МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
имени М.В. ЛОМОНОСОВА

На правах рукописи

Смышляев Станислав Витальевич

Математические методы обоснования оценок уровня информационной безопасности программных средств защиты информации, функционирующих в слабодоверенном окружении

Специальность 05.13.19 — «Методы и системы защиты информации, информационная безопасность»

АВТОРЕФЕРАТ
диссертации на соискание ученой степени
доктора физико-математических наук

Москва — 2021

Работа выполнена на кафедре информационной безопасности факультета вычислительной математики и кибернетики ФГБОУ ВО “Московский государственный университет имени М. В. Ломоносова”.

Научный консультант — *Логачев Олег Алексеевич*,
доктор физико-математических наук, старший научный сотрудник, ФГБОУ ВО “Московский государственный университет имени М. В. Ломоносова”, Центр проблем информационной безопасности (ИПИБ) факультета вычислительной математики и кибернетики, ведущий научный сотрудник

Официальные оппоненты — *Алексеев Валерий Борисович*,
доктор физико-математических наук, профессор, ФГБОУ ВО “Московский государственный университет имени М. В. Ломоносова”, факультет вычислительной математики и кибернетики, кафедра математической кибернетики, профессор

— *Никонов Владимир Глебович*,
доктор технических наук, профессор, Академия криптографии РФ, действительный член

— *Фомичев Владимир Михайлович*,
доктор физико-математических наук, профессор, ФГБОУ ВО “Финансовый университет при Правительстве Российской Федерации”, департамент информационной безопасности, профессор

Защита диссертации состоится 16 марта 2022 г. в 16 часов 45 минут на заседании диссертационного совета МГУ.05.01 ФГБОУ ВО «Московский государственный университет имени М.В. Ломоносова» по адресу: 119234, Москва, ГСП-1, Ленинские горы, д. 1, ФГБОУ ВО «Московский государственный университет имени М.В. Ломоносова», механико-математический факультет, аудитория 14-08.

E-mail: vasenin@msu.ru

С диссертацией можно ознакомиться в отделе диссертаций научной библиотеки МГУ имени М.В. Ломоносова (Ломоносовский просп., д. 27) и на сайте ИАС «ИСТИНА»: `https://istina.msu.ru/dissertations/415255529/`

Автореферат разослан 30 декабря 2021 г.

Ученый секретарь
диссертационного совета МГУ.05.01,
к.ф.-м.н. Кривчиков
Максим Александрович

М. Кривчиков

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Диссертация посвящена решению проблемы получения обоснованных оценок уровня информационной безопасности программных средств защиты информации при их функционировании в условиях слабодоверенного окружения. К такому окружению относятся характерные для массово применяемых средств защиты информации программные и аппаратные компоненты среды функционирования, для которых не в полной мере выполняются предположения, стандартно требуемые для обеспечения целевых свойств безопасности систем.

Проблема получения обоснованных оценок уровня информационной безопасности является важной в теоретическом и в практическом отношении для обеспечения защиты информации, обрабатываемой в информационных системах, в которых средства защиты информации функционируют в условиях ограниченного доверия к окружению. К таким информационным системам относятся, в том числе, системы электронного документооборота. Методы обоснования оценок уровня информационной безопасности применяемых средств защиты информации имеют математическую природу, их разработка проводится в рамках математических моделей, детально описывающих порядок работы средств защиты информации на практике с учетом свойств их сред функционирования, а также целевые свойства информационной безопасности и возможные действия нарушителей данных свойств.

В диссертации разработан математический аппарат для обоснования оценок уровня информационной безопасности в рассматриваемых условиях. Выделены три группы взаимодействий средства защиты информации со средой функционирования, для каждой из которых определен ряд задач по разработке математических методов обеспечения защиты информации в условиях возможных сбоев при взаимодействии с окружением. Для решения каждой из задач выбраны релевантные математические модели, разработаны механизмы обеспечения защиты информации и методы получения обоснованных оценок уровня информационной безопасности, для построенных механизмов доказаны соответствующие оценки. Применение разработанных в диссертации методов позволяет разрабатывать средства защиты информации, обеспечивающие свойства информационной безопасности в условиях ограниченного доверия к среде функционирования, а также проводить всесторонний анализ уровня защищенности этих средств. Таким образом, совокупность разработанных в диссертации математических методов позволяет решить описанную научную проблему, а внедрение изложенных и обоснованных методов при разработке средств защиты информации решает практическую проблему обеспечения безопасности их функционирования в условиях массового применения, имеющую определяющее значение для информационной безопасности государства.

Диссертация представляет результаты исследований в области информационной безопасности. Тема, объект и предмет исследований диссертации соответствуют паспорту специальности 05.13.19 (физико-математические науки) по следующим областям исследования:

1. Теория и методология обеспечения информационной безопасности и за-

щиты информации;

4. Системы документооборота (вне зависимости от степени их компьютеризации) и средства защиты циркулирующей в них информации;

9. Модели и методы оценки защищенности информации и информационной безопасности объекта;

13. Принципы и решения (технические, математические, организационные и др.) по созданию новых и совершенствованию существующих средств защиты информации и обеспечения информационной безопасности.

Актуальность темы. Средства защиты информации, предназначенные для работы с электронной подписью, а также для обеспечения защиты передаваемых и хранимых пользовательских данных, применяются в составе программного обеспечения, используемого гражданами и организациями для решения широкого круга прикладных задач. Их применение в Российской Федерации становится обязательным и массовым в рамках таких процессов, как работа со снабженными электронной подписью юридически значимыми документами в системах электронного документооборота[1], дистанционное открытие счетов в банках[2,3], удаленное получение государственных услуг[4,5], дистанционное электронное голосование[6]. Такие программные средства защиты информации предназначены для использования на личных рабочих станциях или мобильных устройствах рядовых граждан и организаций, не обладающих навыками в области информационной безопасности. В подавляющем большинстве случаев не представляется возможным ограничить множество аппаратных компонент и сред функционирования (операционных систем, системного и прикладного программного обеспечения), работающих в составе таких устройств[7]. Отсюда следует, что такие средства защиты информации необходимо сопровождать в условиях окружения (среды функционирования), от которого можно ожидать только ограниченных гарантий безопасности и надежности.

---

[1]Федеральный закон от 6 апреля 2011 г. N 63-ФЗ «Об электронной подписи»

[2]Федеральный закон от 27 июля 2006 г. N 149-ФЗ «Об информации, информационных технологиях и о защите информации»

[3]Указание Банка России и ПАО “Ростелеком” от 9 июля 2018 г. N 4859-У/01/01/782-18 «О перечне угроз безопасности, актуальных при обработке, включая сбор и хранение, биометрических персональных данных, их проверке и передаче информации о степени их соответствия предоставленным биометрическим персональным данным гражданина Российской Федерации в государственных органах, банках и иных организациях, указанных в абзаце первом части 1 статьи 14.1 Федерального закона от 27 июля 2006 года N 149-ФЗ «Об информации, информационных технологиях и о защите информации», в единой биометрической системе»

[4]Поручение Президента Российской Федерации от 16 июля 2016 года № Пр-1380 «Об обеспечении разработки и реализации комплекса мероприятий, необходимых для перехода органов власти на использование российских криптографических алгоритмов и средств шифрования»

[5]Постановление Правительства Российской Федерации от 30 июня 2020 года № 963 «О реализации пилотного проекта по использованию российских криптографических алгоритмов и средств шифрования в государственных информационных системах»

[6]Модель угроз и нарушителя безопасности для программно-технического комплекса дистанционного электронного голосования, `https://www.comnews.ru/content/215806/2021-08-04/2021-w31/model-ugroz-i-narushitelya-bezopasnosti-dlya-ptk-deg`

[7]Баранов А.П. Российские перспективы развития применения криптосредств в гражданском обществе // Материалы PKI-Форума 2017, `https://pki-forum.ru/files/files/2017/01_Baranov.pdf`, 2017 г.

Средство защиты информации должно реализовывать все целевые функции в рамках собственных модулей, при этом для выполнения свойств информационной безопасности ему в обычных (типовых) условиях требуется[8] обеспечить выполнение следующих свойств окружения: возможность получить случайную последовательность достаточных статистических качеств; отсутствие риска компрометации внутренних конфиденциальных данных из-за ошибок или уязвимостей в системном программном и аппаратном окружении; защита доступа к средству защиты информации и взаимодействий между компонентами составного средства защиты информации с применением высокоэнтропийных секретных значений.

С учетом изложенного выше, указанные средства опираются на три набора предположений об окружении:

1. необходимые для выполнения функций защиты информации системные вызовы позволяют получить случайную последовательность достаточных статистических качеств;

2. отсутствуют свойства программных и аппаратных компонент, полностью или частично влекущие компрометацию конфиденциальной внутренней информации программного средства;

3. доступ к средству защиты информации, а также взаимодействие между компонентами составного средства защиты информации через недоверенную среду могут производиться с применением высокоэнтропийных секретных значений.

Отмеченные три набора предположений критически важны для обеспечения информационной безопасности, однако на практике в случае массово применяемых средств защиты информации они выполняются не в полной мере: функционирование программного средства на десятках миллионов разнородных устройств[9], подавляющее большинство которых эксплуатируется владельцами, слабо осведомленными в вопросах обеспечения личной информационной безопасности[10,11], неминуемо приводит к тому, что все три этих важнейших для защиты информации набора условий так или иначе нарушаются. При этом последствиями нарушения свойств информационной безопасности применяемых средств защиты информации могут быть компрометация хранимой конфиденциальной информации владельцев и подделка любых документов от их лица

[8]Рекомендации по стандартизации Р 1323565.1.012-2017 «Информационная технология. Криптографическая защита информации. Принципы разработки и модернизации шифровальных (криптографических) средств защиты информации»

[9]Баранов А.П. Квалифицированная электронная подпись в массовых системах // Материалы PKI-Форума 2020, `https://pki-forum.ru/files/files/Baranov_2020.pdf`, 2020 г.

[10]Доктрина информационной безопасности Российской Федерации. Утверждена Указом Президента Российской Федерации от 5 декабря 2016 г. №646. Статья III.

[11]Баранов А.П. Перспективные направления исследований в защите информации // Материалы пленарного заседания РусКрипто‘2014, `https://www.ruscrypto.ru/resource/archive/rc2014/files/01_baranov.pdf`, 2014 г.

(вплоть до продажи их собственности)[12,13].

Исходя из приведенных выше соображений, высокую важность для информационной безопасности на уровне государства[14] имеет задача обеспечения безопасности функционирования массово применяемых программных средств защиты информации в условиях такого окружения. Программное и аппаратное окружение средств защиты информации, для которого не в полной мере обеспечиваются указанные выше три набора предположений, в настоящей работе будем называть «слабодоверенным окружением».

Разработка методологии обеспечения безопасности программных средств защиты информации, предназначенных для функционирования в условиях слабодоверенного окружения, является предельно актуальной и сложной научно-технической проблемой. Ее решение требует систематизации возникающих новых задач обеспечения защищенности таких средств в условиях слабодоверенного окружения, построения и выбора релевантных математических моделей, синтеза математических методов и механизмов обеспечения требуемых свойств рассматриваемых средств с учетом этих моделей, а также обоснования оценок уровня информационной безопасности результирующих средств в разработанных математических моделях.

При решении рассматриваемой проблемы, с учетом ее значимости, недопустимо уклоняться от практически важных вопросов и проводить разработку механизмов обеспечения защиты в «удобных» для проведения анализа упрощенных математических моделях. Напротив, необходимо выделять перечень важных с точки зрения практики свойств, определяющих влияние условий слабодоверенного окружения на средства защиты информации, и предельно аккуратно отражать их в уточненных детализированных математических моделях, после чего именно в них проводить синтез и анализ методов обеспечения защиты. Проблема появления уязвимостей реализаций механизмов и протоколов защиты информации в средствах защиты информации в случае проведения их анализа в моделях, не учитывающих реальные свойства их применения, рассматривалась, в частности, Дж.-П. Дегэбриелом, К. Патерсоном и Г. Уотсоном[15]. Авторы исследования Европейского агентства по сетевой и информационной безопасности[16], в дополнение к выводам о недопустимости проведения анализа в не соответствующих практике моделях, также отмечали важность анализа законченных самодостаточных механизмов и протоколов, так как в слу-

---

[12]Электронный документооборот. Применение электронной подписи // Портал Федеральной налоговой службы Российской Федерации, `https://www.nalog.gov.ru/rn77/related_activities/el_doc/use_electronic_sign/`

[13]Мелузов А.С., Никитина О.Ю. Электронная подпись: безопасное использование и предотвращение рисков // `https://iitrust.ru/articles/article/elektronnaya-podpis-bezopasnoe-ispolzovanie-i-predotvrashhenie-riskov/`

[14]Доктрина информационной безопасности Российской Федерации. Утверждена Указом Президента Российской Федерации от 5 декабря 2016 г. №646. Статья IV.

[15]Degabriele J.P., Paterson K.G., Watson G.J. Provable security in the real world // IEEE Security & Privacy 9(3), pp. 33–41, 2011.

[16]Smart N.P, Rijmen V., Stam M., Warinschi B., Watson G. Study on cryptographic protocols // ENISA, Report TP-06-14-085-EN-N, 2014.

чае отсутствия такого анализа даже построенные на базе нескольких стойких компонент конструкции могут иметь критические уязвимости при применении на практике.

Отметим, что для разработанных механизмов не всегда достаточно получить обоснования стойкости, то есть утверждения вида «разработанный механизм обеспечивает уровень защищенности в модели, отражающей условия слабодоверенного окружения, не меньший, чем уровень защищенности тех или иных базовых примитивов в соответствующих стандартных моделях». Как подчеркивали М. Белларе[17], А. Десай, Е. Йокипи, Ф. Рогавей[18], в большинстве случаев необходимо разрабатывать методы обоснования оценок уровня информационной безопасности, позволяющие для конкретных базовых алгоритмов, параметров, свойств окружения и требуемых свойств безопасности результирующей системы выбирать числовые значения параметров разработанных механизмов. Это становится особенно важным в тех случаях, когда механизм разрабатывается не для защиты от разового вырождения уровня информационной безопасности в случае редких экстренных событий, таких как сбои источников случайности, которые через короткий промежуток времени детектируются механизмами динамического контроля и приводят к останову системы, но для обеспечения постоянного уровня защиты, несмотря на потенциальную возможность долговременной работы в условиях недетектированных уязвимостей окружения (например, при утечке частичной информации о состояниях регистров центрального процессора). Разработка механизмов, предназначенных для применения в слабодоверенном окружении, должна начинаться с глубокого анализа условий функционирования, сопровождаться доказательством оценок стойкости в детально отражающих эти условия математических моделях. После внедрения разработанных параметризованных механизмов необходим анализ дополненной системы в практических условиях и выбор на его основе конкретных значений параметров.

Раскрывая общую проблему с целью выделения групп возникающих задач и фокусируясь на основных целевых функциях, решаемых массовыми программными средствами защиты информации (в том числе, предназначенными для применения в системах электронного документооборота), справедливо выделить процессы вычисления и проверки электронной подписи, а также обеспечение конфиденциальности и целостности передаваемых по каналу связи данных. При их решении программное средство опирается на свое окружение (программное и аппаратное) в части трех групп интерфейсных взаимодействий:

1. в начале операций — обращение к датчикам случайных чисел (источникам случайности);
2. в процессе основных вычислений — взаимодействие с программными и ап-

[17]Bellare M. Practice-Oriented Provable-Security. Lectures on Data Security, EEF School 1998 // Lecture Notes in Computer Science. I. Damgard, Vol. 1561, 1999. Pp. 1–15

[18]Bellare M., Desai A., Jokipii E., Rogaway P. A concrete security treatment of symmetric encryption. In Proceedings of 38th Annual Symposium on Foundations of Computer Science (FOCS '97), pages 394–403. IEEE, 1997.

паратными ресурсами для базовых операций, для хранения промежуточных данных и для обращения к внешним устройствам;

3. при завершении своих операций и передаче команд на внешние аппаратные средства (в случае распределенных решений) и/или до начала работы — получение данных пользователя для проведения его аутентификации и авторизации.

При взаимодействии с окружением в рамках решения каждой из этих групп задач возникает зависимость результирующего уровня обеспечиваемой защиты информации от выполнения предположений о соответствии реальных свойств данных взаимодействий ожидаемым и предполагаемым в моделях, использованных при разработке средства защиты информации.

Рассмотрим общие проблемы, возникающие в отношении каждой из выделенных трех групп взаимодействий.

Уязвимости или сбои источников случайности, к которым производятся обращения средств защиты информации в рамках первой из выделенных групп взаимодействий, могут приводить к катастрофическим последствиям для безопасности. Так, вычисление электронной подписи по схемам из семейства Эль-Гамаля (к которому относятся стандартизированные в России схемы подписи[19]) предваряется обращением к датчику случайных чисел, а в случае его сбоя — даже однократного — злоумышленник по значению подписи может восстановить ключ[20]. При этом, в узком смысле, предоставляемые средством защиты информации гарантии по неизвлекаемости ключа подписи и корректности процессов вычисления подписи нарушены не будут, а причиной проблемы будет являться сбой в слабодоверенном окружении — однако результирующая безопасность все равно выродится недопустимым образом. Аналогично, при недостатках базовых источников случайности, используемых средством обеспечения конфиденциальности клиент-серверных соединений, могут быть полностью скомпрометированы все передаваемые в рамках соединений данные[21]. Для противодействия таким уязвимостям целесообразно применять механизмы преобразования выходов датчиков случайных чисел, способные сохранять определенные положительные свойства в случае недостатков базовых источников случайности. Попытки применять такой подход для обеспечения защиты реализаций протоколов предпринимались, в частности, Б. ЛаМаккией, К. Лаутером, А. Митягиным[22], однако предложенные ими методы оказались неприменимы для существующих протоколов ввиду необходимости усложнения ключевой системы.

---

[19]ГОСТ Р 34.10–2012, «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи», Москва, Стандартинформ, 2012

[20]Bos J.W., Halderman J.A., Heninger N., Moore J., Naehrig M., Wustrow E.. Elliptic curve cryptography in practice // International Conference on Financial Cryptography and Data Security, 2014. Pp. 157-175.

[21]Checkoway S., Niederhagen R., Everspaugh A., Green M., Lange T., Ristenpart T., Bernstein D.J., Maskiewicz J., Shacham H., Fredrikson M. On the Practical Exploitability of Dual EC in TLS Implementations. In 23rd USENIX Security Symposium (USENIX Security 14), pages 319–335, San Diego, CA, August 2014. USENIX Association.

[22]LaMacchia B., Lauter K. and Mityagin A. Stronger security of authenticated key exchange // Provable Security, Springer, 2007. Pp. 1–16.

Таким образом, задача построения применимых на практике механизмов указанного типа и обоснования математическими методами оценок уровня их информационной безопасности является актуальной для обеспечения безопасности как средств электронной подписи, так и средств защиты клиент-серверных соединений.

