Это объясняется спецификой профессиональной деятельности работников, занятых в сфере обращения КЗИ, взаимодействия личности и проблемных жизненных

<sup>1</sup> См.: Социальные отклонения. Введение в общую теорию. М., 1984. С. 142.

<sup>2</sup> См.: Социальные отклонения. М., 1989. С. 171.

ситуаций, возникающих в хозяйственной деятельности по поводу охраны коммерческих секретов, имеющих значение для получения личностных характеристик правонарушителей режима КЗИ.

Методологической основой для изучения рассматриваемой категории правонарушителей служат общетеоретические положения философии, права, социологии, психологии и других гуманитарных наук по вопросу о личности как функциональной (ролевой) и социальной характеристике человека. Принципиальное значение имеет понимание личности как результирующей функции социального, биологического начал человека, определяемой совокупностью всех общественных отношений, сущности, раскрываемой в производственной деятельности людей. Как пишет А.Г. Спиркин: «Личность есть индивидуальное средоточие и выражение общественных отношений и функций людей, субъект познания и преобразования мира, прав и обязанностей, этических, эстетических и иных социальных норм, в том числе и юридических. Личностные качества человека есть производное от двух моментов: от его самосознющего разума и от его социального образа жизни. Полеми проявлению личностных свойств служит его социальная жизнь»<sup>1</sup>. В философской литературе отмечается, что свойства личности могут быть различными — более или менее яркими, глубокими, оригинальными, но их наличие неизбежно обязательно в каждом человеке.

Среди юридических наук наибольших успехов в изучении поведения, отклоняющегося от нормы, по оценке В.Н. Кудрявцева, достигли криминологи<sup>2</sup>. При изучении личности преступника наука криминология исходит из того, что формирование личности — результат воздействия на человека многоплановых факторов социальной действительности. Личность рассматривается в контексте и с учетом конкретно-исторических условий ее формирования. Как отмечают В.Н. Кудрявцев и Ю.М. Антонян, «личность преступника можно охарактеризовать как некую модель, социальный и психологический портрет, обладающий специфическими чертами. Преступникам присущи антиобщественные взгляды, отрицательное отношение к нравственным ценностям и выбор общественно опасного пути для удовлетворения своих потребностей. Криминологическое изучение личности преступника осуществляется главным образом для вы-

<sup>1</sup> Спиркин А.Г. Философия: Учебник. 2-е изд. М., 2002. С. 328.

<sup>2</sup> См.: Социальные отклонения. С. 11–15, 181.



явления и оценки тех ее свойств и черт, которые порождают преступное поведение, в целях его профилактики»<sup>1</sup>. При оценке личности наряду с уровнем общественного сознания человека важно учитывать психические процессы, обуславливающие его поведение. Указанные положения о личности в обществе позволяют с достаточной степенью научности подойти к раскрытию характеристики правонарушителей режима КЗИ.

Первичная «клеточка» нарушения режима КЗИ, являясь частью социальных отклонений, имеющих место в обществе, — поступок конкретного индивида, нарушающего правовые нормы законодательства и корпоративные нормы в сфере обращения такой информации. Как отмечает В.Н. Кудрявцев, социально отклоняющееся поведение складывается из взаимодействия трех групп явлений: социальные нормы; свойства личности; особенности конкретной ситуации. Каждая из групп «образует» внешними и внутренними обстоятельствами места и времени. В дисгармонии этих элементов и лежит, как правило, основные причины отклонений. Первая из них — это несоответствие нормы требованиям жизни, вторая — несоответствие требований жизни интересам данной личности<sup>2</sup>. Применительно к целям данного исследования речь идет о противоречии частных интересов собственника и личных интересов наемного работника в сфере обращения КЗИ, об издании корпоративных норм, которые не в полной мере учитывают интересы наемных работников о действиях объективных и субъективных факторов, способствующих совершению индивидуумом антикорпоративного поступка.

Признаки, образующие характеристику правонарушителей режима КЗИ, необходимо рассматривать с позиций их связи с антикорпоративным поведением, которое может привести к утечке охраняемых сведений. Сами по себе, без привязки к анализу правонарушений режима КЗИ, эти признаки с точки зрения их учета в предупредительной работе значения не имеют.

Установление особенностей личности правонарушителей режима КЗИ строилось на основе исследования элементов, образующих структуру личности, в качестве которых выделяются: социально-демографические признаки, социальные проявления в различных

<sup>1</sup> См.: Криминология: Учебник / Под ред. В.Н. Кудрявцева и В.Е. Эминова. 3-е изд., перераб. и доп. М., 2004. С. 152.

<sup>2</sup> См.: Социальные отклонения. М., 1984. С. 187 и далее.

сферах деятельности организаций; нравственные свойства, психологические особенности<sup>1</sup>.

Данная схема представляется достаточно удобной для анализа характеристики личности правонарушителя режима КЗИ. Раскрываемые на ее основе личностные характеристики могут быть плодотворно использованы для решения задач по выявлению возможных каналов утечки (ВКУ) охраняемой информации и воздействию на факторы, их обуславливающие.

**Социально-демографические признаки** позволяют получить представление о типичных признаках лиц, совершивших нарушения режима КЗИ, однако эти особенности не являются такими, которые отличали бы от законопослушных граждан. В.Н. Кудрявцев отмечает, что «...демографические данные личности никогда не могут быть причиной правонарушений»<sup>2</sup>. Результаты проведенного исследования подтверждают общий вывод ученых о том, что «демографические обследования не раскрывают механизмов отклоняющегося поведения, они лишь указывают на статистическое преобладание среди нарушителей социальных норм тех или иных категорий граждан»<sup>3</sup>. Эти признаки тесно взаимосвязаны с правовыми и нравственно-психологическими признаками, которые в целом дают представление о социальном облике лиц, занятых в сфере обращения КЗИ. Однако нельзя говорить о существовании какого-то социального типа личности, нарушающего требования режима КЗИ, даже в условиях существования противоречия между частными интересами организации и личными интересами наемных работников.

Говоря о распределении лиц, совершивших правонарушения режима КЗИ, *по полу*, необходимо отметить, что по совокупным результатам анкетирования личных дел на правонарушителей, которые были заняты в различных сферах материального производства: 65% из них составили мужчины и 35% — женщины. По сравнению с этими данными, доля мужчин в промышленности, а женщин в торговле является доминирующей, что объясняется, во-первых, существованием определенной закономерности в численном соотношении муж-

<sup>1</sup> См.: Личность преступника, М., 1975. С. 31–32; Социальные отклонения. М., 1989. С. 180–190; Криминология / Под ред. В.Н. Кудрявцева и В.Е. Эминова. М., 2004. С. 155–165, и др.

<sup>2</sup> Кудрявцев В.Н. Причины правонарушений. М., 1976. С. 126–127.

<sup>3</sup> См.: Социальные отклонения. М., 1989. С. 181.

чин и женщин, занятых в различных отраслях экономики, например, промышленности и торговле. Традиционно, в силу специфики труда, доля работающих женщин в торговле значительно выше. Во-вторых, преобладанием на конкретных участках производства среди работающих, имеющих доступ к КЗИ, лиц мужского пола (выборочный анализ ряда организаций, занятых в сфере производства, показывает, что в числе работников, имеющих отношение к сфере обращения КЗИ, лица мужского пола составили — 54%, женского — 46%). Объявляя количественное соотношение числа мужчин и женщин, допустивших нарушения в сфере обращения КЗИ, следует подчеркнуть, что не существует какой-либо биологической обусловленности правонарушений мужчин и женщин с позиций различной их физиологии и психологии. Вместе с тем «было бы ошибочно недооценивать биологические особенности женского организма, которые в значительной мере предопределяют выбор женской профессии, выполнение ею определенных функций, социальных ролей»<sup>1</sup>, что следует учитывать при проведении воспитательной работы в трудовых коллективах.

*Возраст* имеет значение для понимания социально-психологического облика лиц, совершивших правонарушения в сфере обращения КЗИ. Исследование показало, что существует определенная закономерность в совершении нарушений режима КЗИ различными возрастными группами. Возрастная характеристика лиц, допустивших нарушения в сфере обращения КЗИ, определяется следующими данными. В возрасте от 18 до 20 лет совершили правонарушения режима КЗИ (пропускного режима) 1%, от 21 до 25 лет — 4%, от 26 до 35 лет — 35%, от 35 до 40 лет — 20%, от 40 до 49 лет — 25%, от 50 до 55 (жен.) лет — 3%, от 50 до 60 (муж.) лет — 10%. Опрос законопослушных граждан показал, что с конфиденциальными документами и изделиями в обследованных организациях трудятся работники в возрасте от 18 до 21 года — 2%, от 21 до 35 лет — 30%, от 35 до 49 лет — 44%, от 49 до 60 лет — 20%, от 60 лет и старше — 5%.

Таким образом, нарушения режима КЗИ совершают чаще всего лица в молодом и зрелом возрасте. При объяснении интенсивности проявления нарушений режима КЗИ среди различных возрастных групп следует учитывать, что, *во-первых*, как указывал И.И. Карпец,

<sup>1</sup> См.: Дубинин Н.П., Карпец И.И., Кудрявцев В.Н. Генетика, поведение, ответственность. М., 1982. С. 125.

«старение человека (биологически) тоже вызывает определенные изменения, влияющие на его взгляды, наконец, на способность к активной общественной деятельности»<sup>1</sup>. Хотя этот признак и не является значимым, позволяющим проводить различия между теми, кто соблюдает установленный режим КЗИ, и теми, кто его нарушает<sup>2</sup>. Психологическая наука подтверждает наличие специфических свойств личности индивида, его психики, закономерно изменяющихся в процессе смены возрастных стадий развития человека<sup>3</sup>, что свидетельствует о необходимости учета рекомендаций по работе с различными возрастными группами в процессе охраны КЗИ.

*Во-вторых*, значительный процент нарушений (35%) отмечается в возрастной группе работников, имеющих доступ к КЗИ, от 26 до 35 лет (муж.), что объясняется общей тенденцией «омоложения» руководящих кадров и менеджеров в коммерческих организациях. В-третьих, наибольшее число нарушений приходится на возрастную группу 35—49 лет, которая отличается определенным опытом работы, хорошим знанием специфики производства и стабильным характером социальных связей. В юридической науке существует устойчивее мнение, что причиной такого явления является не возраст правонарушителей, а уровень их правосознания<sup>4</sup>.

*Уровень образования* лиц, совершивших нарушения режима КЗИ, является достаточно высоким и характеризуется следующими данными: выборочного изучения: 70% имели высшее образование, 20% — среднее профессиональное, 5% — среднее полное общее образование и 5% неполное среднее образование. Высокий уровень образования объясняется тем, что половина из них являлись руководителями среднего и высшего звена управления, остальная часть — менеджеры и специалисты, условия назначения на должность которых требуют наличия диплома о высшем образовании. Важно подчеркнуть наличие определенной связи низкого качества профессиональной подготовки, которое проявляется в процессе выполнения обязанностей, и допускаемыми ошибками в работе. Недостатки могут быть связа-

<sup>1</sup> См.: Карпец И.И. Проблема преступности. М., 1967. С. 78—79.

<sup>2</sup> См.: Социальные отклонения. М., 1989. С. 188.

<sup>3</sup> См.: Теория личности / Под ред. проф. В.Ф. Сержантова. Л., 1989. С. 35—40, и др.

<sup>4</sup> См.: Карпец И.И., Рапинов А.Р. Правосознание и причины преступности // Советское государство и право. 1968. № 12, и мн. др.

ны с образованием ВКУ КЗИ в том случае, если работник выполняет определенную трудовую функцию в сфере обращения КЗИ. Нужно иметь в виду, что высокий уровень образования не определяет, с точки зрения требований корпоративных норм, правильное, т.е. соответствующее интересам организации, поведение. Он может оказывать при прочих условиях положительное влияние на формирование потребностей, интересов, ценностных ориентаций.

Для выявления особенностей данной категории правонарушителей имеет значение анализ соответствия специальности, полученной лицом в высшем учебном заведении, и должности, занимаемой им в структуре управления организацией. Данные выборочного опроса работников показывают, что почти 80% из них работают не по специальности. Это объясняется тем, что, во-первых, ликвидирована ранее существовавшая в СССР система государственного распределения выпускников вузов, во-вторых, трудоустройство в сферах бизнеса ведется в основном при наличии родственных и приятельских связей, порой без учета профессиональных требований, по принципу принадлежности делу хозяина. С одной стороны, это положительно сказывается на обеспечении сохранности имущества, включая коммерческие секреты. С другой стороны, связано с неумением выделить таковыми работниками КЗИ в силу имеющихся пробелов в знаниях, что отрицательно сказывается на обеспечении «технологического» пролива» в производстве за счет использования КЗИ.

Оценка степени ущерба организации, причиненного разглашением (утечкой) КЗИ, имеет определенную связь с *должностным положением работника*. Анализ показывает, что на момент нарушения режима КЗИ работники занимали должности руководителей различных звеньев — 39%, специалистов — 58%. Существует определенная зависимость вредных последствий от объема выполняемых обязанностей в сфере обращения КЗИ. Оценка возможного ущерба от разглашения КЗИ может производиться путем сопоставления содержания должностных инструкций и положений о подразделениях с перечнем сведений, составляющих коммерческую тайну организации.

Для выявления и предупреждения правонарушений в этой сфере необходимо различать признаки невыполнения или *ненадлежащего выполнения работниками обязанностей по охране КЗИ*. Невыполнение обязанностей характеризуется более выраженной деформацией ценностных ориентаций личности и выявляется руководством значительно чаще, так как находится на виду и легко воспринимается лицом, осуществляющим контроль за работником. Ненадлежащее

выполнение обязанностей скрыто от окружающих. Лицо действует, но как бы не «в полную» силу, то есть осуществляет возложенную на него работу не в полном объеме и не так, как этого требуют корпоративные нормы. Своей «мнимой» деятельностью оно способно вводить в заблуждение непосредственных руководителей, порождать у них уверенность в надлежащем обеспечении безопасности соответствующего участка и, исходя из этого, не вызывать тревоги при фактически имеющем место ослаблении контроля за деятельностью подчиненных лиц. Такая деятельность, по указанным причинам, может продолжаться длительный период и причинить значительный ущерб организации от утечки КЗИ. Поэтому усилия администрации следует сосредоточить на установлении признаков, свидетельствующих о ненадлежащем выполнении работниками обязанностей в сфере обращения КЗИ.

*Изучение нравственно-психологических черт лиц, совершивших правонарушения в сфере обращения КЗИ*, имеет значение для познания внутреннего мира работников, не выполняющих требования корпоративных норм по охране КЗИ, для определения причин таковых социальных отклонений и их предупреждения<sup>1</sup>. Нравственно-психологическая основа во многом определяет стиль и методы работы лиц, занятых в производстве товаров с использованием КЗИ. Наличие психологических особенностей не позволяет проводить «различий между теми, кто соблюдает социальную норму, и теми, кто ее нарушает»<sup>2</sup>. Динамические особенности психических процессов могут оказывать влияние на формирование потребностей и интересов, мотивов и целей поведения, на принятие и осуществление решения о совершении поступка<sup>3</sup>. Тем не менее, они еще недостаточно изучены в юридической науке. Их анализ отличается значительной сложностью в получении фактического материала и отсутствием методики. Исследование нравственно-психологических черт лиц, совершивших правонарушения в сфере обращения КЗИ, осуществляется на основе *анализа их потребностей, интересов, ценностных ориентаций, психологических особенностей*, являющихся, по мне-

<sup>1</sup> См.: Сахаров А. Б. Актуальные вопросы учения о личности преступника // Теоретические проблемы учения о личности преступника. М., 1979. С. 17; Социальные отклонения. М., 1989. С. 182–190, и др.

<sup>2</sup> См.: Дубинин Н.П., Карпец И.И., Кудрявцев В.Н. Генетика, поведение, ответственность. М., 1982. С. 28.

<sup>3</sup> См.: Социальные отклонения. М., 1989. С. 188.

нию ученых-психологов, важнейшими признаками в психологической структуре личности<sup>1</sup>.

Анализ данных показывает, что работники, допустившие дисциплинарные поступки в этой сфере, по данному признаку имеют определенные отличия от законопослушных граждан. Отличия состоят в характере проявления социальных потребностей, в различии степени осознания лицами потребностей в труде, в определении путей его удовлетворения, в различном отношении к соблюдению корпоративных норм. Анализируя потребности работников наемного труда, которые имеют доступ к КЗИ, следует исходить, во-первых, из того, что потребности имеют биологическую (питание, самосохранение и др.) и социальную природу (потребности в труде, познании, общении и др.)<sup>2</sup>. Во-вторых, наемный труд гражданина означает, что работник применяет свои способности к труду за вознаграждение в интересах работодателя.

Показательно, что большинство работников, допустивших нарушения в сфере обращения КЗИ, были ознакомлены с обязанностями, однако игнорировали их выполнение, о чем имеются ссылки в приказах организации, знали их содержание поверхностно или вообще не знали. Об этом содержались сведения в письменных объяснениях работников, подвергнутых дисциплинарным взысканиям.

Опрос нарушителей показал, что у них было недостаточно конкретное, расплывчатое представление об обязанностях по охране КЗИ, и поэтому, по их мнению, они совершили нарушения. Опрос работников, не совершавших такие нарушения, показал, что треть из них не могли точно сформулировать свои служебные обязанности. Отсюда вывод о том, что у работников, допустивших утечку КЗИ, насколько принижено чувство ответственности. Являясь работниками наемного труда, они игнорируют корпоративные нормы, при этом легкомысленно рассчитывают предотвратить возможный ущерб, который может наступить вследствие невыполнения обязанностей по охране КЗИ.

Изучение дисциплинарной практики и опрос работников указывают на наличие у лиц, совершивших правонарушения в этой

сфере, специфического отношения к исполнению своих обязанностей. В рыночной экономике труд воспринимается работодателем и работником исключительно сквозь призму его оплаты. В результате произошло смещение акцентов в понимании работниками социальной значимости труда, его материальной оценки. Поэтому *оплата труда существенно влияет на качество труда при возложении обязанностей по охране КЗИ*. Связь этого фактора с возможностью утечки КЗИ может проявляться двояко. С одной стороны, в случаях, когда работодатель не оплачивает эту работу, работник ее просто не выполняет. При этом действует на законных основаниях. С другой стороны, когда оплата производится явно в заниженном, по меркам работника, размере, то работа выполняется не в полном объеме, по принципу «как платят, так и работаем». В любом случае игнорирование работником обязанностей по охране КЗИ ведет к открытию ВКУ такой информации. Материальный интерес работника часто связан с продвижением его в иерархии управления компанией. Если по каким-либо причинам такое продвижение невозможно, то может возникнуть равнодушное и связанное с ним безответственное отношение к исполнению трудовой функции. Формирующийся в таких условиях стиль работы может привести к созданию опасных ситуаций для разглашения КЗИ. Для предупреждения подобного нежелательного явления необходимо совершенствовать систему оплаты и стимулирования труда, что будет препятствием на пути возникновения ВКУ КЗИ.

При изучении отношения лиц к труду важно учитывать такой показатель, как *степень удовлетворенности трудом*. Значительному числу лиц, допустивших нарушения в сфере обращения КЗИ, работа, по их мнению, не принесла полного удовлетворения (об этом заявили 40% опрошенных) в силу невозможности применения на практике знаний, полученных в вузе, принятия на себя обязанностей, к которым лицо не было подготовлено, назначения на должность лиц, представлявших себя в иной социальной роли. Однако они готовы продолжить работу, поскольку нет другой и их устраивает оплата.

На удовлетворенность работой в значительной мере, по мнению большинства опрошенных работников, влияет *стиль руководства*. Субъективные недостатки руководства порой вызывают отрицательные чувства у подчиненных, ведут к безответственности. Неудовлетворенность работой в связи с низкой оплатой труда, о чем заявили более 50% опрошенных лиц, совершивших нарушения в сфере обра-

<sup>1</sup> См.: Ковалев А.Г. Психология личности. 3-е изд. М., 1970. С. 44; Асмолов А.Г. Личность как предмет психологического исследования. М., 1984. С. 36–75, и др.

<sup>2</sup> См.: Дубинин Н.П., Карпец И.И., Кудрявцев В.Н. Генетика, поведение, ответственность. С. 180–181.

шения КЗИ, может влиять на качество выполняемых обязанностей по охране такой информации.

Опрос работников показал, что и в рыночной экономике *соблюдение требований норм морали* является непременным условием успешной работы менеджера. Руководитель, помимо профессиональной компетентности, должен иметь авторитет среди работников, который влияет на четкость его работы. Если он утратил его, то ему очень трудно осуществлять руководство людьми. Связь этого фактора с возможностью открытия каналов утечки КЗИ проясняется в том, что руководители, утратившие авторитет, имеющие плохие отношения с подчиненными, не считающиеся с их мнением, ведущие себя высокомерно и нетактично, не могут рассчитывать на взаимопонимание и доверие со стороны работников, допущенных к КЗИ.

*Характеристика интересов работника*<sup>1</sup> в определенной мере может быть рассмотрена на базе показателей о его трудовом стаже. Трудовой стаж лиц, допустивших правонарушения в сфере обращения КЗИ, составлял в большинстве случаев из числа выборочно изученных материалов дисциплинарной практики от 2 до 5 лет. Связь показателей трудового стажа с нарушениями режима КЗИ может быть объяснена с позиций вхождения человека в сферу выполнения трудовых функций, социальной адаптации лиц, склонных к правонарушениям в производственной обстановке. Около 80% опрошенных руководителей заявили, что человек, пришедший в трудовую коллектив после окончания вуза и впервые выполняющий трудовые функции, как правило, с интересом относится к работе. В основе его деятельности — новизна и творчество, стремление к четкому соблюдению норм. Попадая в обстановку, где отсутствует профессиональный подход к делу и царит косность, нерадивость и застой в работе, эти лица со временем способны пересматривать свои взгляды, причем трансформация может происходить как в положительном, так и в отрицательном плане по отношению к соблюдению трудовой дисциплины и охране КЗИ. Поэтому нужно менять, прежде всего, обстановку, которая отрицательно влияет на правосознание работников.

Далее, каждый работник, занимающий должность, смотрит на нее сквозь призму личных, и, прежде всего, материальных интере-

<sup>1</sup> См.: *Здравомыслов А.Г.* Проблема интереса в социологической теории. Л., 1964. С. 18–28, и др.

сов, удовлетворение которых обеспечивает его плодотворный труд. Изучение дисциплинарной практики перехода работников, совершивших проступки в сфере обращения КЗИ, с одного места работы на другое показывает, что если материальное положение больше не удовлетворяло их, то такие лица либо увольнялись в поисках более высокооплачиваемой работы, либо трудовая активность их ставила крайне низкой. В отдельных случаях, если им не удавалось занять более высокооплачиваемую должность, то такие работники начинали относиться к работе небрежно и безразлично, что отрицательно отражалось на охране КЗИ и могло привести к ее утечке. Опрос работников контрольной группы показал, что материальная заинтересованность играет для них весьма существенную, но, тем не менее, не главную роль при определении их поведения. Об этом заявили 60% опрошенных лиц. Для большинства из них на первом месте была интересная работа (70%), возможность сделать для «родной» организации что-то полезное (40%). Представляется, что с повышением трудового стажа при неблагоприятных условиях, то есть недостаточном стимулировании труда и отсутствии должной воспитательной работы, вероятность совершения правонарушений в сфере обращения КЗИ может быть повышенной. Эта связь должна учитываться администрацией в предупредении правонарушений в этой сфере.

*Ценностные ориентации*<sup>1</sup> дают представление о глубокой внутренней структуре личности, они в наиболее полном виде отражают отношение человека к окружающему миру. Сравнение исследовательских данных позволяет сделать вывод о том, что ценностные ориентации<sup>2</sup> у работников, совершивших дисциплинарные проступки в сфере обращения КЗИ, в отличие от работников контрольной группы, были сосредоточены на обеспечении себе «достойной заработной платы», которая ниже их прожиточного уровня.

В данном случае *интересы* работников находятся в диалектической связи с их *потребностями*<sup>3</sup>. Это проявлялось в содержании

<sup>1</sup> См.: *Водзинская В. В.* Понятие установки, отношения и ценностной ориентации в социологическом исследовании // *Философские науки*. 1969. № 2. С. 50–54, и др.

<sup>2</sup> См.: *Кудрявцев В. Н.* Правовое поведение: норма и патология. М.: Наука, 1982. С. 161–162, и др.

<sup>3</sup> См.: *Кудрявцев В. Н.* Взаимосвязь правового регулирования и социальных интeрeсов // *Вопросы философии*. 1987. № 1, и др.

принимаемых правонарушителями решений, которые не согласовывались с возложенными на них обязанностями по работе и вели порой к утечке КЗИ. Производственная обстановка оценивалась ими только с этой позиции. Ради «достойной зарплаты» они сознательно шли на нарушения законов и корпоративных норм при обращении КЗИ, подчас полагая, что их действия не могут причинить ущерб организации. И только наступление вредных последствий от утечки КЗИ убеждало их в неправомерности своих действий.

Данные опроса показывают, что для них характерным было большее число отвергаемых корпоративных норм, в частности — 30% лиц, совершивших проступки в этой сфере, не знали содержание корпоративных актов и не стремились с ними ознакомиться, 50% — знали нормы, но игнорировали их выполнение. Опрос работников контрольной группы показал, что 50% из них знали содержание корпоративных актов и соблюдали их требования, 35% не знали содержание актов, но стремились с ними ознакомиться. Сравнение этих данных дает основание говорить, что лица, совершившие дисциплинарные проступки, имеют некоторые *дефекты нравственно-правового сознания*<sup>1</sup> в ценностных ориентациях, чем те лица, которые не совершили такие проступки. В этой связи представляется учет ценностно-нормативных представлений работника о корпоративных нормах и отношении к ним. Как отмечает В. Н. Кудрявцев, что без мировоззренческой позиции лица невозможно его ориентация в «нормативной среде». Искажение мировоззренческой позиции, тесно связанной и с деформацией ценностных ориентаций личности, служит важнейшим показателем склонности лица к антинормативному (*антикорпоративному*. — Прим. авт.) поведению<sup>2</sup>.

В отношении лиц, совершивших преступление, учеными было введено понятие *антиобщественной (антисоциальной) установки*<sup>3</sup>, для которой «специфичны отрицание тех или иных общепризнанных ценностей, антиобщественный характер мотивов и целей пре-

ступного поведения»<sup>1</sup>. Однако в последующий период криминологи отказались от использования этого понятия при характеристике личности преступника<sup>2</sup>. Такой подход объясняется тем, что еще в конце 80-х гг. XX в. В. Н. Кудрявцев<sup>3</sup> подвергнул критике столь категоричную позицию А. Р. Ратникова, который утверждал, что субъект, «вступив в самый острый конфликт с обществом, должен чем-то отлучиться от социального норматива по своему пониманию смысла жизни»<sup>4</sup>.

По мнению В. Н. Кудрявцева, «нет такого единственного (и единого) свойства личности, которое вызывало бы отклоняющееся поведение и отличало бы лиц, склонных к такому поведению, от лиц, соблюдающих социальные нормы»<sup>5</sup>. Далее В. Н. Кудрявцев подчеркивает, что «личностные свойства субъекта, совершившего проступок, отклоняющийся от социальной нормы, могут быть описаны в широком диапазоне, начиная со стойкой антиобщественной установкой и кончая такими качествами, которые мало чем отличаются от субъекта от лиц, соблюдающих закон»<sup>6</sup>.

