МИНОБРНАУКИ РОССИИ
федеральное государственное автономное образовательное учреждение
высшего образования
**«Санкт-Петербургский государственный электротехнический университет
«ЛЭТИ» им. В.И. Ульянова (Ленина)»
(СПбГЭТУ «ЛЭТИ»)**
ул. Проф. Попова, д.5, Санкт-Петербург, 197376
Телефон: (812) 346-44-87 Факс: (812) 346-27-58 E-mail: eltech@eltech.ru http:// www.eltech.ru
ОКПО 02068539 ОГРН 1027806875381 ОКВЭД 80.3, 73.1 ОКТМО 40392000000
ИНН/КПП 7813045402/781301001

20.06.16 № 2074/586-1

На № _____ от _____

«УТВЕРЖДАЮ»

ЗАКЛЮЧЕНИЕ

федерального государственного автономного образовательного учреждения высшего образования «Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)»

Диссертация «Методы повышения уровня безопасности защитных преобразований информации» выполнена в федеральном государственном автономном образовательном учреждении высшего образования «Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)» (далее СПбГЭТУ «ЛЭТИ») на кафедре автоматизированных систем обработки информации и управления.

В период подготовки диссертации Березин Андрей Николаевич являлся очным аспирантом кафедры автоматизированных систем обработки информации и управления по специальности: 05.13.19 «Методы и системы защиты информации, информационная безопасность» с 05.07.2012 по 04.07.2016.

университет "ЛЭТИ" им. В.И.Ульянова (Ленина)» по специальности «Компьютерная безопасность» с присуждением квалификации «математик».

Документ о сдаче кандидатских экзаменов № 04-03 выдан 16.03.2016 г. отделом докторантуры и аспирантуры федерального государственного автономного образовательного учреждения высшего образования «Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)».

Научный руководитель – доктор технических наук, профессор Молдовян Николай Андреевич, профессор кафедры «Информационной безопасности» федерального государственного автономного образовательного учреждения высшего образования «Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)».

Диссертация заслушана и обсуждена на расширенном заседании

электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)» 14 июня 2016 г., Протокол № 7 от 14 июня 2016 г.

Присутствовали:

Сотрудники кафедры автоматизированных систем обработки информации и управления федерального государственного автономного образовательного учреждения высшего образования «Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)»:

Водяхо А.И., профессор каф., д-р техн. наук, профессор; Копыльцов А.В., профессор каф., д-р техн. наук, профессор; Кутузов О.И., профессор каф., д-р техн. наук, профессор; Советов Б.Я., профессор каф., д-р техн. наук, профессор; Чертовской В.Д., профессор каф., д-р техн. наук, профессор; Яковлев С.А., профессор каф., д-р техн .наук, профессор; Цехановский В.В., профессор каф., канд.техн. наук, доцент; Гурьянов Д.Ю., доцент каф., канд. техн. наук,; Зорин К.М., доцент каф., канд.техн.наук; Новикова Е.С., доцент каф., канд.техн.наук; Молдовян Д.Н., ассистент, канд.техн.наук; Колбанев М.О., профессор каф., д-р техн. наук, профессор; Падерно П.И., профессор каф., д-р техн. наук, профессор; Воробьев А.И., доцент каф., канд.техн.наук; Воронов Ю.В., доцент каф., канд. техн. наук, доцент; Выговский Л.С., доцент каф., канд. техн. наук; Дубенецкий В.А., доцент каф., канд. техн. наук, доцент; Егоров С.С., доцент каф., канд.техн.наук; Ильин В.П, доцент каф., канд. техн. наук, доцент; Клионский Д.М., доцент каф., канд. техн. наук; Назаренко Н.А., доцент каф., канд. техн. наук, доцент; Пирог В.П., доцент каф., канд. техн. наук, доцент; Соничев А.В., доцент каф., канд. техн. наук, доцент; Шеховцов О.И., доцент каф., канд. техн. наук, доцент; Шилов Н.Г., доцент каф., канд. техн. наук, доцент; Широков В.В., доцент каф., канд. техн. наук, доцент; Кузнецов А.Г., доцент каф., канд. техн. наук, доцент; Васильев Н.В., ассистент каф., канд.техн.наук; Щиголева М.А., доцент каф., канд. техн. наук, доцент; Вайчикаускас М.А, ассистент, аспирант;. Мондикова Я.А., ассистент, аспирант; Синев В.Е., ассистент; Коробкин В.П.,