Для реализации механизмов противодействия деградации источников случайности в программных средствах защиты информации могут применяться параметризованные вспомогательные кодирующие устройства, обеспечивающие неухудшение свойств выходной последовательности при штатной работе датчиков случайных чисел и позволяющие улучшать ее свойства при вырождении входной последовательности (в типичном случае — в линейно-рекуррентную) из-за сбоев. Дискретные функции, необходимые[23] для применения в таких кодирующих устройствах (в зарубежной литературе — «filters») называются совершенно уравновешенными. Они исследовались рядом авторов в рамках теории дискретных функций[24], теории кодирования, символической динамики и криптологии[25]. В теории динамических систем они исследовались как отображения, порождающие сюръективные эндоморфизмы символических динамических систем[26]. При этом оставались нерешенными две важнейшие крупные задачи, важность которых подчеркивалась, в том числе, в работах Р. Андерсона[27], М. Дихтла[28], А. Гуже, Х. Сибера[29]: задача построения невырожденных классов таких функций, обладающих свойством уравновешенности определенных подфункций (в том числе, свойством корреляционной иммунности, устойчивости), а также задача доказательства выдвинутой в 1996 году Гипотезы Голича[30], предлагавшей описание класса булевых функций, сохраняющих совершенную уравновешенность при добавлении любого числа фиктивных переменных. Решение этих двух задач имеет определяющее значение для построения механизмов с указанными выше свойствами для применения в программных средствах защиты информации.

Касаясь второй группы интерфейсных взаимодействий, необходимо отметить критичность последствий сбоев или уязвимостей в окружении, способных в определенные моменты времени приводить к компрометации используемых в

[23]Сумароков С. Н. Запреты двоичных функций и обратимость для одного класса кодирующих устройств // Обозрение прикладной и промышленной математики. 1994. 1(1). 33–55.

[24]Смышляев С. В. Комбинаторные свойства совершенно уравновешенных булевых функций. Диссертация на соискание степени кандидата физико-математических наук. 2012 г.

[25]Логачев О. А. Построение и анализ эффективности алгоритмов обращения дискретных функций в математических моделях информационной безопасности. Диссертация на соискание степени доктора физико-математических наук. 2019 г.

[26]Hedlund G. A. Endomorphisms and automorphisms of the shift dynamical system // Theory of Computing Systems. 1969. Vol. 3(4). Pp. 320–375.

[27]Anderson R. J. Searching for the optimum correlation attack // Lecture Notes in Computer Science, 1995, vol. 1008, pp. 137–143.

[28]Dichtl M. On nonlinear filter generators // Lecture Notes in Computer Science. 1997. Vol. 1267. Pp. 103–106.

[29]Gouget A., Sibert H. Revisiting correlation immunity in filter generators // Lecture Notes in Computer Science. 2007. Vol. 4876. Pp. 378–395.

[30]Golić J. D. On the security of nonlinear filter generators // Lecture Notes in Computer Science. 1996. Vol. 1039. Pp. 173–188.

преобразованиях сессионных векторов защиты[31]: в отсутствие дополнительных мер защиты такое событие может привести к раскрытию злоумышленником всех переданных за текущий сеанс связи и предыдущие сеансы связи на тех же долговременных секретах сторон данных, а ущерб никак не будет ограничен текущим фрагментом данных.

С целью защиты сессионных векторов защиты от их компрометации в условиях слабодоверенного окружения могут применяться методы их преобразования в процессе функционирования блочных симметричных алгоритмов обеспечения конфиденциальности, а также методы рандомизации при вычислениях общих секретных параметров. При этом, в отличие от неприменимых для внедрения в существующие протоколы методов их внешнего преобразования, изучавшихся М. Абдаллой и М. Белларе[32], для допускающих прозрачное встраивание в существующие протоколы механизмы внутреннего преобразования сессионных векторов защиты[33], как продемонстрировали результаты В.О. Миронкина[34], требуется подробный анализ и разработка нового математического аппарата.

Критичные для безопасности последствия могут наступить также в случае проведения операций (таких, например, как формирование электронной подписи) с частичным делегированием вычислений аппаратным модулям, хранящим ключи подписи в неизвлекаемом виде, что целесообразно ради опоры на механизмы инженерной защиты хранимых данных, реализованные в таких компонентах[35]. В случае формирования электронной подписи с применением вычислительных модулей с уязвимостью, влияющей на распределение одноразовых значений, используемых при вычислениях, внешний злоумышленник может полностью раскрыть значение ключа без нарушения инженерных мер защиты, получая доступ к значениям подписи через публично доступные источники (актуальность такой постановки задачи продемонстрирована, в частности, А. Ленстрой, Дж. Хьюсом, М. Ожье, Дж. Босом, Т Кляйнунгом и К. Вахтером[36]).

Относительно третьей группы интерфейсных взаимодействий, возникающих при выполнении основных операций на внешних аппаратных средствах — в том числе, в таких важных для практики случаях, как применение сер-

---

[31]Ramsay C., Lohuis J. «TEMPEST attacks against AES. Covertly stealing keys for 200 euro», 2017, `https://www.fox-it.com/en/wp-content/uploads/sites/11/Tempest_attacks_against_AES.pdf`.

[32]Abdalla M., Bellare M. Increasing the Lifetime of a Key: A Comparative Analysis of the Security of Re-keying Techniques // Lecture Notes in Computer Science, 2000, vol. 1976, pp. 546–559.

[33]Popov V., Kurepkin I., Leontiev S., "Additional cryptographic algorithms for use with GOST 28147-89, GOST R 34.10-94, GOST R 34.10-2001, and GOST R 34.11-94 algorithms", RFC 4357, 2007, `https://www.rfc-editor.org/info/rfc4357`

[34]Миронкин В.О. О некоторых вероятностных характеристиках алгоритма выработки ключа «CRYPTOPRO KEY MESHING». Проблемы информационной безопасности. Компьютерные системы. №4, 2015. С. 140–146.

[35]Сабанов А.Г. Методология формирования иерархии доверия к результатам идентификации и аутентификации субъектов доступа. Диссертация на соискание степени доктора технических наук. 2020.

[36]Lenstra A.K., Hughes J.P., Augier M., Bos J.W., Kleinjung T., Wachter C. Ron was wrong, Whit is right // Cryptology ePrint Archive: Report 2012/064, 2012.

верных компонент в условиях ограничений на стороне клиентского средства доступа[37] и подключаемых аппаратных носителей, обеспечивающих неизвлекаемость хранимых ключей[38], — необходимо решение задачи обеспечения безопасности при передаче управления. Угрозу несут подходы разработчиков программного обеспечения, предполагающие возможность передачи управления на сторону внешнего средства без аутентифицированного должным образом защищенного взаимодействия с таким средством, в частности, посредством NFC-взаимодействий[39]. Они возникают как из-за иллюзии неразрешимости задачи по обеспечению защищенного доступа к долговременным ключам без аутентификации с помощью некоторых других долговременных ключей, так и потому, что, из-за проведения анализа стойкости протоколов в не релевантных практике моделях и на уровне исследований отдельных компонент, в реализациях протоколов аутентифицированной выработки общего ключа на основе низкоэнтропийных данных обнаруживались критические[40] и резонансные[41] уязвимости. При этом, в реализациях, не применяющих защиту соединений с внешним средством, абсолютно любое воздействие злоумышленника на канал взаимодействия с этим средством позволит ему подменить подписываемые данные и получить конфиденциальные данные еще до их попадания на внешнее аппаратное средство. Аналогичный неосмотрительный подход, наивно предполагающий допустимость работы со средством защиты информации без проверки аутентичности самого средства и права его использования, открывает широчайший класс уязвимостей, реализуемых путем подмены самого средства защиты информации. Для противодействия уязвимостям такого рода требуется решение задач разработки и обоснования математическими методами методов построения механизмов проверки аутентичности данных с малой длиной проверочных значений, а также оценок уровня информационной безопасности механизмов построения аутентифицированных защищенных соединений в условиях отсутствия высокоэнтропийных секретов.

Диссертация посвящена решению проблемы, важной в практическом и теоретическом отношении: проблемы обеспечения и оценки информационной безопасности программных средств защиты информации при функционировании в условиях слабодоверенного окружения.

Тема диссертации, посвященной разработке математического аппарата решения проблемы обеспечения и оценки информационной безопасности применяемых в информационных системах средств защиты информации, актуальна

---

[37]Баранов А.П. Актуальные направления в области информационной безопасности // Материалы пленарного заседания РусКрипто‘2016, `https://www.ruscrypto.ru/resource/archive/rc2016/files/01_baranov.pdf`, 2016 г.

[38]Сабанов А.Г. Уровни доверия к аутентификаторам // Вопросы защиты информации, № 2. 2019. С. 10–17.

[39]Sun Y., Kumar S., He S., Chen J., Shi Z. You Foot the Bill! Attacking NFC With Passive Relays // IEEE Internet of Things Journal, vol. 8, no. 2, pp. 1197-1210, 15 Jan.15, 2021.

[40]Clarke D., Hao F. Cryptanalysis of the Dragonfly key exchange protocol. IET Information Security, Volume 8, Issue 6, pp. 283–289, November 2014.

[41]Perrin T. Requesting removal of CFRG co-chair // Crypto Forum Research Group mailing list archives, `https://mailarchive.ietf.org/arch/msg/cfrg/scLoq7DvtXzo9Jl9AG9fQOcSGsM/`, 2013

как в теоретическом, так и в прикладном смысле.

Цель работы — совершенствование математических моделей и методов оценки защищенности информации для программных средств защиты информации массового применения, разработка механизмов защиты информации и новых математических методов получения обоснованных оценок уровня информационной безопасности для программных средств защиты информации при их функционировании в условиях слабодоверенного окружения.

Для достижения поставленной цели были решены следующие сложные и актуальные задачи:

1) Определение структуры множества совершенно уравновешенных булевых функций, которые при применении в параметризованных вспомогательных кодирующих устройствах обеспечивают сохранение равновероятности входной последовательности при добавлении любого числа фиктивных переменных.
2) Построение булевых функций, которые при применении во вспомогательных кодирующих устройствах обеспечивают сохранение равновероятности входной последовательности и обладают свойством уравновешенности определенных подфункций (в том числе, свойством корреляционной иммунности, устойчивости).
3) Построение и обоснование математическими методами оценок уровня информационной безопасности реализуемых программным образом механизмов преобразования выходов датчиков случайных чисел, способных сохранять положительные свойства в случае недостатков базовых источников случайности.
4) Разработка и обоснование математическими методами оценок уровня информационной безопасности методов детерминированного преобразования сессионных векторов защиты при функционировании блочных симметричных алгоритмов обеспечения конфиденциальности с целью защиты от их компрометации в условиях слабодоверенного окружения.
5) Оценка стойкости используемых в массовых программных средствах защиты информации механизмов рандомизации вычислений общего секретного параметра с помощью умножения на разовое случайное значение и оценка влияния их применения на результирующий уровень защищенности.
6) Разработка и обоснование в соответствующих практическим условиям функционирования математических моделях механизмов формирования электронной подписи с применением потенциально уязвимых вычислительных модулей.
7) Обоснование математическими методами оценок уровня информационной безопасности механизмов, применяемых при дистанционном взаимодействии с серверными средствами защиты информации в условиях ограничений на стороне клиентского средства доступа.
8) Обоснование оценок уровня информационной безопасности методов построения механизмов проверки аутентичности данных с малой длиной проверочных значений.

9) Разработка и обоснование математическими методами оценок уровня информационной безопасности механизмов построения аутентифицированных защищенных соединений в условиях отсутствия высокоэнтропийных секретов.

Степень разработанности темы. В диссертации решены сложные и актуальные задачи, представляющие исключительную важность для обеспечения информационной безопасности средств защиты информации.

В рамках вводных разделов диссертации представлен исчерпывающий обзор предшествующих результатов по теме исследования, наиболее важные из которых перечислены далее в автореферате в разделе «Основное содержание работы».

Научная новизна. Получены следующие новые результаты.

– Доказана Гипотеза Голича, выдвинутая в 1996 году и предлагающая окончательное решение вопроса о структуре множества вспомогательных кодирующих устройств, построенных с использованием булевой функции и регистра сдвига, которые сохраняют равновероятность входной последовательности при любом выборе расстояний между точками съема (то есть при добавлении любого числа фиктивных переменных используемой булевой функции). Получен ряд результатов о выполнении обобщений Гипотезы Голича для k-значных дискретных функций при произвольных k, в том числе, отрицательный результат для составных k.

– Построен класс совершенно уравновешенных функций, опровергающий результаты зарубежных исследователей об условиях на коэффициенты Уолша–Адамара функций, сохраняющих равновероятность m-грамм. Описан класс нелинейно зависящих от крайних существенных переменных совершенно уравновешенных булевых функций, являющихся корреляционно-иммунными (устойчивыми).

– В математической модели, детально описывающей функционирование средства защиты информации в условиях потенциально уязвимого источника случайности, доказана стойкость разработанного метода обеспечения защиты с применением обращений к доверенному программно-аппаратному средству вычисления электронной подписи (по результатам исследований метод стандартизирован на международном уровне в IETF/IRTF).

– Для схем электронной подписи семейства Эль-Гамаля разработан механизм, обеспечивающий безопасность их реализаций в условиях потенциально уязвимого источника случайности, совместимый с существующими практиками повышения безопасности реализаций. В отражающей наличие в системе нарушителя с возможностью влияния на источники случайности модели SUF-CMRA разработан математический метод получения обоснованных оценок стойкости реализаций, построенных с применением разработанного механизма.

– Разработан метод обоснования оценок уровня информационной безопасности для процедур обеспечения конфиденциальности данных, применяющих механизмы регулярной смены ключей. В релевантных математических моделях

получены оценки уровня информационной безопасности для ранее разработанного (не в рамках настоящей диссертации) механизма CPKM, обосновывающие повышение стойкости результирующих процедур обеспечения конфиденциальности по сравнению с базовыми режимами. Разработан новый расширенный режим работы блочных симметричных алгоритмов обеспечения конфиденциальности CTR-ACPKM (по результатам настоящих исследований режим стандартизирован на российском (Росстандарт) и международном (ISO/IEC, IETF/IRTF) уровне, став шестым стандартизированным режимом наравне с пятью классическими). Разработаны методы получения обоснованных оценок информационной безопасности реализаций, применяющих данный расширенный режим, в наиболее полно отражающей практические условия функционирования математической модели IND-CPNA.

– Для механизмов VKO, PRFGOST, KDFTREE, а также функций генерации проверочных параметров CVV и PVV в соответствующих математических моделях получены методы обоснования оценок уровня информационной безопасности, которые позволяют выбирать определяющие их конкретный вид числовые параметры исходя из ограничений на вероятность успеха нарушителя при проведении атак на системы, использующие данные механизмы, в том числе, в ряде рассмотренных в работе информационных систем, в рамках которых средства защиты информации функционируют в условиях слабодоверенного окружения.

– Для решения задачи о работе с долговременными ключами подписи, хранящимися и применяемыми с помощью потенциально уязвимых вычислителей, разработан протокол uSign, выполняющийся между логическими компонентами средства защиты информации и обеспечивающий защиту от нарушителя, способного подменять одноразовые секретные значения с целью компрометации ключей. В математической модели, отражающей указанные условия работы, доказан результат о стойкости реализации схемы электронной подписи семейства Эль-Гамаля, построенной с применением разработанного протокола.

– Для трех методов построения модификаций схем электронной подписи семейства Эль-Гамаля, позволяющих получать выходные значения меньшей длины, получены методы обоснования оценок уровня информационной безопасности в математической модели SUF-CMA, позволяющие выбирать числовые параметры с учетом требований конечной системы без необходимости дополнительных исследований получаемых модифицированных схем.

– Разработан протокол установления защищенного соединения с аутентификацией на основе низкоэнтропийных данных и явным подтверждением выработанного общего секрета SESPAKE (по результатам исследований, проведенных в настоящей диссертации, стандартизирован в России в качестве протокола выработки общего ключа с аутентификацией на основе пароля). В построенной математической модели, подробно описывающей условия применения протокола, разработаны методы получения обоснованных оценок уровня информационной безопасности его реализаций.

На защиту выносятся: обоснование актуальности, научная новизна, тео-

ретическая и практическая значимость работы, а также следующие положения, которые подтверждаются результатами исследования, представленными в заключении диссертации.

1) Доказательство Гипотезы Голича, которое позволяет определить структуру множества совершенно уравновешенных булевых функций, сохраняющих равновероятность входной последовательности вспомогательного кодирующего устройства при любом выборе расстояний между точками съема. Исследование вопросов применимости обобщенной Гипотезы Голича в k-значном случае.
2) Развитие аппарата исследований совершенно уравновешенных булевых функций с барьером. Построение класса булевых функций, одновременно сохраняющих при использовании в кодирующих устройствах равновероятность m-грамм и нарушающих сформулированные ранее зарубежными исследователями условия на коэффициенты Уолша–Адамара таких функций. Класс совершенно уравновешенных булевых функций, обладающих свойством корреляционной иммунности (устойчивости).
3) Метод модификации схем электронной подписи семейства Эль-Гамаля, предназначенный для использования в условиях слабодоверенного окружения, а именно, в условиях потенциально деградирующих источников случайности. Обоснование оценок уровня информационной безопасности модифицированных реализаций схем электронной подписи в модели SUF-CMRA, отражающей условия применения потенциально уязвимого датчика случайных чисел. Метод построения механизмов обеспечения информационной безопасности средств защиты информации, функционирующих в условиях потенциально уязвимых источников случайности, при наличии доступа к доверенным программно-аппаратным средствам, предназначенным для формирования электронной подписи.
4) Метод обоснования оценок уровня информационной безопасности для механизмов преобразования сессионных векторов защиты при функционировании блочных симметричных алгоритмов обеспечения конфиденциальности. Обоснование повышения уровня информационной безопасности результирующих процедур обработки данных с применением механизмов регулярного преобразования сессионных векторов защиты CPKM по сравнению с базовыми режимами.
5) Расширенный режим работы блочных симметричных алгоритмов обеспечения конфиденциальности CTR-ACPKM со встроенным преобразованием сессионного вектора защиты. Метод получения оценок уровня информационной безопасности для параметризованного режима CTR-ACPKM в отражающей практические условия его применения математической модели IND-CPNA.
6) Оценки стойкости механизмов VKO, PRFGOST и KDFTREE, предоставляющие возможность получать для заданных значений параметров численные значения преобладаний нарушителей, в том числе при построении

систем дистанционного взаимодействия с серверными средствами защиты информации в случае ограничений на стороне клиентского средства доступа.