Расматривая антисоциальную (антикорпоративную) установку лица, совершившего дисциплинарный проступок в сфере обращения КЗИ, следует иметь в виду, что она представляет собой не просто готовность, а избирательную готовность действовать соответствующим образом<sup>7</sup>, вопреки частным интересам собственника. Специфика ее заключается в том, что под воздействием деформированных элементов, входящих в ценностно-нормативную систему, при соответствующей хозяйственной ситуации и в определенной среде у лица отсутствует установка на добросовестное выполнение трудовой функции, связанной с охраной КЗИ. Свою психическую энергию лицо не

<sup>1</sup> См.: Кудрявцев В. Н., Кудрявцев Ю. В., Нересяни В. С. Социальные отклонения. Введение в общую теорию. М., 1984. С. 204; Социальные отклонения. М., 1989. С. 185.

<sup>2</sup> См.: Криминология: Учебник / Под ред. В. Н. Кудрявцева и В. Е. Эминова. М., 2004. С. 150–196.

<sup>3</sup> См.: Социальные отклонения. М., 1989. С. 185.

<sup>4</sup> См.: Ратников А. Р. К ядру личности преступника // Сб.: Актуальные проблемы уголовного права и криминологии. М., 1981. С. 81–85.

<sup>5</sup> См.: Социальные отклонения. М., 1989. С. 185.

<sup>6</sup> См.: Там же. С. 185–186.

<sup>7</sup> См.: Ойгензихт В. А. Воля и волеизъявление (очерки теории, философии и психологии права). Душанбе: Дониш, 1983. С. 36.

<sup>1</sup> См.: Социальные отклонения. М., 1989. С. 184, и др.

<sup>2</sup> См.: Там же. С. 185.

<sup>3</sup> См.: Сахаров А. Б. О личности преступника и причинах преступности в СССР. Госюриздат. 1961. С. 58–59, 172–195; Ратников А. Р. К ядру личности преступника // Сб.: Актуальные проблемы уголовного права и криминологии. М., 1981. С. 81; Курс советской криминологии. 1985. С. 354–357.

направляет на качественное выполнение обязанностей, вследствие чего выполняет их с отклонениями от действующих норм, что может привести к утечке информации. Пренебрегая своими обязанностями по работе и, следовательно, избирая объективно опасный курс действий, лицо не придает устоявшему в организации режиму охраны КЗИ большого значения и ввиду этого не выполняет или неадекватным образом выполняет свои обязанности. Важным представляется выявление администрации лиц с подобной установкой и проведение с ними предупредительной работы.

Важнейшие выводы науки<sup>1</sup> о том, что «личность изменчива; нет неисправимых нарушений социальных норм», «отклонение от социальной нормы может быть совершено и без прямого воздействия конкретной жизненной ситуации», «динамические особенности психических процессов могут оказывать влияние на формирование потребностей и интересов, мотивов и целей поведения, но они не определяют его социальную направленность и содержание» с достаточной наглядностью проявляется в профессиональной деятельности лиц, связанных с охраной КЗИ.

Переход к рыночной экономике в условиях информационной революции отразился на увеличении степени напряженности человеческой деятельности. Все более сложным становится процесс производства товаров, представляющий повышенные требования к интеллектуальным, эмоциональным и волевым качествам человека, связанным с обеспечением безопасности организации.

Изучение показывает, что руководители отдельных предприятий не обладали необходимым мышлением для реализации конкурентной стратегии, не умели сосредоточить внимание на главных вопросах и распределить объем работы, не отличались психической выносливостью, настойчивостью и решительностью, формирование которых зависело от индивидуальных особенностей их нервной системы?<sup>2</sup>

При оценке роли психологических особенностей личности в генезисе механизма поведения, отклоняющегося от корпоративной нормы, следует иметь в виду, что «то, с чем один тип характера в повсед-

невной жизни справляется легко, для другого может оказаться затруднительным или вообще невозможным»<sup>1</sup>. В этом плане характерным является то, что наблюдавшаяся несостоятельность части лиц, допустивших нарушения в сфере обращения КЗИ, перед начинающейся хозяйственной ситуацией, к которой лицо не было внутренне подготовлено, вызывало, по всей видимости, у них психическое и физическое перенапряжение, сниженную устойчивость к эмоциональным нагрузкам, слабость психологической личностной защиты<sup>2</sup>, которые хотя и могли быть преодолены при надлежащем отношении к служебным обязанностям<sup>3</sup>, в последующем были связаны с принятием неправильных решений по передаче контрагентам КЗИ, закрытию ВКУ информации. Значительное число (85%) опрошенных работников заявили, что в начале и в конце рабочего дня достаточно точно можно наблюдать признаки перенапряжения в работе. Это проявляется в недостаточной способности концентрировать внимание на выполнении конкретного дела, в рутинных действиях и равнодушном отношении к работе, в снижении способностей к координации действий, в отвлечении внимания на мелочи, в непунктуальности, в повышенной раздражительности и апатии. Из этого вытекает, что в этот период может допускаться наибольшее число упущений и недостатков в работе, включая и реализацию мер по охране КЗИ.

Следует также иметь в виду, что *определенная степень перенапряжения в работе* лиц определяется понятием «стресс», причины которого различны. Наиболее характерными, по мнению опрошенных лиц, являются слишком высокие требования к лицу, большое количество служебных поручений, неурядицы в семейной жизни, плохое состояние здоровья и т. д., которые, вместе взятые, могут вызвать стрессовые состояния у работников. Указанные причины, как правило, действуют в совокупности. Ситуация, при которой наступит стресс, в большей степени способствует уклонению от требуемого порядка охраны КЗИ, чем просто перенапряжение в работе, и таким образом обнаруживает более тесную связь с правонарушениями

<sup>1</sup> См.: Полис А.Ф. Единство социального и биологического в гармоническом развитии личности. Рига, 1981. С. 186.

<sup>2</sup> См.: Платонов К.К. Структура и развитие личности. М., 1986. С. 90–112, и др.

<sup>3</sup> См.: Русаков В.М. Биологические основы индивидуально-психологических различий. М., 1979. С. 258, и др.

в этой сфере. Опрос работников показал, что руководители высшего и среднего звена и их заместители испытывали перегрузки в два раза выше, чем руководители нижнего звена. Этому в значительной мере способствовали слабое организационное построение структуры управления, плохая согласованность и недостаточная продуманность поставленных перед ними задач, а также ограничение прав в принятии самостоятельных решений, обилие распоряжений с установлением нереальных сроков исполнения.

Исследование показало, что у большинства работников, допустивших нарушения в этой сфере, преобладала *завышенная или заниженная самооценка своих сил и возможностей*<sup>1</sup>, которые не всегда подкреплялись объективными данными, вследствие чего терялся самоконтроль, и вырабатывалось искаженное отношение к своим поступкам. Это проявлялось в наличии определенных трудностей в отношениях между членами трудового коллектива, влиявшими на выполнение ими обязанностей по работе, связанной с охраной КЗИ.

Администрация, осуществляющей профилактику правонарушений в сфере обращения КЗИ, следует иметь в виду, что для лиц, совершивших этот проступок, характерно наличие комплекса отрицательных свойств и качеств, позволяющих выделить их в отдельную категорию правонарушителей. В числе характерных следует выделить специфическое отношение к труду, нежелание трудиться в полную силу, преобладание личных интересов над корпоративными, недостаточное волевое усилие лица по выполнению трудовых обязанностей, недисциплинированность, легкомыслие, эмоциональная неустойчивость и другие признаки. Рассмотренные группы признаков тесно взаимосвязаны и обеспечивают целостную характеристику лиц, допускающих проступки в сфере обращения КЗИ только в их совокупности. Они могут рассматриваться в качестве информационной модели данного типа личности правонарушителя, то есть абстрактного описания комплекса его особенностей, которые имеют значение для понимания причин этого вида правонарушений, организации и проведения предупредительной работы. Опираясь на них, администрация в состоянии существенно расширить свои возможности по дифференцированному выбору эффективных мер предупреждения таких нарушений.

<sup>1</sup> См.: Столин В.В. Самосознание личности. М.: Изд-во Моск. ун-та. 1983. С. 7, 76–77; Спиркин А.Г. Философия: Учебник. М., 2002. С. 353–361, и др.

#### § 4. Предупреждение правонарушений в сфере обращения коммерчески значимой информации

*Понятие предупреждения правонарушений в сфере обращения коммерчески значимой информации* является составной частью понятийного аппарата механизма правового регулирования обращения КЗИ и охраны ее конфиденциальности в рассматриваемой области общественных отношений. Предупреждение правонарушений в сфере обращения КЗИ является в современных условиях главным направлением обеспечения безопасности корпоративных образований.

Выдвижение профилактики правонарушений, совершаемых в сфере обращения КЗИ, на первый план обусловлено формируемой в России стратегией инновационного прорыва<sup>1</sup>, важную роль в котором играет высокотехнологичный комплекс, определяющий модернизацию экономики. По этому пути идет и действующее законодательство, которое регулирует баланс интересов обладателей информации, составляющей коммерческую тайну, и других участников на рынке товаров, работ и услуг. Пункт 5 части 1 ст. 14 Федерального закона от 26 июля 2006 г. № 135-ФЗ «О защите конкуренции»<sup>2</sup> прямо устанавливает запрет на недобросовестную конкуренцию, которая проявляется в незаконном получении, использовании, разглашении информации, составляющей коммерческую и иную охраняемую законом тайну. Закон о коммерческой тайне (ч. 6 ст. 11) обязывает руководителя организации обеспечить охрану конфиденциальности информации, обладателем которой являются организация и ее контрагенты, однако не раскрывает способы предупреждения недобросовестной конкуренции.

В литературе наряду с термином «предупреждение» встречаются термины: «профилактика», «предотвращение», в понятие которых иногда вкладывается различное содержание. Исходя из значения этих слов, представляется, что они несут одну и ту же смысловую нагрузку, а именно: не допустить возникновения правонарушения, вследствие чего употребляются нами в тексте как идентичные.

<sup>1</sup> См.: Кузык Б.Н., Яковец Ю.В. Россия — 2050: стратегия инновационного прорыва. М., 2005. С. 179–243; Разработка правовых механизмов инновационного развития российского государства / Под ред. проф. С.А. Авакьяна. М.: Изд-во Вегн Group, 2008. С. 5–92, и др.

<sup>2</sup> См.: СЗ РФ. 2006. № 31 (ч. 1). Ст. 3434.



В юридической науке не выработано единого понятия «предупреждение правонарушений в сфере обращения КЗИ». Часть четвертая ГК РФ (ст. 1465) содержит положение о том, что обладатель сведений, составляющих секрет производства (ноу-хау) вводит в отношении таких сведений режим коммерческой тайны. В ст. 10 Закона о коммерческой тайне перечислены меры по охране конфиденциальности информации, принятие которых означает установление в организации режима коммерческой тайны. В этой связи возникает вопрос, носят ли эти меры предупредительный характер или их задача состоит в организационном обеспечении установленного режима коммерческой тайны. Для выяснения этого вопроса необходимо рассмотреть понятие предупреждения правонарушений в сфере обращения КЗИ. Базовым, данное понятие играет существенную роль для освещения всех важнейших аспектов проблемы.

Представляется очевидным, что *понятие предупреждения правонарушений в сфере обращения КЗИ* должно исходить, во-первых, из общего понятия юридического конфликта<sup>1</sup> и предупреждения социальных отклонений, с учетом развитых организационных форм общей и специальной профилактики<sup>2</sup>. Во-вторых, предупреждение правонарушений в этой сфере относится к деятельности организации и должно рассматриваться с учетом ее взаимосвязи с поведением работников. По существу, речь идет о предупреждении правонарушений в сфере обращения КЗИ на корпоративном и индивидуальном уровне. Хотя нельзя не учитывать и общеупреждающую роль государства и, прежде всего, законодательства, регулирующего отношения в сфере обращения КЗИ.

В *общей теории права* понятие «предупреждение правонарушений» рассматривается в рамках категории «профилактика юридического конфликта», под которой, как отмечал В.П. Казимирчук, понимается совокупность предупредительных мероприятий, направленных на сохранение и укрепление нормального состояния юридических отношений<sup>3</sup>. Говоря о времени совершения предупредительных действий, В.П. Казимирчук указывал, что «предупрежде-

ние определенного конфликта заключается в воздействии на его элементы: объект, субъектов, мотивы их поведения, используемые силы и средства до возникновения противоборства»<sup>1</sup>. М.Н. Марченко считает, что «при капитализме, к которому мы возвращаемся, главное противоречие, давно уже установившее экономистами и философами, — между общественным характером труда и частным присвоением его результатов»<sup>2</sup>. Противоречие непосредственно проявляется во взаимоотношениях собственника-организации (работодателя) с наемными работниками по поводу распределения прибыли, в том числе получения, использования и охраны КЗИ. Этот фактор является фундаментальной причиной правонарушений, в том числе совершаемых в сфере обращения КЗИ. Существующие объективные противоречия в этой сфере, угрозы, продуцирующие функционирование каналов утечки информации, порождают правонарушения, выражающиеся в утечке охраняемой информации. Следует иметь в виду, что профилактика юридических конфликтов, возникающих в организациях, по объему шире, чем предупреждение правонарушений в сфере обращения КЗИ. Она связана с задачами обеспечения экономической безопасности организации, предотвращения любых отступлений от требований норм законов и корпоративных актов, устранения причин и обстоятельств, способствующих совершению дисциплинарных проступков и нарушений договорной дисциплины.

*Предупреждение правонарушений в сфере обращения КЗИ охватывает предупреждение проступков и преступлений.* Профилактика проступков в этой сфере направлена на предотвращение нарушений норм трудового права и договорных обязательств, регулирующих процесс передачи, использования и охраны КЗИ внутри организации и при взаимоотношении с контрагентами. Предметом профилактики преступлений в этой сфере является предупреждение преступных проявлений, предусмотренных ст. 183, 272–274 УК РФ, выявление и устранение причин, их порождающих, и обстоятельств, им способствующих. Профилактика проступков и преступлений в сфере обращения КЗИ осуществляется в комплексе на уровне организации. Вместе с тем подход в юридических науках, занимающихся проблемами предупреждения правонарушений, различен, что объяс-

<sup>1</sup> См.: Юридический конфликт: сферы и механизмы / Отв. ред. В.Н. Кудрявцев. М., 1994, и др.

<sup>2</sup> См.: Социальные отклонения. М., 1989. С. 203–215.

<sup>3</sup> Общая теория государства и права. Академический курс в 3-х томах. Т. 3. М., 2001. С. 452.

<sup>1</sup> Общая теория государства и права. Академический курс в 3-х томах. Т. 3. М., 2001. С. 452.

<sup>2</sup> Там же. С. 467.

няется особенностями предмета их исследования. В науке трудового права предупреждение дисциплинарных проступков обычно связано с применением дисциплинарной и материальной ответственности. В науках гражданского и коммерческого права — имущественной ответственности. В криминологии главным направлением исследований является предупреждение преступности и конкретных видов преступлений.

Как известно, общее понятие предупреждения преступности было сформулировано в начале 60-х гг. XX в. и определялось как многообразная деятельность государственных органов, общественных организаций, граждан по устранению причин и условий, способствующих совершению преступлений. По мере развития криминологической науки это понятие уточнялось и конкретизировалось. В последующем были четко разграничены общесоциальное, специально-криминологическое и индивидуальное предупреждение преступлений<sup>1</sup>. Несомненным свидетельством развития и укрепления теоретической базы предупреждения преступности явилась развернутая характеристика понятий предупреждения преступности и отдельных видов преступлений в монографии «Теоретические основы предупреждения преступности». Несмотря на то, что с момента разработки теории прошло более 30 лет, основные ее положения являются актуальными и сегодня. В ней, в частности, подчеркивается, что предупреждение преступности представляет собой специфическую область социального управления, имеет многоуровневый характер и осуществляется в процессе решения как общих задач социального развития, так и специализированных задач. Предупреждение преступности не сводится только к деятельности правоохранительных органов, а включает в себя широкий круг мер, осуществляемых государственными органами и общественными организациями, взаимодействующими на причины и условия преступности<sup>2</sup>. Названные свойства в полной мере характеризуют и предупреждение преступлений, совершаемых в сфере обращения КЗИ. Наряду с отражением общих свойств предупреждения преступлений в этой сфере должно включать и специфику, определяемую особенностями криминологической характеристики таких преступлений и личности преступ-

<sup>1</sup> См.: Криминология. М., 2004. С. 15–27.

<sup>2</sup> См.: Теоретические основы предупреждения преступности. М., 1977. С. 30–31.

ника, порождающих преступления причины и способствующие им условий, средств воздействия на факторы, приводящие к совершению преступлений.

В свете изложенных положений предупреждение преступных проявлений в сфере обращения КЗИ может быть охарактеризовано как деятельность: а) осуществляемая правоохранительными органами на уровне специального предупреждения, иными государственными органами общего предупреждения; б) содержанием которой является устранение причин и условий, способствующих совершению преступлений в сфере обращения КЗИ, среди которых одно из центральных мест занимают недостатки, упущения и нарушения в корпоративном управлении производством; в) представляемая на различных уровнях социальной действительности в процессе деятельности хозяйствующего субъекта; г) проводимая в виде системы взаимосвязанных мер общесоциального и специально-криминологического характера, необходимых для предотвращения преступных проявлений в сфере обращения КЗИ, недопущения либо своевременной ликвидации криминальных ситуаций, возникающих на производстве, при передаче КЗИ контрагентам и государственным органам, оказания профилактического воздействия на лиц, имеющих дефекты ценностно-нормативной сферы личности, которые определяют возможность преступного поведения; д) непосредственно связанной с решением задач достижения конкурентного преимущества, укрепления потенциала высокотехнологического сектора экономики, поскольку криминальные ситуации, возможность преступных проявлений в сфере обращения КЗИ возникают вследствие допускаемых отступлений и нарушений корпоративных норм, регулирующих нормальный процесс использования и охраны КЗИ в организации. Особый криминологический подход к предупреждению правонарушений в сфере обращения КЗИ можно проследить на этапах профилактики преступлений в этой сфере, начиная с ранней профилактики.

Таким образом, совокупность явлений, связанных с преступностью в сфере обращения КЗИ, изучается криминологией. Нарушения преступного характера, их общие черты и особенности, проблемы, связанные с предупреждением административных, дисциплинарных проступков и гражданско-правовых нарушений (невыполнение или ненадлежащее выполнение договорных обязательств и др.) изучаются общей теорией государства и права, административным правом и науками частного права. Соотношение предупреждения преступле-

ний и правонарушений, совершаемых в сфере обращения КЗИ, следует рассматривать как соотношение части и целого. Большинство правонарушений не носят преступного характера. Их предупреждением занимается администрация организаций.

Предупреждение правонарушений преступного характера относится к специфической области корпоративного управления, имеет иерархический характер и осуществляется в процессе решения как общих задач производственной, коммерческой и иной деятельности организаций, так и специализированных задач, решаемых службой безопасности и юридическим отделом.

**Принципы предупреждения правонарушений в сфере обращения КЗИ.** Существенное значение для выявления отличительных особенностей предупреждения правонарушений в сфере обращения КЗИ имеет *анализ принципов*, на которых основывается этот вид деятельности. Для решения этой задачи будут использованы принципы трудового и гражданского права, криминологии, которые достаточно освещены в литературе. В настоящей части работы представляется возможным ограничиться изложением лишь тех из них, которые наиболее тесно связаны со спецификой предупреждения правонарушений в сфере обращения КЗИ.

Одним из ведущих принципов предупреждения правонарушений в сфере обращения КЗИ выступает *обоснованность применяемых мер ее охраны*. В Законе о коммерческой тайне (ч. 5 ст. 10) закреплены условия, при соблюдении которых меры по охране конфиденциальности информации признаются разумно достаточными. Необходимо учитывать особенности хозяйственной ситуации, проявления причин и обстоятельств, способствующих совершению правонарушений в этой сфере, в целях решения профилактических задач. Для осуществления профилактической деятельности нужен *учет рыночных условий в связи с переходом России к капитализму<sup>1</sup> и признания информации, имеющей коммерческую значимость, товаром*. Уголовный кодекс РФ предусматривает уголовную ответственность за незаконное получение и разглашение сведений, составляющих коммерческую тайну (ст. 183). Инициатором заявления в правоохранительные органы должна быть сама организация, права которой на коммерческую тайну нарушены. На основании заявления в установленном порядке возбуждается уголовное дело и проводятся необходимые следствен-

<sup>1</sup> См.: Меньшиков С.М. Анатомия российского капитализма. М., 2004. С. 17–58.

ные действия. Важную роль играет *комплексный подход к проведению профилактических мероприятий*, который предполагает осуществление профилактики на основе координации и взаимодействия производственных подразделений и службы безопасности.

Принцип конкретности тесно связан с принципом *реальности профилактической деятельности*. Осуществляемые меры должны быть исполнимы, целесообразны с экономической точки зрения. В основе их выбора должен лежать объективный анализ реальной хозяйственной ситуации, сложившейся в организации. Во всех без исключения случаях деятельность по предотвращению правонарушений в данной сфере должна строиться с учетом принципа *соблюдения законности*.

Результативность предупредительной деятельности находится в зависимости от уровня ее прогнозирования, кадрового, научно-методического и информационного обеспечения, что должно учитываться при создании системы предупреждения правонарушений. *Прогнозы* имеют значение для оценки фактического положения дел в обеспечении безопасности организаций, определения угроз, выявления направлений предупреждения данного вида правонарушений. На практике чаще всего разрабатываются вероятностные прогнозы относительно угроз конкурентов.

*Кадровое и материально-техническое обеспечение* определяют материальную базу функционирования системы предупреждения правонарушений в сфере обращения КЗИ. Без соответствующего штаба профессионально подготовленных работников и материальной базы невозможно достичь надежного обеспечения этой деятельности. Как отмечает Э.Я. Вольнец-Руссет, «...отечественные разработчики технологии не подготовлены и не представляют, как противостоять промышленному шпионажу. Этим проблемам они не обучались...»<sup>1</sup>. Проводимая в организациях техническая учеба не дает эффекта в освоении слушателями теории правовых защиты информации. Профессиональная подготовка специалистов в области информационной безопасности, которая ведется в ряде вузов, не может удовлетворить имеющиеся потребности коммерческих организаций. Отсутствуют полноценные учебники, предусматривающие

<sup>1</sup> Вольнец-Руссет Э.Я. Международный технологический обмен и его роль в экономическом развитии России. Дисс. в виде научного доклада на соис. уч. ст. д. э. н. М., 2005. С. 36–37.

подготовку специалистов в этой сфере для высокотехнологичного сектора экономики<sup>1</sup>. Подготовка специалистов в этой области не выделяется в качестве самостоятельного направления в вузах, хотя имеются учебные программы<sup>2</sup>. Необходимо внести изменения в образовательные стандарты с учетом профиля вуза. Реализация названных мер возможна с участием государства, бизнеса и вузов.

*Научно-методическое и информационное обеспечение* системы профилактики правонарушений в сфере обращения КЗИ нуждается в дальнейшем совершенствовании. Это в первую очередь касается практики сбора, накопления и переработки информации об угрозах безопасности организаций, формах и методах промышленного шпионажа. В этой части несомненную помощь могла бы оказать разработка методологии обоснования системы информационной безопасности коммерческих организаций, ориентированной на осмысление современных угроз. Учитывая практическую значимость предупредительной деятельности, видимо, полезным будет создание в рамках служб безопасности (СБ) аналитических подразделений, задачей которых будет научно-методическое сопровождение разработки и реализации мер предупреждения правонарушений в этой сфере. Решение задач требует формирования в организациях банка данных о состоянии обеспечения безопасности. Его использование позволит оперативно управлять силами и осуществлять выбор правовых средств для выявления и предупреждения ВКУ КЗИ.

Интересы повышения эффективности борьбы с конкурентной разведкой и промышленным шпионажем требуют, чтобы теоретические разработки в сфере обеспечения безопасности концентрировались в едином информационно-аналитическом центре. Таким центром мог бы стать Институт проблем информационной безопасности МГУ<sup>3</sup>, в рамках которого можно было проводить исследование проблем безопасности коммерческих организаций. Такой подход позволит проводить исследование с использованием сил и средств

<sup>1</sup> См.: *Бачило И.Л., Лопатин В.Н., Федотов М.А.* Информационное право. М., 2001. С. 760–778; *Северин В.А.* Правовая подготовка специалистов в области информационной безопасности организаций: Научные труды РАЮН. М., 2005. Т. 1. С. 697.

<sup>2</sup> См.: *Северин В.А.* Право на информацию и ее защита в коммерческих организациях. Программа спецкурса. М.: Изд-во МГУ, 2005, и др.

<sup>3</sup> См.: *Шерстюк В.П.* МГУ: научные исследования в области информационной безопасности // Информационное общество. 2005. № 1. С. 48–53, и др.

различных организаций, имеющих специфику в обеспечении режима государственной и коммерческой тайны.

Внутри системы правоохранительных органов обмен информацией организован неплохо. Однако такая информация в отдельный массив не выделена и в коммерческие организации практически не поступает. Информационный «голод» утоляется в основном публикациями юридической печати по этим вопросам, но этого недостаточно. Нужна хорошо продуманная система снабжения информацией предприятий-предпринимателей, осуществляющих профилактику правонарушений в сфере обращения КЗИ.

Рассмотренные виды обеспечения тесно взаимосвязаны между собой. Каждый их них необходим для нормального функционирования всей системы предупреждения правонарушений в сфере обращения КЗИ. Естественно, что система обеспечения должна быть динамичной и чутко реагировать на происходящие изменения в хозяйственной ситуации.

**Система предупреждения правонарушений в сфере обращения КЗИ** структурно включает следующие элементы (составные части деятельности коммерческой организации):

- 1) определение субъектов профилактики в коммерческой организации и наделение их полномочиями, необходимыми для осуществления функций «предупреждения»;
- 2) установление объектов профилактики в сфере обращения КЗИ;
- 3) определение содержания профилактики, связанной с разработкой и реализацией комплекса мероприятий по предупреждению правонарушений в рассматриваемой сфере;
- 4) обеспечение предупредительных мероприятий и применение мер юридической ответственности к виновным;
- 5) анализ результатов предупредительных мероприятий с целью оценки их эффективности, разработка дополнительных мер по совершенствованию системы предупреждения<sup>1</sup>.

Совокупность названных явлений и процессов дает общее представление о системе предупреждения, которая в той или иной степени используется в организациях.

<sup>1</sup> См.: *Кобец Н.Г.* Предупреждение правонарушений в производственном коллективе. Вопросы теории и практики. М.: Юрид. лит., 1982. С. 105–119; *Минаев В.А.* Система управления информационной безопасностью коммерческой организации. М., 2002. <http://www.fact.pl>, и др.

При построении системы предупреждения необходимо руководствоваться *общеметодологическими принципами*<sup>1</sup>. Такой подход будет способствовать повышению эффективности проводимых мероприятий. Разработка и функционирование системы предупреждения должны базироваться: 1) на единой концепции обеспечения информационной безопасности, принятой в организации; 2) на адекватных требованиях, предъявляемых к защите соответствующих объектов; 3) на гибкости системы защиты в случае изменения хозяйственной ситуации; 4) на функциональной независимости системы защиты от других систем корпоративного управления; 5) на минимизации предоставляемых прав на доступ лиц к КЗИ; 6) на полноте контроля за процессом обращения КЗИ; 7) на активном реагировании администрации в случае совершения правонарушений; 8) на экономичности системы предупреждения, связанной с ее созданием и функционированием.

Рассмотрим *особенности отдельных групп признаков, раскрывающих систему предупреждения правонарушений в сфере обращения КЗИ*.

**Первая группа признаков, характеризующих деятельность субъектов профилактики в коммерческих организациях.** Предупреждение нарушений в рассматриваемой сфере не сводится только к деятельности служб безопасности организаций, а включает в себя широкий круг мер, осуществляемых государственными органами, органами местного самоуправления, администрацией организаций, воздействующими на причины и условия, способствующие нарушениям. Речь идет о субъектах предупреждения, роль и значение которых в системе предупреждения различна.

