Отзыв
официального оппонента на диссертационную работу
Нестеренко Алексея Юрьевича
«Математические методы обеспечения защищенного взаимодействия средств защиты информации»,
представленную на соискание ученой степени доктора физико-математических наук по специальности 2.3.6 — «Методы и системы защиты информации, информационная безопасность»

Целью диссертационной работы Нестеренко Алексея Юрьевича является получение математически обоснованных оценок безопасности криптографических протоколов, используемых для защиты информации, циркулирующей в информационных системах и сетях.

Решение данной проблемы имеет большое значение в теоретическом и практическом плане для отечественных научно-практических направлений и отраслей разработки, создания и применения средств защиты информации, которые используются в информационных системах и сетях, автоматизированных системах управления, сетях связи различного типа и назначения, а также для защиты критической информационной инфраструктуры.

Выбранный автором диссертации метод обоснования оценок безопасности основывается на оценке сложности решения ряда математических задач. Этот ряд содержит и такие задачи, как :

задача дискретного логарифмирования в группе точек эллиптической кривой,

задача определения начального состояния генератора псевдослучайных последовательностей

и задача построения коллизии для ключевых функций хеширования.

Задача дискретного логарифмирования хорошо известна в теории и практике защиты информации, а сложность ее решения существенным образом влияет на безопасность большого числа криптографических схем и протоколов, применяемых на практике, в частности, действующего стандарта электронной подписи ГОСТ Р 34.10-2012, а также протоколов TLS и IPSec, используемых для защиты информации в сети Интернет. Остальные две задачи, в рассматриваемой автором постановке, тоже важны и могут применяться при разработке новых криптографических схем и протоколов.

Отдельного внимания заслуживает совокупность диссертационных достижений автора, которая включает в себя разработанные автором криптографические протоколы. Один из этих протоколов включен в рекомендации по стандартизации Р 1323565.028-2019. Предложенный для обоснования этого протокола подход лег в основу методики оценки численных значений параметров безопасности, изложенной в последнем параграфе диссертации. Практическая важность указанной методики была подтверждена при проведении криптографических исследований протокола IKEv2, входящего в семейство протоколов IPSec.

Исходя из сказанного, можно констатировать, что актуальность, научная новизна и содержательность, а также высокая степень практической ценности результатов, полученных в диссертационной работе не вызывает сомнений.

Диссертация А.Ю.Нестеренко имеет достаточно большой объем – 426 страниц. Она включает в себя общую характеристику работы, 4 главы, заключение, а также приложения, содержащие тексты программ, использованных автором диссертации для верификации полученных им теоретических результатов.

Среди результатов, выносимых на защиту, наибольшую значимость имеют следующие.

1. Теорема о существовании алгоритма дискретного логарифмирования в группе точек эллиптической кривой, использующего информацию о мультипликативном порядке неизвестного. Автором диссертации впервые показано, что сложность решения указанной задачи зависит не только от параметров эллиптической кривой, но и от самого неизвестного значения, и может быть существенно ниже, чем у известных ранее алгоритмов. Это позволило, по аналогии с алгоритмами блочного шифрования, определить понятие «слабого» ключа и разработать метод определения множества таких ключей, а также указать явное значение мощности данного множества.

2. Усиленные требования к параметрам эллиптических кривых, предложенные с целью минимизации множества «слабых» ключей, а также алгоритм построения таких параметров. В приложении к диссертационной работе приводится перечень установленных и обоснованных автором диссертации значений, которые могут быть использованы в перспективных средствах защиты информации.

3. Метод локальной аутентификации пользователей средств защиты информации, основанный на преобразовании пароля пользователя в псевдослучайную последовательность специального вида. Обоснование безопасности предложенного подхода составляет большую часть второй главы диссертации.

4. Режим работы блочного шифра, реализующий одновременное шифрование и контроль целостности обрабатываемой информации. Доказанные автором теоремы позволяют гарантировать свойство равновероятности сжимающего преобразования, входящего в состав режима, что затрудняет реализацию атак, направленных на компрометацию кода целостности сообщения.

5. Метод построения формальной модели криптографического протокола и вычисления с помощью построенной модели значений

параметров безопасности, к которым автор относит сложность компрометации и вероятность успешного проведения атаки на криптографический протокол.

Все выносимые на защиту результаты являются новыми, полученными автором лично. Результаты четко сформулированы и представлены строгие математические доказательства их справедливости.

К тексту диссертации можно высказать следующие замечания.

1. Имеется ряд незначительных опечаток в схемах криптографических протоколов, например, на стр. 281 и 305.

2. В примере, иллюстрирующем представление числа пи в шестнадцатеричной системе счисления, приводится ссылка на «новую» статью более чем десятилетней давности.

Однако указанные замечания не влияют на общую высокую положительную оценку диссертационной работы А.Ю. Нестеренко.

Автором диссертации проведено разностороннее исследование поставленной проблемы, а предложенные методы ее решения подтверждаются как результатами практических вычислений, так и фактом принятия государственных стандартов и рекомендаций по стандартизации.

В диссертации используется широкий математический аппарат алгебры, теории автоматов, теории сложности вычислений, теории чисел, теории функций комплексного переменного, теории вероятностей.

Диссертация обладает внутренним единством, ее содержание соответствует названию и поставленным задачам.

Основные выводы по диссертации сформулированы достаточно полно и отражают суть полученных результатов.

Диссертация А.Ю. Нестеренко представляет собой завершенную научную работу, в которой на основании выполненных автором исследований сформулированы результаты, совокупность которых можно квалифицировать как новое крупное научное достижение.

Текст автореферата соответствует содержанию диссертации.

Результаты диссертации с достаточной полнотой опубликованы в 29 научных публикациях, среди которых 21 публикация входит в перечень изданий, индексируемых Web of Science, Scopus, RSCI и входящих в списки ВАК Минобрнауки Российской Федерации.

На основании вышеизложенного считаю, что диссертация Нестеренко Алексея Юрьевича на тему «Математические методы обеспечения защищенного взаимодействия средств защиты информации» отвечает всем требованиям, установленным Московским государственным университетом имени М.В. Ломоносова к докторским диссертациям.

Содержание диссертации соответствует паспорту специальности 2.3.6 - «Методы и системы защиты информации, информационная безопасность» (физико-математические науки), а также критериям, определенным пп. 2.1-2.5 Положения о присуждении ученых степеней в Московском государственном университете имени М.В. Ломоносова.

Нестеренко Алексей Юрьевич заслуживает присуждения ему ученой степени доктора физико-математических наук по специальности 2.3.6 - «Методы и системы защиты информации, информационная безопасность» (физико-математические науки).

Официальный оппонент:
доктор физико-математических наук
консультант отдела
Департамента информационных систем
Министерства обороны
Российской Федерации Алиев Физули Камилович

« 05 » октября 2023 г.

Подпись Алиева Физули Камиловича заверяю.