7) Метод вычисления электронной подписи по схеме Эль-Гамаля в условиях использования потенциально уязвимого вычислительного элемента. Обоснование оценок уровня информационной безопасности построенных с использованием данного метода реализаций в условиях наличия уязвимостей в вычислительных модулях, обеспечивающих хранение долговременных ключей подписи в неизвлекаемом виде.
8) Оценки стойкости процедур формирования проверочного параметра платежной карты (CVV) и проверочного значения PIN (PVV) в соответствующих практическим условиям применения математических моделях. Доказательство стойкости усовершенствованных процедур формирования параметров CVV и PVV по отношению к угрозе осуществления подделки.
9) Метод получения оценок уровня информационной безопасности в математической модели SUF-CMA для схем электронной подписи, которые строятся на основе схемы подписи семейства Эль-Гамаля путем применения трех семейств методов, предполагающих модификацию элементов схемы с целью уменьшения длины выхода подписи.
10) Протокол установления защищенного соединения с аутентификацией на основе низкоэнтропийных данных SESPAKE, обеспечивающий явное подтверждение выработанного общего секрета. Оценки стойкости этапов разработанного протокола в расширенной BPR-модели. Метод получения оценок уровня информационной безопасности полного протокола SESPAKE.

Методология и методы исследования. В рамках исследования применяется математический аппарат и подходы различных разделов математики, таких как дискретная математика, теория вероятностей и математическая статистика, теория алгоритмов.

Степень достоверности. Достоверность полученных результатов обеспечивается строгими математическими доказательствами утверждений.

Результаты других авторов, упомянутые в тексте диссертации, отмечены соответствующими ссылками.

Апробация работы. Результаты, полученные в диссертации, докладывались на международных и всероссийских конференциях и научно-исследовательских семинарах:

- семинар отдела дискретной математики Математического института им. В.А. Стеклова РАН;

- семинар «Булевы функции в криптологии» кафедры дискретной математики Механико-математического факультета Московского государственного университета им. М.В. Ломоносова;

- семинар «Математические методы криптографического анализа» кафедры информационной безопасности факультета Вычислительной математики и кибернетики Московского государственного университета им. М.В. Ломоносова;

- цикл из четырех семинаров в Университете Бергена (научный семинар по вопросам информационной безопасности центра “Selmer Center in Secure Communication”, под руководством Тора Хеллесета);

- семинар лаборатории National Engineering Laboratory for Wireless Security, Сиань, КНР;

- международный симпозиум НАТО «Enhancing Cryptographic Primitives with Techniques from Error Correcting Codes», Велико-Тырново, Болгария (2008 г.);

- симпозиум с международным участием «Современные тенденции в криптографии», CTCrypt (2013, 2015, 2016, 2017, 2018, 2019, 2020, 2021 г.);

- международная научная конференция «Progress of Security Protocols» (PSP 2017), Сиань, КНР (2017 г.);

- международные научные конференции по криптографии на территории Республики Куба (2015 и 2017 г.);

- конференции с международным участием «РусКрипто» (2012, 2013, 2014, 2015, 2016, 2017, 2018 г.);

- конференция с международным участием «V Международная научно-практическая конференция “Управление информационной безопасностью в современном обществе”», НИУ ВШЭ (2017 г.);

- международные конференции сообщества IETF/IRTF: Берлин, Германия (2016 г.), Сеул, Республика Корея (2016 г.), Чикаго, США (2017 г.), Прага, Чехия (2017 г.), Сингапур (2017 г.), Монреаль, Канада (2018 г.), Бангкок, Таиланд (2018 г.), Прага, Чехия (2019 г.);

- международные совещания подкомитета ISO/IEC JTC1 SC27 “Information security, cybersecurity and privacy protection”, Ухань, КНР (2018 г.), Гьовик, Норвегия (2018 г.), Тель-Авив, Израиль (2019 г.);

- форум «Безопасность информационных технологий в цифровой экономике», Москва (2020 г.);

- международная конференция «Security Standardisation Research 6th International Conference» (SSR 2020), Лондон, Англия (2020 г.);

- международный симпозиум «IEEE 33rd Computer Security Foundations Symposium» (CSF 2020), Бостон, США (2020 г.).

Публикации по теме исследования. Результаты работы изложены в 32 публикациях; в том числе, в 26 публикациях в изданиях, индексируемых в Web of Science, Scopus, RSCI и из списка ВАК Минобрнауки России; из них 21 — в изданиях, индексируемых в Web of Science, Scopus, RSCI.

Теоретическая значимость. В ходе исследования получены результаты, существенно развивающие математические модели и методы, применяемые при синтезе и анализе механизмов обеспечения информационной безопасности. Доказанные утверждения о кодирующих устройствах, построенных с использованием дискретной функции и регистра сдвига, которые сохраняют равновероятность входной последовательности при любом выборе расстояний между точками съема (в том числе, доказанная Гипотеза Голича, 1996 г.), новые результаты о свойствах спектральных коэффициентов совершенно уравновешен-

ных булевых функций (опровергающие ранее существовавшие предположения, основавшиеся на результатах зарубежных исследователей), а также установленные достаточные условия обладания совершенно уравновешенной булевой функцией свойством корреляционной иммунности существенно развивают методы синтеза и анализа дискретных функций для использования в задачах обеспечения информационной безопасности. Разработанные подходы, позволяющие обеспечить безопасность реализаций схем электронной подписи Эль-Гамаля и протоколов обеспечения защиты каналов связи в условиях потенциально уязвимых источников случайности, строго обоснованы в релевантных математических моделях. Разработанный математический аппарат для исследования механизмов преобразования сессионных векторов блочных симметричных алгоритмов обеспечения конфиденциальности позволил установить оценки уровня информационной безопасности для семейств построенных с их применением режимов (в том числе, новых, синтезированных в рамках настоящего исследования), обосновывающие повышение стойкости результирующих процедур защиты данных по сравнению с базовыми режимами работы блочных симметричных алгоритмов. Для параметризованных семейств механизмов VKO, PRFGOST, KDFTREE, модифицированных схем подписи Эль-Гамаля, а также функций генерации проверочных параметров CVV и PVV в соответствующих математических моделях разработаны методы обоснования оценок уровня информационной безопасности, позволяющие выбирать определяющие их конкретный вид значения параметров исходя из ограничений на вероятность успеха нарушителя при проведении атак. Разработан интерактивный протокол вычисления электронной подписи, для которого в математической модели, отражающей условия наличия уязвимостей в основном вычислительном устройстве, обоснована стойкость. Разработан применимый для защиты доступа к хранимым высокоэнтропийным секретам протокол установления защищенного соединения с аутентификацией на основе пароля и явным подтверждением выработанного общего секрета SESPAKE, для которого в построенной математической модели, подробно описывающей условия его применения, разработаны методы получения обоснованных оценок уровня информационной безопасности. Совокупность разработанных в диссертации математических методов обеспечения достаточного уровня информационной безопасности, математических моделей, а также методов получения обоснованных оценок уровня информационной безопасности средств защиты информации в условиях ограниченного доверия к среде функционирования представляет собой качественное развитие математического аппарата, применяемого при разработке и анализе математических моделей и методов оценки защищенности информации в задачах обеспечения информационной безопасности.

Практическая значимость. Все полученные результаты применимы для синтеза и анализа механизмов обеспечения защиты информации в условиях слабодоверенного окружения. Полученные результаты позволяют для индивидуальных параметров схем получать обоснованные численные значения уровня информационной безопасности, осуществлять выбор параметров схем, опира-

ясь на строгие математические результаты о стойкости, без проведения дополнительных исследований. Кроме того, разработанные методы могут использоваться при подготовке учебных пособий и разработке лекционных курсов. Внедрение изложенных и обоснованных методов при разработке средств защиты информации решает практическую проблему обеспечения безопасности их функционирования в условиях массового применения, имеющую определяющее значение для информационной безопасности государства.

Практическая значимость диссертации подтверждена 16 актами о внедрении, а также 11 свидетельствами о государственной регистрации программы для ЭВМ.

Результаты диссертации используются в деятельности следующих государственных и коммерческих организаций:

- **Министерство обороны Российской Федерации** — при обеспечении информационной безопасности в системах электронного документооборота и удостоверяющего центра Минобороны России;

- **Федеральная налоговая служба Российской Федерации** — при проектировании и оценке защищенности систем электронного документооборота и удостоверяющего центра ФНС России;

- **Центральный банк Российской Федерации** — в деятельности Департамента информационной безопасности Банка России, при оценке защищенности информационных систем кредитных организаций, а также при формировании нормативно-технических актов Банка России по обеспечению защиты информации при осуществлении переводов денежных средств и формировании комплексной системы защиты информации в Системе быстрых платежей Банка России;

- **НИИ «Восход»** — при разработке и оценке уровня информационной безопасности средств головного удостоверяющего центра Российской Федерации, а также паспортов с электронным носителем;

- **Национальная система платежных карт (НСПК)** — при проектировании и оценке уровня информационной безопасности перспективных систем обеспечения информационной безопасности национальной платежной системы «МИР», а также в решениях, обеспечивающих защиту информации в действующих информационных системах национальной платежной системы «МИР»;

- **АНСЕР ПРО** — при оценке защищенности информации в рамках проведения исследований средств и информационных систем на соответствие действующим в Российской Федерации требованиям по информационной безопасности, а также при разработке методологии проведения данных исследований;

- **Актив-Софт** — при разработке и оценке уровня информационной безопасности средств защиты информации, в том числе, в системах дистанционного банковского обслуживания клиентов кредитно-финансовых организаций (в частности, ПАО «Сбербанк»), а также в федеральном проекте, предназначенном для обеспечения конфиденциальности контрольно-измерительных материалов (КИМ) при проведении Единого государственного экзамена (ЕГЭ) в масштабах всей Российской Федерации;

- **Системы практической безопасности** — при разработке и внедрении средств защиты информации, предназначенных для обеспечения информационной безопасности систем платежных карт;

- **КРИПТО-ПРО** — при разработке и оценке уровня информационной безопасности средств защиты информации, обеспечивающих информационную безопасность клиент-серверных соединений, а также систем электронного документооборота в государственных и коммерческих организациях;

- **ИнфоТеКС** — при разработке и оценке уровня информационной безопасности средств защиты информации, обеспечивающих информационную безопасность клиент-серверных соединений, а также систем электронного документооборота в государственных и коммерческих организациях;

- **SafeTech** — при разработке и оценке уровня информационной безопасности средств электронной подписи, применяемых, в частности, в системах электронного документооборота банков ВТБ, Промсвязьбанк, Альфа-Банк, Россельхозбанк;

- **Яндекс** — при разработке сервисов и оценке уровня информационной безопасности средств защиты информации, применяемых в информационных системах ООО «Яндекс.Облако»;

- **Газинформсервис** — при разработке и оценке уровня информационной безопасности средств защиты информации, применяемых для обеспечения информационной безопасности систем электронного документооборота, в том числе, в структурах ПАО «Газпром»;

- **Ростелеком** — при разработке средств и система защиты информации, при обеспечении информационной безопасности взаимодействий с государственной Единой системой идентификации и аутентификации (ЕСИА) и Единой биометрической системой (ЕБС) в рамках процессов регистрации, идентификации и аутентификации;

- **МегаФон** — при обеспечении информационной безопасности процессов работы систем электронной подписи, используемых в системах электронного документооборота ПАО «МегаФон»;

- **Сбербанк** — при обеспечении информационной безопасности процессов электронной подписи в системах электронного документооборота ПАО «Сбербанк».

Разработанный механизм обеспечения защиты от уязвимых источников случайности по результатам данных исследований стандартизирован в IETF/IRTF в RFC 8937 как готовый к внедрению в средства защиты информации без дополнительных исследований.

Разработанный и обоснованный режим работы блочных симметричных алгоритмов CTR-ACPKM, предназначенный для функционирования в условиях слабодоверенного окружения, стандартизирован в российских рекомендациях по стандартизации Р 1323565.1.017–2018 «Информационная технология. Криптографическая защита информации. Криптографические алгоритмы, сопутствующие применению алгоритмов блочного шифрования», в международ-

ном отраслевом стандарте IETF/IRTF RFC 8645, а также в международном стандарте ISO/IEC 10116:2017/AMD 1:2021 «Information technology — Security techniques — Modes of operation for an n-bit block cipher», став шестым режимом работы блочных симметричных алгоритмов в ряду с разработанными более 30 лет назад классическими режимами ECB (простой замены), CTR (гаммирования), CFB (гаммирования с обратной связью по шифртексту), CBC (простой замены с зацеплением), OFB (гаммирования с обратной связью по выходу). Режим CTR-ACPKM и доказанные результаты о его свойствах стали фундаментом для процедур транспорта данных в стандартизированных в России протоколах CMS и TLS 1.2 (Рекомендации по стандартизации Р 1323565.1.020-2020 «Информационная технология. Криптографическая защита информации. Использование российских криптографических алгоритмов в протоколе безопасности транспортного уровня (TLS 1.2)»).

По результатам проведенных исследований семейств механизмов PRFGOST, VKO, KDFTREE, KDFGOST они были стандартизированы в рекомендациях по стандартизации Р 50.1.113–2016 «Информационная технология. Криптографическая защита информации. Криптографические алгоритмы, сопутствующие применению алгоритмов электронной цифровой подписи и функции хэширования», вошли в RFC 7836, на результатах проведенных исследований была основана разработка и анализ процедур выработки ключей всех современных стандартизированных в России версий протоколов CMS, TLS и IPsec. Разработанные для KDFTREE и VKO методы позже позволили при разработке порядка применения российских алгоритмов (с последующей стандартизацией) для платежной системы «МИР» провести анализ стойкости подсистем выработки ключей в процессах персонализации и процессинга, защиты PIN-кода при его проверке в отсутствие доступа к сети, определив строго обоснованным образом допустимые параметры безопасного функционирования данных подсистем.

По результатам проведенных исследований усовершенствованные процедуры формирования параметров CVV/PVV стандартизированы в России в рекомендациях по стандартизации Р 1323565.1.007–2017 «Информационная технология. Криптографическая защита информации. Использование алгоритмов блочного шифрования при формировании проверочного параметра платежной карты и проверочного значения PIN» в качестве процедур формирования проверочного параметра платежной карты и проверочного значения PIN.

Разработанный и обоснованный протокол SESPAKE по результатам проведенных в диссертации исследований стандартизирован в рекомендациях по стандартизации Р 50.1.115–2016 «Информационная технология. Криптографическая защита информации. Протокол выработки общего ключа с аутентификацией на основе пароля» и вошел в RFC 8133, применяется в паспортах с электронным носителем, планируемых к массовой выдаче вместо существующих бумажных паспортов.

Структура и объем диссертации. Диссертация состоит из введения, трех глав, заключения, списка основных обозначений, списка литературы из 339 наименований и приложения. Работа изложена на 593 страницах.

ОСНОВНОЕ СОДЕРЖАНИЕ РАБОТЫ

Во введении обоснована актуальность темы диссертации, сформулированы цели и задачи исследований, отражены научная новизна, теоретическая и практическая значимость полученных результатов, представлены основные результаты, которые выносятся на защиту.

В разделе «Обозначения, определения и общие сведения» вводятся используемые в работе понятия и обозначения, а также приводятся некоторые используемые в работе ранее известные результаты: понятие совершенно уравновешенной дискретной функции и функции с барьером, основные известные утверждения о данных классах функций, используемая далее в работе терминология для определения математических моделей нарушителя, обозначения, определения и некоторые известные результаты для используемых далее в работе механизмов, таких как HMAC, функции хэширования, схемы электронной подписи.

Первая глава посвящена методам применения и преобразования выходов источников случайности в средствах защиты информации с целью обеспечения защищенности в условиях слабодоверенного окружения. В ней развивается математический аппарат дискретных функций, необходимых для построения генераторов псевдослучайных чисел, устойчивых к сбоям источников случайности (то есть позволяющих сохранить положительные качества выходной последовательности в случае сбоев в окружении средства защиты информации), а именно, совершенно уравновешенных функций, а также синтезируются и анализируются математические конструкции, позволяющие обеспечить отсутствие ухудшения свойств защиты информации в случае сбоев исходного датчика случайных чисел — как в общем случае, без применения дополнительных модулей (для схем электронной подписи), так и в ситуациях, в которых возможно применение вспомогательных источников случайности на базе программно-аппаратных модулей HSM (Hardware Security Module).

При реализации генераторов псевдослучайных чисел (ГПСЧ — здесь и далее будем употреблять данный термин для механизмов, предполагаемых для реализации непосредственно в рассматриваемых средствах защиты информации программным образом) в средствах защиты информации типичным подходом является следующий: исходное заполнение генератора псевдослучайных чисел берется с некоторого датчика случайных чисел (ДСЧ — здесь и далее будем употреблять данный термин для программно-аппаратных компонент, применяемых в рассматриваемых средствах защиты информации в качестве внешних источников случайности) аппаратного или биологического[42,43], после чего для порождения сессионных секретов, синхропосылок и прочих критичных для безопасности одноразовых значений используются очередные выходы ГПСЧ (см. [4, 23]).

[42]Задорожный Д.И., Коренева А.М., Фомичев В.М. Построение биодатчика случайных чисел и оптимизация его характеристик с помощью вычислительных экспериментов // Материалы РусКрипто'2016, `https://www.ruscrypto.ru/resource/archive/rc2016/files/02_zadorozhny.pdf`, 2016 г.

[43]Задорожный Д.И., Коренева А.М., Фомичев В.М. Способ генерации случайных двоичных последовательностей с использованием компьютера и действий пользователя. Патент RU2628213C1, 15 августа 2017 г.

Изучаются методы преобразования исходной случайной последовательности, применимые в средствах, предполагаемых для использования в тех системах, в которых целесообразно учитывать возможность сбоев и отказов некоторых из источников случайности. В таких случаях важно обеспечить, с одной стороны, сохранение «идеальных» свойств случайной последовательности в штатном режиме работы (пока сбои и отказы не произошли) и, одновременно, защиту от полного вырождения случайной последовательности в случае сбоев.

Результаты исследований в области преобразований, применяемых при обеспечении защиты информации и сохраняющих положительные качества входной последовательности, представлены в работах С.Н. Сумарокова, В.Г. Никонова, Н.В. Никонова[44], А.В. Бабаша[45], М.И. Рожкова[46], О.А. Логачева[47], С.В. Смышляева, В.В. Ященко[48], Р. Андерсона[49], Г. Хедлунда[50], Ф. Препараты[51] и др.

Выход ДСЧ, применяемых в средствах защиты информации, на практике в типичном случае получается на основе ряда независимых по природе, но не всегда имеющих гарантии стабильного поведения источников. В результате этого в штатном режиме выход ДСЧ является неотличимым от последовательности независимых равномерно распределенных двоичных символов (битов), а в случае сбоев вырождается в снабженную строгими зависимостями последовательность, типичным видом которой является линейно-рекуррентная. С учетом указанных особенностей поведения в слабодоверенном окружении, в программных средствах защиты информации может использоваться такой метод дополнительной защиты, как применение обработки двоичной последовательности вспомогательным кодирующим устройством, построенным на основе регистра сдвига и дискретной функции. Из практических требований вытекает, что данная дискретная функция должна обладать двумя свойствами: в случае последовательности независимых равномерно распределенных двоичных символов на входе преобразования такой должна быть и выходная последовательность (определяемые этим свойством дискретные функции называются совершенно уравновешенными), а в случае вырождения входной последовательности в линейно-рекуррентную она должна обеспечивать улучшение ее качеств

[44]Никонов В.Г., Никонов Н.В. Некоторые классы функций k-значной логики без запрета // Вестник Московского государственного университета леса — Лесной вестник, №1, 2006. С. 117-123

[45]Бабаш А.В. Запреты автоматов и двоичных функций // Труды по дискретной математике. 2006. Т. 9. С. 7–20.