С учетом правового статуса *субъектов профилактики* можно выделить: 1) деятельность государственных органов и органов местного самоуправления, решения которых носят обязательный характер для коммерческих организаций (общесоциальный уровень предупреждения), 2) деятельность правоохранительных органов (специальное криминалистическое предупреждение), 3) деятельность юристических лиц, реализуемая учредителями (акционерами) товарищества (общества), администрацией, руководителями структурных подразделений (общий неспециализированный уровень предупреждения), 4) деятельность подразделений службы безопасности организации (специ-

<sup>1</sup> См.: Герасименко В.А., Малюк А.А. Основы защиты информации. М., 1997. С. 357–360.

ализированный корпоративный уровень предупреждения). Деятельность названных субъектов профилактики объединена внутренним единством и обусловлена условиями рыночной экономики, в которой осуществляется научная, производственная и коммерческая деятельность организаций.

Рассмотрим роль каждого звена в системе профилактики. **Деятельность органов государственной власти, иных государственных органов**<sup>1</sup>. Законодательный орган в лице *Федерального Собрания Российской Федерации* принимает законодательные акты о правовом регулировании коммерческой тайны, устанавливает уголовную ответственность за такие преступления, определяет подсудность уголовных дел о разглашении коммерческих секретов, осуществляет парламентский контроль за исполнением законодательства РФ о коммерческой тайне и решает другие вопросы.

*Президент Российской Федерации* определяет основные направления внутренней и внешней политики государства, затрагивающие частные интересы деятельности коммерческих организаций, и издает в этой связи соответствующие правовые акты.

*Правительство Российской Федерации* обеспечивает разработку комплексных программ экономического развития страны, стимулирует развитие рыночных отношений и предпринимательства, проводит государственную политику по обеспечению безопасности экономики, в частности научно-технической сферы, реализует программу действий по нейтрализации угроз, включающей контроль и анализ данных, наблюдение за ситуацией и ее оперативную оценку, предварительное определение путей преодоления негативных воздействий на экономику, меры по нейтрализации угроз<sup>2</sup>.

Важное место в предупреждении недобросовестной конкуренции занимает деятельность *Федерального антимонопольного органа*, полномочия которого определены ст. 23 ФЗ «О защите конкуренции». Этим органом устанавливается и поддерживается административно-правовой режим защиты коммерческих секретов, представляющий собой совокупность административно-правовых установлений, которыми в целях предотвращения утечки охраняемых сведений определяются порядок деятельности государственных органов и органов

<sup>1</sup> См.: Концепция национальной безопасности Российской Федерации // Указ Президента Российской Федерации от 17 декабря 1997 г. № 1300 (в ред. от 10 января 2000 г. № 24).

<sup>2</sup> См.: Экономическая безопасность России. М., 2005. С. 106–126, и др.

местного самоуправления, коммерческих организаций, а также ответственность должностных лиц и руководителей хозяйствующих субъектов за нарушение антимонопольного законодательства в сфере охраны КЗИ. Законом предусмотрена обязанность антимонопольного органа по наблюдению коммерческой тайны и установлению ответственности его работников за разглашение такой информации (ст. 26).

*Федеральной службе безопасности РФ (ФСБ)* на основании ФЗ от 3 апреля 1995 г. № 40-ФЗ «Об органах федеральной службы безопасности в Российской Федерации»<sup>1</sup> и Указа Президента РФ от 11 августа 2003 г. № 960 «Вопросы Федеральной службы безопасности» (в ред. указов Президента РФ от 11 июля 2004 г. № 870, от 31 августа 2005 г. № 1007, от 11 декабря 2005 г. № 1383) предоставлено право оказывать содействие юридическим лицам независимо от форм собственности в разработке мер по защите коммерческой тайны. Как видим, законодатель предоставляет органам ФСБ право на оказание помощи коммерческим организациям и ни в коей мере не обязывает их заниматься этой работой. Отсюда следует, что забота по охране КЗИ — это обязанность самих организаций. Все действия, совершаемые коммерческой организацией, в части оформления допуска и осуществления доступа работников к КЗИ, установления правового режима, не подлежат согласованию с органами государственной безопасности.

При выполнении работ для государственных нужд, связанных с использованием сведений, составляющих государственную тайну, органы ФСБ обязаны участвовать в разработке и реализации мер по обеспечению режима секретности, независимо от организационно-правовой формы предприятий, включая и коммерческие организации. Другие субъекты, обеспечивающие безопасность личности, общества и государства<sup>2</sup>, в частности: Министерство внутренних дел РФ, Министерство обороны РФ, Федеральное агентство правительственной связи и информации при Президенте РФ, Служба внешней разведки РФ, Государственная техническая комиссия при Президенте РФ и их органы на местах не наделены полномочиями по оказанию организациям помощи в охране КЗИ. Законодательством

на них возложены обязанности по защите государственной тайны в рамках выполняемых ими функций.

Вместе с тем значительная помощь может быть оказана организациям, прежде всего, *Государственной технической комиссией при Президенте РФ и ее органами на местах*<sup>1</sup>, которые занимаются общей организацией противодействия иностранным техническим разведкам (ПД ИТР) и являются общероссийским органом по организации в стране комплексных работ по ПД ИТР, проводимых всеми министерствами и агентствами РФ, выполняющими работы по оборонной тематике. Под противодействием иностранной технической разведке понимается проведение организационных и технических мероприятий, направленных на исключение или существенное затруднение добытия ИТР охраняемых сведений о защищаемых от технических средств разведки объектах или создания у иностранных государств ложных представлений об этих объектах. Аналогичной работой в отношении конкурентной разведки вынуждены заниматься в самостоятельном порядке коммерческие организации и, естественно, нуждаются в правовой и технической помощи государственных органов.

При осуществлении ПД ИТР государственными органами определяются охраняемые сведения (под которыми понимаются сведения, не санкционированные государством для широкого распространения) и демаскирующие признаки, раскрывающие эти сведения; оценивается реальная опасность добывания спецслужбами иностранных государств с помощью технических средств разведки охраняемых сведений за пределами контролируемой территории; разрабатываются технические и экономические обоснованные меры ПД ИТР; проводится контроль эффективности применяемых мер ПД ИТР.

Ответственность за осуществление мер ПД ИТР возлагается на руководителей министерств, предприятий, командиров воинских частей. На всей территории РФ установлен единый порядок ПД ИТР, соблюдение которого является обязательным при выполнении работ в интересах обороны страны. Установленный порядок правового регулирования содержится в Положении по противодействию иностранным техническим разведкам.

<sup>1</sup> См.: СЗ РФ. 1995. № 15. Ст. 1269; 2000. № 1. Ст. 9.

<sup>2</sup> См.: Закон РФ «О безопасности» от 25 декабря 1992 г. № 4235-1 (в ред. ФЗ от 25 июля 2002 г. № 116-ФЗ).

<sup>1</sup> См.: Указ Президента РФ от 19 февраля 1999 г. № 212 «Вопросы Государственной технической комиссии при Президенте Российской Федерации» // СЗ РФ. 1999. № 8. Ст. 1010.

Главное архивное управление при Правительстве РФ издает перечни типовых документальных материалов, образующихся в деятельности министерств, организаций, учреждений и предприятий, включая и коммерческие, с указанием сроков хранения материалов; утверждает инструкции о порядке учета, обращения и хранения документов, содержащих несекретные сведения ограниченного распространения; осуществляет контроль за единообразным применением и толкованием указанных выше нормативных документов на территории РФ.

Министерства и иные федеральные органы исполнительной власти в рамках своей компетенции и с учетом характера их деятельности осуществляют функции отраслевого и межотраслевого регулирования и координации, анализа состояния, прогнозирования и определения основных направлений развития профильных сфер, лицензирования деятельности организаций, тем самым создают предпосылки для формирования необходимых финансовых, трудовых и производственных условий по сохранению КЗИ.

Межотраслевые органы федеральной исполнительной власти осуществляют функции нормативно-координационного характера (например, Министерство финансов РФ) и наделены полномочиями по применению мер административного принуждения (налоговая и таможенная службы и др.). Закон о коммерческой тайне предоставляет государственным органам право на получение КЗИ от организаций в связи с выполнением ими определенных законодательных функций. Решения, принимаемые органами местного самоуправления, на территории которых дислоцируются коммерческие организации, оказывают влияние на хозяйственную деятельность и поэтому должны учитываться в осуществлении предупредительных мер по охране КЗИ.

Деятельность правоохранительных органов по охране прав и законных интересов коммерческих организаций определена законодательством<sup>1</sup>, в частности, такими законами, как Уголовный кодекс РФ, Уголовно-процессуальный кодекс РФ, Кодекс РФ об административных правонарушениях, Налоговый кодекс РФ, Закон о безопасности, Закон о милиции и др. Особое значение для предупредительных правонарушений в сфере обращения КЗИ имеет деятельность

<sup>1</sup> См.: Гуценко К.Ф., Ковалева М.А. Правоохранительные органы. 2-е изд. М., 2006, и др.

органов, осуществляющих оперативно-розыскную работу, органов прокуратуры, судов общей юрисдикции и арбитражных судов. *Органы, осуществляющие оперативно-розыскную деятельность*, в пределах своих полномочий вправе, на основании ст. 7 ФЗ «Об оперативно-розыскной деятельности»<sup>1</sup>, собирать данные, необходимые для принятия решения о выдаче разрешений на частную детективную и охранную деятельность. Это означает, что при создании службы безопасности коммерческая организация обязана предоставить соответствующим органам МВД сведения о структуре, направлениях деятельности и др. данные, составляющие КЗИ.

Деятельность органов прокуратуры<sup>2</sup> оказывает непосредственное воздействие на состояние законности в сфере сохранности коммерческих секретов. В ходе проверок выявляются причины и условия, способствующие совершению правонарушений в сфере обращения КЗИ; принимаются меры по привлечению нарушителей к ответственности. Органы прокуратуры осуществляют надзор за законностью следственных действий по уголовным делам о разглашении коммерческой тайны, об утрате документов и изделий, содержащих такую тайну, предварительное следствие по которым ведется следователями органов внутренних дел либо следователями органа, вышестоящего это преступление (ст. 151 УПК РФ).

Полномочия прокурора, надзирающего за соблюдением законодательства о коммерческой тайне, определены УПК РФ и другими законодательными актами и сводятся к выявлению нарушений законодательства в этой сфере и требованию по устранению выявленных нарушений. Как отмечает В.Б. Ястребов: «По требованию прокурора ему должны быть представлены все документы, которые необходимы для выявления нарушений закона, их причин и способствующих им условий»<sup>3</sup>. Усиление предупредительной роли органов прокуратуры повысит ее роль в выявлении и предупреждении правонаруше-

<sup>1</sup> См.: ФЗ «Об оперативно-розыскной деятельности» от 12 августа 1995 г. // СЗ РФ. 1995. № 33. Ст. 3349; 1997. № 29. Ст. 3502; 1998. № 30. Ст. 3613; 2004. № 27. Ст. 2711.

<sup>2</sup> См.: ФЗ «О внесении изменений и дополнений в Закон РФ «О прокуратуре Российской Федерации» от 17 ноября 1995 г. // СЗ РФ. 1995. № 47. Ст. 4472; 1999. № 7. Ст. 878; № 47. Ст. 5620; 2000. № 2. Ст. 140; № 9. Ст. 1066; № 16. Ст. 1774; 2002. № 26. Ст. 2523; 2003. № 27. Ст. 2700 (ч. 1).

<sup>3</sup> См.: Ястребов В.Б. Учебник прокурорского надзора. 2-е изд., перераб. и доп. М., 2005. С. 154–168.

ний в информационной сфере и обеспечит надзор за соблюдением законодательства по охране коммерческой тайны.

*Основные направления предупредительной деятельности суда* связаны с рассмотрением конкретных уголовных, административных и гражданских дел о разглашении коммерческой тайны и возмещении убытков и организационно вытекают из них<sup>1</sup>. Правовые процессуальные формы, в которых осуществляется деятельность судов, достаточно известны и закреплены нормами федеральных законов. Уголовное наказание сочетается в себе цели общего и специального предупреждения. Превентивное воздействие уголовного наказания заключается в предостережении и наглядной демонстрации нежелательных последствий, которые могут наступить вследствие разглашения сведений, составляющих коммерческую тайну, либо утраты документов или изделий, содержащих такие сведения.

Федеральные суды общей юрисдикции наряду с правильным разрешением уголовных и гражданских дел обязаны выявлять причины и условия, способствующие совершению рассматриваемых преступлений и гражданских правонарушений, принимать меры к их устранению. Закон четко определяет виды, порядок и основания вынесения частных определений. Нужно сказать, что, в свою очередь, уголовно-процессуальным (ст. 241 УПК РФ), гражданско-процессуальным (ч. 2 ст. 10 ГПК РФ) и арбитражно-процессуальным (ст. 11 АПК РФ) законодательством допускается, в виде исключения из принципа гласности, разбирательство дел в закрытом судебном заседании при удовлетворении судом ходатайства участвующего в деле лица, ссылающегося на необходимость сохранения коммерческой тайны. Такая возможность закреплена законом и имеет значение для предупреждения утечки КЗИ.

Рассмотрим *предупредительную деятельность юридических лиц*, их органов управления: общего собрания учредителей (акционеров), совета директоров общества и исполнительного органа (правление, генеральный директор), под которым подразумеваются администрация, по выявлению возможных каналов утечки охраняемых сведений, установлению причин, их обуславливающих, и организацию их предупреждения.

*Учредителям (акционерам) общества* представлены законом полномочия по обеспечению экономической безопасности учреждаемого ими хозяйственного общества. Состояние работы по обеспечению безопасности общества отражается в разделе годового отчета, представляемого исполнительным органом на утверждение общего собрания акционеров (учредителей). Это позволяет акционерам быть в курсе событий производственной и коммерческой жизни, включая и охрану КЗИ, правильно оценивать хозяйственную ситуацию и вносить предложения по устранению нарушений трудовой и договорной дисциплины, способствующих разглашению (утечке) КЗИ. Свои полномочия акционеры реализуют путем обсуждения и принятия соответствующих вопросов на годовом общем собрании. Поскольку общие собрания акционеров созываются не часто, то совет директоров оперативно решает организационные и имущественные вопросы, находящиеся в его компетенции. В частности, анализируются неиспользованные резервы, критикуется стиль работы исполнительных органов, высказываются соображения о конкурентной стратегии, в том числе укреплении режима экономической и информационной безопасности.

Изучение решений общих собраний акционеров ряда организаций за пятилетний период позволило выделить вопросы, которые имеют отношение к предупреждению правонарушений в сфере обращения КЗИ, такие как, в частности: 1) обсуждение результатов хозяйственной деятельности за год с рекомендациями по их улучшению за счет более эффективного использования технологического потенциала, новых форм конкурентной борьбы и методов продвижения товаров на рынок (в 80% случаев речь шла об устранении факторов, обуславливающих низкую конкурентоспособность, об улучшении использования КЗИ, порядка охраны объектов и др.); 2) заслушивание руководителей, допустивших дисциплинарные проступки, связанные с недобросовестным выполнением обязанностей по обеспечению охраны КЗИ (в 1% случаев обсуждались общими собраниями акционеров); 3) обсуждение кадровых вопросов, где анализировались данные о состоянии, структуре и динамике нарушений в сфере обращения КЗИ.

Анализ показывает, что материалы о нарушениях, повлекших разглашение (утечку) КЗИ, ни разу не передавались по инициативе акционеров, совета директоров в следственные органы. Только в 4% случаев в приказах имелись указания о передаче материалов в суд по взысканию ущерба, причиненного неправомерными действиями

<sup>1</sup> См.: Николаев С. О. Особенности рассмотрения информационных споров судами Российской Федерации: Автореф. дисс. канд. юрид. наук. М., 2004, и др.



работников. Поэтому администрация не в полной мере использует правовые средства, содержащиеся в нормах акционерного права.

*Руководители организаций и структурных подразделений* в соответствии с Уставом, иными корпоративными актами:

- несут ответственность за обеспечение установленного режима КЗИ, за разработку и осуществление мероприятий по сохранению коммерческой тайны;
- издают приказы и распоряжения, утверждают положения и инструкции, другие документы, регламентирующие режим КЗИ с учетом специфики деятельности организации;
- осуществляют подбор и специальную подготовку кадров, которым поручается выполнение конфиденциальных работ;
- создают на производственных участках необходимые условия для выполнения работниками требований режима КЗИ;
- осуществляют контроль за соблюдением требований законодательства о коммерческой тайне и корпоративных актов по обеспечению режима КЗИ;
- принимают решения об отстранении от конфиденциальных работ лиц, нарушивших нормы ТК РФ, условия трудового договора в части охраны КЗИ;
- принимают решения о стимулировании труда работников, выполняющих задания по использованию и охране КЗИ;
- в соответствии с положением о премировании могут лишить работников полностью или частично стимулирующих выплат (надбавки и доплаты) при нарушении режима КЗИ;
- организуют воспитательно-профилактическую работу среди работников по разъяснению им требований режима КЗИ.

Таким образом, администрация имеет широкие полномочия по контролю за соблюдением режимных мер. Она проводит мероприятия по сокращению текучести кадров, осведомленных в коммерческой тайне, разрабатывает и применяет эффективные системы оплаты труда и премирования, осуществляет мероприятия по повышению профессиональной подготовки работников, улучшению условий их труда и жизни, обеспечивает привлечение правонарушителей к ответственности. Тем самым реализуется функция общего предупреждения в процессе достижения целей организации.

Решение задач предупреждения правонарушений в рассматриваемой сфере руководством организаций происходит в рамках осуществляемых ими полномочий. У руководителей подразделений такие полномочия ограничены конкретными участками работы. Эф-

фективность их работы оценивается работниками неоднозначно. Опрос лиц, выполняющих конфиденциальные работы, показал, что деятельность администрации и структурных подразделений по борьбе с нарушителями производственной дисциплины и режима КЗИ получила достаточно высокую оценку: 41% отметили ее с оценкой «хорошо», 42% — «удовлетворительно», 3% — «плохо», 5% — затруднились с ответом.

На многих предприятиях действуют первичные профсоюзные организации, которые в зависимости от предоставленных им законом полномочий<sup>1</sup> оказывают предупредительное воздействие на ВКУ, причины, их обуславливающие, и применяемые меры защиты, в процессе защиты трудовых прав работников. Это проявляется в контроле за соблюдением работодателем трудового законодательства. Речь идет о принятии работодателем решений, по которым должно учитываться мнение профсоюзного органа. В частности, при изменении существенных условий труда, выражающихся в доступе работника к КЗИ, и необходимостью совершения действий по охране КЗИ (ст. 73 ТК РФ); при установлении заработной платы с учетом надбавки «за секретность» (ст. 135 ТК РФ); при выполнении работодателем обязанностей по обеспечению безопасных условий и охраны труда, связанных с использованием КЗИ (ст. 212 ТК РФ); при принятии локальных актов, связанных с определением порядка допуска лиц к КЗИ и установлением режима такой информации.

Нужно сказать, что в соответствии с ФЗ «Об общественных объединениях» от 19 мая 1995 г.<sup>2</sup> работники коммерческих организаций могут быть членами различных общественных организаций (партий, общественных движений и т.д.), однако их участие не может оказывать заметного влияния на решения, принимаемые администрацией, включая и вопросы обеспечения безопасности.

*Юридическая служба организации*<sup>3</sup>, выполняя правоохранительную, консультативную, методическую, правоинформационную и аналитическую функции, оказывает влияние на защиту прав организации на КЗИ, на предупреждение правонарушений в этой сфере.

<sup>1</sup> См.: ФЗ от 12 января 1996 г. № 10-ФЗ «О профессиональных союзах, их правах и гарантиях деятельности» // СЗ РФ. 1996. № 3. Ст. 148; 2002. № 12. Ст. 1093.

<sup>2</sup> См.: ФЗ от 19 мая 1995 г. «Об общественных объединениях» // СЗ РФ. 1995. № 21. Ст. 1930; 1997. № 20. Ст. 2231; 1998. № 30. Ст. 3608.

<sup>3</sup> См.: Пугинский Б.И., Неверов О.Г. Правовая работа. М., 2004. С. 53–56, и др.

Это проявляется в контроле за разработкой корпоративных документов, касающихся режима КЗИ, в участии юристов в проверках, в ходе которых могут вскрываться нарушения в системе регулируемых корпоративных отношений, способствующие появлению ВКУ охраняемой информации.

В крупных организациях действуют *постоянно действующие технические комиссии* (ПДТК), которые оценивают результаты исследований в области предупреждения утечки КЗИ. В состав комиссии входят руководители основных подразделений, работники СБ и конкурентной разведки, маркетологи и аналитики. Решения, принимаемые ПДТК, утверждаются приказом руководителя и являются обязательными для исполнения работниками организации.

Рассмотрим деятельность **специализированных подразделений, занимающихся охраной коммерческих секретов в организации**. Эти подразделения, как правило, входят в состав единой службы безопасности (СБ) организации или функционируют отдельно, подчиняясь непосредственно первому руководителю.

К числу специализированных подразделений относятся подразделения конфиденциального делопроизводства и режима, аналитическое подразделение, подразделение конкурентной разведки и отдел охраны. Правовое положение названных подразделений с определением их функций устанавливается руководителем организации. Поэтому важно сформулировать основные направления предупредительной деятельности с позиций СБ, включающей деятельность названных выше подразделений.

*Во-первых*, СБ выявляет факты нарушений со стороны государственных органов и органов местного самоуправления норм Закона о коммерческой тайне при предоставлении по их запросу информации, составляющей коммерческую тайну, например, превышения государственным органом своих полномочий по истребованию КЗИ.

*Во-вторых*, СБ устанавливает факты несоблюдения контрагентом договорных условий о конфиденциальности. Служба информирует об этом руководство организации и принимает меры к взысканию убытков.

*В-третьих*, служба выявляет посяательства на информационные ресурсы организации, факты их нерационального и личного использования, неполной их загрузки и иные действия, которые могут привести к ущербу.

*В-четвертых*, служба выявляет угрозы для стабильной и привычной работы организации, неблагоприятные изменения конъюнктуры рынка; участвует в проведении мероприятий по повышению конкурентоспособности выпускаемой продукции; принимает меры по недопущению заключения договоров на невыгодных условиях; использует силы и средства для нейтрализации действий недобросовестной конкуренции.

*В-пятых*, служба выявляет негативные тенденции в трудовом коллективе, создающие угрозы для ритмичности производства, повышения производительности и качества труда; предупреждает переманивание работников, занятых выполнением НИОКР и осведомленных в КЗИ, конкурентами.

*В-шестых*, служба выявляет угрозы срыва выполнения производственной программы и планов инновационного прорыва за счет эффективного использования высоких технологий; нарушения договорных обязательств; выпуск недоброкачественной и неконкурентоспособной продукции, и принимает меры к их ослаблению или ликвидации. СБ участвует в изучении партнеров по совместному бизнесу, анализирует их финансовое положение и кредитоспособность, наличие ресурсов и научно-технического потенциала, уровень подготовки персонала, репутацию в деловых кругах и наличие международных связей.

*В-седьмых*, служба готовит рекомендации по рассредоточению экономических связей с недобросовестными контрагентами в целях уменьшения «критической зависимости» в отношениях с ними и установлению контактов с надежными партнерами. Служба может участвовать в поиске стабильных источников снабжения, с учетом имеющихся данных о субъектах, и гарантированных рынков сбыта продукции.

*В-восьмых*, служба выявляет и предупреждает угрозы потери организационной технологической лидерства и снижения конкурентоспособности, приоритетности научных исследований и разработок путем анализа научно-производственной деятельности; выявляет и пресекает акции конкурентов по дезинформированию и торможению производственно-технологического освоения передовых научных достижений, включая использование КЗИ.

**Вторая группа признаков, раскрывающих систему предупреждения правонарушений в сфере обращения КЗИ, — это объекты профилактики.** Их установление осуществляется путем анализа научно-производственной и коммерческой деятельности организации с це-

лю выявляя недостатки, имеющихся в сфере обращения КЗИ, выявляя и изучая причины, породивших их, и условий, способствовавших их возникновению. *Объектами профилактики* могут быть обстоятельства организационно-управленческого, воспитательно-го и правового характера, влияющие на возникновение правонарушений и способствующие их совершению, а также работники, осведомленные в коммерческой тайне, совершающие правонарушения, вследствие недобросовестного выполнения своих обязанностей.

**Определение содержания профилактики связано с разработкой мер предупреждения нарушений в сфере обращения КЗИ. Третья и последующие группы признаков позволяют раскрыть систему предупреждения правонарушений** в рассматриваемой сфере с учетом особенностей этих правонарушений, причин и обстоятельств, им способствующих, и личности правонарушителей. Охватываемые системой меры являются достаточно многочисленными, они различаются по целям, уровням применения, масштабам, степени правового регулирования, характеру осуществления<sup>1</sup>. Система мер предупреждения правонарушений в организациях, где циркулирует КЗИ, являясь частью общей системы предупреждения правонарушений, совершаемых в трудовых коллективах, состоит из общесоциальных и специальных мер, осуществляемых на уровне общества (отраслей экономики), социальных групп (коммерческих организаций) и индивида (работника, имеющего доступ к КЗИ).

*К общесоциальным мерам предупреждения* юридическая наука относит меры, направленные на решение социально-экономических, организационно-управленческих, воспитательных и других задач, которые, не будучи социально обусловлены целями предупреждения правонарушений, вместе с тем тесно связаны с деятельностью организаций и создают необходимые предпосылки для ликвидации правонарушений<sup>2</sup>.

В результате реформ в рыночной экономике, наряду с решением общесоциальных задач, одновременно устраняются или нейтрализуются те процессы и явления в жизни трудовых коллективов, с которыми связана сама возможность неправомерного формирования

<sup>1</sup> См.: Кудрявцев В.Н. Причины правонарушений. М., 1976. С. 274; Он же. Правовое поведение: норма и патология. М., 1982. С. 24; Социальные отклонения. М., 1989. С. 210–222, и др.

<sup>2</sup> См.: Саркисов Г.С. Социальная система предупреждения преступности. Ереван: Айтастан, 1975. С. 62; Кобец Н.Г. Указ. соч. С. 111, и др.

личности и возникновения ситуаций, способствующих совершению правонарушений, включая сферу обращения КЗИ. Основные направления профилактики общесоциального уровня, определенные Н.Г. Кобец<sup>1</sup>, без их идеологической части, вполне могут быть взяты за основу, применительно к целям данного исследования. В современных условиях речь идет об укреплении стабильности трудового коллектива, уменьшении текучести кадров, особенно лиц, осведомленных в КЗИ; о совершенствовании инфраструктуры профилактики правонарушений при обращении КЗИ с использованием всего арсенала правовых средств, изучении общественного мнения коллектива и его правильном формировании с учетом частных интересов.

Проведение общесоциальных мер связано с деятельностью государственных органов и органов местного самоуправления, коммерческих организаций и общественных объединений. Значимость этих мер обоснованно подчеркивалась в литературе. Как отмечает А.Э. Жалинский, «любое антиобщественное явление... может быть устранено, и притом окончательно, общесоциальными мерами... Но этот вывод верен лишь в тенденции, в историческом плане»<sup>2</sup>. При изучении общих мер важно проведение анализа перспективных направлений становления рыночной экономики, оглянувшихся устойчивой связью с практикой предупреждения правонарушений в сфере обращения КЗИ, и требующих их первоочередного рассмотрения.