ст.преподаватель каф. Присутствовали: Молдовян А.А., профессор каф. Информационной безопасности, д-р техн. наук, профессор; Молдовян Н.А., профессор каф. Информационной безопасности, д-р техн. наук, профессор; Воробьев В.И., профессор базовой кафедры Автоматизации исследований, Воробьев Е.Г., зав.каф. Информационной безопасности канд. техн. наук, доцент.

По результатам обсуждения принято следующее заключение:

1. Личное участие соискателя в получении результатов работы

Соискателем получены следующие результаты:

– Впервые предложен метод построения алгоритмов и протоколов, нарушение безопасности которых требует одновременного решения двух вычислительно сложных задач, отличающийся использованием задачи дискретного логарифмирования (ЗДЛ) по трудно факторизуемому модулю n, размер множителей которого выбирается таким образом, что, по крайней мере, решение ЗДЛ по модулю одного из делителей модуля имеет вычислительную сложность не ниже заданного уровня стойкости.

– На основе предложенного метода разработаны новые протоколы аутентификации объектов и субъектов информационных процессов, обладающие повышенным уровнем безопасности: протокол электронной цифровой подписи (ЭЦП), отличающийся использованием ЗДЛ по трудно факторизуемому модулю специальной структуры, благодаря чему достигнуто снижение размера, вычислительной сложности процедур генерации и проверки ЭЦП; протокол коллективной ЭЦП, отличающийся использованием ЗДЛ по трудно факторизуемому модулю специальной структуры, благодаря чему достигнуто снижение размера, вычислительной сложности процедур генерации и проверки ЭЦП; протокол утверждаемой групповой ЭЦП, отличающийся использованием ЗДЛ по трудно факторизуемому модулю специальной структуры и механизма маскирования ключей, благодаря чему руководитель и только он может доказывать стороннему проверяющему список лиц, которые подписывали документ, без

разглашения секретных ключей подчинённых и своего собственного; протокол интерактивной аутентификации субъекта, отличающийся использованием ЗДЛ по трудно факторизуемому модулю n специальной структуры; протокол двухшаговой аутентификации субъекта, отличающийся использованием ЗДЛ по трудно факторизуемому модулю специальной структуры и элемента выделенной подгруппы мультипликативной группы кольца вычетов по модулю n в качестве запроса, благодаря чему достигнута возможность безопасной аутентификации субъекта за два шага.

– На основе предложенного метода разработаны новые протоколы защиты информации, обладающие повышенным уровнем безопасности: протоколы обмена ключами, отличающиеся использованием ЗДЛ по трудно факторизуемому модулю специальной структуры и рандомизирующего параметра, благодаря чему обеспечивается случайность значения ключа, формируемого в ходе протокола; протокол защитного преобразования информации, отличающийся использованием ЗДЛ по трудно факторизуемому модулю специальной структуры; протокол коммутативного защитного преобразования информации, отличающийся использованием ЗДЛ по трудно факторизуемому модулю специальной структуры и механизма расщепления сообщений, благодаря чему обеспечивается возможность выполнения защитных преобразований для произвольных сообщений; протокол стойкого защитного преобразования информации с использованием ключа малого размера, отличающийся использованием ЗДЛ по трудно факторизуемому модулю специальной структуры и процедуры бесключевого защитного преобразования совместно с аутентификацией по коротким ключам, благодаря чему возможно задать необходимую стойкость протокола, для малых длин ключа.

– На основе предложенного метода разработаны новые протоколы обеспечения анонимности, обладающие повышенным уровнем безопасности: протокол слепой ЭЦП, отличающийся использованием ЗДЛ по трудно факторизуемому модулю специальной структуры, благодаря чему

достигнуто снижение размера, вычислительной сложности процедур генерации и проверки ЭЦП; протокол слепой коллективной ЭЦП, отличающийся использованием ЗДЛ по трудно факторизуемому модулю специальной структуры, благодаря чему достигнуто снижение размера, вычислительной сложности процедур генерации и проверки ЭЦП.