[46]Рожков М.И. Некоторые алгоритмические вопросы идентификации конечных автоматов по распределению выходных m-грамм I // Обозрение прикладной и промышленной математики. 2008. 15(4). С. 613–630.

[47]Логачев О.А. Критерий совершенной уравновешенности сдвиг–композиции функций над конечным алфавитом // Дискретная математика, 29:4, 2017. С. 59–65.

[48]Логачев О.А., Смышляев С.В., Ященко В.В. Новые методы изучения совершенно уравновешенных булевых функций // Дискретная математика. 2009. Т. 21. Вып. 2. С. 51–74.

[49]Anderson R.J. Searching for the optimum correlation attack // Lecture Notes in Computer Science, 1995, vol. 1008. Pp. 137–143.

[50]Hedlund G.A. Endomorphisms and automorphisms of the shift dynamical system // Theory of Computing Systems. 1969. Vol. 3(4). Pp. 320–375.

[51]Preparata F.P. Convolutional transformations of binary sequences: Boolean functions and their resynchronizing properties // IEEE Transactions on Electronic Computers. 1966. Vol. 15. Pp. 898–909.

(см. [27]), в частности, добавляя нелинейность в зависимости выходных символов от входных. Разделы 1.1 и 1.2 диссертации посвящены исследованию и методам построения соответствующих вспомогательных кодирующих устройств — в случаях произвольного и фиксированного набора точек съема кодирующего устройства соответственно.

Раздел 1.1 посвящен исследованию фундаментального вопроса о возможности сохранения дискретной функцией свойства совершенной уравновешенности при добавлении любого количества фиктивных переменных. В булевом случае предположение о структуре класса функций, обладающих таким свойством, было выдвинуто в 1996 году Йованом Голичем[52]. Начиная с работы М. Дихтла[53], данное предположение известно в качестве Гипотезы Голича.

Гипотеза Голича предполагает, что все булевы функции, сохраняющие совершенную уравновешенность при добавлении любого числа фиктивных переменных, линейны по одной из крайних переменных. С точки зрения практики, это означает, что все параметризованные набором точек съема вспомогательные кодирующие устройства на основе регистра сдвига и булевой функции, которые не ухудшают свойства входной последовательности ни при каком наборе расстояний между точками съема (см. [28]), неминуемо обладают свойством линейности по первому или последнему входу (что, в свою очередь, как следует из результатов О.А. Логачева[54], а также [27] и [30], является нежелательным свойством в случае необходимости избежать применимости простых методов обращения таких кодирующих устройств).

Попытки зарубежных исследователей (Й. Голич, М. Дихтл, А. Канто, А. Гуже, Х. Сибер) продвинуться в доказательстве Гипотезы Голича ранее не только оканчивались неудачами, но и приводили к получению ошибочных результатов (как ранее опровергнутых[55], так и опровергаемых в настоящей работе в разделе 1.2).

В настоящей диссертации Гипотеза Голича полностью доказана. В теореме 5.4 [1] разработан метод построения для произвольной существенно и нелинейно зависящей от крайних переменных булевой функции набора точек съема, для которого с применением доказанного С.Н. Сумароковым[56] критерия и с применением доказанных лемм 5.6, 5.7 и 5.8 [1] обосновывается нарушение свойства совершенной уравновешенности у соответствующей булевой функции.

Таким образом, доказана невозможность построения вспомогательного кодирующего устройства на основе регистра сдвига и отличной от линейной по

[52]Golić J.D. On the security of nonlinear filter generators // Lecture Notes in Computer Science. 1996. Vol. 1039. Pp. 173–188.

[53]Dichtl M. On nonlinear filter generators // Lecture Notes in Computer Science. 1997. Vol. 1267. Pp. 103–106.

[54]Логачев О.А. Построение и анализ эффективности алгоритмов обращения дискретных функций в математических моделях информационной безопасности. Диссертация на соискание степени доктора физико-математических наук. 2019.

[55]Смышляев С.В. Комбинаторные свойства совершенно уравновешенных булевых функций. Диссертация на соискание степени кандидата физико-математических наук. 2012.

[56]Сумароков С.Н. Запреты двоичных функций и обратимость для одного класса кодирующих устройств // Обозрение прикладной и промышленной математики. 1994. 1(1). С. 33–55.

крайней переменной булевой функции, которое не ухудшало бы статистические свойства входной последовательности ни при каком выборе точек съема.

С учетом возможности преобразования входной последовательности блоками длины $m \geqslant 2$, [29], далее рассматривается вопрос о возможности построения таких кодирующих устройств над алфавитом большей мощности — в особенности, в случае алфавита мощности $k = 2^m$, $m \geqslant 2$. Формулируются и рассматриваются два обобщения условия Гипотезы Голича для случая произвольного $k \geqslant 2$:

- Условие Голича. Совершенная уравновешенность, сохраняющаяся при любом выборе набора точек съема (без изменения порядка), эквивалентна перестановочности по первой или последней существенной переменной.
- Слабое условие Голича. Совершенная уравновешенность, сохраняющаяся при любом выборе обобщенного (т.е. с возможностью изменения порядка) набора точек съема, эквивалентна перестановочности по каждой существенной переменной (для функции, отличной от константы).

Из доказанной теоремы 5.4 следует, что Условие Голича и Слабое Условие Голича выполнены для $k = 2$.

Также доказано, что Условие Голича:

1. нарушается на k-значных функциях двух переменных при любом составном k (теорема 2 [2]);
2. не нарушается на k-значных функциях двух переменных при k равном одному из четырех наименьших простых чисел (следствие 7 [2]);
3. нарушается на k-значных функциях с барьером длины 2 при любом составном k (теорема 2 [2]);
4. не нарушается на k-значных функциях с барьером длины 2 при любом простом k (следствие 5 [2]);
5. выполнено на k-значных функциях двух переменных с барьером при любом простом k (следствие 6 [2]);
6. нарушается на существенно зависящих от n переменных k-значных функциях при любом составном k и любом $n \geqslant 2$ (теорема 3 [2]).

Кроме того, доказано, что Слабое условие Голича:

1. нарушается на k-значных функциях двух переменных при любом составном k (следствие 4.6 [5]);
2. не нарушается на k-значных функциях двух переменных при k равном одному из четырех наименьших простых чисел (следствие 3.6 [5]);
3. нарушается на существенно зависящих от трех переменных k-значных функциях при любом составном k (теорема 4.7 [5]).

Итак, обобщенная версия Гипотезы Голича в k-значном случае не является корректной: более того, получен, в определенном смысле, неожиданный результат о связи выполнения обобщенной версии Гипотезы Голича с простотой k.

Из доказательства самой Гипотезы Голича следует, что вспомогательные кодирующие устройства для рассматриваемых задач требуется выбирать сразу с фиксированным набором точек съема.

В разделе 1.2 свойства совершенно уравновешенных булевых функций (в том числе, булевых функций с барьером) исследуются в свете применения во вспомогательных кодирующих устройствах на базе регистра сдвига и булевой функции при фиксированном наборе точек съема; изучается вопрос о методах построения таких функций с положительными свойствами. В большом числе случаев (см. [27]) положительные с точки зрения использования в таких кодирующих устройствах свойства булевых функций выражаются через набор условий на коэффициенты Уолша–Адамара — но, за исключением некоторых ранее полученных частных утверждений[57], содержательные результаты о свойствах коэффициентов Уолша–Адамара совершенно уравновешенных булевых функций отсутствовали.

Более того, попытки использовать данный аппарат с целью получения необходимых или достаточных условий совершенной уравновешенности приводили к серьезным ошибкам. Так, А. Канто в своей диссертации[58] получила соотношения (усиливающие, в определенном смысле, соотношения М. Дихтла и подходы А. Гуже и Х. Сибера[59]), позволявшие простым образом связать свойство сохранения равновероятности m-грамм на входе и выходе кодирующего устройства (в случае добавления квантора всеобщности для m — условие совершенной уравновешенности) с нулями в векторе коэффициентов Уолша–Адамара функции.

Теорема 7 [7] опровергает указанные условия, причем в рамках доказательства для произвольного n конструируется множество из $2^{2^{n-6}}-1$ булевых функций, каждая из которых является совершенно уравновешенной (то есть сохраняющей равновероятность любых m-грамм на входе и выходе кодирующего устройства при любом m) и при этом не удовлетворяет указанным условиям: отличны от нуля коэффициенты Уолша–Адамара на двух векторах веса 1, один из которых содержит единицу на крайней позиции, а другой — на отличной от крайней. Одновременно, с применением построенной последовательности множеств функций опровергаются условие М. Дихтла и достаточность совершенной уравновешенности булевой функции для наличия у нее свойства корреляционной иммунности (функция является корреляционно-иммунной порядка 1 тогда и только тогда, когда ее коэффициенты Уолша–Адамара на всех векторах веса 1 нулевые, см. [27]).

Таким образом, несмотря на ряд ранее предпринятых зарубежными исследователями попыток, результаты, позволявшие строить невырожденные классы совершенно уравновешенных булевых функций, обладающих свойством корре-

[57]Логачев О.А., Смышляев С.В., Ященко В.В. Новые методы изучения совершенно уравновешенных булевых функций // Дискретная математика. 2009. Т. 21. Вып. 2. С. 51–74.

[58]Canteaut A., Analysis and Design of Symmetric Ciphers, Habilitation for directing Theses, University of Paris 6, 2006.

[59]Gouget A., Sibert H. Revisiting correlation immunity in filter generators // Lecture Notes in Computer Science. 2007. Vol. 4876. Pp. 378–395.

ляционной иммунности (как и некоторыми более слабыми свойствами, определяемыми в терминах нулей коэффициентов Уолша–Адамара), отсутствовали либо были опровергнуты. В настоящей диссертации удается построить такие классы функций.

С целью построения таких классов функций (и, соответственно, методов конструирования вспомогательных кодирующих устройств с указанными выше свойствами) исследуются комбинаторные свойства булевых функций с барьером, [3, 7]. С помощью доказательства леммы 1 [7] удается получить результат об уравновешенности отображений, порождаемых кодирующими устройствами с функциями с барьером при фиксации части входных переменных (теорема 8 [7]), из которого вытекает следствие 2 [7] об уравновешенности определенных подфункций функций с барьером.

С помощью полученных результатов доказывается утверждение теоремы 8 [7]: все совершенно уравновешенные функции с обоими барьерами, сумма длин барьеров которых меньше числа переменных, являются корреляционно-иммунными, а именно, 1-устойчивыми. Данный результат позволяет строить для произвольного n совершенно уравновешенные булевы функции n переменных, нелинейно зависящие от крайних переменных и при этом корреляционно-иммунные, предоставляя окончательное решение рассматриваемой задачи.

В разделе 1.3 вопрос о построении вспомогательных конструкций, противодействующих деградации стойкости систем в случае сбоев ДСЧ, рассматривается в случае функционирования программных средств в серверных решениях. В определенных случаях, в частности, при формировании электронной подписи с применением схем семейства Эль-Гамаля, даже единичный сбой ДСЧ может привести к нарушению информационной безопасности системы из-за раскрытия долговременного секретного значения (ключа). Проблема отсутствия полного доверия к выходной последовательности датчика случайных чисел (среди общих исследований по данному направлению можно выделить работы Т. Ристенпарта[60], Д. Бернштейна[61], К. Патерсона[62]) является критичной не только для программных реализаций, функционирующих, как правило, на стороне массового пользователя, но и для гибридных программно-аппаратных решений, состоящих из программной реализации (обеспечивающей основное функционирование) и программно-аппаратных модулей HSM (выполняющих наиболее критичные операции — в том числе, с долговременными секретными значениями). Такие решения, в частности, нередко функционируют на серверной стороне при защите информации по протоколу TLS[63], для которого доверие к

[60]Ristenpart T., Yilek S. When good randomness goes bad: Virtual machine reset vulnerabilities and hedging deployed cryptography. // Proc. ISOC Network and Distributed Security Symposium (2010).

[61]Checkoway S., Niederhagen R., Everspaugh A., Green M., Lange T., Ristenpart T., Bernstein D.J., Maskiewicz J., Shacham H., Fredrikson M. On the Practical Exploitability of Dual EC in TLS Implementations. In 23rd USENIX Security Symposium (USENIX Security 14), San Diego, CA, August 2014. USENIX Association. Pp. 319–335.

[62]Degabriele J.P., Paterson K.G., Schuldt C.N., Woodage J. Backdoors in pseudorandom number generators: Possibility and impossibility results // Lecture Notes in Computer Science, Vol. 9814, CRYPTO 2016, Part I, 2016. Pp. 403-432.

окружению является критичным, [22]. На серверной стороне ошибки функционирования ДСЧ средств защиты информации, опирающихся на источники из окружения, могут приводить к полной компрометации серверов (и, как следствие, к полному нарушению защиты информационных систем — например, систем электронного документооборота). Задача обеспечения защиты протоколов в подобных условиях рассматривалась Б. ЛаМаккией, К. Лаутером и А. Митягиным[64], однако предложенный ими подход оказался неприменимым на практике для использования на серверной стороне из-за условий хранения ключей в отдельных защищенных модулях. Задачей, следующей из практики и решаемой в разделе 1.3, является дополнение реализаций вспомогательной конструкцией, задействующей доступ к защищенным модулям (например, HSM) для подписи Sig с помощью хранимого в HSM ключа sk и обеспечивающей отсутствие ухудшения свойств случайных чисел в случае отсутствия сбоев исходного ДСЧ с одновременным обеспечением вычислительной неотличимости выходов конструкции от последовательности независимо равномерно распределенных случайных величин даже при полной компрометации исходного ДСЧ.

Разработанная в настоящей диссертации конструкция опирается на механизмы выработки псевдослучайных строк и диверсификации ключей (требуемые от данных механизмов PRF и KDF свойства определяются в начале проведения анализа), при ее использовании вместо обращения к ДСЧ $G(n)$ для получения двоичного набора длины n применяется дополненный вызов $G'(n)$: $G'(n) = \mathrm{PRF}(\mathsf{KDF}(\mathrm{H}(\mathrm{Sig}(\mathrm{sk}, \mathtt{tag}_1)), y), \mathtt{tag}_2, n)$, где двоичная строка y получается путем обращения к $G(\cdot)$, H — функция хэширования, $\mathtt{tag}_1$ — фиксированная строка, значение которой выбирается для конкретного контекста использования конструкции, а $\mathtt{tag}_2$ — уникальная для вызова строка (например, значение счетчика обращений).

Разработанный механизм предназначен для обеспечения следующих свойств информационной безопасности:

1. Если ДСЧ функционирует штатно и в соответствии с заданной моделью функционирования, обеспечивая порождение двоичных наборов длины n, неотличимых (в определенной модели нарушителя) от равновероятно выбранных из $\{0,1\}^n$, то наборы с тем же свойством порождаются и на выходе разработанного механизма.
2. При условии, что ДСЧ уязвим или находится под контролем нарушителя, выходы разработанного механизма остаются неотличимыми от равновероятно выбранных из $\{0,1\}^n$ наборов, если хранимый в HSM ключ sk остается неизвестным для нарушителя.
3. Нарушитель с полным контролем над потенциально уязвимым ДСЧ и доступом к выходным значениям, порождаемым разработанным механизмом, не получает преимущества, отличного от пренебрежимо малого, при попытке восстановления долговременного ключа sk (атаки по побочным каналам

[63]Dierks T., Rescorla E., "The Transport Layer Security (TLS) Protocol Version 1.2", RFC 5246, August 2008.

[64]LaMacchia B., Lauter K. and Mityagin A. Stronger security of authenticated key exchange // Provable Security, Springer, 2007. Pp. 1–16.

на sk не рассматриваются: считаем, что от них предоставляют защиту те меры, которые реализованы в HSM).

Данные целевые свойства безопасности строго формализованы (см. [17]) детально описана модель нарушителя, обладающего возможностями по влиянию на ДСЧ (запросы типа `«получить выход»` — предполагается не только возможность наличия в ДСЧ уязвимостей, но даже возможность нарушителя непосредственно влиять на ДСЧ), возможностью компрометации долговременных ключей и результатов операций с ними (запросы типов `«завершить»` и `«подписать»` — при этом накладывается условие на отсутствие одновременной реализации нарушителем атак и на ДСЧ, и на долговременные ключи), а также стандартными для моделей нарушителя для протоколов возможностями узнать часть выходных значений механизма (запросы типа `«раскрыть»`).

В теореме 1 [17] путем построения двух цепочек формально описанных экспериментов (промежуточных моделей нарушителя) и получения оценок разностей между вероятностями успеха нарушителя в соседних экспериментах цепочек доказывается утверждение о стойкости описанной конструкции в предположении выполнения условий функциями PRF, KDF, Sig и H.

Синтезированная и проанализированная в релевантной модели нарушителя конструкция обеспечивает запас прочности на практике, являясь первым не требующим модификации ключевой системы протоколов механизмом, для которого в детальной математической модели функционирования сервера с уязвимым источником случайности обоснована стойкость, что в полной мере решает поставленную задачу. По результатам исследования, проведенного в настоящей диссертации, разработанная конструкция была стандартизирована в RFC 8937[65] в 2020 году.

В разделе 1.4 решается задача построения способа модификации схем подписи семейства Эль-Гамаля (в частности, ГОСТ Р 34.10-2012[66]), обеспечивающего повышение безопасности в сценариях использования в слабодоверенном окружении (при отсутствии надежных датчиков случайных чисел). В отличие от подхода, применявшегося Т. Порнином[67] и Д. Бернштейном[68], для которого в условиях слабодоверенного окружения К. Эмброузом[69], Л. Вайссбартом[70], М. Фишлином[71] и другими были разработаны методы снижения стойкости, за

[65]Cremers C., Garratt L., Sullivan N., Smyshlyaev S., Wood C., "Randomness Improvements for Security Protocols", RFC 8937, 2020.

[66]ГОСТ Р 34.10–2012, «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи», Москва, Стандартинформ, 2012.

[67]Pornin T., "Deterministic Usage of the Digital Signature Algorithm (DSA) and Elliptic Curve Digital Signature Algorithm (ECDSA)", RFC 6979, 2013.

[68]Josefsson S., Liusvaara I. Edwards-Curve Digital Signature Algorithm (EdDSA) RFC 8032, 2017.

[69]Ambrose, C., Bos, J. W., Fay, B., Joye, M., Lochter, M., Murray, B. Differential attacks on deterministic signatures // Cryptographers' Track at the RSA Conference, Springer, 2018. Pp. 339–353.

[70]Weissbart, L., Picek, S., Batina, L. One trace is all it takes: Machine learning-based side-channel attack on EdDSA // International Conference on Security, Privacy, and Applied Cryptography Engineering, Springer, 2019. Pp. 86–105.