Общие меры предупреждения оказывают непосредственное воздействие на устранение ошибок и недостатков, допускаемых при разрешении противоречий в сфере охраны коммерческих секретов, на искоренение негативных явлений из жизни общества в связи с переходом к рыночной экономике, способствующих проявлению нарушений режима КЗИ. Вместе с тем, как отмечает В.Н. Кудрявцев, «наряду с долговременными, перспективными общесоциальными мерами необходимы и профилактические мероприятия более узкого, конкретного характера, которые именуются специальными предупреждениями»<sup>3</sup>.

<sup>1</sup> См.: Кобец Н.Г. Указ. соч. С. 113.

<sup>2</sup> Жалинский А.Э. Специальное предупреждение преступлений в СССР. Львов, 1976. С. 86.

<sup>3</sup> Кудрявцев В.Н. Социальные отклонения. Введение в общую теорию. М., 1984. С. 263.

*Специальные меры предупреждения правонарушений в сфере обращения КЗИ* непосредственно направлены на устранение причин и условий, с которыми связано совершение этой категории правонарушений. При этом имеется в виду, что эти меры проводятся там и тогда, где и когда в силу определенных причин общие экономические, воспитательные и организационные мероприятия, реализуемые на уровне государства и отдельной коммерческой организации, оказались недостаточными. Эти меры разрабатываются и проводятся правоохранительными органами, а также подразделениями организаций, созданными специально для охраны коммерческих тайн и предупреждения правонарушений в этой сфере.

В целях обеспечения предупреждения правонарушений в рассматриваемой сфере целесообразно различать основные уровни проведения профилактических мероприятий — *общество в целом (отдельные отрасли экономики), социальные группы (коммерческие организации), индивидуальный уровень*. На уровне микросреды, индивидуальном уровне, меры более высоких уровней представляют собой конкретизацию общесоциальных и специальных мер в отношении отдельного лица, имеющего доступ к КЗИ, или группы таких лиц. Индивидуальная профилактика направлена на устранение неправильно сформированных (деформированных) потребностей, интересов, ценностных ориентаций, которые при наличии соответствующей хозяйственной ситуации способны привести к правонарушениям. Меры индивидуального характера включают общеобразовательные мероприятия, правовое корпоративное воздействие, контроль за поведением лиц, совершивших дисциплинарные проступки, связанные с нарушениями режима КЗИ, которые в большинстве случаев реализуются на практике администрацией организаций.

В литературе практически не раскрыто содержание и объем понятия «меры предупреждения правонарушений, совершаемых в сфере обращения КЗИ». Многие исследователи<sup>1</sup> используют это понятие для обозначения конкретных действий администрации по проверке персонала, допускаемого к коммерческой тайне, ограничению доступа работников к таким сведениям, усилению контроля на различных этапах обращения информации. Отсутствие единообразного понимания мер предупреждения правонарушений в сфере обра-

щения КЗИ отрицательно отражается на решении практических задач. Представляется, что на основании ФЗ «Об информации, информационных технологиях и о защите информации», ГОСТ Р52069.0-2003 «Защита информации. Система стандартов. Основные положения» и ГОСТ Р50922-96 «Защита информации. Основные термины и определения» можно сформулировать понятие мер предупреждения правонарушений, которые направлены на предотвращение деятельности, связанной с неправомерным использованием КЗИ.

*Во-первых*, мера — это использование административной организации правовых средств для обеспечения установленного режима охраны КЗИ и ее защиты от непреднамеренного воздействия (ошибки персонала, сбои технических и программных средств и др.), несанкционированного воздействия (нарушение установленных правил, приводящее к утрате, уничтожению или сбою функционирования носителя информации); несанкционированного доступа (получение работником КЗИ с нарушением разрешительной системы доступа); неконтролируемого распространения КЗИ (утечка) и несанкционированного доведения КЗИ (разглашения); предотвращение получения КЗИ конкурентной разведкой. *Во-вторых*, содержание мер предупреждения направлено на устранение обстоятельств, приводящих к утечке (разглашению) КЗИ. *В-третьих*, действия администрации, составляющие содержание мер, основываются на сложившемся в организации порядке, который урегулирован законами и корпоративными актами.

Рассмотрим меры организационно-управленческого, воспитательного и правового характера, которые дают достаточно полное представление о содержании профилактики в сфере обращения КЗИ.

*Меры предупреждения обстоятельств организационно-управленческого характера*. Действие этих мер направлено на наведение должного порядка, повышение уровня трудовой и договорной дисциплины в сфере обращения КЗИ. Нарушения в корпоративном управлении производством относятся к числу факторов, оказывающих влияние на механизм совершения правонарушений в данной сфере. В условиях нестабильности и противоречивости реформационных процессов курс на обеспечение безопасности корпоративных образований является неизменным и последовательным в деятельности организаций.

*Совершенствование структуры корпоративного управления производством*. Эта мера способствует формированию устойчивого, но

<sup>1</sup> См.: Фатьянов А.А. Правовое обеспечение безопасности информации в Российской Федерации. М., 2001. С. 199–207, и др.

подвижного механизма обеспечения безопасности организации в условиях рыночной экономики. Устойчивость механизма объясняется закреплением прав субъектов на КЗИ, а подвижность предполагает их изменение в связи с возникновением либо прекращением тех или иных направлений деятельности либо прекращением тех КЗИ. Речь идет о четком распределении компетенции между подразделениями СБ и производственными подразделениями, что позволяет избежать дублирования в работе и улучшить координацию совместных действий по обеспечению режима КЗИ. Регулирование деятельности этих звеньев непосредственно связано с практикой предупреждения правонарушений в сфере обращения КЗИ.

Наибольшее число опрошенных (37%) заявили, что недостатки в организации труда являются основной причиной и условием, способствующим нарушениям режима конфиденциальности работ. Изучение дисциплинарной практики подтверждает, что меры, которые проводились по устранению или нейтрализации таких причин и условий, в большинстве случаев носили организационный характер. В целях борьбы с нарушениями режима КЗИ издавались приказы и распоряжения, которые были ориентированы на усиление воспитательно-профилактической работы (32%), устранение недостатков пропускного и внутриобъектового режима (27%), предупреждение каналов утечки информации (17%), улучшение порядка учета, хранения и движения грифованных документов и изделий (16%).

Важное профилактическое значение имеет конкретизация служебных обязанностей работников СБ и руководителей производственных подразделений в сфере сохранности коммерческих секретов. На это обстоятельство как меру предупреждения указали 42% опрошенных лиц. Одновременно отмечена слабая работа руководства организации в этом направлении. Закрепление прав и обязанностей работников в должностных положениях и инструкциях способствует устранению дублирования, повышает ответственность, устраняет возможность производного толкования полномочий как со стороны руководителей, так и работников, что ведет к качественному выполнению обязанностей и предупреждению возможности утечки охраняемых сведений. При совершенствовании структуры управления необходимо четко разграничить функции отделов конфиденциального делопроизводства и режима, что позволит высвободить часть работников, переклочить их на выполнение аналитической и контрольно-проверочной работы.

*Совершенствование системы стимулирования деятельности по охране коммерческих секретов.* Опрос работников, имеющих доступ к КЗИ, показал, что большинство из них считают эффективной мерой предупреждения правонарушений — повышение авторитета сотрудников СБ за счет расширения их прав и улучшения материального положения. Были названы как материальные (зарплата, премии, ссуды, льготные кредиты, бесплатное лечение, путевки, транспортные расходы и др.), так и нематериальные (престижность труда, общественное признание, возможность служебного роста, дополнительная отпуск и др.) стимулы. Чаще всего отмечалась необходимость такого стимула, как установление работникам, имеющим доступ к коммерческой тайне, «надбавки за секретность». Применительно к государственной тайне этот вопрос решается субъектами Федерации на основании Закона о государственной тайне (ст. 29). Например, решением Правительства Москвы были установлены надбавки к должностному окладу лицам, допущенным к особой важности документам и изделиям — 25%, к совершенно секретным — 15%, секретным — 10%. Средства на эти цели предусмотрены в федеральном бюджете. Вопрос о «надбавке за секретность» решается коммерческими организациями самостоятельно в рамках фонда заработной платы подразделений, с учетом объема работ по охране КЗИ. Закон «О коммерческой тайне» не устанавливает каких-либо ограничений на этот счет. Важно, чтобы администрация закрепила в корпоративных актах процедуру установления и выплаты надбавок, и дифференцированно использовала этот стимул для повышения качества работы по охране КЗИ. Используя надбавки, важно создать такие условия, которые бы стимулировали качественный труд по использованию и охране КЗИ.

*Совершенствование системы учета и контроля* предполагает наведение порядка в отчетной документации при обращении КЗИ, унификацию системы согласования и исполнения документов. Опрос работников, имеющих доступ к КЗИ, показал, что в числе первоочередных мер должны быть действия, направленные на определение фактической необходимости раскрытия КЗИ контрагентам, ограничение доступа к документам, содержащим тактико-технические характеристики, установление контроля, исключающего утечку сведений при ведении служебных переговоров и выполнении НИОКР.

Совершенствование приемов обработки конфиденциальной информации на ЭВМ требует, во-первых, наведения порядка доступа к персональным компьютерам, серверу или рабочей станции, кото-

рые используются для обработки конфиденциальной информации, что предполагает закрепление за подразделением специалиста СБ в области информационной безопасности, определение работников, имеющих право доступа в помещение, в котором находится вычислительная техника, установление режима нахождения лиц в таких помещениях; контроль вносимых и выносимых персоналом машинных и бумажных носителей информации. *Во-вторых*, нужен контроль за доступом работников к машинным носителям конфиденциальной информации, хранящихся вне ЭВМ<sup>1</sup>. Речь идет об организации учета и выдачи работникам машинных носителей информации, учетных в отделе конфиденциального делопроизводства, о контроле за сохранностью и целостностью информации, порядком ее физического уничтожения на носителе. *В-третьих*, доступ к конфиденциальным базам данных и файлам предполагает контроль системы доступа администратором базы данных, фиксирование в машинной памяти имен пользователей и операторов, имеющих право доступа к ним; регистрацию несанкционированного входа в базу данных, ошибочных действий пользователя, автоматическую передачу сигнала тревоги в СБ и отключение компьютера<sup>2</sup>.

Поскольку существуют угрозы несанкционированного получения информации, то должен действовать механизм защиты, состоящий из системы опознавания пользователей с использованием паролей, проверки полномочий субъекта на право использования запрашиваемого им ресурса, шифрования данных, используемых для обеспечения конфиденциальности находящихся в сети<sup>3</sup>.

**Меры воспитательного характера**, используемые для предупреждения правонарушений в сфере обращения КЗИ, должны рассматриваться как часть общей программы действий по устранению из жизни общества явлений, препятствующих построению правового государства, и лежащих в основе антиобщественного (антикорпоративного) поведения. Реализация мер предусматривает повышение уровня правовых знаний и общей правовой культуры работников, имеющих доступ к КЗИ.

Проблема *правового воспитания* в современный период заключается в том, чтобы использовать такие методы воспитания, которые отвечали развитию российского капитализма<sup>1</sup>. Основологающим методом управления персонала в рыночной экономике является мотивация труда работников с применением административных, экономических и социально-психологических методов. Названные методы являются основой *воспитательно-профилактической работы* (ВПР), состоящей в воспитательном и профилактическом воздействии на генезис правонарушения, включающего «потребности — возможности — цели — средства — поступок — результат»<sup>2</sup>. Предложенная В.Н. Кудрявцевым система основных профилактических мероприятий применительно к отдельным звеньям деформированного генезиса поведения является актуальной и сегодня, применительно к сфере обращения КЗИ, и включает следующую классификацию мер: а) в сфере потребностей и интересов: удовлетворение социальных одоляемых потребностей и интересов; исправление возможных деформаций в системе потребностей личности или группы; б) в сфере возможностей: расширение социально-экономических, культурных, общественных возможностей для каждого члена общества; укрепление правовых и иных гарантий, обеспечивающих широкое использование прав и законных интересов граждан и коллективов; в) в сфере целей и ценностных ориентаций: воспитание социально полезной направленности личности; усиление общеправового воздействия права; г) в сфере выбора средств достижения целей: обеспечение беспрепятственного использования правомерных средств достижения социально полезных целей; пресечение использования запрещенных средств; воспитательная работа и общая превенция (угроза наказанием за использование запрещенных средств); д) в сфере принятия решений: воспитательное и предупредительное воздействие на индивида<sup>3</sup>.

Далее, В.Н. Кудрявцев отмечает, что «профилактическое воздействие по своей направленности и результативности заключается как в устранении объективных предпосылок противоправного поведе-

<sup>1</sup> См.: *Меньшиков С.М.* Анатомия российского капитализма. М., 2004. С. 5–58, и др.

<sup>2</sup> См.: *Кудрявцев В.Н.* Правовое поведение: норма и патология. М.: Наука, 1982. С. 240.

<sup>3</sup> *Кудрявцев В.Н.* Указ. соч. С. 240.

<sup>1</sup> См.: *Степанов Е.А., Корнеев И.К.* Информационная безопасность и защита информации. М., 2001. С. 90–93, и др.

<sup>2</sup> См.: *Герасименко В.А., Малюк А.А.* Основы защиты информации. М., 1997. С. 284–499, и др.

<sup>3</sup> См.: Там же. С. 472–477.

ния, так и в изменении сознания лиц, склонных к правонарушению, устранении существующих у них трудностей и конфликтов, в позитивном влиянии на их взгляды и убеждения»<sup>1</sup>. Исходя из концепции правового воспитания<sup>2</sup>, задачами правового воспитания в сфере обращения КЗИ являются: *во-первых*, повышение уровня знаний работников о формах и способах защиты КЗИ; *во-вторых*, формирование убеждений в необходимости усвоения работником корпоративных требований в целях привития навыков правомерного поведения.

Цель ВПР — оказание воздействия на лиц, которым доверены секреты. ВПР выступает важным звеном в системе предупреждения утечки охраняемых сведений, организационной частью общей воспитательной работы в трудовых коллективах. Основными задачами ВПР являются: воспитание у работников чувства осознанного корпоративного долга и личной ответственности за сохранение коммерческих секретов; создание в коллективе обстановки нормального психологического климата, нетерпимости к актам нарушения режима КЗИ; привитие работникам навыков по предупреждению утечки информации.

Содержанием ВПР является воспитание и обучение работников, имеющих доступ к КЗИ, а также профилактика правонарушений в сфере обращения такой информации. Повышение эффективности ВПР среди работников, выполняющих конфиденциальные работы, возможно достичь, если будут учитываться следующие факторы:

- 1) к участию в ВПР должны быть привлечены опытные воспитатели — работники СБ и руководители производственных подразделений, хорошо знающие характер и степень конфиденциальности работ, имеющие неформальные связи в трудовых коллективах;
- 2) вооружить воспитателей знаниями о возможностях использования правовых средств для охраны КЗИ, систематически информировать их об изменениях оперативной обстановки и социально-психологическом климате в трудовом коллективе;
- 3) разработать и внедрить систему корпоративного управления воспитательным процессом;

Основные требования, которым должно отвечать обучение, вытекают из сознательности обучения, наглядности, систематичности и последовательности, доступности и индивидуального подхода. Важными направлениями обучения следует считать: *Во-первых*, изучение в рамках производственной учебы структуры информационного обращения КЗИ, особенностей охраны КЗИ в трудовых и гражданско-правовых отношениях. Программа обучения должна быть составлена дифференцированно к разным категориям слушателей (руководители подразделений и НИОКР, работники СБ, работники, имеющие доступ к КЗИ, и др.). *Во-вторых*, привитие навыков по применению корпоративных норм в сфере обращения КЗИ. *В-третьих*, проверка знаний исполнителями законов и корпоративных актов, регулирующих обращение КЗИ.

В организациях чаще всего используются такие формы воспитания, как: проведение инструктажа работников, имеющих доступ к КЗИ; беседы в трудовых коллективах о необходимости соблюдения требований экономической безопасности; использование информационных технологий, раскрывающих формы и методы конкурентной разведки и промышленного шпионажа; учет состояния режима охраны КЗИ как показателя производственной деятельности подразделения при подведении итогов работы и другие.

Опрос показал, что устранение недостатков, способствующих совершению правонарушений в сфере обращения КЗИ, возможно силами администрации в 94% случаев. Проведение мер воспитательно-характера не может отменить воздействия других обстоятельств, способствующих утечке информации. Вместе с тем, давая им правильное объяснение, эти меры способствуют формированию негритимости к ним со стороны руководителей, воспитывают добросовестное отношение работников к сохранению коммерческих секретов. На воспитательный процесс воздействуют также изменения в условиях труда, рост или снижение материальных доходов, что должно правильно оцениваться в конкретной хозяйственной ситуации.

Центральное место в воспитательной работе должно отводиться формированию добросовестного отношения работника к выполнению трудовой функции, включая охрану коммерческих секретов, что достигается с помощью психологических приемов превращения трудовой обязанности в осознанный долг, внутреннюю потребность человека. Тот, кто обладает такими качествами, нарушений в сфере обращения КЗИ не допустит.

<sup>1</sup> Кудрявцев В.Н. Указ. соч. С. 240—241.

<sup>2</sup> См.: Бойко А.Д. Некоторые вопросы теории правового воспитания // Правовая культура: вопросы правового воспитания. М., 1974. С. 19; Каминская В.И., Ратинов А.Р. Там же. С. 40; Общая теория государства и права / Отв. ред. проф. М.Н. Марченко. Т. 3. М., 2001. С. 303—326, и др.

Воспитание связано с преодолением работниками равнодушия, чувства самоуспокоенности в работе, вредных привычек и инертности. Решение этих вопросов зависит от подготовленности воспитателей, осуществляющих эти функции, от их умения и смелости вести откровенный разговор о действительной или мнимой несправедливости материального стимулирования труда, о недостатках руководства корпорацией. При реализации мероприятий воспитательного характера следует помнить о том, что «каждый человек — продукт реальных обстоятельств, что его совершенствование зависит в первую очередь от изменения материальных условий его жизни, а не от усилья проповедников»<sup>1</sup>. В этом состоит главная сила, формирующая человека в рыночной экономике. Было бы ошибкой думать о том, что с помощью одних воспитательных мер будет решена проблема обеспечения безопасности в организации. Эти меры тесно связаны и должны применяться в комплексе с другими мерами. Усилия администрации должны быть сосредоточены на устранении противоречий между публичными, частными и личными интересами в сфере обращения КЗИ, а также дефектов правосознания у части работников, допущенных к КЗИ.

**Меры правового характера** занимают особое место в числе других предупредительных мер, направленных на обеспечение установленного режима коммерческой тайны. Изучение обстоятельств, способствующих нарушениям режима КЗИ, показывает, что многие из них связаны с имеющимися проблемами в законодательстве о коммерческой тайне, несовершенством и противоречивостью отдельных норм, регулирующих отношения в сфере защиты коммерческих секретов. Правовое регулирование предупредительной деятельности в сфере обращения КЗИ осуществляется в двух направлениях. *Первое* носит материальный характер и состоит в воздействии с помощью права на различные факторы в целях устранения обстоятельств неблагоприятного развития хозяйственной ситуации, негативно влияющих на обеспечение информационной безопасности организации. *Второе* заключается в закреплении прав и обязанностей субъектов профилактики, осуществляющих предупредительную деятельность в сфере обращения КЗИ. Это указывает на необходимость их дальнейшего совершенствования на законодательном и корпоративном уровне.

<sup>1</sup> Бутенко А.П. Социалистический образ жизни: проблемы и суждения. М., Наука, 1978. С. 325.

Этот процесс исключительно сложный, требующий проведения ряда исследований и охвата более широкого круга вопросов, связанных с защитой коммерческих секретов. Полученные данные позволяют сделать выводы о направлении совершенствования правового регулирования в области сохранения коммерческих секретов, взаимосвязанных с практикой предупреждения нарушений режима КЗИ.

Первоочередными из них являются совершенствование правового регулирования деятельности по предупреждению утечки (разглашения) КЗИ и улучшение практики применения правовых норм, регулирующих обращение КЗИ.

*Совершенствование правового регулирования деятельности по предупреждению утечки КЗИ* связано в определенной мере с реализацией уже принятых законов в этой сфере, и, прежде всего, части четвертой ГК РФ, Закона о коммерческой тайне, наведением должного порядка в корпоративном регулировании охраны КЗИ, закреплением порядка в толковании правовых норм, регламентирующих процесс забвения государственными органами КЗИ и обеспечения в этой связи установленного в организации режима коммерческой тайны, осуществлением на законных основаниях противодействия конкурентным разведкам и промышленному шпионажу путем улучшения аналитической работы по выявлению ВКУ информации и разработки рекомендаций по их предупреждению.

Вопросы о необходимости законодательного закрепления права коммерческих организаций на информацию, содержащую коммерческую тайну в учредительных документах, о принципах разработки перечня сведений, составляющих коммерческую тайну, о правотверности использования процедуры допуска лиц к КЗИ и проведении проверочных мероприятий, о взаимоотношении с государственными органами при предоставлении им КЗИ и других отношениях, складывающихся в связи с деятельностью по охране коммерческих секретов, были предметом обсуждения в литературе<sup>1</sup>. Однако они не нашли своего решения в ныне действующем Законе о коммерческой тайне<sup>2</sup>. В этой связи были сформулированы предложения по со-

<sup>1</sup> См.: Северин В.А. К вопросу о коммерческой тайне // Законодательство. 2004. № 12.

<sup>2</sup> См.: Северин В.А. Эволюция законодательства о коммерчески значимой информации в России // Вестн. Моск. ун-та. Сер. 11 «Право». 2005. № 4.



вершенствованию Закона<sup>1</sup>, реализация которых позволит устранить имеющиеся недостатки в использовании правовых средств при регулировании трудовых и гражданско-правовых отношений, что имеет значение для улучшения практики предупреждения правонарушений в сфере обращения КЗИ.

Укрепление правовых основ предупреждения правонарушений режима коммерческой тайны в торговом обороте во многом зависит от решения общих вопросов правового регулирования обращения КЗИ, что в определенной мере связано с принятием Торгового кодекса РФ. Вопрос о кодификации коммерческого законодательства продолжает оставаться дискуссионным в научной среде и практически трудно решаемым. Не ставя перед собой задачи подробно его анализировать, отметим лишь, что одна группа ученых выступает за принятие кодекса<sup>2</sup>, по их мнению, он «...должен служить формированию российского товарного рынка, созданию его структуры, налаживанию торгово-хозяйственных связей и их развитию»<sup>3</sup>. *Вторая* — выступает против его принятия, считая, что «это приведет к разрушению принципа единства правового регулирования имущественных отношений, основанных на равенстве, автономии воли и имущественной самостоятельности их участников...»<sup>4</sup>. Вместе с тем представляется, что принятие кодекса позволит систематизировать нормы, регулирующие коммерческую деятельность, включая защиту частных интересов организаций, использующих КЗИ и осуществляющих ее охрану.

Существенное значение имеет законодательное закрепление *порядка предоставления информации, составляющей коммерческую тайну, по запросу органа государственной власти, иного государственного органа, органа местного самоуправления*. В Законе о коммерческой тайне необходимо перечислить основания истребования государственным органом информации, составляющей коммерческую тайну, поскольку в отдельных случаях отмечается их «передерживание»

в угоду ведомственным интересам. Такая практика способна породить правовой нигилизм у чиновников по отношению к соблюдению прав организаций на КЗИ. Должны быть определены гарантии против принятия ведомственных актов, устанавливающих порядок изъятия документов, содержащих КЗИ, которые противоречат Закону о коммерческой тайне, и тем самым создают бюрократические лазейки для утечки КЗИ.

Отдельную группу составляют *меры по совершенствованию практики применения организациями норм по охране коммерческих секретов*. Анализ показывает, что в 48% случаев лицам, совершившим дисциплинарный проступок, был объявлен выговор, в 31% — замечание, в 9% — увольнение было произведено не на основании подпункта «в» пункта 6 ст. 81 ТК РФ, а по другим мотивам, в 12% — взыскание не применялось в силу различных причин (сложность доказывания ущерба, администрацией не был установлен режим коммерческой тайны и др.). Характерно, что в 31% случаев администрацией не был соблюден порядок применения дисциплинарных взысканий, половина работников, допустивших нарушения, не представили письменные объяснения, и только в 20% случаев от них были получены объяснения в письменной форме. Факт совершения лицом правонарушения режима КЗИ в 35% случаев обсуждался в трудовом коллективе, что имеет общепреventивное значение для предупреждения таких нарушений. Опрос законопослушных работников, имевших доступ к КЗИ, показывает, что эффективными мерами по предупреждению данных нарушений являются: уменьшение или прекращение выплат в денежной форме — 90%; увольнение — 70%; материальная ответственность — 65%; обсуждение поведения нарушителя на собрании трудового коллектива — 43%; беседа руководителя подразделения с нарушителем — 29%; ограничение профессионального роста и карьеры — 25%; иные дисциплинарные взыскания — 15%.

Эти данные свидетельствуют о сложившейся в организациях системе реагирования на совершение правонарушений в сфере обращения КЗИ и необходимости совершенствования практики применения дисциплинарных взысканий, использования материальных стимулов, а также о степени восприятия работниками ограничений, которые могут быть установлены в отношении лиц, нарушающих нормы, что должно учитываться в воспитательно-профилактической работе.

<sup>1</sup> См.: *Северин В.А.* Развитие законодательства о коммерческой тайне // Право и государство: теория и практика. 2006. № 1. С. 38—49.

<sup>2</sup> См.: Сб. статей «Актуальные проблемы коммерческого права. Вып. 2 / Под ред. проф. Б.И. Пугинского. М., 2005.

<sup>3</sup> *Пугинский Б.И.* Коммерческое право России. М., 2005. С. 35.

<sup>4</sup> *Попондуполо В.Ф.* Природа коммерческого (предпринимательского) права // Актуальные проблемы науки и практики коммерческого права. Вып. 5. СПб.: Изд-во гос. ун-та. М., 2005. С. 12—13.

информации, а также для разработки дополнительных мер по предупреждению или нейтрализации внешних и внутренних факторов, угрожающих жизнедеятельности организации. Методы, применяемые в процессе контрольной деятельности и АИ в сфере обращения КЗИ, имеют свои недостатки и преимущества. Комплексное их использование позволит повысить уровень достоверности результатов исследования. Рассмотрим методы, которые применяются в контрольной деятельности.

В литературе большинство авторов исходит из концептуальных положений, сформулированных В.Г. Афанасьевым, Ю.М. Козловым, А.П. АLEXИНЫМ и др., о том, что контроль — это функция управления, содержанием которой является: 1) наблюдение и проверка соответствия процесса функционирования объекта принятым управленческим решениям, основанным на законах и подзаконных актах, стандартах, правилах и приказах; 2) выявление результатов воздействия субъекта на объект, допущенных отклонений от требований управленческих решений, от принятых принципов организации и правового регулирования<sup>1</sup>.

Вопросы организации контроля в сфере хозяйственной деятельности достаточно полно рассмотрены в монографии Е.А. Кочерина<sup>2</sup> еще в советский период, и многие из них не потеряли своей актуальности сегодня. Вместе с тем в рыночных условиях большая часть сформулированных им положений нуждается в пересмотре и дополнении. В настоящей работе определены теоретические положения, позволяющие раскрыть специфику организации контроля на корпоративном уровне в сфере обращения КЗИ с учетом новых управленческих технологий, включающих контроль в число важнейших средств достижения целей коммерческой организации. Закон о коммерческой тайне (ст. 10) обязывает правообладателя осуществлять контроль обращения КЗИ, однако речь идет не об административном контроле со стороны органов государства, а о корпоративном контроле, на уровне организации.

<sup>1</sup> См.: Афанасьев В.Г. Человек в управлении обществом. М., 1977. С. 107–125; Управление и корпоративный контроль в акционерном обществе: практическое пособие / Под ред. Е.П. Губина. М., 1999. С. 18–76; АLEXIN А.П., Кармолицкий А.А., Козлов Ю.М. Административное право Российской Федерации. Учебник. М., 2005. С. 377–392, и др.