– Впервые предложен метод построения алгоритмов и протоколов, нарушение безопасности которых требует одновременного решения двух вычислительно сложных задач, отличающийся использованием задачи дискретного логарифмирования (ЗДЛ) по трудно факторизуемому модулю n, размер множителей которого выбирается таким образом, что, по крайней мере, решение ЗДЛ по модулю одного из делителей модуля имеет вычислительную сложность не ниже заданного уровня стойкости.

2. Достоверность полученных результатов работы

Достоверность полученных результатов работы подтверждается строгими математическими доказательствами, обеспечивается анализом состояния исследований в этой области на сегодняшний день, и апробацией основных результатов на конференциях различного уровня.

3. Научная новизна работы:

– Впервые предложен метод построения алгоритмов и протоколов, нарушение безопасности которых требует одновременного решения двух вычислительно сложных задач, отличающийся использованием задачи дискретного логарифмирования (ЗДЛ) по трудно факторизуемому модулю n, размер множителей которого выбирается таким образом, что, по крайней мере, решение ЗДЛ по модулю одного из делителей модуля имеет вычислительную сложность не ниже заданного уровня стойкости.

– На основе предложенного метода разработаны новые протоколы аутентификации объектов и субъектов информационных процессов, обладающие повышенным уровнем безопасности: протокол электронной цифровой подписи (ЭЦП), отличающийся использованием ЗДЛ по трудно

факторизуемому модулю специальной структуры, благодаря чему достигнуто снижение размера, вычислительной сложности процедур генерации и проверки ЭЦП; протокол коллективной ЭЦП, отличающийся использованием ЗДЛ по трудно факторизуемому модулю специальной структуры, благодаря чему достигнуто снижение размера, вычислительной сложности процедур генерации и проверки ЭЦП; протокол утверждаемой групповой ЭЦП, отличающийся использованием ЗДЛ по трудно факторизуемому модулю специальной структуры и механизма маскирования ключей, благодаря чему руководитель и только он может доказывать стороннему проверяющему список лиц, которые подписывали документ, без разглашения секретных ключей подчинённых и своего собственного; протокол интерактивной аутентификации субъекта, отличающийся использованием ЗДЛ по трудно факторизуемому модулю n специальной структуры; протокол двухшаговой аутентификации субъекта, отличающийся использованием ЗДЛ по трудно факторизуемому модулю специальной структуры и элемента выделенной подгруппы мультипликативной группы кольца вычетов по модулю n в качестве запроса, благодаря чему достигнута возможность безопасной аутентификации субъекта за два шага.

– На основе предложенного метода разработаны новые протоколы защиты информации, обладающие повышенным уровнем безопасности: протоколы обмена ключами, отличающиеся использованием ЗДЛ по трудно факторизуемому модулю специальной структуры и рандомизирующего параметра, благодаря чему обеспечивается случайность значения ключа, формируемого в ходе протокола; протокол защитного преобразования информации, отличающийся использованием ЗДЛ по трудно факторизуемому модулю специальной структуры; протокол коммутативного защитного преобразования информации, отличающийся использованием ЗДЛ по трудно факторизуемому модулю специальной структуры и механизма расщепления сообщений, благодаря чему обеспечивается возможность выполнения защитных преобразований для произвольных

сообщений; протокол стойкого защитного преобразования информации с использованием ключа малого размера, отличающийся использованием ЗДЛ по трудно факторизуемому модулю специальной структуры и процедуры бесключевого защитного преобразования совместно с аутентификацией по коротким ключам, благодаря чему возможно задать необходимую стойкость протокола, для малых длин ключа.

– На основе предложенного метода разработаны новые протоколы обеспечения анонимности, обладающие повышенным уровнем безопасности: протокол слепой ЭЦП, отличающийся использованием ЗДЛ по трудно факторизуемому модулю специальной структуры, благодаря чему достигнуто снижение размера, вычислительной сложности процедур генерации и проверки ЭЦП; протокол слепой коллективной ЭЦП, отличающийся использованием ЗДЛ по трудно факторизуемому модулю специальной структуры, благодаря чему достигнуто снижение размера, вычислительной сложности процедур генерации и проверки ЭЦП.

