

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ УНИТАРНОЕ ПРЕДПРИЯТИЕ
«НАУЧНО-ТЕХНИЧЕСКИЙ ЦЕНТР «АТЛАС»
(ФГУП «НТЦ «Атлас»)
Пензенский филиал

Проспект Победы, д 69, г. Пенза, 440028
Тел. (8412) 64-38-63, Факс (8412) 47-78-80, e-mail: atlas@sura.ru

ОКПО 08859495, ОГРН 1027739411402,
ИНН/КПП 7715027275/583543001

УТВЕРЖДАЮ

Директор
ПФ ФГУП «НТЦ «Атлас»

Ю.Г. Юранов

«__» _____ 2019 г.

АКТ

о внедрении результатов диссертационной работы Миронкина В.О. в деятельность
Пензенского филиала ФГУП «Научно-технический центр «Атлас» при криптографических
исследованиях действующих и создаваемых средств защиты информации

Комиссия в составе: председатель - заместитель директора специальным вопросам Кузнецов С.Е.; члены комиссии: начальник криптографического отдела Пономарев М.И., заместитель начальника криптографического отдела Матвеев С.В., научный сотрудник криптографического отдела Васин А.В., к.ф.м.н., составила настоящий акт о том, что результаты диссертационной работы Миронкина В.О. были использованы в деятельности ПФ ФГУП «НТЦ «Атлас» при проведении криптографического анализа в рамках сертификационных исследований создаваемых средств защиты информации.

Результаты главы 1 (теоремы о вероятностных характеристиках алгоритма преобразования ключа «CryptoPro Key Meshing») использованы для обоснования криптографических качеств алгоритмов формирования производных ключей, а также, для оценки влияния алгоритма преобразования ключа «CryptoPro Key Meshing» и алгоритмов подобных данному алгоритму на стойкость блочных шифров для основных методов анализа. Алгоритм преобразования ключа «CryptoPro Key Meshing» и подобные ему механизмы, реализованы в ряде изделий и программных СКЗИ, разработанных в ПФ ФГУП «НТЦ «Атлас». В частности, данный механизм используется в реализации протокола защиты информации TLS в соответствии с Методическими рекомендациями Технического комитета по стандартизации «Криптографическая защита информации» (ТК 26) МР 26.2.001-2013 «Использование наборов алгоритмов шифрования на основе ГОСТ 28147-89 для протокола безопасности транспортного уровня (TLS)» во встроенном программном средстве криптографической защиты информации СледопытSSL защищенной мобильной операционной системы на базе Sailfish Mobile OS RUS.

Председатель комиссии: _____ /Кузнецов С.Е./

Члены комиссии: _____ /Пономарев М.И./

_____ /Матвеев С.В./

_____ /Васин А.В./