[71]Fischlin, M., Gunther, F. Modeling Memory Faults in Signature and Encryption Schemes, Cryptology ePrint Archive, Report 2019/1053, 2019.

основу берется идея комбинирования при вычислении разовых секретов случайных и порождаемых детерминированным образом значений (в 2019 году Дж. Мэттссоном был сформирован набросок[72] схемы, применяющей близкие принципы, но на его основе так и не был создан обоснованный механизм, применимый в существующих реализациях). Данный вопрос изучается в математической модели, отражающей возможность нарушителя влиять на значения случайных чисел, применяемых в процессе вычисления подписи: для анализа стойкости модифицированной схемы подписи применяется модель нарушителя SUF-CMRA (Strong Unforgeability under Chosen Message and Randomness Attack).

Разрабатывается механизм на основе внесения зависимости разовых секретных значений от ключа подписи и самого подписываемого сообщения с применением механизма HMAC. Разработанный метод учитывает такой важнейший для обеспечения безопасности реализаций при функционировании в слабодоверенном окружении аспект, как использование случайно порождаемых «масок»: случайных множителей, участвующих в тех вычислениях, где операции производятся с участием долговременных секретов, и применяемых в целях противодействия ряду практических инженерных методов атак на долговременные ключи при хранении ключей и вычислении значений подписи.

Основным результатом раздела является доказательство утверждения теоремы 1 [19]: на основе построения цепочки промежуточных моделей нарушителя и оценок разностей вероятностей успехов нарушителей в этих моделях, с учетом доказанных утверждений 1 и 2 [19], обоснована стойкость для модифицированной реализации схемы подписи в модели SUF-CMRA в условиях стойкости базовой схемы подписи в модели SUF-CMA и стойкости функции HMAC в модели PRF. Разработан и обоснован метод модификации реализации схемы подписи Эль-Гамаля, сохраняющий свойство недетерминированности схемы и обеспечивающий стойкость в модели SUF-CMRA с сохранением совместимости с существующими практиками повышения безопасности реализаций. Результат предоставляет метод получения для конкретных параметров схемы численных значений уровня информационной безопасности.

Вторая глава посвящена математическим моделям и методам обеспечения защиты информации (передаваемых или хранимых данных, в том числе, в рамках протоколов клиент-серверного взаимодействия) при функционировании программных средств защиты информации в условиях возможности нарушителя получать частичную информацию о выполняемых операциях: либо в рамках сценариев частичной утечки данных, актуальных на практике при невозможности жесткой фиксации разработчиком средств программного и аппаратного окружения (результаты исследований последствий подобных уязвимостей представлены, в частности, в работах Д. Бернштейна, Т. Ланге[73], А.П. Бара-

[72]Mattsson J., Thormarker E., Ruohomaa S. Deterministic ECDSA and EdDSA Signatures with Additional Randomness, draft-mattsson-cfrg-det-sigs-with-noise-02.

[73]Bernstein D.J., Chang Y.A., Cheng C.M., Chou L.P., Heninger N., Lange T., van Someren N. Factoring RSA keys from certified smart cards: Coppersmith in the wild // Lecture Notes in Computer Science 8270, 2013.

нова[74,75,76], Дж. Хальдермана, Н. Хеннингер[77]), либо в определенных случаях функционирования на одной системе нескольких пользователей, часть из которых для других является нарушителями, то есть в условиях, рассмотренных в работе [15].

В разделе 2.1 рассматривается задача о защите передаваемых по каналам связи данных с использованием средств, функционирующих в слабодоверенном окружении (без специальных средств защиты от атак по побочным каналам, с пониженными гарантиями надежности узлов, выполняющих основные преобразования с секретными параметрами). Обработка большого количества сообщений без преобразований секретных значений в таком окружении может привести к нарушению информационной безопасности: к компрометации секретов, раскрытию передаваемых данных. Исследования, посвященные подходам к выбору ограничений в отсутствие смены ключей, проводились, в частности, И.В. Лавриковым, В.А. Шишкиным[78].

В отличие от подхода, разрабатывавшегося М. Абдаллой и М. Белларе[79], не применимого для существующих протоколов из-за необходимости усложнения ключевой системы (а также, дополнительно, существенного снижения производительности на данных малой длины), в настоящей диссертации механизмы, предназначенные для обеспечения возможности работы транспортных протоколов на объемах данных, существенно превышающих вытекающие из описанной проблемы ограничения, строятся на следующем принципе: непосредственная обработка данных производится с помощью последовательности ключей, получаемых из первоначально согласованного секрета путем применения специально подобранных детерминированных преобразований. Для сохранения уровня защищенности протокола такие преобразования должны обеспечивать ряд свойств вырабатываемых ключей. Проведено исследование ранее разработанных механизмов преобразования сессионных ключей, выработан общий подход, связанный с рассмотрением механизмов регулярной смены ключей в паре с базовыми режимами работы блочных симметричных алгоритмов (далее — БСА) в качестве новых расширенных режимов.

В математической модели LOR-CPA получены оценки стойкости для режима CTR-CPKM, разработанного ранее[80] для применения при обработке данных

Pp. 341–360.

[74]Баранов А.П. Актуальные направления в области информационной безопасности // Материалы пленарного заседания РусКрипто‘2016, 2016 г.

[75]Баранов А.П., Баранов П.А. Информационная безопасность больших данных в массовых системах // Материалы пленарного заседания РусКрипто‘2017

[76]Баранов А.П., Баранов П.А. Криптография и информационная безопасность в цифровом обществе // Материалы пленарного заседания РусКрипто‘2019, 2019 г.

[77]Bos J.W., Halderman J.A., Heninger N., Moore J., Naehrig M., Wustrow E.. Elliptic curve cryptography in practice // International Conference on Financial Cryptography and Data Security, 2014. Pp. 157-175.

[78]Lavrikov I.V., Shishkin V.A. How much data may be safely processed on one key in different modes? // Матем. вопр. криптогр., 10:2, 2019. С. 125–134.

[79]Abdalla M., Bellare M. Increasing the Lifetime of a Key: A Comparative Analysis of the Security of Re-keying Techniques // Lecture Notes in Computer Science, 2000, vol. 1976. Pp. 546–559.

[80]Popov V., Kurepkin I., Leontiev S., “Additional cryptographic algorithms for use with GOST 28147-89, GOST

большой длины. Введена промежуточная модель IND-KM и гипотетический режим, использующий последовательность независимых равновероятных ключей секций. Для данного режима в модели LOR-CPA получена оценка стойкости (лемма 6.1 [10]), а на ее основе установлено итоговое соотношение для режима CTR-CPKM (теорема 6.1 [10]), позволяющее получать для любых фиксированных параметров режима численные значения уровня информационной безопасности.

Доказанные оценки стойкости демонстрируют существенное увеличение уровня информационной безопасности по сравнению с базовыми режимами работы БСА за счет применения регулярного преобразования ключей, данный подход позволяет существенно повысить безопасность конечных систем. Однако с учетом нежелательных свойств преобразования CPKM, связанных как с замедлением реализаций, [6], так и с определенными свойствами безопасности, [10], в том числе, рассмотренными В.О. Миронкиным[81], для применения в современных протоколах защиты информации была актуальна задача синтеза нового усовершенствованного механизма.

В разделе 2.1 разработан новый механизм, а именно, расширенный режим работы БСА CTR-ACPKM, [13]. Он содержит встроенное внутреннее преобразование ключей и предназначен для применения в условиях слабодоверенного окружения, в котором по частичной информации, получаемой нарушителем в процессе работы средства защиты информации, при превышении некоторого достижимого на практике порогового значения объема данных, допустимого для обработки на одном сессионном секрете, становится возможна компрометация сессионных секретов; в режиме отсутствует негативное свойство существования возможности получения нарушителем части ключа при событиях (пусть и достаточно редких) совпадения блоков гаммы с заданными константами.

Режим CTR-ACPKM принимает на вход ключ $K \in \{0,1\}^k$, вектор инициализации $IV \in \{0,1\}^{n/2}$ ($ctr = IV \| 0^{n/2}$) и открытый текст $P \in \{0,1\}^*$, возвращает $C \in \{0,1\}^{|P|}$. Режим CTR применяется для обработки секций $P^1, \ldots, P^l$ открытого текста P с помощью соответствующих секционных ключей. Механизм ACPKM порождает новый ключ секции K^{i+1} на базе предыдущего ключа секции K^i: $K^{i+1} = \text{ACPKM}(K^i) = \mathsf{msb}_k(E_{K^i}(D_1) \| \ldots \| E_{K^i}(D_s))$, где $msb_k(\cdot)$ — операция усечения до старших k бит, k — длина ключа, n — длина блока, $s = \lceil k/n \rceil$, $D_1, D_2, \ldots, D_s \in \{0,1\}^n$ — попарно различные константы, $(n/2)$-й справа бит каждой равен 1. На длину открытого текста накладывается ограничение сверху в $2^{n/2-1}$ блоков.

Данный режим анализируется в детально отражающей порядок функционирования режима в современных протоколах защиты данных TLS, IPsec и CMS математической модели IND-CPNA. Доказана оценка стойкости режима CTR-ACPKM (теорема 1 [13], теорема 1 [16]), явно выражающая уровень

R 34.10-94, GOST R 34.10-2001, and GOST R 34.11-94 algorithms", RFC 4357, 2007.

[81]Миронкин В.О. О некоторых вероятностных характеристиках алгоритма выработки ключа «CRYPTOPRO KEY MESHING». Проблемы информационной безопасности. Компьютерные системы. №4, 2015. С. 140–146.

информационной безопасности преобразования, которое применяет данный режим совместно с некоторым БСА E, через стойкость этого алгоритма в модели PRP-CPA. Полученные результаты показывают, что в предположении стойкости используемого БСА свойства безопасности режима CTR-ACPKM существенно улучшены (квадратичным образом относительно числа секций) по сравнению со свойствами базового режима CTR во всех практически интересных случаях.

Таким образом, разработан новый математический аппарат, позволяющий оценивать стойкость механизмов внутреннего преобразования ключей. Доказанные с применением данного аппарата оценки уровня информационной безопасности позволили разработанному механизму CTR-ACPKM стать стандартизированным как в России[82], так и на международном уровне, войдя в международный стандарт ISO[83], определяющий режимы работы БСА (разработанный и происследованный режим стал шестым стандартизированным на международном уровне, в ряду с разработанными более 30 лет назад классическими режимами ECB (простой замены), CTR (гаммирования), CFB (гаммирования с обратной связью по шифртексту), CBC (простой замены с зацеплением), OFB (гаммирования с обратной связью по выходу), а также в определяющем рекомендации для работы сети Интернет сообществе IETF/IRTF[84]. Кроме того, режим CTR-ACPKM стал основой для протокольных решений, [32], стандартизированных в России[85,86] и применяемых на практике для защиты информации в массовых системах.

Важным сценарием применения программных средств защиты информации массового использования, не допускающих жесткой фиксации программного и аппаратного окружения, в котором предполагается функционирование средств защиты информации, является клиент-серверное взаимодействие (например, в рамках протокола TLS[87,88]). В разделе 2.2 исследуется семейство механизмов VKO, предназначенных для противодействия атакам на используемые в процедурах выработки общих секретных параметров долговременные ключи x и y при функционировании в случаях слабодоверенного окружения. Эти механизмы предполагают вычисление общих секретных парамет-

[82]Рекомендации по стандартизации Р 1323565.1.017–2018 «Информационная технология. Криптографическая защита информации. Криптографические алгоритмы, сопутствующие применению алгоритмов блочного шифрования», Москва, Стандартинформ, 2018.

[83]ISO/IEC 10116:2017/AMD 1:2021 Information technology — Security techniques — Modes of operation for an n-bit block cipher — Amendment 1: CTR-ACPKM mode of operation. ISO/IEC JTC 1/SC 27 Information security, cybersecurity and privacy protection, 2021.

[84]Smyshlyaev S. (Ed.), "Re-keying Mechanisms for Symmetric Keys", RFC 8645, 2019.

[85]Рекомендации по стандартизации Р 1323565.1.025–2019 «Информационная технология. Криптографическая защита информации. Форматы сообщений, защищенных криптографическими методами», Москва, Стандартинформ, 2019.

[86]Рекомендации по стандартизации Р 1323565.1.020-2020 «Информационная технология. Криптографическая защита информации. Использование российских криптографических алгоритмов в протоколе безопасности транспортного уровня (TLS 1.2)», Москва, Стандартинформ, 2020.

[87]Dierks T., Allen C., "The TLS Protocol Version 1.0", RFC 2246, 1999.

[88]Rescorla E., "The Transport Layer Security (TLS) Protocol Version 1.3", RFC 8446, 2018.

ров на базе процедуры Диффи-Хеллмана[89] с применением умножения на рандомизирующие множители UKM и использованием функций хэширования: $\mathrm{VKO}(x, y, UKM) = H\left(\left(\frac{m}{q} \cdot (UKM \cdot x \mod q)\right) \cdot (yP)\right)$, где m — порядок используемой группы точек эллиптической кривой, а P — порождающий элемент ее подгруппы простого порядка q.

Методы рандомизации множителей при вычислении ключей согласования, использованные в механизме VKO, исследованы в двух семействах математических моделей, соответствующих практическим условиям функционирования в рамках протокольных решений: моделях, в которых нарушитель стремится по открытым данным и выработанному ключу получить информацию об используемых долговременных ключах, а также моделях, целью нарушителя в которых является нахождение вырабатываемого ключа, зная открытые данные и, опционально, некоторую дополнительную информацию о нем. Параметризация моделей с помощью функций, определяющих вид частичной информации, позволяет рассматривать элементы конкретных моделей нарушителя для итоговых протоколов (например, относительно пассивного нарушителя, имеющего только доступ к каналу связи) в виде частных случаев.

Доказанные утверждения (теоремы 5.5 и 5.6 [8]) позволяют сделать выводы о стойкости механизмов VKO в рассматриваемых семействах моделей в предположении стойкости применяемых функций хэширования и эллиптических кривых. Они явным образом связывают стойкость VKO в первом семействе моделей с задачей получения информации о долговременных ключах при заданном распределении $\mathcal{D}$ параметра UKM по известным открытым ключам, ключу обмена и вспомогательной информации, а стойкость во втором семействе моделей — со сложностью решения распознавательной задачи Диффи–Хеллмана в применяемой группе точек эллиптической кривой.

При этом VKO является базовым механизмом, а выводы его самостоятельного анализа необходимо развивать при исследовании каждого итогового протокола, такого, например, как рассматриваемый в третьей главе применяющий его протокол SESPAKE: при этом, в дополнение к свойствам VKO необходимо учитывать характеристики ключевой системы (в частности, такие аспекты, как применение эфемерных или долговременных ключей для выработки ключа обмена), а при анализе итогового протокола пользоваться полученными оценками при конкретных значениях функций, определяющих вид частичной информации.

Рассмотрен вопрос о результирующей безопасности процедур выработки общих параметров VKO в случаях наличия ошибок или сбоев в реализациях для эллиптических кривых составного порядка, в частности, скрученных кривых Эдвардса ([12,24]), а также отсутствия гарантий константного времени вычисления кратных точек. Умножение на рандомизирующие множители в условиях реализации с ошибками может приводить к тому, что малозначимые на практи-

[89]Diffie W., Hellman M. New Directions in Cryptography // IEEE Transactions on Information Theory. November 1976. 22 (6): 644–654.

ке атаки, позволявшие сокращать перебор долговременного секрета всего лишь в 2–4 раза, потенциально могут превращаться в применимые на практике для полного восстановления долговременных секретов. Описаны ([21]) общие сценарии для проведения таких усиленных атак на реализации протоколов TLS и CMS в случае ошибок в реализации.

Таким образом, показано, что положительные свойства данных механизмов, крайне желательные для использования в предназначенных для работы в слабодоверенном окружении средствах защиты информации, неразрывно связаны с существенным повышением критичности последствий уязвимостей при реализации для результирующей безопасности. Рандомизирующие множители позволяют «размывать» влияние секретных величин на значения, которые нарушитель может перехватывать по побочным каналам, предотвращая атаки, требующие накопления существенной статистики для уменьшения перебора секретных величин. Однако одновременно с этим могут становиться опаснее методы атак, предполагающие получение информации о секретных величинах по одному значению, без необходимости накопления. Следовательно, обратной стороной методов обеспечения безопасности в слабодоверенном окружении может становиться абсолютная недопустимость ошибок реализации программной части, защитные механизмы при ошибках разработки превращаются в оружие против самих защищаемых объектов.

По итогам исследований, проведенных в настоящей диссертации, механизм VKO стандартизирован в Российской Федерации[90], кроме того, на его основе разработаны и стандартизированы высокоуровневые протокольные решения[91,92,93]), в частности, именно с применением данного механизма производится выработка общих параметров в российских механизмах протокола TLS 1.2[94] — основных на текущий момент механизмах обеспечения конфиденциальности в российском сегменте сети Интернет с применением отечественных алгоритмов.

Разработанные в диссертации методы, позволяющие получать в описанных моделях нарушителя для индивидуальных параметров механизма обоснованные числовые значения уровня информационной безопасности, позже позволили Е.К. Алексееву, Г.А. Карпунину, Д.А. Мошниной и В.Д. Николаеву провести

[90]Рекомендации по стандартизации Р 50.1.113–2016 «Информационная технология. Криптографическая защита информации. Криптографические алгоритмы, сопутствующие применению алгоритмов электронной цифровой подписи и функции хэширования», Москва, Стандартинформ, 2016.

[91]Рекомендации по стандартизации Р 1323565.1.025–2019 «Информационная технология. Криптографическая защита информации. Форматы сообщений, защищенных криптографическими методами», Москва, Стандартинформ, 2019.

[92]Методические рекомендации МР 26.2.001-2013, «Использование наборов алгоритмов шифрования на основе ГОСТ 28147-89 для протокола безопасности транспортного уровня (TLS)», Москва, Технический комитет по стандартизации «Криптографическая защита информации», 2013.

[93]Методические рекомендации МР 26.2.002-2013 «Использование алгоритмов ГОСТ 28147-89, ГОСТ Р 34.10 и ГОСТ Р 34.11 в криптографических сообщениях формата CMS», Москва, Технический комитет по стандартизации «Криптографическая защита информации», 2013.

[94]Рекомендации по стандартизации Р 1323565.1.020-2020 «Информационная технология. Криптографическая защита информации. Использование российских криптографических алгоритмов в протоколе безопасности транспортного уровня (TLS 1.2)», Москва, Стандартинформ, 2020.

анализ стойкости подсистемы защиты PIN-кода при его проверке в отсутствие доступа к сети для платежной системы «МИР» и определить допустимые параметры безопасного функционирования системы в рамках работ по стандартизации порядка применения механизмов защиты информации при проверке PIN-кодов[95].