– Впервые предложен метод построения алгоритмов и протоколов, нарушение безопасности которых требует одновременного решения двух вычислительно сложных задач, отличающийся использованием задачи дискретного логарифмирования (ЗДЛ) по трудно факторизуемому модулю n, размер множителей которого выбирается таким образом, что, по крайней мере, решение ЗДЛ по модулю одного из делителей модуля имеет вычислительную сложность не ниже заданного уровня стойкости.

4. Практическая значимость работы

Практическая значимость определяется тем, что разработанные протоколы аутентификации, алгоритмы защитных преобразований информации и протоколы обеспечения анонимности, обеспечивающие повышенный уровень безопасности, имеют широкое применение в информационно-телекоммуникационных технологиях.

5. Ценность научных исследований соискателя

Теоретическая значимость работы определяется тем, что предложен новый подход к построению алгоритмов и протоколов, имеющих повышенный уровень безопасности, свободный от недостатков существующих аналогов.

6. Утверждение темы диссертации

Тема диссертации утверждена советом факультета компьютерных технологий и информатики СПбГЭТУ «ЛЭТИ», протокол № 8 от 15 октября 2015 г.

7. Специальность, которой соответствует диссертация

Диссертация соответствует специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность» - п.п. 5, 11, 13 раздела 2 «Области исследования» паспорта специальности: «Методы и средства (комплексы средств) информационного противодействия угрозам нарушения информационной безопасности в открытых компьютерных сетях, включая Интернет»; «Технологии идентификации и аутентификации пользователей и субъектов информационных процессов. Системы разграничения доступа»; «Принципы и решения (технические, математические, организационные и др.) по созданию новых и совершенствованию существующих средств защиты информации и обеспечения информационной безопасности».

8. Отличие полученных в работе результатов от результатов, полученных в работах других авторов

– Впервые предложен метод построения алгоритмов и протоколов, нарушение безопасности которых требует одновременного решения двух вычислительно сложных задач, отличающийся использованием задачи дискретного логарифмирования (ЗДЛ) по трудно факторизуемому модулю n, размер множителей которого выбирается таким образом, что, по крайней мере, решение ЗДЛ по модулю одного из делителей модуля имеет вычислительную сложность не ниже заданного уровня стойкости.

– На основе предложенного метода разработаны новые протоколы аутентификации объектов и субъектов информационных процессов, обладающие повышенным уровнем безопасности: протокол электронной цифровой подписи (ЭЦП), отличающийся использованием ЗДЛ по трудно факторизуемому модулю специальной структуры, благодаря чему достигнуто снижение размера, вычислительной сложности процедур генерации и проверки ЭЦП; протокол коллективной ЭЦП, отличающийся использованием ЗДЛ по трудно факторизуемому модулю специальной структуры, благодаря чему достигнуто снижение размера, вычислительной сложности процедур генерации и проверки ЭЦП; протокол утверждаемой групповой ЭЦП, отличающийся использованием ЗДЛ по трудно факторизуемому модулю специальной структуры и механизма маскирования ключей, благодаря чему руководитель и только он может доказывать стороннему проверяющему список лиц, которые подписывали документ, без разглашения секретных ключей подчинённых и своего собственного; протокол интерактивной аутентификации субъекта, отличающийся использованием ЗДЛ по трудно факторизуемому модулю n специальной структуры; протокол двухшаговой аутентификации субъекта, отличающийся использованием ЗДЛ по трудно факторизуемому модулю специальной структуры и элемента выделенной подгруппы мультипликативной группы кольца вычетов по модулю n в качестве запроса, благодаря чему достигнута возможность безопасной аутентификации субъекта за два шага.

