ЗАКЛЮЧЕНИЕ ДИССЕРТАЦИОННОГО СОВЕТА МГУ.012.3
ПО ДИССЕРТАЦИИ НА СОИСКАНИЕ УЧЕНОЙ СТЕПЕНИ ДОКТОРА НАУК

Решение диссертационного совета от «18» октября 2023 г., протокол № 6

О присуждении Нестеренко Алексею Юрьевичу, гражданин Российской Федерации, ученой степени доктора физико-математических наук.

Диссертация **«Математические методы обеспечения защищенного взаимодействия средств защиты информации»** по специальности 2.3.6 – «Методы и системы защиты информации, информационная безопасность» (физико-математические науки) принята к защите диссертационным советом 21 июня 2023 г., протокол № 4.

Соискатель **Нестеренко Алексей Юрьевич** 1973 года рождения, **в 1996 году** окончил ФГБОУ ВО «Московский государственный университет имени М.В. Ломоносова», механико-математический факультет, и получил квалификацию «математик» по специальности «математика, прикладная математика» (диплом ЭВ 475767). В 2009 году закончил заочную аспирантуру механико-математического факультета ФГБОУ ВО «Московский государственный университет имени М.В. Ломоносова».

В 2010 году соискатель защитил диссертацию на соискание ученой степени кандидата физико-математических наук на тему «Алгоритмические приложения эллиптических кривых, задаваемых тэта-соотношениями» в диссертационном совете при ФГБОУ ВО «Московский педагогический государственный университет» по специальности 01.01.06 – математическая логика, алгебра и теория чисел (диплом ДКН 115234).

Соискатель работает с 2012 года на кафедре компьютерной безопасности Московского института электроники и математики Национального исследовательского университета «Высшая школа экономики» (МИЭМ НИУ ВШЭ) по настоящее время.

Диссертация выполнена в Московском институте электроники и математики Национального исследовательского университета «Высшая школа экономики», кафедра компьютерной безопасности.

Научный консультант – доктор физико-математических наук **Чирский Владимир Григорьевич**, профессор, профессор кафедры математического анализа механико-математического факультета МГУ им. М.В. Ломоносова.

Официальные оппоненты:

Алиев Физули Камилович, доктор физико-математических наук, Министерство обороны Российской Федерации, консультант департамента информационных систем;

Логачев Олег Алексеевич, доктор физико-математических наук, доцент кафедры информационной безопасности факультета вычислительной математики и кибернетики МГУ им. М.В. Ломоносова;

Смышляев Станислав Витальевич, доктор физико-математических наук, заместитель генерального директора ООО КРИПТО-ПРО

дали **положительные отзывы** на диссертацию.

Соискатель имеет 52 опубликованные работы, в том числе по теме диссертации 29 работ, из которых 15 публикаций в рецензируемых научных изданиях, рекомендованных для защиты в диссертационном совете МГУ по специальности 2.3.6 – Методы и системы защиты информации, информационная безопасность (физико-математические науки).

Результат диссертационной работы опубликованы в открытой печати.

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

1. Chirskii V., Nesterenko A.Yu. An approach to the transformation of periodic sequences. Discrethe Mathematics and Applications. – 2017. – Vol. 27. – № 1.– P.1 – 7. (импакт-фактор SJR: 0,265) // На русском яз.: Чирский В.Г., Нестеренко А.Ю. Об одном подходе к преобразованию периодических последовательностей. Дискретная математика. – 2015. – Т. 27, № 4. – С. 150 – 157. (doi: 10.4213/dm1354, импакт-фактор РИНЦ: 0,297) / Постановка задачи выполнена Чирским В.Г., остальные результаты получены Нестеренко А.Ю. /

2. Nesterenko A.Yu. Cycle detection algorithms and their applications. Journal of Mathematical Sciences. – 2012. Vol. 182, № 4. – P. 518 – 526. (импакт-фактор SJR: 0,23) // На русском яз.: Нестеренко А.Ю. Алгоритмы поиска длин циклов в последовательностях и их приложения. Фундаментальная и прикладная математика. – 2010. – Т. 16, № 6. – С. 109– 122. (doi: 10.1007/s10958-012-0755-x, импакт-фактор SJR: 0,23).

3. Nesterenko A.Yu. Constructions of elliptic curves endomorphisms. Математические вопросы криптографии. – 2014. – V. 5, № 2. – pp. 99 – 102. (doi: 10.4213/mvk121, импакт-фактор РИНЦ: 0,36).

4. Nesterenko A.Yu. Some remarks on the elliptic curve discrete logarithm problem. Математические вопросы криптографии. – 2016. – V. 7, № 2. – pp. 115–120. (doi: 10.4213/mvk189, импакт-фактор РИНЦ: 0,36).