При проектировании и реализации программных средств электронной подписи, предполагающих хранение ключей на отчуждаемых ключевых носителях, неминуемо возникает задача нахождения баланса между преимуществами переноса реализации части операций на аппаратные средства самого ключевого носителя и преимуществами вычислений программным образом. Дополнительные угрозы безопасности возникают в случае применения потенциально уязвимых вычислительных модулей. Вопросам обеспечения безопасности в таких случаях посвящен раздел 2.3 (в общем случае также возникает задача защиты канала связи между взаимодействующими при вычислении подписи аппаратными компонентами — эта задача решается в третьей главе диссертации).

Даже если рабочие места надежно защищены техническими методами или вовсе изолированы от сети, не допуская появления классических условий для построения модулями нарушителя скрытых каналов (см., в первую очередь, работы А.А. Грушо, Н.А. Грушо и Е.Е. Тимониной[96,97,98]), сохраняется угроза компрометации информации о долговременных ключах потенциально уязвимыми аппаратными компонентами посредством самих значений подписи. Речь идет о постановке задачи, возникающей на практике при применении вычислительных компонент, которые оснащены высоким уровнем инженерной защиты носителя, но имеют потенциальные уязвимости в реализациях вычислений — в худшем случае, произведены компанией, потенциально заинтересованной в незаметной компрометации хранимых ключей пользователей.

В настоящей диссертации применительно к ключевым носителям рассматривается постановка задачи по защите от использования нарушителем самих значений подписи для недетектируемой передачи информации о ключах: задача защиты от утечек по техническим каналам в случае средств электронной подписи, способных работать автономно, может быть решена полной изоляцией системы, но от сбора нарушителем значений подписи она не защитит (уместно привести пример практической атаки на реализации RSA путем сбора значений подписи из открытых источников[99]). С учетом свойств схем электронной подписи семейства Эль-Гамаля (к которому относится и российский стандарт

[95]Рекомендации по стандартизации Р 1323565.1.011–2017 «Информационная технология. Криптографическая защита информации. Использование алгоритмов согласования ключа и блочного шифрования при офлайновой проверке PIN», Москва, Стандартинформ, 2017.

[96]Грушо А.А. Скрытые каналы и безопасность информации в компьютерных системах // Дискретная математика, 10:1, 1998. С. 3–9.

[97]Грушо А.А. О существовании скрытых каналов // Дискретная математика, 11:1, 1999. С. 24–28

[98]Грушо А.А., Тимонина Е.Е. Оценка времени, требуемого для организации скрытого канала // Дискретная математика, 15:2, 2003. С. 40–46

[99]Lenstra A.K., Hughes J.P., Augier M., Bos J.W., Kleinjung T., Wachter C. Ron was wrong, Whit is right // Cryptology ePrint Archive: Report 2012/064, 2012.

подписи[100], исследования стойкости для которого в общем случае проводились Н.П. Варновским[101]), для скрытой передачи информации о долговременном ключе достаточно детерминированным образом (или в соответствии с распределением, обладающим малой энтропией), известным нарушителю, получающему позже значение подписи, выбрать значение разового секрета в момент формирования подписи. Данный тип атаки может быть актуален даже в случае полностью изолированной системы, такой, например, как изолированный от внешних сетей удостоверяющий центр.

С учетом жизненного цикла ключевого носителя описаны два вида нарушителя: внешний нарушитель и «нарушитель с агентом», перечислены их возможности, а затем для каждого из них формально определена математическая модель, подробно описывающая возможности нарушителя на стороне производителя системного программного обеспечения ключевых носителей.

Разработан протокол uSign, обеспечивающий безопасность процессов формирования электронной подписи в указанных условиях. Ключевым элементом протокола является интеграция в процесс формирования подписи доказательства с нулевым разглашением, основанного на принципах схемы К. Шнорра[102], который используется для подтверждения использования значения разового секрета, выбранного случайно в соответствии с равномерным распределением. Применение этого протокола между компонентами, участвующими в процессе вычисления подписи (аппаратные компоненты, устанавливаемый апплет, а также программный провайдер, функционирующий на стороне основного вычислительного устройства), направлено на защиту итоговой реализации схемы подписи от злонамеренных действий со стороны аппаратных компонент.

Стойкость разработанного протокола доказана в описанной модели, а именно, доказаны основные утверждения раздела (теоремы 1 и 2 [20]), обосновывающие стойкость разработанного метода реализации электронной подписи. Обоснованы соотношения, связывающие уровень информационной безопасности такой реализации относительно нарушителя с агентом (внешний нарушитель и модуль в ключевом носителе) со стойкостью базовой схемы подписи относительно построения экзистенциальной подделки, а также стойкость относительно классического внешнего по отношению к вычислительному устройству нарушителя. Таким образом, разработан метод, который позволяет получать численные значения уровня информационной безопасности конкретных реализаций для любых заданных параметров системы и предположений о вычислительных ресурсах нарушителей.

Таким образом, разработана новая схема взаимодействия компонент средств защиты информации с ключевыми носителями, при которой долговременные ключи не покидают защищенную память устройства, но при этом производи-

[100]ГОСТ Р 34.10–2012, «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи», Москва, Стандартинформ, 2012.

[101]Варновский Н.П. Стойкость схем электронной подписи в модели с защищенным модулем // Дискретная математика, 20:3, 2008. С. 147–159.

[102]Schnorr C. P. Efficient identification and signatures for smart cards // Conference on the Theory and Application of Cryptology. Springer, New York, NY, 1989. С. 239-252.

тель аппаратных компонент не имеет возможности с применением намеренно заложенных и не детектируемых по внешнему поведению устройства уязвимостей получить информацию о долговременном ключе. Для реализаций, выполненных по данной схеме, обоснован метод получения оценок уровня информационной безопасности.

В третьей главе решаются задачи анализа безопасности механизмов и протоколов, которые используются для обеспечения защищенного доступа к средствам защиты информации, хранящим долговременные секретные значения и выполняющим основные операции с ними, в условиях как слабодоверенной среды функционирования программных компонент защиты информации, используемых пользователем для аутентифицированного доступа, так и невозможности применения пользователями для защиты таких взаимодействий хранимых секретов достаточной длины.

Вопросы анализа некоторых механизмов и протоколов, применимых для обеспечения защищенного удаленного доступа, ранее рассматривались в работах М. Белларе[103], Ф. Рогавея[104], Р. Канетти[105], Д. Пуаншваля[106], Х. Кравчика[107], А.В. Черемушкина[108] и др.

В разделе 3.1 исследуются механизмы, предназначенные для решения задачи реализации аутентифицированных обращений пользователей к серверным средствам с применением существенно ограниченных по ресурсам клиентских компонент: без хранимых данных для аутентификации или без возможности применения механизмов с применением операций в группах точек эллиптических кривых и случайных чисел.

В первой части раздела рассматриваются используемые в платежных системах процедуры работы с проверочными значениями банковских карт и PIN-кодами (CVV и PVV), применяемые для получения владельцами карт доступа к операциям со своими счетами (совершаемыми на серверной стороне) по запоминаемому секрету малой длины. Разрабатывается механизм, альтернативный применяемой в зарубежных системах функции двухпроходной децимализации[109], распределение вероятностей на множестве выходов которого существенно ближе к равномерному, чем для исходной функции, с его помощью строятся

[103]Bellare M., Rogaway P. Entity Authentication and Key Distribution // Lecture Notes in Computer Science, vol. 773, 1994. Pp. 232–249.

[104]Bellare M., Pointcheval D., Rogaway P. Authenticated key exchange secure against dictionary attacks. Lecture Notes in Computer Science, vol. 1807, 2000. Pp. 139–155.

[105]Bellare M., Canetti R., Krawczyk H. A modular approach to the design and analysis of authentication and key exchange protocols (extended abstract) // In 30th Annual ACM Symposium on Theory of Computing, 1998. Pp. 419–428.

[106]Fouque P. A., Pointcheval D., Zimmer S. HMAC is a randomness extractor and applications to TLS // Proceedings of the 2008 ACM symposium on Information, computer and communications security, 2008. Pp. 21–32.

[107]Bellare M., Canetti R., Krawczyk H. Keyed Hash Functions and Message Authentication // Proceedings of Crypto'96, Springer. 1996. Pp. 1–15.

[108]Черемушкин А.В. Криптографические протоколы: основные свойства и уязвимости // Прикладная дискретная математика, 2009, приложение к № 2. С. 115–150.

[109]Application Programmer's Guide, Appendix F. Cryptographic Algorithms and Processes, PIN Formats and Algorithms, VISA PIN Algorithms // IBM Knowledge Center, 2011.

новые процедуры работы с CVV и PVV.

Описаны три модели нарушителя, стремящегося нарушить безопасность указанных процедур в платежной системе:

- Поиск корректного значения CVV (выводимого для конкретной банковской карты из основного ключа CVK) для некоторой целевой карты.
- Поиск корректной пары (PIN, PVV) для некоторой целевой карты.
- Поиск корректного значения PIN для некоторой целевой карты при известном PVV.

На основе результатов о свойствах разработанной функции децимализации (леммы 8.3, 8.4, 8.5 [11]) обоснованы оценки стойкости (теоремы 8.6 и 8.7 [11]) процедур генерации параметров CVV и PVV по отношению к угрозе отличения от случайной функции и угрозе подделки проверочного параметра, а также показано, как полученные оценки для конкретных примитивов позволяют получать численные значения уровня информационной безопасности.

Доказано утверждение (теорема 8.8 [11]), предоставляющее оценки стойкости рассматриваемых функций по отношению к угрозе восстановления значения PIN. Установлено, что при применении разработанных функций вероятность осуществления подделки нарушителем, который может получить не более 10^7 значений CVV и PVV (данные значения являются характерными для одного сегмента платежной системы), незначительно отличается от априорной вероятности угадывания, а также обоснована стойкость по отношению к угрозе восстановления PIN (вероятность ее осуществления нарушителем с ограниченными типичным образом возможностями незначительно отличается от априорной).

Таким образом, доказанные оценки для разработанных вариантов процедур работы с проверочными значениями банковских карт и PIN-кодами CVV/PVV, в отличие от применяемых в зарубежных системах Visa/Mastercard функций, позволяют сделать положительные выводы о стойкости при актуальных на практике значениях параметров систем. Разработанные варианты процедур работы с проверочными значениями банковских карт и PIN-кодами стандартизированы[110] и рекомендованы для применения в российской платежной системе «МИР».

Одним из основных сценариев работы массовых пользователей со средствами защиты информации при эксплуатации систем электронного документооборота является формирование электронной подписи. С учетом переноса существенной части взаимодействий пользователя на мобильные устройства важнейшей задачей является разработка решений, как позволяющих пользователю безопасно работать с электронными документами в системах документооборота и подписывать их без риска компрометации своего долговременного секрета, так и учитывающих возможность утери или поломки устройства. Безопасная

[110]Рекомендации по стандартизации Р 1323565.1.007–2017 «Информационная технология. Криптографическая защита информации. Использование алгоритмов блочного шифрования при формировании проверочного параметра платежной карты и проверочного значения PIN», Москва, Стандартинформ, 2017.

реализация процедур вычисления электронной подписи непосредственно на мобильном устройстве может быть существенно затруднена, проблемы вытекают из повышенных требований к ресурсам любых безопасных алгоритмов, применяемых в данной области.

Одним из подходов к решению данной задачи, учитывающим особенности мобильных устройств как обладающих слабодоверенным окружением, является разработка систем дистанционного формирования электронной подписи (см. [25]). Аутентификация и подтверждение операций в таких системах может осуществляться посредством не требующих доверенных датчиков случайных чисел механизмов PRFGOST и KDFTREE на основе HMAC_GOSTR3411_2012_256[111].

С целью получить оценки уровня информационной безопасности для механизмов PRFGOST и KDFTREE доказана теорема 5.4 [8], предоставляющая оценки преобладания нарушителя, стремящегося отличить данные функции от случайно равновероятно выбранных функций.

По результатам проведенных исследований семейств механизмов PRFGOST и KDFTREE они были стандартизированы в Российской Федерации[112], вошли в RFC 7836. Разработанные в диссертации методы, позволяющие получать для индивидуальных параметров схем обоснованные численные значения уровня информационной безопасности, позже позволили Е.К. Алексееву, И.Б. Ошкину и В.Д. Николаеву провести анализ стойкости подсистем выработки ключей в процессах персонализации и процессинга платежной системы «МИР» и определить допустимые параметры безопасного функционирования данных подсистем в рамках работ по стандартизации порядка использования функции диверсификации для формирования производных ключей платежного приложения[113].

С целью решения задач по доверенной доставке программных средств защиты информации по каналам связи и по обеспечению их поэкземплярного учета, без необходимости синтеза, анализа и внедрения специализированных эллиптических кривых для каждого требуемого на практике набора параметров безопасности, в разделе 3.2 исследованы вопросы анализа методов построения механизмов электронной подписи с уменьшенной длиной выхода.

При рассмотрении задачи обеспечения безопасности указанных процессов в условиях возможности получения нарушителем экземпляра средства защиты информации и его декомпиляции (то есть в реальных условиях) любой механизм, опирающийся на зафиксированные в самом коде программного средства ключи, не является безопасным: нарушитель может извлечь этот секрет путем

[111] Smyshlyaev S. (Ed.), Alekseev E., Oshkin I., Popov V., Leontiev S., Podobaev V., Belyavsky D., "Guidelines on the Cryptographic Algorithms to Accompany the Usage of Standards GOST R 34.10-2012 and GOST R 34.11-2012", RFC 7836, 2016.

[112] Рекомендации по стандартизации Р 50.1.113–2016 «Информационная технология. Криптографическая защита информации. Криптографические алгоритмы, сопутствующие применению алгоритмов электронной цифровой подписи и функции хэширования», Москва, Стандартинформ, 2016.

[113] Рекомендации по стандартизации Р 1323565.1.010–2017 «Информационная технология. Криптографическая защита информации. Использование функции диверсификации для формирования производных ключей платежного приложения», Москва, Стандартинформ, 2017.

декомпиляции и создать генератор поддельных лицензионных номеров (так называемый «keygen»). Разумным методом защиты является использование схем, предполагающих проверку лицензионного номера с использованием открытого ключа, то есть схем электронной подписи. Безусловно, похитить некоторый конкретный лицензионный ключ нарушитель по-прежнему сможет, но не сможет сгенерировать его сам, а с единичными украденными номерами нетрудно бороться явной их блокировкой в обновленных версиях программных средств. Тем не менее, при таком подходе возникает естественное требование существенно сократить размер проверочной информации, ведь вводить его пользователю в общем случае придется вручную.

С учетом особенностей указанной области применения выделяются специфичные требования к реализациям схем подписи для решения данной задачи. В отличие, например, от задач обеспечения безопасности электронного документооборота, существенный «запас прочности» в части единичной подделки лицензионного номера в данном случае, как указано выше, не требуется, а уровень защиты может задаваться каждый раз для очередной версии программного продукта с учетом актуальных предположений о вычислительных ресурсах потенциального нарушителя. При этом, безусловно, синтез для каждого значения уровня стойкости своего набора параметров (например, эллиптических кривых) и отдельной реализации в программном средстве защиты информации недопустим: параметры схем подписи вводятся в действие на основании глубоких обоснований в результате исследований (в том числе, для стандартизированных в России эллиптических кривых, [12]). С другой стороны, в рассматриваемой задаче, с учетом ручного ввода, вполне возможно допустить определенное увеличение трудоемкости проверки, а с учетом возможности заблаговременной генерации значений лицензионных номеров на стороне разработчика — и увеличение трудоемкости формирования значений подписи.

Использование функции хэширования для уменьшения длины выхода подписи упоминалось Ю. Женгом[114], но при этом предполагалось применение хэширования совместно сообщения и первого из компонентов подписи, а уменьшение длины выхода подписи было возможно только в случае применения для обработки сообщений функций хэширования с более коротким выходом, чем предполагалось параметрами самой схемы подписи. Кроме того, Ю. Женгом для оценок стойкости были представлены только асимптотики, а не методы получения численных значений стойкости. В 2016 году М. Мохамедом и А. Петзольдтом[115] была предложена частная конструкция схемы подписи с уменьшенной длиной выхода, однако имела сравнительно большой размер ключа (около 100 КБ) и существенное время проверки, что делает ее неприменимой для рассматриваемой задачи. Для ряда ранее построенных схем, основанных на скры-

[114]Zheng Y. Digital signcryption or how to achieve cost (signature & encryption) $\ll$ cost(signature) + cost(encryption) // Lecture Notes in Computer Science, Vol. 1294, Advances in Cryptology — CRYPTO'97, 1997.

[115]Mohamed M.S.E., Petzoldt A. The Shortest Signatures Ever // Lecture Notes in Computer Science, Vol. 10095, Progress in Cryptology, INDOCRYPT 2016, 2016.

тых отображениях полей (Hidden Field Equations[116]) и позволявших получать сравнительно короткие выходные значения, в работах В. Дюбуа, А. Шамира[117], Н. Куртуа[118] и др., были построены эффективные методы снижения стойкости.

В разделе 3.2 рассматриваются три подхода к построению механизмов электронной подписи с уменьшенной длиной выхода на основе модификации схем семейства Эль-Гамаля. Влияние применения рассматриваемых методов на уровень стойкости исследуется в отражающей практические условия модели SUF-CMA: описаны и обоснованы математические методы получения оценок уровня информационной безопасности результирующих схем электронной подписи. Первый метод меняет внутреннюю структуру схемы подписи. Установлено, что трудноразрешимость задачи дискретного логарифмирования и стандартные предположения о безопасности функции хэширования достаточны для безопасности модифицированной схемы в модели SUF-CMA, путем построения последовательности промежуточных вспомогательных моделей и вычисления оценок разностей вероятностей успехов нарушителей при решении соответствующих задач с применением ряда вспомогательных утверждений установлены соотношения для оценок стойкости модифицированной схемы (теорема 1 [18]). Второй и третий методы рассмотрены путем сведения задачи анализа исходной схемы к соответствующим задачам для модифицированных схем: получены соотношения (теоремы 2, 3 [18]) для оценок стойкости схем, модифицированных с помощью второго и третьего методов.

В итоге, исследованы производные схемы электронной подписи, получаемые из произвольной стойкой схемы подписи Эль-Гамаля с помощью трех методов, предполагающих модификацию соответствующих элементов схемы. Для каждого из трех методов полученные оценки позволяют получать конкретные численные значения уровня информационной безопасности законченной реализации модифицированной схемы подписи, что необходимо для практического решения поставленной задачи без необходимости проведения дополнительных исследований.

Отметим, что исследуемые методы не предполагают уменьшение размера ключа (он остается тем же, что и в исходной схеме подписи) или снижение стойкости схем по отношению к угрозе восстановления ключа: это важно для возможности применять один и тот же ключ для разных версий, постепенно увеличивая параметры стойкости применяемой модифицированной схемы по мере необходимости.

Полученные результаты позволяют применять в средствах защиты информации вспомогательные механизмы электронной подписи для сопутствующих задач, осуществляя выбор параметров безопасности без необходимости дополнительных исследований получаемых модифицированных схем.

---

[116]Маховенко Е.Б., Сюсюгина Н.Г. Анализ криптосистем на скрытых отображениях полей нечетных характеристик // Безопасность информационных технологий, т. 17, № 1, 2010.