– На основе предложенного метода разработаны новые протоколы защиты информации, обладающие повышенным уровнем безопасности: протоколы обмена ключами, отличающиеся использованием ЗДЛ по трудно факторизуемому модулю специальной структуры и рандомизирующего параметра, благодаря чему обеспечивается случайность значения ключа, формируемого в ходе протокола; протокол защитного преобразования информации, отличающийся использованием ЗДЛ по трудно факторизуемому модулю специальной структуры; протокол коммутативного

защитного преобразования информации, отличающийся использованием ЗДЛ по трудно факторизуемому модулю специальной структуры и механизма расщепления сообщений, благодаря чему обеспечивается возможность выполнения защитных преобразований для произвольных сообщений; протокол стойкого защитного преобразования информации с использованием ключа малого размера, отличающийся использованием ЗДЛ по трудно факторизуемому модулю специальной структуры и процедуры бесключевого защитного преобразования совместно с аутентификацией по коротким ключам, благодаря чему возможно задать необходимую стойкость протокола, для малых длин ключа.

– На основе предложенного метода разработаны новые протоколы обеспечения анонимности, обладающие повышенным уровнем безопасности: протокол слепой ЭЦП, отличающийся использованием ЗДЛ по трудно факторизуемому модулю специальной структуры, благодаря чему достигнуто снижение размера, вычислительной сложности процедур генерации и проверки ЭЦП; протокол слепой коллективной ЭЦП, отличающийся использованием ЗДЛ по трудно факторизуемому модулю специальной структуры, благодаря чему достигнуто снижение размера, вычислительной сложности процедур генерации и проверки ЭЦП.

– Впервые предложен метод построения алгоритмов и протоколов, нарушение безопасности которых требует одновременного решения двух вычислительно сложных задач, отличающийся использованием задачи дискретного логарифмирования (ЗДЛ) по трудно факторизуемому модулю n, размер множителей которого выбирается таким образом, что, по крайней мере, решение ЗДЛ по модулю одного из делителей модуля имеет вычислительную сложность не ниже заданного уровня стойкости.

9. Полнота изложения материалов диссертации

Основные положения диссертации достаточно полно изложены в 25 научных публикациях, в том числе 5 работ опубликованы в изданиях,

входящих в перечень ведущих рецензируемых научных журналов и изданий Российской Федерации.

Публикации в журналах из Перечня ведущих рецензируемых научных журналов и изданий ВАК Российской Федерации:

1) Березин А.Н., Молдовян Н. А., Латышев Д. М. Протокол 240–битовой коллективной подписи над нециклической конечной группой // Вопросы защиты информации.— 2013.— № 3.— С. 81–85.

2) Березин А.Н., Молдовян Н. А. Построение криптосхем на основе задачи дискретного логарифмирования по трудно разложимому модулю // Известия СПбГЭТУ «ЛЭТИ».— 2013.— № 7.— С. 54–59.

3) Березин А.Н., Молдовян Н. А., Щербаков В.А. Общий метод построения криптосхем, основанных на трудности одновременного решения задач факторизации и дискретного логарифмирования // Вопросы защиты информации.— 2014.— №2.— С. 3–11.

4) Березин А.Н., Молдовян Н.А., Рыжков А.В. Коммутативные шифры на основе трудности одновременного решения задач факторизации и дискретного логарифмирования // Информационно управляющие системы.— 2014.— №4.— С. 106–110.

5) Березин А.Н. Протокол стойкого шифрования по ключу малого размера, взлом которого требует решения задач факторизации и дискретного логарифмирования // Вопросы защиты информации. — 2016. — № 2. — С. 3-8.

Другие публикации по теме диссертации:

1) Berezin A.N., Moldovyan N.A., Shcherbakov V.A. Cryptoschemes Based on Difficulty of Simultaneous Solving Two Different Difficult Problems // Computer Science Journal of Moldova.— 2013.— V. 21.— № 2(62).— P. 280–290.

2) Березин А.Н., Биричевский А.Р., Молдовян Н.А. Особенности задачи дискретного логарифмирования по составному модулю как криптографического примитива // Труды VII Санкт–Петербургской

межрегиональной конференции «Информационная безопасность регионов России (ИБРР–2011)».— Санкт–Петербург, 26–28 октября 2012 г. / СПб.: СПОИСУ, 2012.— С. 104–108.