<sup>2</sup> См.: Кочерин Е.А. Контроль в системе управления социалистическим производством. Вопросы теории и практики. М., 1982.

## ГЛАВА 5

### Научно-методическое обеспечение деятельности по охране конфиденциальности информации

#### § 1. Система и методы контроля в сфере обращения коммерчески значимой информации

**Контроль в сфере обращения коммерчески значимой информации: понятие, система, основные признаки.** Осуществление контроля за соблюдением установленного порядка обеспечения режима коммерческой тайны (далее — *контрольная деятельность*) и проведение *аналитических исследований* (АИ) в сфере обращения КЗИ выступают обязательным и необходимым направлением деятельности по выявлению и предупреждению правонарушений, связанных с неправомерным использованием и охраной конфиденциальной информации, и требуют применения научных методов для получения знания о явлениях и процессах, происходящих в данной сфере. Названные направления составляют основу научно-методического обеспечения охраны конфиденциальности информации и являются составной частью механизма правового регулирования обращения КЗИ и охраны ее конфиденциальности.

Использование научных методов при осуществлении контрольной деятельности и АИ создает предпосылки для получения обоснованных выводов и рекомендаций о возможных каналах утечки (ВКУ) КЗИ, о причинах и обстоятельствах, способствующих нарушениям режима, последствием которых является разглашение (утечка) такой

Результаты исследований позволили выявить специфику контроля в сфере обращения КЗИ. *Во-первых*, нужно учитывать объективную необходимость контроля, обусловленного факторами развития организации. К. Маркс писал, что «труд по надзору и управлению необходимо возникает всюду, где непосредственный процесс производства имеет вид общественно-комбинированного процесса, а не является разьединенным трудом самостоятельных производителей»<sup>1</sup>. *Во-вторых*, контроль осуществляется с ведома и по указанию собственника, который наделяет соответствующие органы управления<sup>2</sup> и отдельных лиц полномочиями по реализации контроля над трудовым процессом, включая и контрольные функции в сфере обращения КЗИ.

Контроль в сфере обращения КЗИ нужно рассматривать как действия по установлению состояния защищенности жизненно важных интересов организации в информационной сфере от угроз, как осуществление проверок качества и своевременности выполнения требований по сохранению коммерческой тайны, включая сведения, составляющие государственную тайну, переданные в порядке выполнения госзаказа, и персональные данные на работников.

Контроль осуществляется собственником или администрацией в соответствии с их полномочиями, определенными в ГК РФ, иных законах и корпоративных актах. В зависимости от объема контролируемой информации в организациях создаются органы защиты информации, получившие название «службы безопасности» (СБ), которые выполняют функцию контроля.

**Сферами контрольной деятельности** являются разработка и осуществление мер по защите собственником или уполномоченным им лицом информации, имеющей коммерческую значимость. В этой связи контроль можно рассматривать, *во-первых*, как функцию управления в области информационной безопасности (ИБ), выражающейся в целенаправленной деятельности по защите частных интересов организации. *Во-вторых*, контроль как завершающая стадия процесса производства и обмена товаров, включая маркетинг, ценообразование, финансы, планирование, бухгалтерский учет, управление персоналом. *В-третьих*, контроль как неотъемлемая часть лобой выполняемой работы и оказываемой услуги, связанной с ис-

пользованием КЗИ, и его проведение связано с принятием решений по обеспечению ИБ организации. Такой подход к раскрытию понятия контроля в сфере ИБ связан с обращением КЗИ и позволяет избежать ошибки, когда контроль связывается только с деятельностью СБ и рассматривается лишь как средство обнаружения недостатков. Возможность контроля значительно шире. Он может рассматриваться как средство активного побуждения к дозволительным действиям лиц, вовлеченных в сферу обращения КЗИ, как инструмент получения данных о состоянии производства и сбыта товаров, связанных с использованием и охраной КЗИ, как рычаг управления сферой безопасности организации.

В системе контроля важное место занимает **объект и субъект контроля**<sup>1</sup>. К числу *объектов контроля* в сфере обращения КЗИ могут быть отнесены системы производства, маркетинга, планирования, трансакционные издержки при заключении сделок и их элементы, а также отдельные процессы и операции. Примерами подконтрольных объектов можно назвать процесс создания продукции с охраняемыми параметрами, документов, содержащих КЗИ, и порядок доступа к ним и другие. *Субъектом контроля* выступает человек. Причем контролем могут заниматься отдельно уполномоченное лицо, группа лиц либо подразделение СБ, которые осуществляют в соответствии с корпоративными нормами и трудовым договором контрольные функции. Примером контроля, где субъектом выступает отдельное лицо, является ежедневная проверка руководителем подразделения либо работником СБ правильности учета движения грифованных документов.

По характеру взаимодействия и уровню управления, на котором находится субъект контроля, различают *внутренний и внешний контроль*<sup>2</sup>. Внутренним считается такой контроль, когда субъект и объект входят в одну систему, а внешним — когда они находятся на разных уровнях управления. В зависимости от задач, решаемых субъектами контроля, и предоставленных полномочий различают *линейный, функциональный и операционный типы контроля*<sup>3</sup>. При линейном контроле общее собрание акционеров принимает решение о состоянии

<sup>1</sup> См.: Кочерин Е.А. Указ. соч. С. 16–26; Котлер Ф. Основы маркетинга. М., 1990. С. 594–598, и др.

<sup>2</sup> См.: Кочерин Е.А. Указ. соч. С. 27–28.

<sup>3</sup> Там же. С. 20.

обеспечения безопасности общества. При функциональном — контролируется отдельное направление, например, обращение в организации документов с грифом «Коммерческая тайна». Получение характеристики состояния режима КЗИ по конкретной НИОКР или коммерческой сделке возможно при использовании операционного типа контроля. От объекта контроля следует отличать предмет контроля, т.е. то главное, существенное, что позволяет субъекту судить о состоянии объекта контроля. Объектом контроля могут быть различные виды работ, при выполнении которых используются КЗИ. Предметом контроля будет соблюдение корпоративных норм, регулирующих процесс обращения КЗИ при выполнении работ. Предмет контроля определяется для каждой системы контроля и каждого объекта контроля. Например, в СБ организации может быть создана система контроля за исполнением конфиденциальных документов. Объектом контроля в данном случае являются документы, имеющие гриф «Коммерческая тайна», а предметом контроля — сроки их исполнения работниками.

Изучение состояния работы по установлению режима коммерческой тайны и его обеспечению предполагает правильной выбор **целей, задач и функций контроля**. Цель контроля состоит в обеспечении единства решений и их исполнения, получении достоверной информации о состоянии предупредительной работы на ВКУ КЗИ и внесении корректив в эту деятельность с использованием различных правовых средств. *Общими задачами контроля* являются: оценка обособности установления мер режима КЗИ; определение фактического состояния подконтрольного объекта для получения данных об оперативной обстановке; получение, накопление, обработка и анализ данных о функционировании отдельных элементов системы охраны КЗИ; анализ деловых качеств и уровня профессиональной подготовки кадров в области обеспечения ИБ и другие. Исходя из общих задач, могут быть определены частные и конкретные задачи по каждому подконтрольному объекту с учетом полномочий, предоставленных субъекту.

Цель и задачи контроля определяют *функции субъектов контроля*, к которым можно отнести: наблюдение за ходом работ, связанных с использованием и охраной КЗИ; установление причин и обстоятельств, которые могут привести к утечке информации; вскрытие недостатков в использовании правовых средств и оказание помощи в реализации мер режима КЗИ; оказание воспитательного воздействия на формирование чувства «фирменного патриотизма» за

сохранность доверенных работникам коммерческих секретов и другие.

Реализация названных функций контроля по установлению режима коммерческой тайны и его обеспечению связана с наблюдением определенных требований, предъявляемых к его осуществлению. Контроль по возможности должен быть, во-первых, всеобъемлющим, т.е. охватывать все направления деятельности, по которым ведется работа, связанная с использованием и охраной КЗИ. Во-вторых, плановым, т.е. мероприятиям по установлению режима КЗИ и контроля за его исполнением должны отражаться не только в планах СБ, но и в производственных подразделениях, и быть доведены до исполнителей. В-третьих, целенаправленным, т.е. предусматривать достижение целей по всем направлениям в сфере обеспечения безопасности. В-четвертых, объективным, т.е. основанным не на личных взглядах и суждениях, а на основе анализа выполнения режимных требований. В-пятых, доказательным, т.е. основанным на фактах, документах и событиях, а не на догадках, домыслах и предположениях.

Анализ практики контроля при обращении КЗИ позволяет выделить его недостатки, которые имеют место в организациях.

Нарушается принцип комплексного и системного контроля в сфере обращения КЗИ. В организации порой контролируются не все направления, где обращается КЗИ. Отдельные из них остаются вне поля зрения СБ либо контролируются те, которые имеют второстепенный характер.

Контрольная работа не всегда ориентирована на изменения в хозяйственной ситуации, что требует ее совершенствования за счет внедрения информационных технологий и применения научных методов.

Контроль часто направлен не на предупреждение, а на фиксацию уже допущенных недостатков, а то и правонарушений, в деятельности, связанной с использованием и охраной КЗИ. Выявляются недостатки, которые невозможно устранить либо нецелесообразно в силу увеличения затрат на обеспечение режима КЗИ.

Не ведется должным образом предупредительная работа, поэтому одни и те же нарушения фиксируются при каждой очередной проверке.

Нарушается принцип планового ведения контроля, когда проверки состояния режима КЗИ организуются по факту разглашения (утечки) КЗИ и иных чрезвычайных происшествий.

Устранение названных недостатков возможно при условии привлечении к контролю ведущих специалистов, которые профессионально смогут расширить предметную сферу контроля и обеспечить его качество за счет использования знаний и умений; проведения исследований эффективности контроля на всех этапах установления режима коммерческой тайны и его обеспечения и разработки мер по совершенствованию контроля в сфере обращения КЗИ.

Получение объективной информации о состоянии режима КЗИ зависит от применения известных в науке *методов контроля*. Состояние и поведение объекта контроля определяются с помощью общих методов, а отдельных его характеристик — частных методов. Отдельные пространственные, временные, количественные, качественные и структурные характеристики объекта контроля познаются с помощью таких *частных методов контроля*<sup>1</sup>, как счетный, визуальный, сравнения, инвентаризации и другие. Изучение состояния режима КЗИ требует получения его характеристики с использованием так называемых *общих методов контроля*, как предварительный, направляющий, фильтрующий и последующий контроль<sup>2</sup>. *Метод предварительного контроля* используется на стадии формирования нового направления деятельности организации, разработки, проектирования какого-либо вида изделий, в процессе которых будет использоваться КЗИ. С его помощью устанавливается правильность сформулированных целей, достоверность и точность прогнозов об объекте контроля для определения сил и средств, стратегии и тактики контрольной деятельности. *Метод направляющего контроля* используется непрерывно с момента начала действий по слежению за состоянием контролируемого объекта до момента достижения цели. Это может быть начало коммерческих переговоров и подписание договора по их завершению. В ходе данного контроля осуществляется сравнение и оценка позиций участников переговоров, состояние поведения объекта контроля, корректирующее воздействие на их поведение. *Метод фильтрующего контроля* применяется на определенных, узловых этапах деятельности по установлению режима коммерческой тайны и его обеспечению. Чаще всего этот метод применяется в управленческой деятельности, связанной, например, с визированием в различ-

<sup>1</sup> См.: Кочерин Е.А. Указ. соч. С. 21.

<sup>2</sup> См.: Омаров А.М. Предпринимчивость руководителя. М., 1990. С. 186; Кочерин Е.А. Указ. соч. С. 21–26, и др.

ных подразделений грифованных документов. *Метод последующего контроля* применяется для определения результатов эффективности работы по охране КЗИ на этапах ее обращения, например, ежегодная проверка наличия грифованных документов. На практике характерным является комплексное применение названных методов.

В организациях применяются различные *виды и формы контроля*, выбор которых зависит от целей и задач контроля. Большое распространение получили такие *виды проверок*, как: плановые, внеплановые, разовые, внезапные, сплошные, выборочные, целевые, комплексные, а также *формы контроля*, как, в частности: заслушивание руководителей подразделений о состоянии режима КЗИ, оценка и учет работы в области безопасности при аттестации работников, прием зачетов по знанию режимных требований.

Использование сил и средств, обеспечивающих реализацию контрольной функции, зависит от хозяйственной ситуации, которая требует от руководителей соответствующих оценок, распоряжений и других организационных действий, объединенных понятием *процесс контроля*<sup>1</sup>, который рассматривается как упорядоченная деятельность уполномоченных лиц за установлением режима коммерческой тайны и его обеспечением. Процесс контроля характеризуется содержательной частью, позволяющей убедиться в том, что происходит в процессе контроля, организационной, отвечающей на вопрос — кем, где и когда производился контроль. Технологическая составляющая процесса контроля, объясняет — каким образом и в какой последовательности следует выполнять контрольные функции. *Структурно процесс контроля* может быть представлен в виде таких тесно связанных элементов, как: определение источников информации, от которых будут поступать сведения о состоянии объекта контроля; фиксирование контролируемых характеристик объекта; систематизация, обработка и получение контрольной информации; принятие решений по итогам контроля в зависимости от предоставленных полномочий; выработка и осуществление корректирующего действия на подконтрольный объект.

Важным элементом характеристики процесса контроля являются *действия*, связанные с возможностью оказания субъектами корректирующего воздействия на объект в ходе проведения контроля. Это позволяет поддерживать систему охраны конфиденциальности КЗИ

<sup>1</sup> См.: Кочерин Е.А. Указ. соч. С. 118–121.

в постоянной готовности реагирования на любые изменения в хозяйственной ситуации и отклонения в исполнении корпоративных норм.

Объективный характер процесса контроля зависит от установленных в организации требований к состоянию контролируемого объекта и осуществлению контроля за соблюдением порядка при обращении КЗИ. Решение этой задачи на практике представляет определенную сложность. Для предотвращения субъективизма нужно, во-первых, решить, какими параметрами можно измерить уровень безопасности, который, по мнению собственника организации, отвечает его представлениям. Во-вторых, определить комплекс мер по установлению режима КЗИ и систему контроля по его обеспечению.

Эффективность деятельности по установлению режима коммерческой тайны и его обеспечению требует *системного подхода к организации контроля*. Система контроля<sup>1</sup> в сфере обращения КЗИ представляет собой совокупность субъектов, объектов и средств контроля, которые взаимодействуют как единый механизм, включающий возможность выбора методов и процедур, используемых в процессе контрольной деятельности. Такой подход важен при проектировании системы контроля. Проектируемая система контроля должна быть уникальной, поскольку создается для каждого конкретного объекта контроля. В зависимости от объекта контроля определяются полномочия субъекта контроля. Средства контроля включают не только технические средства наблюдения и фиксации поведения объектов, но и используемые субъектом формы и методы контроля. Различают *простые и сложные системы контроля*. Первые служат только для получения сигнала, например, контроль за своевременностью возврата исполнителями документов в конце рабочего дня в СБ. Вторые служат для определения общего состояния объекта контроля или отдельных его направлений. Такая система выполняет аналитико-корректирующие функции. Например, контроль за первомерным доступом исполнителей к документам должен осуществляться непрерывно, что позволит вносить изменения в разрешительную систему в случае выявления нарушений.

**Проектирование системы контроля** предусматривает разработку первоочередном порядке корпоративных актов и других документов

организационно-методического характера. Выборочный анализ показывает, что такие руководящие и методические документы с различным содержанием и наименованием имеются у большинства организаций. В зависимости от целей, объектов и субъектов контроля организационные документы могут быть сгруппированы следующим образом: документы, содержащие общие положения о контрольной деятельности в сфере обеспечения безопасности организации; документы о контрольно-методической работе службы безопасности; документы, содержащие положения о контрольной деятельности в сфере безопасности филиалов, представительств и дочерних обществ; документы, включающие положения об участии руководящего состава в установлении режима коммерческой тайны и его обеспечении.

Правовое значение данных документов состоит в закреплении функции контроля за структурными звеньями организации и определении правомочий лиц, осуществляющих контроль в сфере обращения КЗИ. Разработка и принятие таких документов позволит, во-первых, избежать частых согласований по поводу уточнения и распределения прав и обязанностей в этой сфере, издания дублирующих документов, во-вторых, будет способствовать единообразному пониманию роли и места контроля в системе корпоративного управления сферой безопасности.

Кратко рассмотрим структуру организационных документов. В большинстве крупных организаций чаще всего разрабатывается отдельный документ, содержащий *общие положения о контрольной деятельности в сфере обеспечения безопасности*. В средних организациях и на малых предприятиях такие положения могут содержаться в различных внутренних документах. Анализ документов, которые разрабатываются в организациях, показывает, что в них включаются положения, раскрывающие понятия безопасности и угроз применительно к хозяйственной ситуации, цели и задачи контроля с учетом специфики деятельности на рынке товаров (работ, услуг); определяющие условия финансирования контрольной деятельности.

*Документы о контрольно-методической работе службы безопасности* учитывают особенности, которые присущи профессиональному подразделению, специально созданному для разработки и осуществления мер безопасности в организации. Учитывая задачи, решаемые СБ, за ней закрепляются определенные полномочия в проведении контрольно-методической работы. Кроме того, регламентируются порядок учета и отчетности, дополнительно определяется круг

<sup>1</sup> См.: Конерин Е.А. Указ. соч. С. 145–146; Стрельченко О. Организация защиты коммерческой тайны предприятия // Контроллинг. 1992. № 2, и др.

полномочий каждого подразделения, входящего в состав СБ, что позволяет исключить дублирование в сфере контроля и обеспечить взаимодействие с производственными подразделениями.

*Документы, содержащие положения о контрольной деятельности в сфере безопасности филиалов, представительств и дочерних обществ,* учитывают специфику их взаимоотношений с основным обществом. В организациях, имеющих обособленные подразделения, возникают общие вопросы обеспечения безопасности при производстве и реализации продукции, что требует единого подхода в осуществлении контроля за сферой обращения КЗИ. Права и обязанности по контролю за состоянием режима КЗИ определяются исходя из задач обособленного подразделения, или условий договора с дочерним обществом, а организационно-методическая работа ведется силами основного общества.

*Выбор сферы и объектов контроля за исполнением требований по установлению режима коммерческой тайны и его обеспечению.* Задачей любой организации является определение сфер, направлений и объектов контроля, сил и средств, используемых в процессе контроля. Подход к выбору сферы контроля объясняется сосредоточенностью КЗИ в определенных местах, возможно, и в различное время, при выполнении работ и оказании услуг. Это могут быть места постоянного и временного хранения документированной КЗИ и сведения, которые используются в процессе хозяйственной деятельности, являющейся критериями для выделения сфер контроля.

Заслуживает внимания контроль *корпоративного управления в области обеспечения безопасности организации.* Можно выделить такие направления, как проверка исполнения требований законов и корпоративных актов, решений органов управления на угрозы в сфере обращения КЗИ, исполнение документов, определяющих порядок установления режима коммерческой тайны и его обеспечения, что, по существу, определяет эффективность механизма охраны КЗИ. На практике чаще всего внимание уделяется контролю тех сфер, где документы и изделия, содержащие КЗИ, *постоянно находятся на хранении в специально выделенных помещениях,* и поэтому требуют их физической сохранности от хищения, недостачи (утраты). Не меньшее внимание уделяется *документам и изделиям, временно хранящимся у исполнителей,* используемым ими при выполнении производственных функций.

Безусловно, каждой сфере присущи свои характерные направления контроля, которые определяют *объекты контроля.* В сфере

корпоративного управления в области обеспечения безопасности организации объектом контроля может быть исполнение решений общего собрания акционеров (учредителей), приказов и указаний по вопросам безопасности, своевременность разработки и внедрения документов, определяющих порядок охраны КЗИ в подразделениях; эффективность реализации планов мероприятий по охране КЗИ и др. В сфере обеспечения сохранности документов и изделий в местах их постоянного или временного хранения объектами контроля являются, во-первых, выполнение требований корпоративных норм, определяющих порядок хранения документов и изделий в специально оборудованных и охраняемых помещениях, в целях изготовления продукции и местах, где проводятся исследования, опытно-конструкторские работы и испытания опытных образцов. Во-вторых, учет обработки документов и технической документации к изделиям.

В литературе большинство авторов<sup>1</sup> отмечают сложившуюся на практике определенную схему обработки конфиденциальных документов. Технологическая схема обработки конфиденциальных документов включает следующие этапы: прием, первичная обработка, предварительное рассмотрение и распределение поступивших документов; традиционный учет поступивших документов и формирование справочно-информационного банка данных по документам; автоматизированный учет поступивших документов и формирование справочно-информационного банка данных по документам; оформление и учет носителей конфиденциальной информации; изготовление конфиденциальных документов; проверка наличия документов, дел и носителей информации; уничтожение документов, дел и носителей информации<sup>2</sup>. Этапы обработки в различных комбинациях могут использоваться организациями. Документооборот, сопровождающий деятельность организации, урегулирован внутренними документами, и поэтому необходим контроль исполнения требований режима на каждом этапе обработки документов.

<sup>1</sup> См.: *Александров А.И.* О составе защищаемой информации // Безопасность информационных технологий. М., 1999. № 2; *Герасименко В.А., Малюк А.А.* Основы защиты информации. М., 1997. С. 321, 501–503, и др.

<sup>2</sup> См.: *Степанов Е.А., Корнеев И.К.* Информационная безопасность и защита информации. М., 2001. С. 272–298.

Периодичность и сроки проверок устанавливаются отдельно для каждого объекта контроля с учетом специфики сферы контроля-ной деятельности, что связано с *проектированием системы контроля*. Суть этой работы состоит в определении руководством организации алгоритма действий по решению задач контроля, которые описаны в *регламенте контрольных работ*. Для каждого уровня управления системой охраны КЗИ присущи свои правила, регулирующие порядок контрольной деятельности. Использование регламента контрольных работ в иерархии управления организацией и отдельными подразделениями, позволяет получать информацию об объекте контроля, о составе лиц, занятых контролем с использованием конкретных методик, о результатах контроля по выявлению и предупреждению правонарушений в сфере обращения КЗИ. С учетом периодичности контроля, например, установленного каждый день по окончании рабочего дня, еженедельно или ежемесячно, такая работа позволяет, во-первых, установить фактическое положение дел в сфере охраны КЗИ в местах постоянного хранения документов, на рабочих местах при выполнении НИОКР, изготовлении продукции, при заключении сделок. Во-вторых, судить о том, кто из субъектов осуществлял контроль и какие методики при этом были использованы. В-третьих, выявить частоту нарушений норм корпоративного и трудового права, степень возможного ущерба организации вследствие утраты документов, содержащих КЗИ, либо утечки такой информации к конкурентам. В-четвертых, данные контроля используются для усовершенствования системы мер по установлению режима и его обеспечению. В-пятых, использование регламента требует, с учетом меняющейся хозяйственной ситуации, внесения в него изменений в части выбора объектов, использования сил и средств контроля.

**Общая характеристика систем контроля в организациях.** Анализ материалов о контрольной деятельности в сфере обращения КЗИ показывает, что *в организациях функционируют различные системы контроля*. Многие из них были разработаны еще в советский период и успешно применяются в настоящее время. Системы контроля в рассматриваемой сфере являются частью управленческих информационных систем контроля, описывающих систему управления организацией с помощью сбалансированных показателей ее деятельности. Их техническое и программное обеспечение напрямую зависит от используемых базовых технологий информационных систем.

Система контроля в области обеспечения безопасности организации в ее функциональном выражении должна рассматриваться как

единый механизм, включающий различные, относительно самостоятельные, но взаимосвязанные и дополняющие друг друга системы, работающие на различных уровнях управления. В этом направлении на концептуальном уровне еще в советский период были сформулированы предложения<sup>1</sup> по созданию и внедрению в практику деятельности режимно-секретных органов (РСО) оборонных отраслей промышленности *автоматизированной системы управления режимным обеспечением* (АСУРО) работ. Одной из функций системы был контроль за обеспечением режима секретности. В частности, были подготовлены предложения по автоматизации контроля за режимным обеспечением НИОКР, сформулированы принципы и этапы исследовательских и проектных работ, связанных с решением задач справочного, учетного и контрольного характера в подразделениях РСО, технико-экономическое обоснование целесообразности работ по созданию АСУРО на базовом предприятии, предложения по программно-математическому<sup>2</sup> и техническому<sup>3</sup> обеспечению АСУРО. Отдельные элементы данной системы контроля сегодня используются организациями.

Опираясь на многолетний опыт организаций в сфере обеспечения режима охраняемой информации, охарактеризуем известные и зарекомендовавшие себя на практике отдельные системы контроля. Система *коллективного контроля* предназначена для наблюдения за исполнением корпоративных требований по обеспечению режима конфиденциальности работ, выполняемых в структурных подразделениях. Имеющаяся база данных характеризует состояние работ по выполнению режимных требований, подлежащих контролю (объект контроля), и используется для удовлетворения информационных потребностей пользователей, осуществляющих контроль (субъект контроля). Внесение в картотеку отметок о выполнении режимных требований осуществляется уполномоченными работниками.

Электронная картотека ведется СБ или одним из ее подразделений. Администратором базы данных является, как правило, на-

<sup>1</sup> См.: Северин В.А., Савков Н.П. К вопросу о разработке АСУРО // Сб. докладов межотраслевой научной конференции «Защита информации на объектах ЭВТ». М.: ЦНИИ «Монолит», 1988.

<sup>2</sup> См.: Северин В.А., Барменков А.Н. Вопросы программно-математического обеспечения АСУРО. М.: ЦНИИ «Монолит», 1988.

<sup>3</sup> См.: Северин В.А., Васин О.Н. Технические средства АСУРО. М.: ЦНИИ «Монолит», 1988.



чальник или заместитель начальника подразделения СБ, который ознакомлен с функциями персонала, участвующего в охране КЗИ, осуществляет доступ пользователей к базе данных с учетом установленных ограничений, поддерживает технологию обеспечения безопасности данных. Он осуществляет постановку документов на контроль; напоминает исполнителям о приближении сроков окончания работы; вносит в карточку данные о состоянии исполнения режимных требований, поступающих от руководителей подразделений; информирует руководство организации о ходе исполнения режимных требований и причинах их нарушения; вносит по необходимости изменения в сроки исполнения задания и состав работников-исполнителей; снимает по решению руководства с контроля ранее установленные режимные требования. Обязательной функцией администратора является подготовка итоговых документов по результатам контроля с анализом состояния дисциплины и возможных потерь, которые могут наступить вследствие неисполнения режимных требований. Данная система контроля с использованием ЭВМ позволяет вести оперативный контроль за исполнением режимных требований, корректировать действия персонала, закрепленного за конкретными объектами контроля, накапливать информацию о функционировании системы и эффективности ее работы.

Следующей системой, которая давно используется в крупных организациях, является *автоматизированная система контроля исполнения документов*, содержащих КЗИ. Система представляет собой комплекс правил, определяющих разрешительный порядок выдачи заданий работникам и их доступа к документам, проверки сроков и качества их исполнения, а также процедуры автоматизированной обработки контролируемой информации<sup>1</sup>. Она позволяет оценивать уровень исполнительской дисциплины с использованием коэффициента качества работы, включающего критерии своевременности выполнения задания и его значимости для организации. Функционирование системы связано с кодированием объектов и субъектов контроля, разработкой форм документов, приемом и оценкой данных о фактическом исполнении документов. Возможности системы используются в деятельности СБ, которая осуществляет контроль за соблюдением формальных процедур, связанных с передачей документов, содержащих КЗИ, в подразделения и ознакомлением с ними

работников. Решение задачи осложняется тогда, когда в организациях имеются обособленные подразделения, территориально находящиеся в различных субъектах Федерации. В этих условиях без эффективной системы контроля за обращением грифованных документов увеличивается опасность утечки информации. Контроль за исполнением таких документов ведется централизованно работниками конфиденциального делопроизводства основного общества с участием представителей филиалов и дочерних обществ. Определяются последовательность прохождения документов в обособленных подразделениях и порядок ознакомления с ними исполнителей. Указывается срок возврата документов. Такой порядок позволяет контролировать процесс прохождения документов, содержащих КЗИ, иметь данные о месте их нахождения и осуществлять координацию действий работников по срокам исполнения.