5. Nesterenko A.Yu. A new authenticated encryption mode for arbitrary block cipher based on universal hash function. Математические вопросы криптографии. – 2017. – V. 8, № 2. – pp. 117–130. (doi: 10.4213/mvk228, импакт-фактор РИНЦ: 0,36).

6. Nesterenko A.Yu. Construction of strong elliptic curves suitable for cryptographic applications. Математические вопросы криптографии. – 2019. – V. 10, № 2. – pp. 135– 144. (doi: 10.4213/mvk291, импакт-фактор РИНЦ: 0,36).

7. Nesterenko A.Yu., Semenov A.M. On the practical implementation of Russian protocols for low-resource cryptographic modules. Journal of Computer Virology and Hacking Techniques. – 2020. – V. 16, № 4. – pp. 305 – 312. (doi: 10.1007/s11416-020-00362-y, импакт-фактор SJR: 0,53).

8. Лебедев П.А., Нестеренко А.Ю. Арифметика эллиптических кривых с использованием графических вычислителей. Чебышевский сборник. – 2012. – Т. 13, № 2. – С. 91 – 105. (импакт-фактор SJR: 0,18) /Нестеренко А.Ю. принадлежат теоретические результаты, Лебедеву П.А. – результаты практических экспериментов./

9. Нестеренко А.Ю. О некоторых свойствах эллиптической кривой в форме Якоби. Чебышевский сборник. – 2010. – Т.11, № 1. – С.202 – 208. (импакт-фактор SJR: 0,18).

10. Nesterenko A.Yu. Parameters Recovering Algorithm for One Class of Irrationalities // Izvestia of Saratov University. New Series: Mathematics, Mechanics, Informatics. – 2013. – V. 13, № 4 (part 2). – P. 89 – 93. (doi: 10.18500/1816-9791-2013-13-4-89-93, импакт-фактор SJR: 0.25).

11. Нестеренко А.Ю. Об одном подходе к построению защищенных соединений. Математические вопросы криптографии. – 2013. – Т. 4, № 2. – С. 101 – 111. (doi: 10.4213/mvk86, импакт-фактор РИНЦ: 0,36).

12. Нестеренко А.Ю. Об одном семействе универсальных функций хеширования. Математические вопросы криптографии. – 2015. – Т. 6, № 3. – С. 135 – 151. (doi: 10.4213/mvk164, импакт-фактор РИНЦ: 0,36).

13. Нестеренко А.Ю. Об одном подходе к разложению иррациональных чисел. Математические вопросы криптографии. – 2018. – Т. 9, № 1. – С. 89 – 106. (doi: 10.4213/mvk189, импакт-фактор РИНЦ: 0,36).

14. Нестеренко А.Ю., Пугачев А.В. Об одной схеме гибридного шифрования. Прикладная дискретная математика. – 2015. – № 4. – С. 56 – 71. (doi: 10.17223/20710410/30/5, импакт-фактор SRJ: 0.20). / Нестеренко А.Ю. принадлежат результаты оценки стойкости, а Пугачеву А.В. – оценки скорости работы рассматриваемой схемы шифрования. /

15. Нестеренко А.Ю., Семенов А.М. Методика оценки безопасности криптографических протоколов. Прикладная дискретная математика. – 2022. – № 56. – С. 33 – 82. (doi: 10.17223/20710410/56/4, импакт-фактор SJR: 0.22) /Семенову А.М. принадлежат формализация и анализ свойств безопасности криптографических протоколов, Нестеренко А.Ю. – формулировка модели и метод оценки показателей мер защиты./

На автореферат диссертации поступили 4 **дополнительных отзыва, все положительные**.

Выбор официальных оппонентов обоснован их высокой профессиональной квалификацией, наличием научных публикаций по направлениям, тесно связанным с темой диссертации автора, а также их соответствием критериям, установленным в Положении о присуждении ученых степеней в Московском государственном университете имени М.В. Ломоносова.

Диссертационный совет отмечает, что представленная диссертация на соискание ученой степени доктора физико-математических наук **является научно-квалификационной работой**, в которой на основании выполненных автором исследований **решена важная проблема** обеспечения безопасности криптографических протоколов, применяемых для защищенного обмена информацией по открытым каналам связи, а **внедрение методов, представленных в работе, вносит значительный вклад в развитие инфраструктуры обеспечения информационной безопасности Российской Федерации**.