3) Березин А.Н., Васильев И.Н., Молдовян Н.А. Обоснование криптосхем на основе задачи дискретного логарифмирования по трудно разложимому модулю// 65–я научно–техническая конференция профессорско–преподавательского состава университета.— Санкт-Петербург, 24 января – 4 февраля 2012 г. / Труды конференции.— СПб.:СПбГЭТУ «ЛЭТИ», 2012.— С. 120–124.

4) Березин А.Н., Демьянчук А.А., Молдовян Д.Н., Рыжков А. В. Протоколы аутентификации с нулевым разглашением секрета: приложения, повышение безопасности и новые реализации // XIII Санкт–Петербургская международная конференция «Региональная информатика – 2012»,— Санкт–Петербург, 24–26 октября 2012 г. / Труды конференции.— СПб.:СПОИСУ, 2013.— С. 82–83.

5) Березин А.Н. Подходы к построению криптосхем на основе трудности одновременного решения задач факторизации и дискретного логарифмирования // Инновационная деятельность в Вооруженных силах Российской Федерации: Труды всеармейской научно-практической конференции.— Санкт-Петербург, 21-22 ноября 2013 г. / СПб.:ВАС, 2013.— С. 72–76.

6) Березин А.Н. Подходы к повышению безопасности криптографических алгоритмов и протоколов // 68–я научно–техническая конференция профессорско–преподавательского состава университета.— Санкт-Петербург, 28 января – 5 февраля 2015 г. / Труды конференции.— СПб.:СПбГЭТУ «ЛЭТИ», 2015. С.— 105–108.

7) Березин А.Н., Хо Н.З., Синев В.Е. Методические аспекты обоснования задачи дискретного логарифмирования по трудно разложимому модулю в дисциплине «Криптографические протоколы» // XVIII международная научно–методическая конференция «Современное образование: содержание,

технологии, качество».— Санкт–Петербург, 18 апреля 2012 г. / Материалы конференции.— Т. 1.— СПб.:СПбГЭТУ «ЛЭТИ», 2012.— С. 246–248.

8) Березин А.Н., Демьянчук А.А., Краснова А.И. Протоколы с нулевым разглашением на основе трудности вычисления порядка элементов конечной группы // XIII Санкт–Петербургская международная конференция «Региональная информатика – 2012».— Санкт–Петербург, 24–26 октября 2012 г. / Материалы конференции.— СПб.:СПОИСУ, 2012.— С. 82–83.

9) Березин А.Н., Рыжков А.В. Подход к повышению безопасности процедуры коммутативного шифрования // XIII Санкт–Петербургская международная конференция «Региональная информатика – 2012».— Санкт–Петербург, 24–26 октября 2012 г. / Материалы конференции.— СПб.:СПОИСУ, 2012.— С. 123.

10) Березин А.Н., Демьянчук А.А., Кишмар Р.В. Двухпроходные протоколы аутентификации с нулевым разглашением // XIII Санкт–Петербургская международная конференция «Региональная информатика – 2012».— Санкт–Петербург, 24–26 октября 2012 г. / Материалы конференции.— СПб.:СПОИСУ, 2012.— С. 89.

11) Березин А.Н., Демьянчук А.А. Расширенное изложение протоколов с нулевым разглашением секрета в дисциплине “Криптографические протоколы” // XIX международная научно–методическая конференция «Современное образование: содержание, технологии, качество».— Санкт–Петербург, 24 апреля 2013 / Материалы конференции.— Т. 1.— СПб.:СПбГЭТУ «ЛЭТИ», 2013.— С. 138–140.

12) Березин А.Н. Подходы к построению криптосхем на основе задач факторизации и дискретного логарифмирования // Материалы VIII СПб межрегиональная конференция «Информационная безопасность регионов России (ИБРР-2013)».— Санкт–Петербург, 23-25 октября 2013 / СПб.:СПОИСУ, 2013.— С. 80–81.

13) Березин А.Н. Варианты задачи дискретного логарифмирования по составному модулю // Материалы VIII СПб межрегиональная конференция

«Информационная безопасность регионов России (ИБРР-2013)».— Санкт–Петербург, 23-25 октября 2013 г. / СПб.:СПОИСУ, 2013.— С. 81–82.

