Экз. № 1

АКЦИОНЕРНОЕ ОБЩЕСТВО
«НАУЧНО-ТЕХНИЧЕСКИЙ ЦЕНТР
«АТЛАС»
(АО «НТЦ «Атлас»)
Пензенский филиал
Проспект Победы, д. 69, г. Пенза, 440028
Тел. (8412) 64-38-63, Факс (8412) 47-78-80
e-mail: atlas@atlas-pf.ru

УТВЕРЖДАЮ
Директор ПФ АО «НТЦ «Атлас»
Юранов Ю.Г.

Отзыв на автореферат диссертации
Нестеренко Алексея Юрьевича на тему
«Математические методы обеспечения защищенного взаимодействия средств защиты информации», представленной на соискание ученой степени доктора физико-математических наук по специальности 2.3.6 — методы и системы защиты информации, информационная безопасность

Диссертационная работа Нестеренко Алексея Юрьевича содержит в себе решение нескольких актуальных задач как теоретического, так и практического характера. Хорошо известно, что задача поиска эффективного алгоритма дискретного логарифмирования в группе точек эллиптической кривой является одной из трудных математических задач. Сложностью ее решения обосновывается безопасность большого числа отечественных криптографических схем и протоколов, в частности, схемы электронной подписи ГОСТ Р 34.10-2012. Получение каких-либо содержательных результатов в этом направлении приводит к пересмотру оценок безопасности средств защиты информации и к корректировке методов выбора параметров криптографических схем. Полученные в диссертационной работе результаты относятся именно к такому классу.

К безусловным достоинствам диссертации можно отнести следующее.

Во-первых, автор предложил метод дискретного логарифмирования в группе точек эллиптической кривой, использующий информацию о мультипликативном порядке неизвестного. Этот метод позволяет определить множество неизвестных значений, трудоемкость нахождения которых меньше чем методов, известных ранее. Для защиты от указанного метода автором диссертации уточнены требования к параметрам эллиптических кривых и предложен алгоритм построения таких параметров.

Во-вторых, предложен класс генераторов псевдослучайных последовательностей, позволяющий вырабатывать непериодические последовательности. Проведенные в диссертационной работе исследования позволяют обосновать сложность восстановления начального состояния генераторов из рассматриваемого класса по значениям вырабатываемых последовательностей. Примером применения предложенного подхода является алгоритм локальной аутентификации пользователей средств защиты информации, существенно затрудняющий опробование паролей пользователя с использованием специальных вычислительных средств.

В-третьих, предложен новый режим аутентифицированного шифрования, т.е. процедура одновременного шифрования и контроля целостности передаваемых данных. Разработанный режим ориентирован на применение в программных средствах защиты информации. Полученные в диссертационной работе теоретические результаты позволяют говорить о сложности применения известных методов построения коллизии для вырабатываемых кодов целостности, а практические результаты иллюстрируют преимущество разработанного режима по скорости реализации над другими отечественными алгоритмами.

В-четвертых, в диссертационной работе предложен подход к получению обоснованных оценок безопасности криптографических схем и протоколов. Предложенный подход позволяет построить теоретико-автоматную модель криптографического протокола и формализует с ее помощью основные свойства безопасности. Данный подход применяется при проведении тематических исследований средств защиты информации, в частности, он был использован при проведении анализа криптографического протокола выработки общего ключа IKEv2.

Эти и другие результаты составляют научное содержание рецензируемой диссертации и являются существенным продвижением в области защиты информации.

Представленный на отзыв автореферат позволяет понять основные принципы и научные результаты проведенных исследований.

Вместе с тем, имеются некоторые критические замечания к тексту автореферата.

1. В нескольких случаях в тексте автореферата содержится упоминание о разработанном алгоритме, однако детальное описание самого алгоритма не

приводится. Это относится ко второй модификации алгоритма дискретного логарифмирования с известным мультипликативным порядком, а также к алгоритму локальной аутентификации пользователей средств защиты.

2. В тексте автореферата содержатся мелкие опечатки, а также отсылки к номерам параграфов диссертации, которых нет в тексте автореферата.

Перечисленные замечания носят редакционный характер и не затрагивают научной сути диссертации, результаты которой востребованы при проведении тематических исследований средств защиты информации.

В целом диссертация Нестеренко А.Ю. на тему «Математические методы обеспечения защищенного взаимодействия средств защиты информации» соответствует требованиям, предъявляемым к диссертациям на соискание учёной степени доктора физико-математических наук, и является существенным продвижением в решении крупной научной проблемы обеспечения стойкости средств защиты информации.

Учитывая все вышеизложенное, считаем, что Нестеренко А.Ю. заслуживает присуждения ученой степени доктора физико-математических наук по специальности 2.3.6 – методы и системы защиты информации, информационная безопасность.

к.ф.-м.н. Васин Алексей Валерьевич
Старший научный сотрудник ПФ АО НТЦ «Атлас»
Проспект Победы, д. 69, г. Пенза, 440028.
atlas@atlas-pf.ru 8(8412)64-31-60

к.т.н. Рязанцев Владимир Андреевич
Старший научный сотрудник ПФ АО НТЦ «Атлас»
Проспект Победы, д. 69, г. Пенза, 440028.
atlas@atlas-pf.ru 8(8412)64-31-60

Отзыв рассмотрен на НТС.
Протокол заседания от 03.10.2023 № 13
Ведущий научный консультант ПФ АО НТЦ «Атлас»
Десятов Владимир Дмитриевич