На практике достаточно распространено является *система контроля за соблюдением режима конфиденциальности информации при осуществлении организацией внешних связей*. Контроль за обеспечением режима КЗИ при проведении совместных работ с контрагентами ведется на основании договора, с учетом принятых сторонами обязательств по соблюдению условий конфиденциальности. В документах, прилагаемых к договору (единый план мероприятий по обеспечению режима и др.), определяются сферы и объекты контроля, круг работников, участвующих в совместных работах, порядок доступа к КЗИ и процедуры контроля. Система в этом плане может выполнять предупредительную роль, т.е. фиксировать несанкционированные контакты участников, выполняющих совместные работы, с лицами, не имеющими к ним отношения. Решение задачи по созданию такой системы зависит от предварительного согласования с контрагентом режимных требований, которые в одинаковой степени должны соблюдаться сторонами. Желательно, чтобы договоренность об этом была достигнута перед подписанием договора о совместной работе. Такой порядок позволит СБ предварительно организовать работу по установлению режима коммерческой тайны в подразделениях, которые будут участвовать в совместных работах.

Рассмотренные принципиальные положения, касающиеся работы отдельных систем контроля, используются при формировании *системы контроля за деятельностью работников-исполнителей в сфере обращения КЗИ*. В ряде организаций используются с применением ЭВМ различные модифицированные варианты *универсальной автоматизированной системы контроля исполнения (УАСКИ)*, кото-

<sup>1</sup> См.: Степанов Е.А., Корнеев И.К. Указ. соч. С. 154–162.

рая была разработана и внедрена в 70-х гг. XX в. на предприятиях промышленности, торговли, строительства и транспорта<sup>1</sup>. Система УАСКИ позволяла на функциональном уровне осуществлять упорядочение выдачи заданий и контроль за сроками их исполнения, учет оценки качества выполнения заданий, определять текущие значения обобщающих показателей качества работы, готовить предложения по стимулированию и повышению качества работы. Система являлась непрерывной частью комплекса общей системы управления предприятием. Принципы этой системы были использованы при внедрении ЭВМ в практику РСО отдельных предприятий. Автоматизированный контроль исполнения корпоративных решений продолжает оставаться актуальным и в рыночных условиях. Сегодня эта система успешно применяется СБ на основе использования принципов линейного контроля в общей структуре управления информационными системами. Проектирование системы ориентировано на предметную область контроля за исполнением мероприятий в сфере безопасности и состоянием качества работы исполнителей по охране КЗИ. Среди ученых, занимающихся проблемами информации о безопасности, нет единства по поводу показателей, характеризующих эту предметную область<sup>2</sup>. Принцип линейного контроля, на наш взгляд, позволяет руководителям различных уровней систематически осуществлять контроль за выполнением работниками обязательных договоров и закрепленных в трудовых договорах, положениях о структурных подразделениях, должностных инструкциях, приказах и распоряжениях.

Контроль исполнения режимных требований, как функция системы управления безопасностью организации, имеет двоякий характер. С одной стороны, контролю подвергается производственный процесс, связанный с производством и реализацией товаров (работ, услуг), в рамках которого циркулирует охраняемая информация, а с другой — участие в этом процессе конкретного работника или подразделения, обеспечивающих охрану конфиденциальности КЗИ. Результаты контроля позволяют одновременно судить о положении дел в подразделениях и качестве работы исполнителей, которые являются критериями оценки для материального стимулирования.

<sup>1</sup> См.: Кочерин Е.А. Указ. соч. С. 194–195.

<sup>2</sup> См.: Критерии оценки состояния информационной безопасности России в гуманитарной области. М.: МГУ, 2003.

Данные контроля о состоянии исполнительской дисциплины используются администрацией в воспитательной работе. Существует тесная взаимосвязь *контрольной деятельности и воспитательной работы*. Известно, что в условиях бесконтрольности даже хорошие работники постепенно теряют свои деловые качества, эффективность труда их снижается. Требованиям бесконтрольности и систематический контроль за исполнением обязанностей руководителя и систематически способствуют воспитанию у работников чувства ответственности за порученное дело, вносят элементы организованности и аккуратности при работе с КЗИ, способствуют совершенствованию стиля руководства на всех уровнях управления по обеспечению безопасности.

Контроль за исполнением работниками возложенных на них обязанностей должен увязываться с *оценкой их труда*. Опыт многих предприятий подтверждает, что воспитательная функция контроля за исполнением режимных требований будет эффективной в том случае, когда контроль за деятельностью работников сочетается с оценкой качества выполненных ими обязанностей в сфере обращения КЗИ. Результаты контроля исполнения, выраженные в количественной форме, дают возможность наглядно сравнивать показатели качества трудового участия работников в отделном трудовом коллективе, анализировать динамику изменения уровня исполнительской дисциплины, увязывать показатели качества работы со стимулированием трудовой деятельности.

Необходимо подчеркнуть, что *оценка качества работы* всегда является важным организационным моментом в трудовых отношениях. Независимо от того, выражается ли эта оценка в виде конкретного показателя, словесного одобрения или порицания, поощрения или взыскания, она дает возможность работнику лучше понять характер предъявляемых к нему требований по поводу охраны КЗИ, определить линию своего поведения с учетом сложившейся ситуации и принятых управленческих решений. Хотелось отметить ряд недостатков, связанных с оценкой труда работников. Во-первых, оценка качества труда работников порой зависит от результатов деятельности всего трудового коллектива, подразделения или организации. Обезличенная оценка труда работников, игнорирование их личных результатов, уравниловка в оплате труда, имевшая место в советский период, противоречит принципам рыночной экономики, отрицательно влияет на уровень дисциплины и ответственности работников за порученное дело, ведет к снижению их трудовой актив-

ности. Во-вторых, на этом фоне могут процветать недисциплинированность и безынициативность отдельных работников, поведение которых приводит к снижению общих показателей работы подразделения, что в конечном итоге отражается на материальном стимулировании добросовестных работников.

*Внедрение в организациях системы контроля исполнения и оценки качества работы исполнителей конфиденциальных работ* оказывает, во-первых, эффективное воздействие на практику корпоративного планирования деятельности в области обеспечения безопасности подразделения, стимулирует исполнителей. Во-вторых, способствует реализации планов режимных мероприятий по охране КЗИ; выявлению и предупреждению несвоевременного и некачественного исполнения обязанностей в сфере обращения КЗИ. В-третьих, позволяет осуществлять координацию и взаимодействие с контрагентами по поводу охраны конфиденциальности КЗИ при выполнении совместных работ, используя для этого необходимые ресурсы.

Разработка и внедрение различных систем контроля за обеспечением режима КЗИ тесно связаны с выбором определенных **технологий контроля**. Под технологией контроля понимается механизм, включающий выбор методов и процедур<sup>1</sup>, с помощью которых происходит отбор данных о состоянии контролируемого объекта в сфере обращения КЗИ. Сущность технологических процессов контроля в сфере обращения КЗИ раскрывается непосредственно путем определения методов контроля, которые будут применяться в данной системе контроля; установления показателей, позволяющих оценивать и описывать состояние объектов контроля; определения порядка и сроков получения информации о состоянии подконтрольного объекта; определения последовательности сбора, обработки, фиксации и передачи информации о состоянии подконтрольного объекта с учетом сил и средств, привлекаемых для этих целей; установления порядка и сроков реагирования на полученную в ходе контроля информацию и осуществления корректирующего воздействия на подконтрольные объекты.

Нужно отметить, что для каждой системы контроля, действующей в сфере охраны КЗИ, может быть разработана своя технология контроля. Технологическая цепочка изучения состояния обеспечения безопасности организации состоит из узловых звеньев,

<sup>1</sup> См.: Кочерин Е.А. Указ. соч. С. 171.

исследование которых имеет практическое значение. Информация об этом может быть получена, во-первых, путем изучения договорной, финансово-экономической, управленческой и иной документации, относящейся к контролируемому объекту; во-вторых, обследования практики обеспечения охраны КЗИ; в-третьих, установления неформальных контактов с руководителями и исполнителями конфиденциальных работ.

Проведение проверок состояния обеспечения безопасности организации требует использования различных *методов практической осуществления контрольной деятельности*, в частности, по своему значению выделяют методы стратегического и тактического контроля. Суть первого метода заключается в том, что для получения нужной информации о состоянии охраны коммерческих секретов не нужен сплошной контроль всех без исключения материалов. Как правильно отмечает А.М. Омаров, «стратегический контроль оправдан тем более, что по сравнению с контролем всех видов деятельности он требует меньших затрат и оставляет больше места для неформального контроля»<sup>1</sup>. Достаточно охватить контролем узловые вопросы, значение которых позволит понять, где сосредоточиваются важные сведения, каким образом осуществляется их обращение и какие приняты меры охраны. При изучении этих вопросов работники СБ знакомятся с документами и материалами, содержащими информацию о состоянии обеспечения безопасности. К их числу следует отнести: 1) материалы предыдущих проверок о состоянии режима КЗИ (заключения о надежности охраны коммерческих секретов с использованием различных средств; акты о состоянии учета документов и изделий, содержащих КЗИ, др.; 2) реагирование администрации на имеющиеся недостатки в сфере обеспечения безопасности (годовые отчеты о работе службы безопасности, доклады на общих собраниях акционеров (учредителей), промежуточные отчеты руководителей подразделений о состоянии режима КЗИ; протоколы общих собраний акционерного общества, где обсуждались вопросы, относящиеся к охране коммерческих секретов.

Важные сведения могут быть получены путем изучения документальных материалов, относящихся к *аналитической работе*, в частности, сделать выводы не только о количестве проведенных аналитических исследований, но и использовании их результатов для со-

<sup>1</sup> См.: Омаров А.М. Указ. соч. С. 186.

вершения системы безопасности. Изучение материалов, относящихся к аналитической работе, осуществляется в первоочередном порядке, что способствует осмыслению других направлений обеспечения безопасности организации и определяет ход дальнейшей проверки.

*Метод тактического контроля* ориентирован на проверку отдельных направлений и объектов контроля. Он применяется для *изучения порядка учета документов и изделий, содержащих КЗИ*, с целью оценки эффективности действующей системы сохранения секретов и правомерности принимаемых решений. В получении информации о фактическом состоянии дел в сфере обращения КЗИ важное место занимают *отчеты и доклады предыдущих лет о состоянии безопасности*, которые содержат обобщенную, в основном субъективную, оценку результатов работы по обеспечению охраны коммерческих секретов. Изучение таких документов позволяет, во-первых, структурно выделить главные направления, на которых было сосредоточено внимание подразделений по охране КЗИ, а также установить, какие меры предпринимались по предупреждению правонарушений в этой сфере. Во-вторых, раскрывает своего рода «панорамы» предстоящей проверки, способствует более четкому определению направлений проверки и мер по совершенствованию обеспечения безопасности. Определенные данные можно получить при *изучении протоколов, приказов и распоряжений*, в которых фиксируются сведения о фактах и событиях, имевших место в предшествующий период обращения КЗИ (сведения об утрате документов и изделий, о разглашении КЗИ, о результатах служебного расследования и наказании работников и т.д.). Изучение материалов о *планировании мероприятий по охране КЗИ* позволяет получить представление об уровне профессиональной подготовки работников СБ, занятых разработкой планов по защите КЗИ; оценить содержание планов с учетом изменения хозяйственной ситуации, а также эффективность используемыхправовых средств по обеспечению безопасности.

Широкое применение в практике получил *сравнительный метод*, сущность которого состоит в сопоставлении определенных показателей, характеризующих состояние обеспечения безопасности организации и соответствие его требованиям законодательства и корпоративных актов. Метод сравнения позволяет установить количественные и качественные показатели состояния режима КЗИ и определить тенденции использования форм и методов обеспечения безопасности. С помощью этого метода можно выявить тенден-

ции расширения или ограничения круга лиц, допускаемых к документам и работам, содержащим КЗИ. Объяснение причин уменьшения или увеличения числа лиц, имеющих допуск и фактически ознакомившихся с КЗИ, следует увязывать с тенденцией спада или роста производства и продаж товаров, при изготовлении и реализации которых используется КЗИ. Если причины не установлены, то не исключены нарушения в порядке доступ лиц к КЗИ. Применение сравнительного метода позволяет установить тенденцию роста или снижения нарушений режима КЗИ в подконтрольном подразделении путем анализа количества выявленных нарушений за определенный период. Отдельно по годам учитывается размер возможного ущерба. Тенденции уменьшения или увеличения количества нарушений следует увязывать с числом проведенных проверок и реализацией режимных мер.

Проверка различных аспектов практической деятельности по охране коммерческих секретов требует использования и других методов, таких как *наблюдение, устный опрос и анкетирование. Наблюдение*, как представляется, должно проводиться не беспорядочно, а по определенному плану. Должны быть заранее сформулированы вопросы, ответы на которые будут получены в ходе наблюдения. Данные наблюдения фиксируются и служат доказательством совершения правонарушения, а также используются в предупредительной работе. *Устный опрос* позволяет выяснить мнение работников производственных подразделений и СБ о системе обеспечения безопасности и ее отдельных элементах. *Метод анкетирования* позволяет сократить время на проведение устных опросов. Для проведения письменного опроса разрабатываются анкеты, которые заполняются работниками подразделений. Названные методы используются в комплексных проверках обеспечения безопасности организации.

При оценке фактического состояния дел в области обеспечения безопасности организации следует учитывать *психологические аспекты*<sup>1</sup>, влияющие на объективность выводов. На характер оценки состояния дел могут оказывать воздействие предвзятые прогнозы и ожидания конкретных событий, которые были сделаны субъектом

<sup>1</sup> См.: Ратинов А.Р. Применение психологических методов в социально-правовых исследованиях // Проблемы методологии и методики правоисследования. М., 1974. С. 124–136, и др.

контроля до начала проверки. Особенно их воздействие усиливается, когда руководитель СБ, например, заранее убежден в том, что в подконтрольном подразделении имеют место нарушения, слабо поставлены учет и отчетность. Оценка будет объективной, если субъект контроля не будет заранее прогнозировать итоги проверки до ее окончания; оценивать состояние дел без учета мнения заинтересованных сторон, не будет формулировать выводы о состоянии обеспечения безопасности объекта без учета документально подтвержденной тенденции. Порой субъект контроля, оценивающий состояние дел в организации, находится под воздействием последнего события, произошедшего в конце проверки. Для исключения отрицательного воздействия «эффекта последнего события» на оценку состояния дел следует возвратиться к ранее сделанным выводам по подконтрольному объекту и расположить их в обратной последовательности. Другими словами, последнее событие сделать первым выводом и проследить логику и взаимосвязь с ним всех других выводов.

Обобщение материалов ряда организаций по установлению фактического состояния защиты охраняемой информации позволяет сделать вывод о комплексном применении различных методов. Критериями оценки состояния дел в сфере обращения КЗИ являются: количество и характер выявленных ВКУ КЗИ и меры, принятые по их нейтрализации и предупреждению; число и характер допущенных нарушений режима и реагирование на них руководством; соответствие содержания мер, направленных на установление режима коммерческой тайны и его обеспечение, фактически сложившийся хозяйственной ситуации; уровень управления системой обеспечения безопасности и его соответствие задачам организации.

## § 2. Организация и методика аналитических исследований в сфере обращения коммерчески значимой информации

*Характеристика аналитической работы в системе научнометодического обеспечения деятельности по охране конфиденциальности информации.* Деятельность коммерческой организации требует надежного комплексного правового, организационного и информационно-аналитического обеспечения. Принятие управленческих решений напрямую зависит от получения качественной, до-

стоверной и своевременной информации о конкурентах для получения преимуществ в конкретном секторе рынка. Такая информация может быть получена организацией путем ведения конкурентной разведки и противодействия недозволенным законом способам промышленного шпионажа, используемым конкурентами. Понятие «конкурентная разведка» постепенно входит в лексику рыночной экономики России. Происходит своего рода «конверсия» государственных разведывательных технологий в сферу деятельности коммерческих организаций. В печати появляется все больше статей, посвященных этой проблеме. Конкурентная разведка ведется, как правило, с легальных позиций путем анализа открытых опубликованных источников информации<sup>1</sup>. Появление новых информационных технологий значительно облегчает решение задачи поиска информации. Относительная дешевизна доступа к информационным ресурсам Интернет, базам данных, системам поиска информации позволяет работникам организации готовить качественные материалы, пригодные для принятия решений. Стратегические решения по достижению конкурентных преимуществ на рынке принимаются организацией с учетом наличия собственной базы данных, часть которой составляет КЗИ, защищаемая от промышленного шпионажа.

Учитывая возможность получения конкурентами КЗИ с использованием различных способов промышленного шпионажа, организации должны принимать адекватные меры по предупреждению утечки (разглашения) сведений. Важным направлением в решении данной задачи является осуществление аналитической деятельности в сфере обращения КЗИ, которая тесно связана с правовой работой<sup>2</sup>. Она направлена на поиск и объяснение фактов правонарушений, совершаемых в сфере обращения КЗИ, причем на ранней стадии их обнаружения, в ходе проведения контрольной работы. Результаты аналитических исследований (АИ) в этой сфере позволяют судить о состоянии обеспечения безопасности в организации, о фактах, свидетельствующих о возникновении угроз и связанных с ними каналах возможной утечки КЗИ, о причинах и условиях, способствующих совершению правонарушений в этой сфере; формулировать реко-

<sup>1</sup> См.: Громова Ю. Тайное оружие конкурентной борьбы // Секрет фирмы. 2001. № 1; Материалы ЗАО «Специальная информационная служба» ([www.sins.ru](http://www.sins.ru)) и компании «Русское информационное пространство-М» ([www.ris.ru](http://www.ris.ru)) и др.

<sup>2</sup> См.: Пугинский Б.И., Неверов О.Г. Правовая работа: Учебник. М., 2004. С. 9–21.

мендации о возможных вариантах действий руководства относительно устранения последствий утечки КЗИ и о принятых мерах предупреждения нарушений в сфере обращения КЗИ.

В этой связи необходимо раскрыть **сущность аналитической работы**, занимающей центральное место в системе научно-методического обеспечения деятельности по охране конфиденциальности информации. Выполнение аналитической работы в сфере обращения КЗИ требует использования определенных способов и приемов, составляющих методологический аппарат. В науке принято различать общую и частную методологию. В философской литературе под общей методологией науки понимается учение о методах познания и преобразования действительности. В различных отраслях юридического образования действует частная методология. Цивилистической науке знания используются способы и приемы, которые используются для анализа и познания ее предмета и получения необходимого результата<sup>1</sup>. Судя по большинству публикаций в литературе, содержание общественных и естественнонаучных методов познания не претерпело существенных изменений при их применении в рыночных условиях хозяйствования. Вместе с тем о необходимости изменения направленности в научных исследованиях и получения научных фактов в процессе анализа хозяйственной деятельности справедливо отмечают многие ученые<sup>2</sup>. Специальное описание совокупности приемов и способов, применяемых в какой-либо деятельности или исследовании, составляет частную методологию. В данную совокупность входят не только технические приемы исследования, но и принципиальные теоретические положения, аксиомы мировоззренческого характера, определяющие путь научного исследования, пределы (границы) последнего, его основные взаимосвязи — внешние и внутренние. Аналитическая работа включает в свой арсенал не только метод анализа, но и другие методы.

Аналитические исследования в сфере обращения КЗИ опираются на основные философские категории, методы и приемы исследования, базирующиеся на теоретических положениях науки гражданского и коммерческого права и ряда отраслей публичного права

(криминология, административное и уголовное право и др.) и других наук гуманитарного цикла (социология, социальная психология, экономическая теория и др.).

Методология, используемая при проведении исследований этой сфере, включает не только категории, выражающие наиболее общие законы развития природы, общества и мышления, но и категории, отражающие специфические стороны, связи процесса познания и его воплощения в хозяйственную деятельность. При выполнении исследований в сфере обращения КЗИ используются следующие принципы: 1) причастность к действительности как к объективной реальности (применительно к возникающим угрозам безопасности организации и связанных с ними существующих возможных каналов утечки (ВКУ) КЗИ); 2) необходимость отличия существующих элементов от второстепенных, связанных с изучением хозяйственной ситуации в сфере обращения КЗИ; 3) признание постоянства и изменчивости элементов, составляющих систему ВКУ КЗИ, и мер по предупреждению нарушений режима в данной сфере; 4) учет историчности (фактора времени) изучаемых явлений, оказывающих влияние на процесс отнесения сведений к КЗИ, их использование и правовую охрану; 5) признание значения противоречий в развитии феномена КЗИ в условиях рыночной экономики; 6) конкретность и объективность при выборе объекта исследования.

Использование методологии имеет значение для получения научно обоснованных результатов исследования. Она позволяет четко определить границы исследования в сфере обращения КЗИ и возможность использования его результатов для развития теории и практики обеспечения безопасности организации; дает возможность избежать недооценки роли теории в объяснении процессов возникновения причин и обстоятельств, ведущих к образованию ВКУ, использованию правовых средств для предупреждения нарушений режима КЗИ; обеспечивает научную организацию АИ в сфере обращения КЗИ и оценку исследования проблем охраны конфиденциальности такой информации; предоставляет исследователям от упрощенного подхода к проблеме взаимосвязей ВКУ КЗИ с нарушениями режима КЗИ и другими, не изученными в правовом отношении явлениями, которые возникают в процессе информационной революции; позволяет получить не только новое знание о ВКУ, причинах и обстоятельствах, их обуславливающих, и об эффективности принимаемых мер предупреждения, но и понять существо изучаемых явлений применительно к деятельности организации.

<sup>1</sup> См.: Гражданское право. В 2 т. Т. 1 / Отв. ред. проф. Е.А. Суханов М., 2000. С. 49–52.

<sup>2</sup> Пугинский Б.И., Сафуллин Д.Н. Правовая экономика: проблемы становления. М., 1991. С. 27.

Методология имеет определенную связь с методикой исследования, которая разрабатывается на основе определенных его положений. Осуществление аналитической работы возможно на основе использования определенной методологии и методики, которые представляют собой систему своеобразных научных правил. Методология определяет общие правила, точнее, философские принципы, использование которых учитывает специфику объекта исследования в сфере обращения КЗИ. В этом смысле методология является механизмом, реализующим процесс аналитического исследования. Использование методики позволяет определить применительно к конкретному объекту исследования, в каком порядке и в какой последовательности следует применять те или иные методы. При этом определяется набор необходимых методов и устанавливаются правила их применения в АИ. Сама процедура использования методов есть техника исследования. С этой точки зрения, методика и техника АИ приближаются к практике осуществления такого исследования. В литературе аксиоматичным является утверждение о том, что между методологией и методикой АИ всегда существует тесная связь через методы научного исследования<sup>1</sup>. Причем каждая категория выполняет свою функциональную роль в научном исследовании. В этом плане можно говорить, что методология является своего рода стратегией, а методика позволяет решать тактические задачи в конкретном исследовании.

На практике исследователи чаще всего имеют дело с методикой АИ. *Под методикой АИ в сфере обращения КЗИ* следует понимать совокупность конкретных приемов, способов, средств (инструментариев) сбора, обработки и анализа информации о нарушениях режима КЗИ, о причинах и обстоятельствах, способствующих утечке охраняемой информации, о личности нарушителя режима КЗИ и мерах предупреждения нарушений в этой сфере. Результаты АИ принято считать выводы о состоянии обеспечения безопасности организации и рекомендации субъектам, осуществляющим предупредительную деятельность в сфере обращения КЗИ.

**Программа проведения аналитических исследований в сфере обращения КЗИ.** Подготовка АИ требует наблюдения определенных условий его организации и учета имеющихся ресурсов, и этим оно мало чем отличается от маркетингового исследования. Исследование но-

сит плановый характер и включает разработку программы и отдельных планов по анализу конкретных объектов исследования.

Программа содержит мероприятия, раскрывающие цель, задачи, объект, предмет и сроки исследования, силы, средства и используемые методики. Реализация программы предусматривает разработку плана проведения АИ с указанием сроков исполнения мероприятий и исполнителей. Программой определяются общие задачи АИ, содержание которых должно раскрывать масштабность и последовательность действий исследователей. К числу первоочередных задач следует отнести: изучение явлений и процессов, связанных с выявлением угроз безопасности организации, ВКУ КЗИ, и разработку мер по их предупреждению; обобщение эмпирических данных и получение новых фактов по предметной области исследования; рекомендации субъектам, занимающимся использованием и охраной КЗИ.

Наряду с постановкой общих вопросов определяют конкретные способы и процедуры исследования, в частности, по сбору и обработке информации. Например, когда целью АИ является выявление ВКУ КЗИ в связи с разработкой нового изделия и продвижением его на рынок, то задачами соответственно могут выступать: получение данных о состоянии режима конфиденциальности на объектах, где сосредоточены коммерческие секреты; определение ВКУ информации на участках деятельности таких объектов; установление причин и обстоятельств, способствующих утечке охраняемой информации; выработка рекомендаций по воздействию на условия, способствующие проявлению ВКУ, и мер по предупреждению нарушений. В процессе проведения исследования задачи могут уточняться, что может быть связано с изменением хозяйственной ситуации, недостаточно-стью финансирования исследований, возможностями использования сил и средств.

При выполнении исследований следует проводить различие между объектом и предметом исследования. Объектом исследования является сфера обращения КЗИ в отдельных подразделениях или в целом организации либо ее часть при выполнении договорных работ с контрагентами. Предмет исследования составляет та сторона объекта, которая непосредственно подлежит изучению в ходе проведения АИ, например, анализ обращения КЗИ при ведении коммерческих переговоров.

Важным является не только получение результатов исследования, но и правильное их оформление с учетом целей использования. В большинстве случаев по результатам АИ составляется отчет, к кото-

<sup>1</sup> См.: Спиркин А.Г. Указ. соч. С. 452–463, и др.

рому могут быть приложены цифровые, графические и иные данные, характеризующие состояние режима КЗИ на конкретных объектах, методики по выявлению ВКУ КЗИ и предложения по предупреждению нарушений в этой сфере. Материалы исследований используются для подготовки управленческих решений, поэтому должны содержать четкие, а не расплывчатые выводы и рекомендации, адресованные субъектам, о порядке внедрения результатов исследования.

Рекомендации, вытекающие из отчета, должны содержать сведения об использованных источниках информации. В зависимости от целей АИ используются различные источники, подтверждающие существование внешних и внутренних угроз безопасности организации, связанные с незаконным использованием КЗИ, раскрытием технологий производства и реализации товаров. Это могут быть отчетные данные о деятельности организации по обеспечению безопасности, ежегодно представляемые руководству и акционерам (учредителям). Изучение опыта ряда организаций показывает, что к таким сведениям следует относиться весьма осторожно. Порой они искажены в подразделениях и не всегда отражают реальное состояние дел по обеспечению безопасности.

В аналитической работе важно учитывать данные, характеризующие хозяйственную ситуацию на различных участках деятельности организации. В частности, это могут быть данные о контроле за использованием новейших технологий производства; о практике подбора и расстановки кадров на участках, где обращается КЗИ, и результаты их проверки на предмет лояльности фирме; о системе поощрения и взыскания работников; о прогнозах деятельности по продвижению товаров на рынок; о партнерах, контрагентах, конкурентах и их финансовом положении; о кредитной и инвестиционной стратегии организации; о результатах коммерческих переговоров по заключению договоров; о юридическом сопровождении коммерческих сделок и системе контроля за их исполнением, о порядке использования и передачи КЗИ; о методах защиты КЗИ от несанкционированного доступа. Такие данные можно получить на различных уровнях управления фирмой.