[117]Dubois V., Fouque PA., Shamir A., Stern J. Practical Cryptanalysis of SFLASH // Lecture Notes in Computer Science, Vol. 4622, Advances in Cryptology - CRYPTO 2007, 2007.

[118]Courtois N.T., Daum M., Felke P. On the Security of HFE, HFEv- and Quartz // Lecture Notes in Computer Science, Vol. 2567, Public Key Cryptography, PKC 2003, 2003.

Вопросы работы с аппаратными носителями, используемыми для хранения долговременных ключей в неизвлекаемом виде, являются одними из важнейших для безопасности средств защиты информации, в том числе, при их использовании для реализации двухфакторной аутентификации совместно со средствами разграничения доступа. Для реализации второго фактора аутентификации (в соответствии с методологией, разработанной А.Г. Сабановым[119,120,121], а также с учетом действующих в России требований по информационной безопасности[122]), при доступе к носителю необходимо аутентифицировать самого пользователя — и это необходимо делать с использованием низкоэнтропийных секретов (паролей). При этом необходимо иметь в виду актуальные для современных сценариев работы с пользовательскими устройствами, [26], проблемы с доверием к окружению: средства пользователей могут как использоваться удаленно (доступ к хранимому секрету осуществляется при этом по каналу связи), так и применяться совместно с бесконтактными считывателями с передачей команд по воздуху (Bluetooth, NFC, Wi-Fi) — то есть по заведомо доступному нарушителю для перехвата каналу. Таким образом, актуальной является задача обращения к носителям по контролируемому нарушителем каналу, причем с проведением аутентификации только по низкоэнтропийному секрету. Результаты раздела 3.3 обеспечивают исчерпывающее решение этой задачи.

В разделе 3.3 разработан двухэтапный протокол SESPAKE, который позволяет провести взаимную аутентификацию программного средства защиты информации и ключевого носителя с выработкой общего сессионного секрета. При использовании SESPAKE в канале связи между ключевым носителем и прикладной системой не оказывается ни ключевой информации, ни иной чувствительной информации, а при аутентификации в канале происходит обмен одноразовыми случайными величинами: воспроизведение или модификация активным нарушителем передаваемых сообщений не влияет на безопасность. При использовании данного протокола в канале связи между ключевым носителем и программным средством защиты не появляется (даже при активном вмешательстве нарушителя в канал) информация, предоставляющая нарушителю критерии для перебора паролей.

Перед синтезом и анализом данного протокола в разделе 3.3 на основе рассмотрения как модельных, так и реально существующих протоколов, схожих по принципам построения, выделены необходимые условия обеспечения стойкости, [9]. С учетом выделенных необходимых условий определены основные принципы и конструктивные особенности разрабатываемого протокола SESPAKE.

---

[119]Сабанов А.Г. Аутентификация как часть единого пространства доверия // Электросвязь, №8, 2012. С. 40–44.

[120]Сабанов А.Г. Уровни доверия к аутентификаторам // Вопросы защиты информации, №2. 2019. С. 10–17.

[121]Сабанов А.Г. Методология формирования иерархии доверия к результатам идентификации и аутентификации субъектов доступа. Диссертация на соискание степени доктора технических наук. 2020.

[122]Рекомендации по стандартизации Р 1323565.1.012-2017 «Информационная технология. Криптографическая защита информации. Принципы разработки и модернизации шифровальных (криптографических) средств защиты информации», Москва, Стандартинформ, 2017.

Протокол SESPAKE содержит в качестве неотъемлемых элементов этап подтверждения согласованного сессионного секрета и встроенные механизмы контроля попыток перебора пароля. Для протоколов без этапа подтверждения[123] и для некоторых протоколов, содержащих варианты этого этапа[124], ранее существовали частичные результаты о стойкости, но она доказывалась лишь относительно угрозы отличения выработанного секрета от случайной строки, а для протоколов с этапом подтверждения ключа модель нарушителя с такой угрозой является вырожденной: в случаях, когда на этапе подтверждения применяется сам выработанный ключ, у нарушителя априори появляется критерий отличения целевой строки от случайной. Эта проблема гипотетически может решаться искусственным образом путем введения дополнительного «ветвления» ключей, но при этом строится малоприменимый на практике протокол. Данный прием, позволявший получать результаты о стойкости, приводил к появлению существенных различий между стойкостью в теоретической модели и реальной безопасностью используемого протокола (важность получения численных оценок вероятности ложной аутентификации для законченных средств защиты информации подчеркивалось, например, А.П. Барановым[125]). В SESPAKE на втором этапе используется непосредственно сам выработанный на первом этапе ключ, а для анализа предложена существенно более точная детализированная модель на основе неотличимости с угрозой ложной аутентификации.

Получение обоснованных оценок стойкости SESPAKE делится на три этапа, на первом из которых частично применяются идеи работы М. Абдаллы и П. Пуаншваля[126] (при этом ряд утверждений в указанной работе требовал существенной переработки, так как в них не учитывались важные особые случаи — соответствующие замечания приведены в рамках представленных в настоящей диссертации доказательств), а второй и третий этапы являются полностью оригинальными, в рамках которых строится расширение BPR-модели с целью разработки метода проведения анализа полного самодостаточного протокола с явным подтверждением ключа и встроенными механизмами защиты от активного нарушителя. Разработанный подход оказывается полезным при анализе и обосновании стойкости иных современных протоколов аутентифицированной выработки общих ключей на основе низкоэнтропийных данных, таких как применяемые в семействе протоколов Wi-Fi[127].

Доказаны (теоремы 2, 3 [14]) соотношения между промежуточными моделями нарушителя, требуемыми для обоснования общей оценки для первого этапа протокола (теоремы 4, 5 [14]).

---

[123]Michel Abdalla. Reducing The Need For Trusted Parties In Cryptography. Cryptography and Security. Ecole Normale Superieure de Paris - ENS Paris, 2011.

[124]Boyko V., MacKenzie P., Patel S. Provably secure password authenticated and key exchange using Diffie-Hellman // Lecture Notes in Computer Science, vol. 1807, 2000. Pp. 156-171.

[125]Баранов А.П., Баранов П.А. Госключ — успех или катастрофа // Материалы PKI-Форума 2021.

[126]Abdalla M., Pointcheval D. Simple Password-Based Encrypted Key Exchange Protocols // Lecture Notes in Computer Science, vol. 3376, 2005. Pp. 191-208.

[127]Vanhoef M., Ronen E. Dragonblood: Analyzing the Dragonfly Handshake of WPA3 and EAP-pwd // Proceedings of the Symposium on Security & Privacy (SP). IEEE, 2020.

Далее с помощью такого приема, как введение промежуточной модели нарушителя «с предупреждением» с получением ряда оценок в этой модели (теоремы 6, 7, 8 [14]), удается перейти к оценке стойкости всего протокола SESPAKE в целевой расширенной BPR-модели. Доказано утверждение теоремы 9 [14], определяющее метод получения обоснованных численных оценок уровня информационной безопасности реализаций протокола с учетом конкретной используемой группы точек эллиптической кривой, функции хэширования и предположений о вычислительных ресурсах нарушителей.

Таким образом, разработан математический аппарат, применимый для получения оценок уровня информационной безопасности самодостаточных протоколов установления защищенного соединения с аутентификацией на основе низкоэнтропийных данных: с явным подтверждением выводимых ключей и защитой от перебора активным нарушителем.

Разработанный и обоснованный протокол SESPAKE, по результатам исследований, представленных в настоящей диссертации, был стандартизирован[128], вошел в RFC 8133 и применяется в Российской Федерации, в частности, в паспортах с электронным носителем[129,130,131], планируемых к массовой выдаче вместо существующих паспортов.

В заключении перечислены основные результаты диссертации.

В приложении содержатся доказательства вспомогательных технических утверждений.

ЗАКЛЮЧЕНИЕ

В диссертации поставлена и решается проблема разработки, анализа и обоснования методов обеспечения безопасности массовых программных средств защиты информации в условиях ограниченного доверия к среде функционирования (слабодоверенного окружения). Проведен всесторонний анализ аспектов слабодоверенного окружения, актуальных для рассмотрения в отношении программных средств защиты информации, предназначенных для работы с электронной подписью, а также для обеспечения защиты передаваемых и хранимых пользовательских данных. Для каждого из таких аспектов разработаны методы построения механизмов защиты информации, для которых в математических моделях, отражающих все их практически значимые особенности, проведен подробный анализ и доказаны утверждения о свойствах безопасности данных механизмов. Таким образом, с учетом актуальных угроз, возникающих при обеспечении информационной безопасности функционирования программного

[128]Рекомендации по стандартизации Р 50.1.115–2016 «Информационная технология. Криптографическая защита информации. Протокол выработки общего ключа с аутентификацией на основе пароля», Москва, Стандартинформ, 2016.

[129]Вдовина М.С. Внедрение электронного паспорта в Российской Федерации // Материалы PKI-Форума 2019.

[130]Пьянченко А.А. Перспективные планы по развитию института усиленной электронной подписи для взаимодействия граждан и государства // Материалы РусКрипто‘2021, 2021

[131]Пьянченко А.А. О реализации мероприятий по переходу на отечественную криптографию между государством и обществом // Материалы PKI-Форума 2021.

средства защиты информации в условиях слабодоверенного окружения, разработаны математические методы обеспечения достаточного уровня информационной безопасности, а также методы получения обоснованных оценок уровня информационной безопасности применяющих их конечных средств, успешно решая рассматриваемую важную проблему.

Решение этой проблемы существенным образом влияет на уровень обоснованности оценок информационной безопасности в конкретных информационных системах (в том числе, системах электронного документооборота) и на развитие принципов создания программных средств защиты информации.

Основные результаты диссертации состоят в следующем.

1. Для булевых функций доказана Гипотеза Голича (1996 г.), имеющая важное значение для построения параметризованных вспомогательных кодирующих устройств на основе булевых функций и регистров сдвига, способных обеспечить необходимые статистические свойства последовательностей, вырабатываемых генераторами псевдослучайных последовательностей, как в штатных режимах, так и в условиях возможных сбоев. Доказана также справедливость аналога Гипотезы Голича для ряда классов k-значных функций с барьером в случае простых k. Кроме того, установлено, что для k-значных функций в случае составных k аналог Гипотезы Голича не выполняется.

2. Построен класс булевых функций, которые позволяют синтезировать кодирующие устройства, сохраняющие равновероятность m-грамм входных последовательностей, и при этом обладают свойствами спектральных коэффициентов, опровергающими ранее существовавшие (основавшиеся на результатах зарубежных исследователей) предположения. Впервые установлены условия для булевых функций, позволившие обеспечить для них наличие одновременно свойств совершенной уравновешенности и корреляционной иммунности (устойчивости). Для булевых функций, не являющихся линейными по своим крайним переменным и имеющих барьеры определенного вида, доказано наличие свойства 1-устойчивости. Эти результаты позволяют строить широкие классы совершенно уравновешенных булевых функций, обладающих одним из важнейших для задач защиты информации комбинаторным свойством корреляционной иммунности.

3. Разработан метод модификации схем электронной подписи семейства Эль-Гамаля (в частности, российского стандарта электронной подписи), предназначенный для использования в условиях слабодоверенного окружения, а именно в условиях потенциально деградирующих источников случайности. Построенный механизм сохраняет свойства схем и соответствие стандарту, а также возможность применения важных для защиты реализаций способов работы с ключами подписи, предполагающих применение случайных масок. В модели SUF-CMRA, отражающей наличие в системе нарушителя с возможностью влияния на источники случайности, путем сведéния между моделями нарушителя, предполагающей и не предполагающей влияние на источники случайности, обоснованы оценки уровня информационной безопасности модифицированных реализаций схем электронной подписи семейства Эль-Гамаля. Данные оценки

позволяют сделать вывод о достаточном уровне защищенности модифицированных реализаций в указанных условиях слабодоверенного окружения.

Разработан метод построения механизмов обеспечения информационной безопасности средств защиты информации, функционирующих в условиях потенциально уязвимых источников случайности, при наличии доступа к доверенным программно-аппаратным средствам, предназначенным для формирования электронной подписи. Доказана стойкость разработанной конструкции относительно наиболее сильного типа нарушителя, который может полностью контролировать источник случайности: в математической модели, путем построения последовательности промежуточных моделей безопасности и доказательства утверждений об оценках разностей между вероятностями успехов гипотетических нарушителей в соответствующих моделях, обоснована стойкость разработанного механизма и установлена его достаточность для обеспечения защиты информации в рассматриваемых условиях. По результатам проведенных исследований разработанный механизм был стандартизирован в IETF/IRTF в качестве RFC 8937.

4. Разработан метод получения оценок уровня информационной безопасности для механизмов регулярного преобразования сессионных ключей, предназначенных для применения при обработке данных большой длины с целью преодоления эксплуатационных ограничений, вытекающих из условий функционирования средств защиты информации в слабодоверенном окружении. Оценки стойкости для механизма CPKM, полученные в математических моделях, которые предполагают проведение анализа механизмов регулярного преобразования сессионных ключей в контексте расширенных режимов работы блочных симметричных алгоритмов обеспечения конфиденциальности методами теоретико-сложностных сведéний, позволили обосновать повышение уровня информационной безопасности результирующих процедур обработки данных с использованием механизма CPKM по сравнению с базовыми режимами.

5. Разработан новый расширенный режим работы блочных симметричных алгоритмов обеспечения конфиденциальности CTR-ACPKM, который предназначен для использования в средствах защиты информации, функционирующих в условиях потенциальной компрометации частичной информации о сессионных ключах. Обоснован метод получения оценок уровня информационной безопасности реализаций данного расширенного режима в релевантной практическим условиям математической модели IND-CPNA. Доказанные результаты о стойкости позволили сделать вывод о возможности существенного увеличения ограничений на длину обрабатываемых сообщений, квадратичным относительно количества секций образом.

Полученные оценки уровня информационной безопасности результирующих процедур обработки данных в модели IND-CPNA и высокие эксплуатационные качества, обеспечиваемые использующими данный метод средствами защиты информации при обработке сообщений большой длины, позволили разработанному механизму стать фундаментом как российских документов по стандартизации, определяющих протоколы защиты информации, так и меж-

дународных документов: войти в RFC 8645, разработанный определяющей механизмы защиты информации в Интернете исследовательской группой CFRG сообщества IETF/IRTF, а также стать шестым вошедшим в международный стандарт ISO режимом применения блочных симметричных алгоритмов наряду с пятью классическими режимами (ECB, CBC, CFB, OFB, CTR).

6. Установлены обоснованные оценки уровня информационной безопасности механизмов VKO, PRFGOST и KDFTREE, предоставляющие возможность получать для заданных значений параметров численные значения преобладаний нарушителей. Так, в двух математических моделях, соответствующих практическим условиям функционирования реализаций средств защиты информации, обеспечивающих работу протоколов защиты информации клиентских и серверных компонент, доказана стойкость механизма VKO вычисления ключей согласования, который за счет рандомизации множителей обеспечивает защиту от уязвимостей реализаций средств защиты информации в условиях слабодоверенного окружения, потенциально допускающего частичную компрометацию информации о сессионных ключах. При этом также установлено, что положительные свойства механизмов умножения на рандомизирующие множители влекут одновременно потенциальное увеличение негативного влияния уязвимостей реализаций самих механизмов на результирующую безопасность. Доказанные оценки стойкости для механизмов KDFTREE и PRFGOST позволяют сделать вывод о достаточности стойкости данных механизмов для обеспечения безопасности при дистанционном взаимодействии с серверными средствами защиты информации в случае ограничений на стороне клиентского средства доступа.

По результатам проведенных исследований указанные функции были стандартизированы в Российской Федерации для применения совместно со стандартом функции хэширования, позже вошли в RFC 7836.

7. Разработан протокол uSign формирования электронной подписи по схеме подписи Эль-Гамаля (в частности, по российскому стандарту электронной подписи), предназначенный для выполнения между логическими компонентами средств защиты информации, которые используют для операций с долговременными ключами потенциально уязвимые вычислительные модули, допускающие компрометацию определенной части защищаемой информации. Протокол построен путем внедрения в процесс формирования подписи элементов доказательства с нулевым разглашением для подтверждения использования вычислительными модулями корректных одноразовых секретных значений. По результатам исследований в математической модели функционирования указанных средств, учитывающей существование нарушителя с расширенными возможностями по модификации промежуточных величин, установлены соотношения между оценками вероятности успеха нарушителя при построении экзистенциальной подделки для базовой схемы подписи (в классических условиях) и для применяющих протокол uSign ее реализаций (в условиях работы с потенциально уязвимым вычислительным модулем). Из доказанных оценок уровня информационной безопасности следует стойкость построенных по разработанной схеме реализаций в условиях наличия уязвимостей в вычислительных модулях.

8. Доказаны оценки стойкости процедур формирования проверочного параметра платежной карты и проверочного значения PIN с применением функций DEC^2 и DEC^M. Для процедур на основе функции DEC^2, применяемой в ряде существующих зарубежных систем, установлено, что при вытекающих из практических соображений ограничениях на параметры они не обеспечивают необходимую защищенность. Для разработанной схемы с применением функции DEC^M в трех математических моделях нарушителя, отражающих сценарии использования платежных карт через терминалы и в рамках процедур электронной коммерции, доказаны оценки стойкости функций генерации проверочных параметров CVV и PVV по отношению к угрозе осуществления подделки. Полученные результаты позволяют для индивидуальных параметров схемы получать обоснованные численные значения уровня информационной безопасности.

По результатам проведенных исследований указанные механизмы были стандартизированы в Российской Федерации в качестве процедур формирования проверочного параметра платежной карты и проверочного значения PIN.

9. Разработан метод получения оценок уровня информационной безопасности для схем электронной подписи с уменьшенной длиной выхода, которые строятся на основе стойкой схемы подписи Эль-Гамаля путем применения трех методов, предполагающих модификацию соответствующих элементов схемы и допустимых для применения независимо друг от друга. Это позволяет дополнять средства защиты информации реализациями вспомогательных механизмов, требующих применения схем электронной подписи с индивидуальными параметрами, без дополнительных исследований модифицированных схем.

10. Разработан протокол SESPAKE, предназначенный для установления защищенного соединения с аутентификацией на основе низкоэнтропийных данных и позволяющий разделяющим их компонентам вырабатывать высокоэнтропийный общий ключ, взаимодействуя по каналу, в котором действует активный нарушитель. Благодаря входящим в протокол SESPAKE в качестве неотъемлемых элементов процедуре явного подтверждения ключа и механизму ограничения активных попыток подбора низкоэнтропийного секрета, протокол применим для распределенных средств защиты информации, функционирование которых подразумевает доступ к долговременным секретам через недоверенное окружение. На этапе синтеза протокола SESPAKE с учетом обзора ряда существующих протокольных решений схожего типа, в том числе, путем построения методов эксплуатации уязвимостей для них, установлены требования к протоколу для использования при доступе к ключевым носителям через недоверенное окружение.