Диссертация представляет собой **самостоятельное законченное исследование, обладающее внутренним единством**. Положения, которые выносятся на защиту, содержат новые научные результаты, свидетельствующие **о личном вкладе автора** в науку:

1) теорема об оценке числа шагов алгоритма Госпера, используемого для поиска двух совпадающих элементов числовых последовательностей;

2) алгоритм решения задачи дискретного логарифмирования в группе точек эллиптической кривой, основанный на методе Госпера, и асимптотическая оценка сложности данного алгоритма;

3) теорема о существовании алгоритма дискретного логарифмирования в группе точек эллиптической кривой, использующего информацию о мультипликативном порядке неизвестного, а также точные оценки как трудоемкости такого алгоритма, так и объема используемой им памяти;

4) два варианта (однопоточный и параллельный) алгоритма решения задачи дискретного логарифмирования в группе точек эллиптической кривой, использующего информацию о мультипликативном порядке неизвестного;

5) алгоритм вычисления явного представления эндоморфизмов эллиптических кривых, а также явный вид эндоморфизмов для всех эллиптических кривых, чье кольцо эндоморфизмов изоморфно порядку мнимого квадратичного поля с числом классов равным единице;

6) теорема о представлении натуральных чисел значениями многочленов в точках мнимого квадратичного поля и алгоритм вычисления кратной точки эллиптической кривой, основанный на утверждении доказанной теоремы;

7) алгоритм построения эллиптических кривых, удовлетворяющих усиленным, по сравнению с ГОСТ Р 34.10-2012, требованиям к параметрам эллиптических кривых, а также явные значения построенных параметров;

8) теоремы об иррациональности одного класса действительных чисел, задаваемых быстросходящимися рядами, об оценке неизвестных параметров чисел из данного класса при известном рациональном приближении, а также доказательство критерия нормальности действительных чисел;

9) алгоритм преобразования парольной информации, используемый для локальной аутентификации пользователей средств защиты информации;

10) новый класс ключевых функций хеширования, представляющих собой линейные формы от перестановок на множестве кодов аутентификации, включая доказательство теорем о том, что функции из этого класса являются равновероятными функциями относительно сжимаемых сообщений и строго равновероятными функциями относительно множества ключей;

11) режим аутентифицированного шифрования и доказательство теоремы о выполнении свойства равновероятности для сжимающего отображения предложенного режима при фиксированных ключах шифрования и аутентификации;

12) гибридная схема, реализующая процесс шифрования с помощью полиномиального преобразования, а также доказательство теоремы о безопасности предложенной схемы шифрования относительно задач определения секретного ключа аутентификации, дешифрования и навязывания сообщений;

13) протокол выработки общего ключа со взаимной аутентификацией субъектов взаимодействия, а также доказательство теоремы о безопасности предложенного протокола относительно задач определения общего ключа, дешифрования и навязывания передаваемой информации;

14) формальная модель, имитирующая криптографический протокол в виде дискретной динамической системы, а также метод получения численных значений показателей безопасности, использующий оценки трудоемкости компрометации криптографических преобразований, изменяющих состояния дискретной динамической системы;

15) методика проведения исследования безопасности криптографических протоколов.

Результаты диссертации базируются на известных теоретических положениях алгебры, теории чисел, алгебраической геометрии и теории функций комплексного переменного, теории вероятностей, математической статистики и теории автоматов, **являются четко сформулированными**, а их **достоверность обеспечивается** строгими математическими доказательствами.

Все результаты диссертации являются новыми. Результаты других авторов, упомянутые в диссертации, отмечены соответствующими ссылками. **Результаты диссертации прошли апробацию** на многочисленных международных и всероссийских конференциях, симпозиумах и научно-исследовательских семинарах. Основные результаты опубликованы в научных изданиях, рекомендованных для защиты в диссертационном

совете МГУ по специальности 2.3.6 - «Методы и системы защиты информации, информационная безопасность» (физико-математические науки).

Сформулированные в диссертации положения доказаны автором самостоятельно, **они теоретически и практически значимы, являются существенным продвижением в решении важной в теоретическом плане и практическом отношении проблемы** обеспечения защищенного взаимодействия средств защиты информации, циркулирующей в открытых сетях связи. Результаты диссертации были учтены при разработке ряда государственных стандартов и рекомендаций по стандартизации в области криптографической защиты информации.

На заседании 18 октября 2023 года диссертационный совет принял решение присудить Нестеренко А.Ю. ученую степень доктора физико-математических наук.

При проведении тайного голосования диссертационный совет в количестве 21 человека, из них 4 доктора наук по специальности рассматриваемой диссертации, участвовавших в заседании, из 26человек, входящих в состав совета, проголосовали: за - 19 , против - 2 , недействительных бюллетеней - нет.

Заместитель председателя
диссертационного совета МГУ.012.3,
доктор физико-математических наук, профессор В.А. Васенин

Ученый секретарь
диссертационного совета МГУ.012.3,
кандидат физико-математических наук А.В. Галатенко

«18» октября 2023 г.