Данные анализа хозяйственной ситуации позволяют, во-первых, получить характеристику эффективности системы обеспечения безопасности на отдельных направлениях возникновения угроз, а также оценить уровень достаточности режимных мер. Во-вторых, сформулировать выводы о направлениях возникновения угроз, о причинах и обстоятельствах, способствующих совершению правонарушений, и

эффективности мер борьбы с ними. В-третьих, предложить прогнозы развития возможных изменений хозяйственной ситуации вследствие реализации угроз. В-четвертых, разработать предложения по повышению эффективности принимаемых предупредительных мер.

**Функциональные направления деятельности аналитических подразделений.** Реализация программы АИ предполагает организацию материального и кадрового обеспечения. В организациях для этой цели используются различные организационные структуры. В отдельных крупных и средних организациях создаются специальные штатные подразделения, выполняющие аналитическую работу. На малых предприятиях эта работа выполняется в основном в рамках нештатных творческих трудовых коллективов, образуемых для решения конкретных задач. Большинство подразделений, ведущих аналитическую работу в сфере обращения КЗИ, используют опыт аналогичных структур, которые функционировали в СССР в основном на предприятиях оборонной промышленности. Это объясняется существованием определенной преемственности в кадровом и методическом обеспечении этой деятельности, имеющей специфику в рамках правовой работы.

Аналитической работой по выявлению и предупреждению возможной утечки охраняемой в интересах государства информации начали заниматься в Советском Союзе в первой половине 60-х гг. XX в. Первые штатные аналитические подразделения появились на предприятиях министерств оборонных отраслей промышленности, в частности, в 1968 г. на предприятиях Министерства среднего машиностроения (МСМ) СССР, а спустя 20 лет они были созданы и в структуре Министерства радиопромышленности (МРП) СССР. Нужно отметить, что и в других отраслях народного хозяйства имелись аналогичные структуры. Подразделения, занимавшиеся аналитической работой, имели различное наименование («специальные научно-технические подразделения» (СНТП), аналитические отделения, сектора и т. д.). Изучение опыта их работы важно для определения направлений деятельности подразделений, действующих в настоящее время.

Аналитические подразделения, действовавшие в советский период, структурно состояли из двух групп специалистов-аналитиков. Первая группа специалистов занималась анализом организационно-правовых каналов утечки информации, вторая — технических каналов, с использованием различных технических устройств и аппаратуры. Такое разделение функций позволяло учитывать особенности



процесса выявления нарушений организационно-правового и технического характера и формулировать научно обоснованные предложения по разработке мер предупреждения.

**Правовой статус аналитических подразделений, действовавших в советский период**, определялся *типовым положением о специальном научно-исследовательском (научно-техническом), аналитическом подразделении предприятия*, утвержденным министерством. В нем была определена компетенция таких подразделений, права, обязанности и ответственность руководителей, направления деятельности по предупреждению утечки секретных сведений (ПУСС), охраняемых в интересах государства, и по противодействию иностранным техническим разведкам (ПД ИТР).

Аналитические подразделения являлись самостоятельным структурным подразделением и подчинялись непосредственно руководителю предприятия. Научно-техническое руководство их работой осуществлялось одним из заместителей руководителя предприятия, ответственного за научную (производственную) деятельность. Организационно-методическое руководство в части разработки и осуществления организационно-правовых мер по ПУСС, координации и методического обеспечения АИ и контроля эффективности ПД ИТР было возложено на заместителя руководителя предприятия по режиму. Оплата труда работников была отнесена к системе оплаты труда научных и инженерно-технических работников. Штатная численность подразделений определялась директором предприятия по согласованию с министерством, в зависимости от объема работ по ПУСС и ПД ИТР.

Начальник аналитического подразделения назначался на должность и освобождался от нее приказом руководителя предприятия по согласованию с руководителями главных управлений министерства по режиму, производственной либо научно-технической деятельности. Комплектование подразделений осуществлялось из числа инженерно-технических и научных работников, имевших опыт работы по основному направлению деятельности предприятия. Работа подразделений определялась перспективными и текущими планами предприятий по ПУСС и ПД ИТР и велась во взаимодействии с научными и производственными подразделениями, органами КГБ СССР, военными представительствами МО СССР и РСО министерств.

Анализ нормативных документов, определявших правовой статус аналитических подразделений в советский период, показывает,

что **основными направлениями их деятельности были выполнение исследований, методическая и организационная работа**. В части *выполнения исследований* — это выполнение НИР и ОКР (составных частей) по проблемам ПУСС и ПД ИТР; изучение технологического цикла разработки, производства, испытания образцов вооружения (В) и военной техники (ВТ), особенностей и условий проведения испытаний, начиная с ранних стадий; выявление возможных утечек сведений, разведоопасных участков работ; проведение анализа особенностей и зарубежных публикаций по междугосударственному научно-техническому сотрудничеству для определения осведомленности и разведустремлений спецслужб иностранных государств, стремящихся получить информацию о деятельности предприятия; сбор, систематизация и анализ данных, необходимых для разработки дополнительных мероприятий по ПУСС и ПД ИТР; изучение и анализ возможностей иностранной технической разведки (ИТР) по получению секретной информации с учетом профиля работ предприятия и особенностей его дислокации, определение видов и средств ИТР, которым необходимо осуществлять противодействие; исследование и оценка демаскирующих признаков признаков предприятия и разработка дополнительных мер защиты.

*Методическая работа* включала такие функции, как, в частности: разработка совместно с научно-техническими подразделениями и РСО руководящих и методических документов, определявших порядок организации и проведения работ по ПУСС и ПД ИТР; подготовка предложений к проектам ведомственных перечней сведений, подлежащих засекречиванию, перечней сведений, запрещенных к опубликованию в открытой печати, передачах по радио и телевидению; методическое руководство аналитической работой по ПУСС и ПД ИТР, планирование, координация и контроль этих работ.

*Организационная работа* состояла в рассмотрении и согласовании проектов технических заданий (ТЗ), приказов и указаний по предприятию, хозяйственных договоров на выполнение работ, стандартов предприятия, инструкций по ПД ИТР, соответствующих разделов конструкторской, технологической и отчетной документации с целью оценки полноты предусмотренных в них требований и мероприятий по ПУСС и ПД ИТР; осуществление контроля за выполнением норм по ПД ИТР при проведении работ и подготовка заключений о возможности эксплуатации объекта защиты; участие в работе по проверке состояния защиты объекта по ПУСС и ПД ИТР; учет выявленных ВКУ информации и принимаемых мер по их предупре-

ждению; составление годового отчета о работе по ПУСС и ПД ИТР для представления его в министерство и органы КГБ.

Анализ материалов ряда коммерческих организаций показывает, что для них в современный период характерными функциональными направлениями являются организационная и методическая работа и в меньшей степени выполнение исследований. Что касается держательной части функций в сфере защиты КЗИ, то они претерпели изменения. Это обусловлено условиями рыночной экономики и необходимостью защиты частных интересов. Хотя по-прежнему, как и в советский период, результаты аналитической работы используются главным образом, руководителями службы безопасности (СБ) и конкурентной разведки при разработке мероприятий, направленных на обеспечение эффективности разрабатываемых изделий и продвижения товаров на рынок. В этой связи *задачами аналитической работы* являются: изучение производственной, научной-исследовательской, опытно-конструкторской, коммерческой и иной деятельности с целью выявления и оценки противостоящих угрозам, анализ нарушений режима КЗИ, сбор и анализ данных об устремлениях и осведомленности конкурирующих фирм о проводимых в организации работах, позволяющих получить конкурентные преимущества на рынке.

Для решения этих задач в крупных организациях создаются *аналитические центры*<sup>1</sup>. Структурно такие центры входят в состав СБ и с учетом деятельности организации специализируются на охране КЗИ. Аналитическая работа рассматривается руководством фирм как неотъемлемая часть производственной деятельности, что отражается на правовом статусе и ресурсном обеспечении аналитических подразделений. Финансирование обеспечивается за счет выполнения договоров с контрагентами, в которых предусматриваются условия об охране КЗИ.

*Основными направлениями аналитической работы* являются: определение целей и задач по выявлению ВКУ КЗИ, оценка обоснованности мер по установлению режима КЗИ с учетом конкурентного развития техники и технологий; учет и анализ правонарушений режима КЗИ; изучение осведомленности конкурентов о результатах выполненных НИОКР и способах внедрения новаций в производ-

ство; подготовка рекомендаций по использованию правовых средств в сфере обращения КЗИ; рассмотрение и согласование тактико-технических заданий, технических заданий на проведение НИОКР в части выделения и охраны конфиденциальной информации; системный анализ состояния обеспечения безопасности организации о выявленных угрозах и ВКУ КЗИ, о принятых мерах по локализации и возмещению ущерба; разработка совместных заключений, положений и др. документов по обеспечению режима КЗИ с контрагентом, предложений по совершенствованию механизма корпоративного и договорного регулирования в сфере обращения КЗИ. Содержание конкретных функций аналитических подразделений зависит от специфики работы организаций.

Полученные результаты исследования позволили сформулировать предложения по **совершенствованию аналитической работы в сфере обращения КЗИ**. Одним из важных направлений является *формирование банка данных о состоянии обеспечения безопасности организации и научно-методическое сопровождение разработки автоматизированной системы управления режимным обеспечением (АСУРО) работ*. Создание и обеспечение функционирования АСУРО применительно к крупным коммерческим структурам либо к зонам свободного предпринимательства и отдельным федеральным научным центрам, требуют решения следующих задач. Во-первых, это комплексная разработка и научно-техническое сопровождение средств АСУРО<sup>1</sup>. Речь идет о разработке научных прогнозов, планов и программ решения научно-технических и производственных проблем создания технических средств системы и системы в целом; о разработке общетехнических требований к системе; обоснование технических принципов построения системы и подсистем; разработке эскизных и технических проектов, функциональных схем, конструировании аппаратуры и узлов для различных вариантов системы, эксплуатации аппаратуры и узлов для различных вариантов системы, эксплуатационной документации на систему; о размещении аппаратуры системы на различных объектах контроля; о проведении испытаний системы и ее опытной эксплуатации.

Во-вторых, это математическое моделирование и автоматизация процессов обработки информации о состоянии обеспечения безопасности, о внутренних и внешних угрозах организации и вариантах

<sup>1</sup> См.: Ващенко В.П., Далиев М.И., Урсул А.Д. Безопасность предпринимательской деятельности. М., 2002. С. 255, и др.

<sup>1</sup> См.: ГОСТ 34.003 - 90 «Информационные технологии. Комплекс стандартов и руководящих документов на автоматизированные системы». М., 1990.

возможных мер по их предотвращению и нейтрализации, включая мониторинг обеспечения безопасности коммерческой организации<sup>1</sup>. Речь идет о построении автоматизированной системы управления обработкой информации на основе математической формализации признаков, выбора критериев, позволяющих структурировать массив информации с определенными параметрами; о моделировании процессов обработки информации с целью выявления ВКУ КЗИ; об анализе адекватности построенной математической модели обработки информации реальному процессу преобразования информации; об изменении параметров математической модели и выборе уточненных критериев качества обработки информации; о разработке методики и инструкций, направленных на закрытие обнаруженных в процессе моделирования ВКУ КЗИ, а также обеспечения безопасности самой системы обработки информации.

Вторым, не менее важным направлением совершенствования аналитической деятельности в этой сфере является *работа с кадрами*. Изучение требований, предъявляемых к личным и деловым качествам лиц, выполняющих аналитическую работу в сфере обращения КЗИ, является предметом самостоятельного исследования. Вместе с тем при подборе кадров в такие подразделения нужно учитывать ряд особенностей. Серьезной предпосылкой развития способностей специалистов-аналитиков являются природные задатки, хотя в целом, как признают ученые-психологи, нельзя полностью их считать врожденными и не зависящими от воли человека. Развитие способностей зависит от общественных условий труда, воспитания, воли человека, его отношения к труду и своей профессии<sup>2</sup>. Из общего числа способностей человека следует выделить те, которые, на наш взгляд, должны быть присущи работникам аналитических подразделений. Это внимание, наблюдательность, сообразительность, умение правильно принимать решение даже при неполноте сведений, рассудительность, корректность, коммуникабельность и др. Лавинообразный рост информации в XXI в. связан с определенными трудностями усвоения знаний в различных областях науки и техники. Это обстоятельство следует учитывать при подборе кадров в анали-

<sup>1</sup> См.: Северин В.А. Информационная безопасность предприятия: правовые проблемы и методология исследования // Безопасность информационных технологий. 2001. № 1. С. 38–39.

<sup>2</sup> См.: Теоретические проблемы психологии личности. М., 1974. С. 180–218, и др.

тические подразделения. Как представляется, преимущество должны иметь лица с адекватной решаемым задачам организацией процесса мышления<sup>1</sup>.

### **Методика выявления возможных каналов утечки информации и изучения системы предупреждения нарушений в сфере обращения КЗИ.**

Концептуальные положения, лежащие в основе данной методики, носят общий характер и могут быть использованы в АИ при изучении различных аспектов предметной области КЗИ, обрабатываемой в сфере производства и реализации товаров (работ, услуг). При построении методики с учетом целей и задач АИ важно учитывать следующие принципиальные положения:

общую хозяйственную ситуацию в части финансовой устойчивости и конкурентоспособности технологического потенциала, безопасности персонала, имущества и капитала, правовой защищенности коммерческих интересов;

существование угроз, возникающих в связи с использованием КЗИ на различных направлениях хозяйственной деятельности;

устремление конкурентов по выявлению отличительных признаков вновь создаваемых изделий и продвижению их на рынок с использованием методов конкурентной разведки, а при необходимости и способов промышленного шпионажа;

состояние установленного в организации режима КЗИ и эффективность принимаемых мер по его обеспечению;

использование типичных способов выявления ВКУ КЗИ независимо от этапов обращения КЗИ при производстве и реализации товаров (работ, услуг), базирующихся на установлении нарушений требований правовых норм;

применение метода распознавания образов<sup>2</sup> для поиска новых, еще не установленных ВКУ КЗИ с учетом накопленных в банке данных ЭВМ фактических сведений о причинах и обстоятельствах, способствующих совершению правонарушений при обращении КЗИ;

моделирование процессов образования новых ВКУ на основе анализа практики соблюдения правовых норм при обращении КЗИ на конкретных участках хозяйственной деятельности (выявленные

<sup>1</sup> См.: Спиркин А. Г. Философия: Учебник. М., 2002. С. 439–447.

<sup>2</sup> См.: Гаверцлов О.А. Математические методы и модели в социально-правовом исследовании. М., 1980. С. 152–181.

несовпадения могут свидетельствовать о признаках правонарушения, связанного с появлением неконтролируемой ВКУ КЗИ); характер установленного режима КЗИ и содержание реализации с целью мероприятий по обеспечению безопасности организации с целью эффективного использования правовых средств для устранения имеющихся недостатков организационно-управленческого, воспитательного и правового характера.

Предлагаемая методика, на наш взгляд, позволяет выявить *подразделения, насыщенные охраняемой информацией*, являющейся предметом устремлений конкурентов, *работников-исполнителей, обладающих или могущих обладать такой информацией*, причем с учетом ее основных параметров (важности, полноты и качества); *работников, инициативно принимающих усилия по получению КЗИ* в обход действующей разрешительной системы доступа к такой информации, а также *сформулировать предложения по рассредоточению наиболее важных сведений, составляющих коммерческую тайну в иностранстве* (например, при выполнении НИОКР, заключении коммерческой сделки и т.д.) и *по лицам*, среди работников, выполняющих конкретные трудовые функции (с целью затруднения получения конкурентами полного объема информации о параметрах нового изделия, способов продвижения товара на рынок и другие).

В целях получения информации о рассредоточении обрабатываемой КЗИ проводятся анализ и изучение направлений деятельности организации с использованием различных методов исследования. На основании Перечня категорий сведений, составляющих коммерческую тайну организации, проводится отбор признаков, раскрывающих охраняемые параметры, которые, по данным службы маркетинга и конкурентной разведки, в первую очередь могут представлять коммерческий интерес для конкурентов. Уточняются все источники (документы, базы данных ЭВМ и т.д.), в которых содержится информация, имеющая коммерческую значимость. Затем составляются электронные таблицы исполнителей, допущенных к источникам (документы, БД ЭВМ и т.д.), содержащим признаки охраняемых параметров и таблицы исполнителей, пользовавшихся этими документами (БД ЭВМ). Полученная таким образом информация зашифровывается с применением криптографических методов и закладывается в память ЭВМ. Использование ЭВМ позволяет периодически решать задачу: кто из работников-исполнителей может располагать или уже располагает полным или частичным объемом информации, раскрывающей характеристики конкретных параметров нового изделия, кото-

рые могут в первую очередь заинтересовать конкурентов, и в этой связи они могут предпринимать шаги по получению таких сведений.

Такой подход с учетом действия разрешительной системы доступа к документам (БД ЭВМ) позволяет: 1) установить работников-исполнителей, получивших охраняемую информацию, которая нужна им для выполнения обязанностей, но находится в сфере интересов потенциальных конкурентов; 2) выявлять исполнителей, стремящихся получить такой объем информации об охраняемых параметрах, который представляет интерес для конкурирующей стороны; 3) рассредоточить охраняемую информацию о параметрах, например, о новом издании по отдельным документам (БД ЭВМ), и ввести ограничения меры на доступ к ним исполнителей, с целью затруднения получения конкурентами полного объема информации от данного лица; 4) ограничивать количество документов, содержащих важную охраняемую информацию; 5) отслеживать динамику изменений объема охраняемой информации, числа и состояния ее носителей и осуществлять предупредительную деятельность в сфере обращения КЗИ (например, своевременное ограничение доступа исполнителей к КЗИ, рассредоточение информации в иностранстве и по лицам), при условии постоянного обновления базы данных.

**Процесс обеспечения информационной безопасности в сфере обработки КЗИ представлен на рис. 5.2.1 на примере отечественного автомобильного бизнеса**, в котором, как известно, сложилось критическое положение в реализации собственной конкурентной стратегии, во взаимоотношении с ведущими зарубежными автомобильными компаниями. *Одним из методов обеспечения конкурентных преимуществ является охрана конфиденциальности КЗИ* технологических процессов, связанных с повышением качества, надежности, безопасности и экономичности (основные параметры), *на стадиях разработки и выхода на рынок новой модели автомобиля*. Речь идет о выпуске уникальных моделей автомобилей, их высоком качестве и особенностях дизайна за счет внедрения технических и технологических новшеств; реагировании на потребности рынка; опережении конкурентов за счет более мобильной работы коммерческих структур в продвижении товара к потребителю.

<sup>1</sup> См.: Экономическая безопасность России: Общий курс: Учебник / Под ред. В.К. Сенчагова. 2-е изд. М., 2005. С. 739.

Решение задач достижения конкурентных преимуществ связано с анализом деятельности конкурентов в сфере автомобильного бизнеса, определением их рыночной доли и отношения потребителей к их товарам, сопоставлением коммерческих характеристик конкуррирующих товаров и особенностями ценовой политики. Важное значение для инновационного прорыва в российской автомобильной промышленности имеет рациональное использование КЗИ по научно-техническому и технологическому ускорению процесса разработки новых моделей автомобиля и реализации продукции.

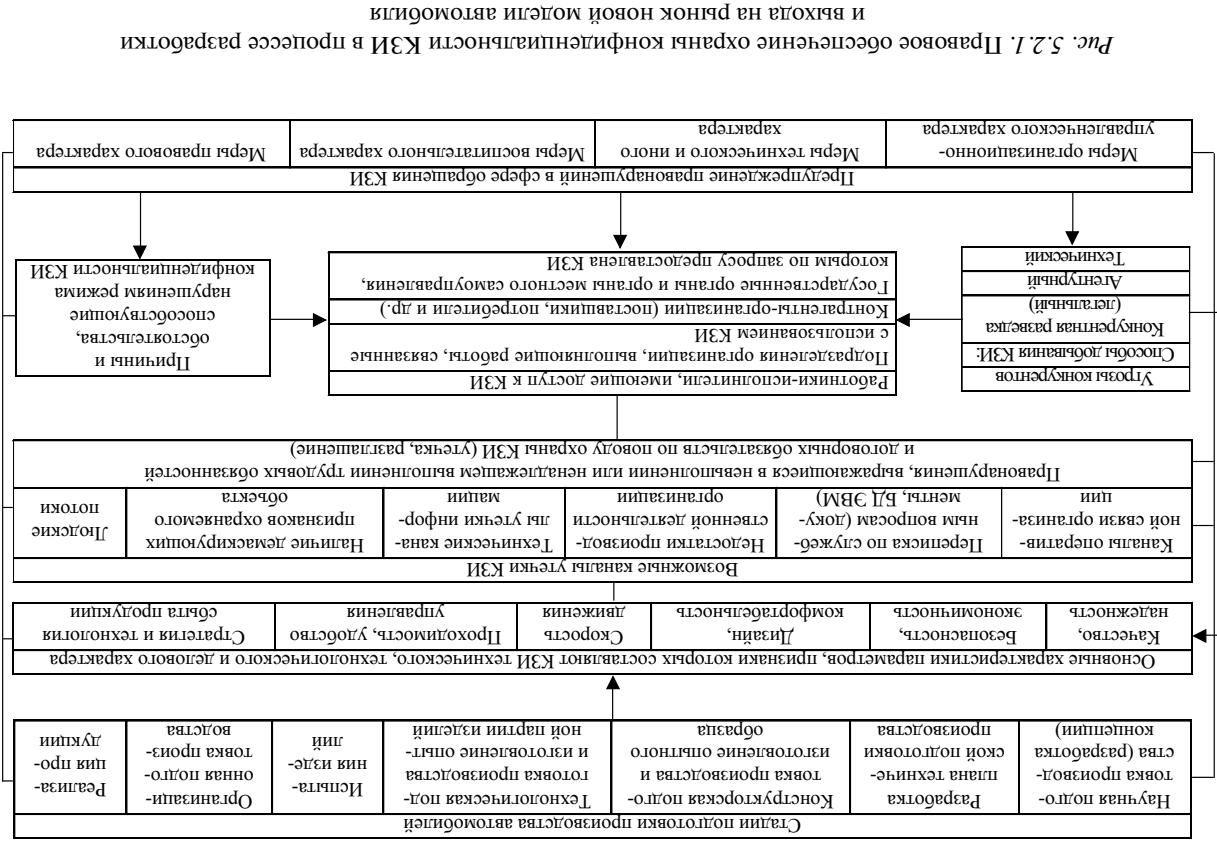
Речь идет об интенсификации информационных взаимосвязей между стадиями подготовки производства, предусматривающих использование КЗИ на этапах проектирования и создания опытного образца автомобиля.

Рассмотрим основные стадии подготовки производства автомобилей и их реализацию на рынке в целях определения КЗИ, которая акцентируется в содержании основных и дополнительных параметров, определяемых техническим заданием и к которым проявляется коммерческий интерес потенциальных конкурентов.

Стадия научной подготовки производства автомобилей включает комплекс научно-исследовательских, конструкторских, технологических и организационных мероприятий<sup>1</sup>, выполняемых в целях разработки концепции новой модели автомобиля. На этом этапе устанавливаются основные параметры и характеристики изделий, предназначаются к освоению производством, конструктивно-технологические и другие особенности типа моделей автомобилей. Эти работы связаны с выполнением значительного объема исследований и экспериментов, которые ведутся с участием многих организаций-контрагентов. При исследовании конструктивных и эксплуатационных характеристик изделий учитываются условия использования автомобилей, и, прежде всего, такие показатели, как дизайн, комфортабельность, скорость движения, проходимость, удобство управления, приспособленность к дорожным и климатическим условиям.

Следующий этап стадии научной подготовки производства состоит в разработке конструкции и изготовления конкретного изделия с учетом определяемых к нему требований. Работы выполняются заводами либо по их заданию научно-исследовательскими или кон-

<sup>1</sup> См.: Власов Б.В. Организация, планирование и управление предприятиями автомобилестроения. М., 1979. С. 95–109, и др.



структурскими организациями, имеющими производственную базу. Переход к интенсивной технологии инженерно-технической подготовки способствовал внесению организационных изменений в работу организаций. Это проявляется в создании мобильных проектных групп специалистов, которые осуществляют прогнозирование развития автомобильного бизнеса адекватно передаваемой им информации.

На этой стадии информацией, имеющей коммерческую значимость, являются основные параметры и характеристики изделий, параметрический ряд изделий, предназначенных к освоению, конструктивно-технологические особенности типа моделей автомобилей. Доступ к этим сведениям имеет широкий круг специалистов в научно-исследовательских, проектных и других организациях — контрагентах, с которыми заключены договоры на выполнение совместных работ.

**Стадия технической подготовки производства** состоит из нескольких этапов. Первый этап включает проектирование новых и совершенствование существующих конструкций изделий. Второй этап — разработка новой и совершенствование существующей технологии изготовления изделий. Третий этап — разработка плана освоения, процедур документооборота и материального обеспечения. Содержание конструкторской и технологической подготовки зависит от объема производства, применительно к которому разрабатывается машина, а также от новизны, сложности конструкции и технологии. Разработка конструкций новых изделий осуществляется отделами главного конструктора и конструкторскими бюро заводов-изготовителей или научно-исследовательскими и проектно-конструкторскими организациями.

**Конструкторская подготовка начинается с разработки технического задания**, которое определяет технические и экономические требования к новой продукции. Техническое задание может быть получено от организации-заказчика или самостоятельно разрабатывается конструкторской организацией. Оно содержит описание назначения изделия с указанием дорожных и климатических условий его использования, основные технические параметры, требования к техническому обслуживанию, долговечности, безопасности, унификации и др. требования. К проекту технического задания прилагается технико-экономическое обоснование целесообразности разработки новой конструкции изделия. Требования, раскрывающие основные параметры будущего автомобиля, его унификацию, эскизную ком-

поновку и технико-экономическое обоснование, содержат сведения, составляющие коммерческую тайну. Проект технического задания рассылается на отзыв основным потребителям данного изделия, организациям, использующим отдельные агрегаты и узлы (двигатель, шасси).

**На этапе эскизного проекта** разрабатываются принципиальная схема гидравлических и электрических соединений, эскизные чертежи общих видов и компоновки машины, составляется спецификация узлов и механизмов, проводится анализ патентной чистоты и расчет предварительной эффективности новой конструкции машины. Все сведения, включаемые в эскизный проект, составляют коммерческую тайну. На основе эскизной компоновки изготавливаются макет изделия, который рассматривается с позиции эстетических требований, рациональности компоновки и комфортабельности.

Следующим этапом конструкторской подготовки является *разработка технического проекта*, в котором определяется основное конструктивное устройство изделия. Он включает комплект чертежей общих видов и сборочных чертежей узлов изделия и его модификаций, чертежи установки и крепления агрегируемого навесного и прицепного оборудования. К проекту прилагается пояснительная записка, в которой раскрываются назначение изделия и условия его использования, результаты анализа технического уровня и его сопоставления с лучшими образцами, конкурентоспособность изделия, данные об использовании в изделии узлов и деталей стандартных модификаций, а также ранее освоенных производством, с применением перечня покупных изделий; содержатся расчеты технико-экономической эффективности внедрения изделия, по повышению долговечности и сокращению трудоемкости работ по техническому обслуживанию, приводятся показатели уровня унификации изделия и прилагается патентный формуляр. Сведения, содержащиеся в техническом проекте и пояснительной записке, составляют КЗИ.