Доказаны результаты о стойкости протокола SESPAKE. Обоснование проведено в наиболее близких практическим условиям применения протокола математических моделях на основании ряда сведéний между промежуточными задачами безопасности. Так, в модели на основе неотличимости с угрозой ложной аутентификации, формализуемой с помощью задачи отличения выработанной аутентификационной информации от случайной, доказаны результаты, позволяющие получить оценки стойкости для полного протокола установле-

ния защищенного соединения с аутентификацией на основе низкоэнтропийных данных, включающего подтверждение ключа. Безопасность обеспечивается в предположении стойкости используемых примитивов и неизвестности для нарушителя дискретных логарифмов используемых в качестве параметров точек эллиптических кривых: последнее достигается с помощью выбора «проверяемо случайным» образом как параметров самого протокола, так и параметров эллиптических кривых. Установленные оценки позволяют сделать вывод о безопасности применения данного протокола с целью доступа к долговременным секретам. Полученные результаты предоставляют метод выбора конкретных численных значений параметров протокола для достижения требуемых уровней информационной безопасности.

Благодаря строго обоснованным в релевантных математических моделях оценкам уровня информационной безопасности разработанный протокол SESPAKE был стандартизирован в Российской Федерации в качестве протокола выработки общего ключа с аутентификацией на основе пароля, позже вошел в RFC 8133.

В целом результаты диссертации можно квалифицировать как новое крупное научное достижение в области совершенствования математических методов обеспечения информационной безопасности функционирования программных средств защиты информации. Развитие математических моделей, новые методы построения архитектуры средств защиты информации и углубленные исследования свойств механизмов обеспечения информационной безопасности способствуют совершенствованию методов построения средств защиты информации и повышению уровня обоснованности оценок обеспечиваемой ими информационной безопасности. Внедрение изложенных и обоснованных в диссертации методов позволяет решить проблему разработки средств защиты информации, обеспечивающих свойства информационной безопасности в условиях ограниченного доверия к среде функционирования, и проведения всестороннего анализа их уровня защищенности — проблему, которая имеет определяющее значение для информационной безопасности государства.

Разработанные в диссертации подходы могут применяться при разработке и исследованиях средств защиты информации, а также быть интересны специалистам в областях математических методов анализа систем и средств защиты информации, теории алгоритмов, дискретных функций.

Благодарности. Автор диссертации выражает благодарность своему научному консультанту доктору физико-математических наук, старшему научному сотруднику Логачеву Олегу Алексеевичу за консультации, постоянное внимание к работе и поддержку, а также доктору физико-математических наук Васенину Валерию Александровичу, доктору физико-математических наук Зубкову Андрею Михайловичу, доктору физико-математических наук Черепневу Михаилу Алексеевичу, доктору технических наук Сабанову Алексею Геннадьевичу, кандидату физико-математических наук Матюхину Дмитрию Викторовичу, кандидату физико-математических наук Попову Владимиру Олеговичу,

кандидату физико-математических наук Алексееву Евгению Константиновичу, кандидату физико-математических наук Елистратову Андрею Алексеевичу, кандидату физико-математических наук Ошкину Игорю Борисовичу, кандидату физико-математических наук Чижову Ивану Владимировичу, кандидату физико-математических наук Шишкину Василию Алексеевичу, кандидату физико-математических наук Ролдугину Павлу Владимировичу, кандидату физико-математических наук Карпунину Григорию Анатольевичу, Ахметзяновой Лилии Руслановне, Маршалко Григорию Борисовичу, Бондаренко Александру Ивановичу, Лаврикову Ивану Викторовичу, Гребневу Сергею Владимировичу, Бабуевой Александре Алексеевне, Николаеву Василию Дмитриевичу, Божко Андрею Алексеевичу, а также Тору Хеллесету, Касу Кремерсу, Нику Салливану и Кристоферу Вуду за полезные обсуждения и рекомендации. Автор признателен также заведующему кафедры Информационной безопасности ВМК МГУ имени М.В. Ломоносова академику Соколову Игорю Анатольевичу за полезные обсуждения и рекомендации.

СПИСОК ПУБЛИКАЦИЙ АВТОРА ПО ТЕМЕ ДИССЕРТАЦИИ

Публикации в рецензируемых научных изданиях, индексируемых в базах данных Web of Science (WoS), Scopus, RSCI:

[1] Smyshlyaev S.V. Perfectly Balanced Boolean Functions and Golić Conjecture // Journal of Cryptology. 2012. Vol. 25 (3). Pp. 464–483 (Scopus, ИФ SJR 2020: 0.444).

[2] Смышляев С.В. Совершенно уравновешенные дискретные функции и условие Голича // Дискретная математика. 2013. Т. 25. № 1. С. 63–75 (RSCI WoS, ИФ РИНЦ 2019: 0.685).
/ Пер. на англ. яз.: Smyshlyaev S.V. Perfectly balanced k-valued functions and the Golić condition // Discrete Mathematics and Applications. 2013. Vol. 23 (1). Pp. 75–89 (Scopus, ИФ SJR 2020: 0.254). /

[3] Смышляев С.В. О связях между некоторыми параметрами совершенно уравновешенных булевых функций// Прикладная дискретная математика. 2013. № 2 (20). С. 19–25 (RSCI WoS, ИФ РИНЦ 2020: 0.380).

[4] Smyshlyaev S.V. Construction of RNG using random automata and “one-way” functions / Popov V.O., Smyshlyaev S.V. // Математические вопросы криптографии. 2014. Т. 5. № 2. С. 109–115 (RSCI WoS, ИФ РИНЦ 2020: 0,327).
/ В.О. Попову принадлежит постановка задачи, С.В. Смышляевым получены основные результаты статьи. /

[5] Smyshlyaev S.V. On the invariance of perfect balancedness property under the choice of tapping sequence // Математические вопросы криптографии. 2014. Т. 5. № 2. С. 127–135 (RSCI WoS, ИФ РИНЦ 2020: 0,327).

[6] Smyshlyaev S.V. On the performance of one perspective LSX-based block cipher / Alekseev E.K., Popov V.O., Prokhorov A.S., Smyshlyaev S.V., Sonina L.A. // Математические вопросы криптографии. 2015. Т. 6. № 2. С. 7–17 (RSCI WoS, ИФ РИНЦ 2020: 0,327).
/ С.В. Смышляеву принадлежит постановка задачи и методика исследований. /

[7] Смышляев С.В. Об 1-устойчивых совершенно уравновешенных булевых функциях // Дискретная математика. 2016. Т. 28. № 2. С. 117–126 (RSCI WoS, ИФ РИНЦ 2019: 0.685).
/ Пер. на англ. яз.: Smyshlyaev S.V. On 1-stable perfectly balanced Boolean functions // Discrete Mathematics and Applications. 2017. Vol. 27 (2). Pp. 109–115 (Scopus, ИФ SJR 2020: 0.254). /

[8] Смышляев С.В. О криптографических свойствах алгоритмов, сопутствующих применению стандартов ГОСТ Р 34.11-2012 и ГОСТ Р 34.10-2012 / Алексеев Е.К., Ошкин И.Б., Попов В.О., Смышляев С.В. // Математические вопросы криптографии. 2016. Т. 7. № 1. С. 5–38 (RSCI WoS, ИФ РИНЦ 2020: 0,327).
/ Соавторам принадлежат обзор моделей нарушителя и экспериментальные исследования. Остальные результаты статьи получены С.В. Смышляевым. /

[9] Смышляев С.В. Обзор уязвимостей некоторых протоколов выработки общего ключа с аутентификацией на основе пароля и принципы построения протокола SESPAKE / Алексеев Е.К., Ахметзянова Л.Р., Ошкин И.Б., Смышляев С.В. // Математические вопросы криптографии. 2016. Т. 7. № 4. С. 7–28 (RSCI WoS, ИФ РИНЦ 2020: 0,327).
/ Соавторами проведен обзор существующих протоколов (за исключением новых атак и необходимых условий). Остальные результаты статьи получены С.В. Смышляевым. /

[10] Smyshlyaev S.V. On the properties of the CTR encryption mode of Magma and Kuznyechik block ciphers with re-keying method based on CryptoPro Key Meshing / Ahmetzyanova L.R., Alekseev E.K., Oshkin I.B., Smyshlyaev S.V., Sonina L.A. // Математические вопросы криптографии. 2017. Т. 8. № 2. С. 39–50 (RSCI WoS, ИФ РИНЦ 2020: 0,327).
/ Соавторам принадлежат обзор моделей нарушителя и экспериментальные исследования. Остальные результаты статьи получены С.В. Смышляевым. /

[11] Smyshlyaev S.V. On cryptographic properties of the CVV and PVV parameters generation procedures in payment systems / Ahmetzyanova L.R., Alekseev E.K., Karpunin G.A., Smyshlyaev S.V. // Математические вопросы криптографии. 2018. Т. 9. № 2. С. 23–46 (RSCI WoS, ИФ РИНЦ 2020: 0,327).
/ Соавторам принадлежат обзор моделей нарушителя и уточнение вытекающих из практических ограничений требований к механизмам. Остальные результаты статьи получены С.В. Смышляевым. /

[12] Smyshlyaev S.V. On the security properties of Russian standardized elliptic curves / Alekseev E.K., Nikolaev V.D., Smyshlyaev S.V. // Математические вопросы криптографии. 2018. Т. 9. № 3. С. 5–32 (RSCI WoS, ИФ РИНЦ 2020: 0,327).
/ С.В. Смышляеву принадлежит постановка задачи и методика исследований. /

[13] Smyshlyaev S.V. Practical significance of security bounds for standardized internally re-keyed block cipher modes / Ahmetzyanova L.R., Alekseev E.K., Sedov G.K., Smyshlyaeva E.S., Smyshlyaev S.V. // Математические

вопросы криптографии. 2019. Т. 10. № 2. С. 31–46 (RSCI WoS, ИФ РИНЦ 2020: 0,327).
/ Соавторам принадлежит синтез и анализ режимов OMAC-ACPKM-Master (доказательство утверждения Теоремы 2 по тексту статьи). Остальные результаты статьи получены С.В. Смышляевым. /

[14] Смышляев С.В. О безопасности протокола SESPAKE / Алексеев Е.К., Смышляев С.В. // Прикладная дискретная математика. 2020. № 4 (50). С. 5–41 (Scopus, RSCI WoS, ИФ РИНЦ 2020: 0.380).
/ Е.К. Алексееву принадлежит обзор моделей нарушителя. Остальные результаты статьи получены С.В. Смышляевым. /

[15] Смышляев С.В. Защищенное хранение данных и полнодисковое шифрование / Алексеев Е.К., Ахметзянова Л.Р., Бабуева А.А., Смышляев С.В. // Прикладная дискретная математика. 2020. № 3 (49). С. 78–97 (Scopus, RSCI WoS, ИФ РИНЦ 2020: 0.380).
/ Автору диссертации принадлежит постановка задачи, а также принципы обеспечения конфиденциальности по модулю δ и целостности по модулю δ. /

[16] Smyshlyaev S. On Internal Re-keying / Akhmetzyanova L., Alekseev E., Smyshlyaev S., Oshkin I. // Lecture Notes in Computer Science, 2020, vol. 12529, pp. 23–45 (Scopus, ИФ SJR 2020: 0.249).
/ Соавторам принадлежит доказательство утверждения Теоремы 2 (по тексту статьи), выводы о защищенности режима GCM-ACPKM в части обеспечения имитозащиты, сравнение с базовым режимом GCM. Остальные результаты статьи получены С.В. Смышляевым. /

[17] Smyshlyaev S. Limiting the impact of unreliable randomness in deployed security protocols / Akhmetzyanova L., Cremers C., Garratt L., Smyshlyaev S., Sullivan N. // IEEE Computer Security Foundations, CSF, 2020, pp. 277-287 (Scopus, ИФ SJR 2020: 0.837).
/ Соавторам принадлежит первый вариант разработанной конструкции, предварительный анализ безопасности, экспериментальные оценки производительности предложенных механизмов, а также предложения о порядке использования разработанной конструкции в протоколе TLS. Остальные результаты статьи получены С.В. Смышляевым. /

[18] Smyshlyaev S.V. On methods of shortening ElGamal-type signatures / Akhmetzyanova L.R., Alekseev E.K., Babueva A.A, Smyshlyaev S.V. // Математические вопросы криптографии. 2021. Т. 12. № 2. С. 75–91 (RSCI WoS, ИФ РИНЦ 2020: 0,327).
/ Соавторам принадлежит доказательство достаточности устойчивости к нахождению прообраза с точностью до знака и устойчивости к нахождению прообраза нуля для выполнения свойства SDR. Остальные результаты статьи получены С.В. Смышляевым. /

[19] Смышляев С.В. О повышении безопасности схем подписи Эль-Гамаля / Алексеев Е.К., Ахметзянова Л.Р., Бабуева А.А., Смышляев С.В. // Математические вопросы криптографии. 2021. Т. 12. № 3. С. 5–30 (RSCI WoS, ИФ РИНЦ 2020: 0,327).
/ Соавторам принадлежит разработка моделей SUF-CMMA и SUF-CMRA,

а также дальнейшие модификации исследованной схемы. Остальные результаты статьи получены С.В. Смышляевым. /

[20] Смышляев С.В. Безопасная реализация электронной подписи с использованием слабодоверенного вычислителя / Алексеев Е.К., Ахметзянова Л.Р., Божко А.А., Смышляев С.В. // Математические вопросы криптографии. 2021. Т. 12. № 4. С. 5–23 (RSCI WoS, ИФ РИНЦ 2020: 0,327).
/ Соавторам принадлежит анализ влияния на результирующую безопасность возможности нарушителя провоцировать ошибки на стороне носителя, а также описание сценария атаки, позволяющей нарушителю восстановить ключ подписи в этом случае. Остальные результаты статьи получены С.В. Смышляевым. /

[21] Смышляев С.В. Влияние рандомизации в механизмах VKO на безопасность средств защиты информации / Алексеев Е.К., Николаев В.Д., Смышляев С.В. // Прикладная дискретная математика. 2021. № 4 (54). С. 78–94 (Scopus, RSCI WoS, ИФ РИНЦ 2020: 0.380).
/ Соавторам принадлежит обзор предшествующих результатов, классификация типов использования VKO, а также экспериментальные исследования. Остальные результаты статьи получены С.В. Смышляевым. /

Публикации в рецензируемых научных изданиях, входящих в перечень ВАК Минобрнауки России:

[22] Смышляев С.В. Противодействие атакам на протокол TLS / Леонтьев С.Е., Попов В.О., Смышляев С.В. // Системы высокой доступности. 2012. Т. 8. № 2. С. 109–115.
/ Соавторами предложена постановка задачи и проведен обзор существующих спецификаций протокола, С.В. Смышляевым получены основные результаты статьи. /

[23] Смышляев С.В. Подход к построению датчиков случайных чисел в программных средствах криптографической защиты информации / Попов В.О., Смышляев С.В. // Системы высокой доступности. 2013. Т. 9. № 3. С. 24–28.
/ В.О. Попову принадлежит постановка задачи, С.В. Смышляевым получены основные результаты статьи. /

[24] Смышляев С.В. О перспективах использования скрученных эллиптических кривых Эдвардса со стандартом ГОСТ Р 34.10-2012 и алгоритмом ключевого обмена на его основе / Алексеев Е.К., Ошкин И.Б., Попов В.О., Смышляев С.В., Сонина Л.А. // Проблемы информационной безопасности. Компьютерные системы. 2014. № 3. С. 60–66.
/ С.В. Смышляеву принадлежит постановка задачи и методика исследований. /

[25] Смышляев С.В. Обеспечение безопасности систем дистанционного формирования электронной подписи в условиях слабодоверенного окружения / Смирнов П.В., Смышляев С.В. // International Journal of Open Information Technologies. ISSN: 2307-8162 vol. 8, no.12, 2020. С. 77–84.
/ П.В. Смирнову принадлежит техническая реализация разработанной архитектуры. Остальные результаты статьи получены С.В. Смышляевым. /

[26] Смышляев С.В. Повышение безопасности доступа к ключам электронной подписи в условиях слабодоверенного окружения / Агафьин С.С., Смышляев С.В. // International Journal of Open Information Technologies. ISSN: 2307-8162 vol. 9, no.10, 2021. С. 84–89.
/ С.С. Агафьину принадлежит обзор типов ключевых носителей. Остальные результаты статьи получены С.В. Смышляевым./

Другие публикации:

[27] Смышляев С.В. Булевы функции в теории кодирования и криптологии (3-е изд.) / Логачев О.А., Сальников А.А., Смышляев С.В., Ященко В.В. // Ленанд, 2015. 576 стр.
/ Данная работа является монографией четырех авторов, при этом в разделах 10.2-10.5 представлены результаты, полученные лично С.В. Смышляевым. /

[28] Smyshlyaev S.V. Symbolic Dynamics, Codes and Perfectly Balanced Functions / Logachev O.A., Salnikov A.A., Smyshlyaev S.V., Yashchenko V.V. // Proceedings of the NATO Advanced Research Workshop on Enhancing Cryptographic Primitives with Techniques from Error Correcting Codes. 2009. Pp. 222–233.
/ С.В. Смышляеву принадлежит доказательство несуществования не являющихся линейными ни по одной переменной булевых функций, сохраняющих совершенную уравновешенность при введении произвольного набора фиктивных переменных (часть доказательства Гипотезы Голича). /

[29] Смышляев С.В. Совершенная уравновешенность дискретных функций и условие Голича // Прикладная дискретная математика. Приложение. 2012. № 5. С. 28-30.

[30] Смышляев С.В. О неавтономных двоичных регистрах сдвига, обладающих свойством синхронизации / Логачев О.А., Смышляев С.В. // Электроника инфо. 2013. № 6. С. 183–185.
/ С.В. Смышляеву принадлежит доказательство утверждения Теоремы 14 (по тексту статьи). /

[31] Smyshlyaev S. On methods of shortening ElGamal-type signatures / Akhmetzyanova L., Alekseev E., Babueva A., Smyshlyaev S. // Proceedings of the 9-th Workshop on Current Trends in Cryptology (CTCrypt), Dorokhovo, Ruza District, Moscow Region, Russia. Pp. 252-286; IACR Cryptology ePrint Archive, Report 2021/148, 2021.
/ Соавторам принадлежит построение нарушителей D и M в доказательстве Леммы 5 в Приложении В.3, а также анализ условий выполнения свойства SDR в Приложении В.4 (по тексту статьи). Остальные результаты статьи получены С.В. Смышляевым. /

[32] Smyshlyaev S.V. On Security of TLS 1.2 Record Layer with Russian Ciphersuites / Ahmetzyanova L.R., Alekseev E.K., Sedov G.K., Smyshlyaev S.V. // Proceedings of the 8-th Workshop on Current Trends in Cryptology (CTCrypt), Svetlogorsk, Kaliningrad region, Russia. Pp. 254-292.
/ С.В. Смышляеву принадлежит постановка задачи и архитектура применения механизмов ACPKM и PRFGOST в синтезируемом протоколе. /