На основе технического проекта разрабатываются *рабочие чертежи, включающие комплект технической документации для изготовления опытных образцов*. По результатам испытаний чертежи корректируются непосредственно для подготовки производства и эксплуатации изделий новой конструкции. Результатом конструкторской подготовки производства является *выпуск конструкторской документации*, включающей технические условия на изделие, конструкторские чертежи всех деталей, узлов, рабочие чертежи, кинематические, электрические, гидравлические схемы и спецификации дета-

лей, ведомости деталей и узлов, заимствованных из других машин, стандартных, нормализованных и покупных материалов, паспорт автомобиля и инструкцию по его эксплуатации. Все перечисленные выше документы, за исключением паспорта автомобиля и инструкции по эксплуатации, содержат сведения, составляющие коммерческую тайну.

Важным этапом конструкторской подготовки производства являются *изготовление, испытание и доводка опытных образцов изделий*. Содержание и объем опытных работ зависят от типа производства, применительно к которому разрабатывается новая конструкция изделия. В целях выявления и устранения недостатков конструирования и повышения качества конструкции новых изделий до их запуска в массовое производство на заводах серийного производства создаются экспериментальные цехи или опытные заводы. Заводские испытания позволяют установить соответствие изделия требованиям технического задания и технического проекта, пригодность изделия по назначению, трудоемкость и удобство обслуживания, долговечность и надежность изделия. Сведения о результатах заводских испытаний изделия составляют КЗИ. По результатам испытаний проводится окончательная доработка макета внешности изделия, рабочих чертежей подготовки производства нового изделия, изготавливается эталонный образец, по которому производится опытная партия автомобилей для окончательных доводочных испытаний перед началом серийного выпуска.

Следующей стадией подготовки производства автомобилей является **технологическая подготовка производства**, содержание и объем которой зависят от типа производства и характера подлежащего изготовлению изделия. Эта стадия включает такие работы, как определение маршрута прохождения деталей по цехам; планирование экспериментальных работ по новым технологическим процессам; разработку технических условий и технологических чертежей на заготовку; проектирование технологических процессов сборки и изготовления деталей и узлов; составление спецификаций на материалы, покупные изделия, полуфабрикаты и инструмент; разработку методов технического контроля по основным деталям; проектирование и изготовление специального технологического оснащения; разработку технических норм времени (трудоемкость), станочных и ручных работ, расходы материалов, инструментов, технологического топлива и энергии; приемку и установку основного и вспомогательного технологического оборудования; обеспечение материалами, заготов-

ками, узлами и деталями, поставляемыми контрагентами, подготовку и комплектацию кадров; изготовление опытной партии изделий в цехах основного производства; окончательную отладку технологического процесса на рабочих местах.

На этой стадии к КЗИ относятся сведения, касающиеся составления планов проведения экспериментальных работ по новым технологическим процессам, разработки технических условий и технологических чертежей на заготовки, проектирования технологических процессов, сборки и изготовления технологического оснащения. Унифицированность изготавливаемой технологии обеспечивается результативностью экспериментальных исследований, технико-экономическим анализом и выбором оптимальных вариантов технологических процессов.

**Организационная подготовка производства** включает выбор метода перехода на выпуск нового автомобиля, разработку планов-графиков технической подготовки и освоения производства, разработку нормативной базы и документации, обеспечение производства материалами, заготовками, деталями и узлами, подготовку кадров. Коммерческию значимость на этой стадии могут представлять сведения о планах технической подготовки, освоении производства и времени выхода на рынок новой модели автомобилей.

Итак, наибольшее сосредоточение технической и технологической информации, имеющей коммерческую значимость, отмечается на стадиях конструкторской и технологической подготовки производства. На этих же стадиях, по сравнению с другими, задействована большая часть работников, допущенных к КЗИ.

Завершающей является **стадия реализации продукции**, которая связана с продвижением товаров от изготовителей и оптовых посредников в розничные торговые сети для продажи населению. На этой стадии КЗИ могут составлять сведения, *во-первых*, о результатах маркетинговых исследований (данные о конкурентной среде, о стимулировании конкуренции на автомобильном рынке, о средствах влияния потребителей и поставщиков на конкурентную ситуацию, о намерениях конкурентов в борьбе за потребителей и новые рыночные «ниши» и др.). *Во-вторых*, сведения о ценовой политике организации (данные о практике изменения цен в связи с возникновением неблагоприятных для конкурента рыночных ситуаций, включая тенденцию предоставления скидок, о влиянии эластичности спроса на динамику цены, о

направлений ценовой дискриминации со стороны конкурентов, занимающих доминирующее положение на рынке, о влиянии доходов потребителей на изменение цен и др.). *В-третьих*, сведения о создании разветвленной сбытовой сети реализации автомобилей (данные об иерархии сбытовой сети, издержках товародвижения и средствах стимулирования реализации товаров, удельном весе деталей и узлов, самостоятельно производимых на отечественных заводах и приобретаемых за рубежом на конкурентной основе, о планах расширения поставщиков деталей и узлов для исключения «давления» поставщиков за счет их монополии, о пропорциях между объемами оптовых и розничных продаж, позволяющих регулировать повышение отдачи торгового капитала, и др.). *В-четвертых*, сведения о построении организационных структур управления организациями, работающими в автомобильном бизнесе (данные о поглощении и слиянии компаний, создании финансово-промышленных групп, в том числе с участием европейских, японских и американских автомобильных компаний; о планах развития таких компаний с учетом консолидированных интересов, касающихся сопоставимости и совместимости результатов деятельности финансовых, производственных и технических служб корпорации; о прогнозировании роста количества выпуска модельного ряда автомобилей и диверсификации деятельности автомобильных компаний; об организационной перестройке структуры подразделений автосборочного предприятия, о создании более гибких ориентированных на нововведения структур, выполняющих конструкторские и технологические работы, занимающихся продуктовой маркетинговой деятельностью, и др.).

*Выделение КЗИ на каждом из этапов подготовки производства автомобилей позволяет перейти к решению следующей задачи — формулированию алгоритма поиска демаскирующих признаков, раскрываемых охраняемые параметры, выявлению правонарушений режима КЗИ, причин и обстоятельств, им способствующих, и определении достаточности осуществляемых мер пресечения.*

При решении данной задачи гипотетически следует исходить из того положения, что каждый охраняемый параметр может быть описан совокупностью демаскирующих его признаков, которые проявляются в силу действия причин и обстоятельств, обуславливающих совершение правонарушений в процессе обращения КЗИ. Степень распознавания охраняемого параметра конкурентом будет зависеть от количества зарегистрированных им демаскирующих признаков и их «весового» значения в общей совокупности сведений, дающих

представление о полноте этого параметра. Нужно иметь в виду, что распознавание конкурентом процесса разработки и выхода на рынок новой модели автомобиля ведется на основании изучения совокупности признаков и параметров, позволяющих определить тактико-технические характеристики в целом изделия. Каждый в отделимости демаскирующий признак может быть зарегистрирован различным путем с помощью использования конкурентами методов легально-го получения информации (конкурентная разведка) и ведения промышленного шпионажа (агентура и иные недовольные законом способы и средства). Последовательно регистрируя все новые признаки, конкурент постепенно убеждается в полноте и объективности полученных сведений об одном, а затем и совокупности охраняемых параметров, раскрывающих ТТХ нового изделия.

*Выделенные параметры и признаки, их характеризующие, содержатся в КЗИ, являются частью системы информации, обеспечивающей всех этапах жизненного цикла разрабатываемой новой модели автомобиля.* Причем с позиций конкурентной разведки информация, циркулирующая и обеспечивающая процесс разработки и выхода на рынок новой модели изделия, может быть сгруппирована, в зависимости от новизны, актуальности и доступа к ней, следующим образом.

*Во-первых*, это открывая информация, анализ которой укладывается в общие представления конкурентной разведки о стратегии развития модельного ряда автомобилей, разрабатываемых конкретной коммерческой организацией. Доступ к такой информации не ограничен.

*Во-вторых*, это демаскирующие признаки, свидетельствующие о разработке и использовании высоких технологий, о подготовке инновационного «технологического прорыва» и выходе на рынок с высокотехнологической продукцией. Об этом могут дополнительно указывать повышенные меры безопасности по охране КЗИ технического и технологического характера на всех этапах разработки изделия.

*В-третьих*, демаскирующие признаки, подтверждающие разработку высокотехнологической продукции в период испытания опытного образца (КЗИ технологического характера) и использование новейших технологий по реализации товаров (КЗИ коммерческого характера). Доступ к такой информации определяется требованиями разрешительной системы, установленной в организации.

Названные последние две группы демаскирующих признаков об охраняемых параметрах выявляются конкурентами с помощью спо-



сборов, позволяющих регистрировать утечку (разглашение) КЗИ по одному или нескольким каналам, произошедшую в результате невыполнения или ненадлежащего выполнения трудовых обязанностей и договорных обязательств, а также разглашения или незаконного использования этой информации должностными лицами государственных органов, получившими доступ к КЗИ по мотивированному запросу. Типовые нарушения режима конфиденциальности на каналах возможной утечки КЗИ, которые чаще всего имеют место в организациях, достаточно хорошо известны конкурентам. Ключом к пониманию важности информативности того или иного демаскирующего признака является изучение конкурентами сведений, характеризующих *особенности* совершения правонарушений и их связь с ВКУ информации, личности правонарушителей, возникновения причин и обстоятельств, способствующих нарушениям режима КЗИ, и осуществлению мер по их предупреждению, которые, безусловно, должны учитываться при разработке методики изучения конкретного объекта исследования.

Учитывая *существование определенной совокупности градаций совершения правонарушений<sup>1</sup> в сфере обращения КЗИ*, следует подчеркнуть, что, с одной стороны, существуют всегда (или почти всегда) демаскирующие признаки вновь создаваемого изделия, по которым может быть определена КЗИ, а с другой — меры, предпринимаемые организацией по закрытию или нейтрализации ВКУ КЗИ путем воздействия на причины и обстоятельства, способствующие их функционированию. Причем этот процесс является неотъемлемой частью научно-производственной и коммерческой деятельности организации и связан с постоянным выявлением демаскирующих признаков и оценкой уровня защиты охраняемых параметров с использованием предупредительных мер организационно-управленческого, воспитательного и правового характера. Каждый защищаемый параметр может быть формализован определенной формулой<sup>2</sup>, которой условно можно обозначить «*объект защиты*». Под «объектом защиты» в данном случае понимается информация или носитель информации (физическое лицо или материальный объект, в которых информация

<sup>1</sup> В данном случае имеется в виду постепенный, хаотичный характер совершения нарушений на различных стадиях производства, обусловленных конкретными причинами и обстоятельствами.

<sup>2</sup> См.: Гаврилов О.А. Указ. соч. С. 156—157.

находит отображение в виде символов, образов, сигналов, технических решений и процессов), в отношении которых необходимо обеспечить защиту в соответствии с задачей, стоящей перед коммерческой организацией<sup>1</sup>. Формулу «объекта защиты» можно записать так

$$\text{Фохр. пар.} \rightarrow X_{1, \dots, n}^{1 \dots n} X_{1, \dots, k, \dots, n}^{1 \dots n} X_{n, n}^{Rn},$$

где Фохр. пар. — формула охраняемого параметра (объект защиты);  $X_{1, \dots, k, \dots, n}$  — совокупность чисел, характеризующих состояние защиты охраняемого параметра; 1 — текущий номер реализации мер предупреждения; K — текущий номер градации демаскирующих признаков; n — общее число градаций мер предупреждения; № — количество охраняемых параметров; R — общее число демаскирующих признаков, раскрывающих ТТХ охраняемых параметров.

В целях получения «*образа фактической защиты объекта*» путем описания его защиты градациями демаскирующих признаков и мерами предупреждения важными являются учет и оценка известных причин и обстоятельств, обуславливающих совершение правонарушений в этой сфере. Конечно, полнота описания объекта защиты во многом зависит от интуиции специалиста-аналитика при подборе градаций и признаков. Поэтому, как правильно отмечает О.А. Гаврилов, «...само распознавание имеет вероятностный характер»<sup>2</sup>. Нужно учитывать, что сами градации признаков, которыми описывается объект защиты, имеют различную направленность и не являются равнозначными. Их действие проявляется в социальной системе и тесно связано с мотивацией человека в коммерческой организации<sup>3</sup>. По мнению В.А. Герасименко и А.А. Малюк, «процессы защиты информации подвержены сильному влиянию случайных факторов и особенно тех из них, которые связаны с злоумышленными действиями людей — нарушителей защищенности»<sup>4</sup>, поэтому необходимо учитывать особенности лиц, допускающих нарушения в сфере обращения КЗИ.

Каждый признак, включаемый для описания объекта защиты, имеет свою «весовую» значимость в общей совокупности сведений,

<sup>1</sup> См.: ГОСТ Р 50922-96 «Защита информации. Основные термины и определения» // СПС «Консультант Плюс».

<sup>2</sup> Гаврилов О.А. Указ. соч. С. 156.

<sup>3</sup> См.: Радаев В.В. Экономическая социология. М., 2005. С. 216.

<sup>4</sup> Герасименко В.А., Малюк А.А. Основы защиты информации. М., 1997. С. 60.

позволяющих определить уровень защиты объекта. Важным является определение удельного веса градаций демаскирующих признаков. Это необходимо для того, чтобы определить уровень защиты охраняемого параметра реализуемыми в организации мерами предупредительными и ввести при необходимости дополнительные меры защиты.

Решение этой задачи требует выполнения следующего условия. Если сумма «весовой» значимости обнаруживаемых градаций демаскирующих признаков объекта защиты (в данном случае причин и обстоятельств, способствующих совершению правонарушений) превышает сумму «весовой» значимости обнаруживаемых в ходе проверки и анализа градаций признаков, то объект дополнительной охраны КЗИ от конкурентов не требует. Достаточно тех мер, которые были первоначально установлены и осуществляются на различных этапах разработки нового изделия. Допустим, если это условие не выполняется, то необходимо продолжить аналитическую работу по поиску обнаруживаемых градаций и предпринимать предупредительные меры, затрудняющие распознавание конкурентом охраняемых параметров (объектов защиты).

Оценка «весовой» значимости градаций признаков объекта защиты проводится с использованием *метода экспертных оценок*, который относится к числу наиболее известных, неформальных методов, позволяющих вести поиск сложных решений, не поддающихся формализации задач, на основе суждений и высказываний экспертов<sup>1</sup>. Для оценки «весовой» значимости признаков объекта защиты составляется таблица, в которой отражаются цифровые значения их качественной важности в форме ранжирования, а также оценка по способу парных сравнений в балльном и лингвистическом выражении. На основании полученных данных определяется суммарный вес не обнаруживаемых градаций демаскирующих признаков (причин и обстоятельств, способствующих совершению правонарушения) и делается вывод о достаточности реализуемых мер предупредительных, позволяющих надежно сохранить в тайне охраняемые параметры. Если после оценки выясняется, что объект нуждается в дополнительной защите, то определяются участки, требующие в первоочередном порядке охраны КЗИ.

Объект защиты считается защищенным в том случае, если градации демаскирующих признаков будут не доступны для регистрации

их конкурентами. Выбор дополнительных мер защиты определяется результатами экономической оценки их стоимости и возможностью осуществления в concreto сложившейся хозяйственной ситуации.

Сказанное выше позволяет сформулировать *алгоритм выявления ВКУ КЗИ и изучения действующей системы предупреждения нарушений в сфере обращения информации*. Его использование необходимо для того, чтобы на практике можно было последовательно осуществить разработку содержательной части методики. К числу основных действий, предпринимаемых организациями, относятся: выделение коммерчески значимой информации технического, технологического и коммерческого (делового) характера на различных стадиях (этапах) производства и реализации товаров; привязка выделенных сведений по градациям демаскирующих признаков к конкретным охраняемым параметрам; моделирование процессов выявления конкурентами демаскирующих признаков, раскрывающих характеристики охраняемых параметров, выражающихся в нарушении установленного режима коммерческой тайны и его обеспечении; установление реально охраняемых параметров (объекта защиты); определение «весовой» значимости градаций демаскирующих признаков объекта на распознавание с помощью метода экспертных оценок и признаков, характеризующих эффективность применения конкретных предупредительных мер организационно-управленческого, воспитательного и правового характера; оценка необходимости разработки дополнительных мер защиты и затрат, связанных с их реализацией.

В заключение следует отметить, что богатый опыт организации и проведения аналитической работы на предприятиях бывшего СССР в сочетании с современными материалами и оценками может быть плодотворно использован хозяйствующими субъектами при защите коммерческих секретов в современной России.

<sup>1</sup> См.: Герасименко В.А., Малюк А.А. Указ. соч. С. 68–70.

**Предмет учебного курса:** Теория, методология, методики и технологии формирования и реализации механизмов правового регулирования коммерчески значимой информации и охраны ее конфиденциальности в инновационной рыночной экономике.

**Основная цель:** Изучение механизма законодательного, корпоративного и договорного регулирования информации по реализации стратегии инновационного прорыва России; развитие практических навыков анализа организационного, правового и научно-методического обеспечения деятельности по охране конфиденциальности информации в организациях.

**Программа является модульной и рассчитана** для использования при повышении квалификации преподавателей и специалистов, имеющих высшее профессиональное образование по различным направлениям гуманитарного и технического знаний, руководителей и работников организаций, включая специалистов подразделений служб безопасности, менеджмента, юридического, маркетинга, управления персоналом, а также государственных и муниципальных служащих.

#### **В программе обучения:**

**Концепция обращения коммерчески значимой информации в России.** Понятие и сущность обращения коммерчески значимой информации (КЗИ) в рыночной экономике. Опыт правового регулирования информации с ограниченным доступом в советский период. Современное законодательство о коммерческой тайне.

**Использование правовых средств в сфере обращения коммерчески значимой информации.** Понятие правовых средств и их применение при обращении КЗИ. Роль норм трудового права в регулировании обращения КЗИ. Гражданско-правовое регулирование обращения КЗИ. Формирование договорных условий об охране конфиденциальности информации.

**Организационное обеспечение деятельности по охране конфиденциальности информации.** Сущность обеспечения деятельности по охране конфиденциальности информации. Угрозы интересам коммерческой организации и основные параметры построения системы ее безопасности. Опыт защиты секретной информации в советский период. Осуществление организацией права на установление режима коммерческой тайны. Методология и методика определения степени конфиденциальности КЗИ. Система мер по установлению режима коммерческой тайны.

**Правовое обеспечение деятельности по охране конфиденциальности информации.** Характеристика нарушений режима конфиденциальности информации и каналов ее возможной утечки. Причины и обстоятельства, способствующие нарушениям режима конфиденци-

## **МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ М.В. ЛОМОНОСОВА**

### **ИНСТИТУТ ПЕРЕПОДГОТОВКИ И ПОВЫШЕНИЯ КВАЛИФИКАЦИИ ПРЕПОДАВАТЕЛЕЙ ГУМАНИТАРНЫХ И СОЦИАЛЬНЫХ НАУК (ИППК МГУ)**

#### **Уважаемые господа!**

Реализация стратегии инновационного прорыва России требует дифференцированной и специализированной переподготовки и повышения квалификации кадров преподавателей и специалистов в области правового обеспечения формирования государством структуры национальной инновационной системы. Производство и реализация конкурентоспособных товаров (работ, услуг) невозможны без использования и защиты технической, технологической и деловой информации, имеющей коммерческую значимость. Решение задач по совершенствованию механизмов взаимодействия участников инновационного процесса с целью продвижения новых технологий в производство требует в эпоху инноваций повышения уровня и содержания подготовки преподавателей и специалистов, обучению их методам защиты прав на результаты интеллектуальной деятельности.

Учитывая важность формирования государственной инновационной политики и ее организационно-правового обеспечения, ИППК МГУ предлагает Вашему вниманию обучение персонала в области экономической и информационной безопасности фирм и корпоративных образований по программе **краткосрочного повышения квалификации «Правовой механизм регулирования и защиты коммерчески значимой информации»**.

альности информации. Характеристика лиц, допускающих нарушения в сфере обращения КЗИ. Предупреждение правонарушений в сфере обращения КЗИ.

**Научно-методическое обеспечение деятельности по охране конфиденциальности информации.** Система и методы контроля в сфере обращения КЗИ. Организация и методика аналитических исследований в сфере обращения КЗИ.

**В ходе занятий слушатели** получат профессиональные знания и будут

**знать:**

сущность и формы проявления КЗИ в различных сферах производства и реализации товаров, выполнения работ и оказания услуг;

законодательное и корпоративное регулирование отношений по поводу использования и охраны КЗИ;

регулирование трудовых отношений, связанных с использованием и защитой КЗИ;

особенности гражданско-правового регулирования обращения КЗИ и способы формирования договорных условий об охране конфиденциальности информации;

содержание правового режима коммерческой тайны; меры, устанавливающие и обеспечивающие режим коммерческой тайны;

содержание работ по выявлению, предупреждению и пресечению правонарушений в сфере обращения КЗИ;

специфику контрольно-проверочной деятельности в сфере обращения КЗИ;

меры юридической ответственности лиц, совершивших правонарушения в сфере обращения КЗИ;

**уметь:**

применять законы и иные правовые акты при осуществлении прав на использование и защиту КЗИ;

разрабатывать документы правового характера, осуществлять экспертизу корпоративных актов, давать заключения и консультации, касающиеся регулирования, использования и защиты КЗИ;

принимать правовые решения и совершать иные юридические действия по осуществлению права на информацию и ее защиты в интересах организации;

разрабатывать проекты гражданско-правовых договоров в сфере обращения КЗИ;

**владеть:**

методикой определения сведений, составляющих коммерческую тайну организации;

методикой формирования договорного условия о конфиденциальности;

приемами разработки планов (положений и др. документов) мероприятий по обеспечению безопасности фирмы;

методикой ведения контроля за состоянием защиты КЗИ;

методами аналитической работы по выявлению и предупреждению правонарушений в сфере обращения КЗИ;

методикой определения убытков, причиненных организации вследствие разглашения сведений, составляющих коммерческую тайну.

**Продолжительность курса:** в течение 2,5–4 мес. (72 час., из них 32 часа — лекции, 40 час. — семинарские занятия, экзамен).

**Периодичность занятий:** с 15 февраля 2009 г. (весенний набор), с 15 сентября 2009 г. (осенний набор). Зачисление и начало занятий — по мере набора учебной группы (10–15 чел.). Предусмотрена дневная и вечерняя форма обучения.

**Слушатели обеспечиваются учебными материалами:**

Северин В.А. Коммерческая тайна в России. Изд. второе, перераб. и доп. М.: ИКД «Зерцало-М», 2009.

Северин В.А. Программа курса. Право на информацию и ее защита в коммерческих организациях. М.: МГУ, 2005.

**Стоимость обучения** по договоренности сторон с учетом специфики корпоративного заказчика.

**По итогам обучения** слушателям выдается удостоверение государственного образца.

**Иногородним слушателям** предоставляется общежитие в Главном здании МГУ им. М.В. Ломоносова.

**Для корпоративных клиентов** ИППК МГУ разрабатывает индивидуальные программы в соответствии с потребностями Вашей организации. Наши учебные материалы и пособия будут адаптированы к проблематике и специфике Вашего предприятия и учреждения. Мы готовы организовать и провести корпоративные занятия как в ИППК МГУ, так и на территории Вашего предприятия.

Все преподаватели ИППК являются признанными специалистами в своей области и хорошо владеют аудиторией. Сложный теоретический материал преподносится слушателям в доступной форме, подкрепляется примерами из практического опыта работы преподавателей.

ИППК МГУ создан в 1949 году и является ведущим центром в области переподготовки и повышения квалификации преподавателей гуманитарных и социальных наук. Современная техническая база позволяет нам вести учебный процесс на высоком организационном и методическом уровне.

Надеемся, что наши предложения будут Вам интересны. Мы готовы обсудить различные формы и условия сотрудничества.

**Подробную информацию о содержании курса и условиях зачисления** Вы можете узнать на нашем сайте в Интернете по адресу: [www.iprk.msu.ru](http://www.iprk.msu.ru)

**Наш адрес:** 119991, ГСП-1, Москва, Ленинские горы, 2-й учебный корпус МГУ, ИППК, 8-й этаж, комн. 846.

**Проезд:** станция метро «Университет», далее автобусами 1, 113, 130, 661 или троллейбусом 34 до остановки «Улица Лебедева».

**Контактный телефон:** (495) 939-21-13, факс (495) 932-88-73.  
E-mail: [iprkmsu@yandex.ru](mailto:iprkmsu@yandex.ru)

**Директор ИППК МГУ им. М.В. Ломоносова,  
профессор ПАНКОВА Людмила Николаевна**

**Руководитель образовательной программы «Правовой механизм регулирования и защиты коммерчески значимой информации» — СЕВЕРИН Виталий Андреевич, профессор ИППК МГУ, доктор юридических наук.**

**Тел.: 8-916-932-57-78.**

#### **Сведения об авторе:**

**Северин Виталий Андреевич** — доктор юридических наук, с 1996 г. работает на кафедре коммерческого права и основ правоведения юридического факультета МГУ им. М.В. Ломоносова, имеет многолетний опыт подготовки специалистов в сфере правового обеспечения безопасности фирм и корпоративных образований. С 1991 по 2004 г. являлся генеральным директором юридической фирмы. Автор более 100 научных публикаций. С 2008 г. — профессор Института переподготовки и повышения квалификации преподавателей гуманитарных и социальных наук МГУ им. М.В. Ломоносова, разработчик и руководитель образовательной программы краткосрочного повышения квалификации «Правовой механизм регулирования и защиты коммерчески значимой информации».

**Северин В.А.** Коммерческая тайна в России. 2-е изд., перераб. и доп. — М.: ИКД «Зерцало-М», 2009. — 472 с.

**ISBN** —

Настоящая книга является вторым, переработанным и дополненным, изданием книги автора «Коммерческая тайна в России» (2007 г.) и представляет собой фундаментальный труд, содержащий комплексное научное учение о коммерчески значимой информации и ее защите. Освещен опыт правового регулирования и защиты информации в советский и современный период. Проанализированы пути становления и развития законодательства о коммерческой тайне.

Центральное место в книге занимает анализ теории и практики использования правовых средств в сфере обращения коммерчески значимой информации. Даны предложения по формированию договорных условий об охране конфиденциальности информации, установлению режима коммерческой тайны и учету параметров построения системы безопасности. Разработана методика определения степени конфиденциальности информации и реализации мер по установлению режима коммерческой тайны. Обоснована классификация причин и обстоятельств, способствующих нарушениям режима коммерческой тайны. Определены содержание и направления осуществления предупредительной деятельности по защите информации.

В книге изложены теоретические и методологические основы организационного, правового и научно-методического обеспечения деятельности по охране конфиденциальности информации. Разработаны способы и приемы ведения контрольной деятельности и методика аналитических исследований в сфере обращения охраняемой информации. Рассмотрены особенности защиты информации в отдельных отраслях экономики, на предприятиях малого и среднего бизнеса.

Издание адресовано преподавателям, научным работникам и студентам вузов, руководителям и специалистам коммерческих структур, органов государственной и муниципальной власти, а также всем читателям, интересующимся проблемами гражданского, коммерческого и информационного права в области правового регулирования, использования и защиты информации.

Северин Виталий Андреевич

## **Коммерческая тайна в России**

Монография

ИКД «Зерцало-М»

Лицензия № 003601 от 20 ноября 2000 г.

Подписано в печать 02.04.2009.

Формат 60x90/16. Усл. печ. л. 29,5.

Тираж 500 экз.

Заказ № 1360

Отпечатано с готовых диапозитивов в типография ЕВСТИ

По вопросам приобретения книг  
издательства «Зерцало»  
и Издательского книготоргового дома «Зерцало-М»  
обращаться по телефонам:

(495) 689-75-36

(495) 689-72-45 (Факс)