14) Березин А.Н., Демьянчук А.А., Рыжков А.В. Протоколы с нулевым разглашением, использующие алгоритмы открытого шифрования // Материалы VIII СПб межрегиональная конференция «Информационная безопасность регионов России (ИБРР-2013)».— Санкт–Петербург, 23-25 октября 2013 г. / СПб.:СПОИСУ, 2013.— С. 82–83.

15) Березин А.Н. Новый способ повышения уровня безопасности криптографических механизмов обеспечения информационной безопасности // Восемнадцатая Санкт-Петербургская ассамблея молодых учёных и специалистов.— Санкт-Петербург, 13 декабря 2013 г. / СПб.:ЦОП РГГМУ, 2013.— С. 34.

16) Березин А.Н. Коммутативные шифры на основе двух трудных задач // XIV Санкт–Петербургская международная конференция «Региональная информатика – 2014».— Санкт–Петербург, 29–31 октября 2014 г. / Материалы конференции.— СПб.:СПОИСУ, 2014.— С. 121–122.

17) Березин А.Н. Расширение типов криптографических схем с повышенным уровнем безопасности // 19 Санкт-Петербургская ассамблея молодых учёных и специалистов.— Санкт-Петербург, 21 декабря 2014 г. / СПб.:ЦОП РГГМУ, 2014— С. 211 .

18) Березин А.Н. Протоколы стойкого шифрования по ключу малого размера, основанные на коммутативных преобразованиях // 20 Санкт-Петербургская ассамблея молодых учёных и специалистов.— Санкт-Петербург, 18 декабря 2014 г. / СПб.:ЦОП РГГМУ.— С. 41.

19) Березин А.Н., Галанов А.И., Синев В.Е. Протокол утверждаемой групповой цифровой подписи на основе двух трудных задач // Информационная безопасность регионов России (ИБРР-2015). IX Санкт-Петербургская межрегиональная конференция.— Санкт-Петербург, 28-30 октября 2015 г. / Материалы конференции.— СПб.:СПОИСУ, 2015.— С. 101-102.

20) Березин А.Н., Молдовян Н.А., Муравьев А.В. Протокол шифрования на основе двух трудных задач по ключу малого размера // Информационная безопасность регионов России (ИБРР-2015). IX Санкт-Петербургская межрегиональная конференция.— Санкт-Петербург, 28-30 октября 2015 г. / Материалы конференции.— СПб.:СПОИСУ, 2015.— С. 116-117.

Соответствие диссертации и документов требованиям ВАК

Диссертация и документы оформлены в соответствии с требованиями п. 9 «Положения о присуждении ученых степеней», утвержденного Постановлением Правительства Российской Федерации от 24.09.2013 №842 и требованиями Приложений 2, 3, 4 «Положения о совете по защите диссертаций на соискание ученой степени кандидата наук, на соискание ученой степени доктора наук», утвержденного Приказом Министерства образования и науки Российской Федерации от 13.01.2014 № 7. Содержание диссертации соответствует требованиям норм Закона РФ «О средствах массовой информации» (Закон о СМИ) от 27.12.1991 № 2124-1 в части, касающейся отсутствия призывов к экстремизму и терроризму и ненормативной лексики. В содержании диссертации отсутствует государственная и иная охраняемая законом тайна.

10. Выводы, заключение

На основании вышеизложенного следует сделать вывод о том, что диссертационное исследование Березина А.Н. «Методы повышения уровня безопасности защитных преобразований информации» выполнено на актуальную тему и представляет законченную научно-квалификационную работу, в которой содержится решение научной задачи разработки совокупности алгоритмов и протоколов аутентификации, обеспечения конфиденциальности и анонимности, основанных на задачах дискретного логарифмирования и факторизации, имеющей существенное значение для повышения уровня информационной безопасности информационно-телекоммуникационных технологий, базирующихся на алгоритмах и протоколах такого типа.

Диссертация «Методы повышения уровня безопасности защитных преобразований информации» Березина Андрея Николаевича рекомендуется к защите на соискание ученой степени кандидата технических наук по специальности 05.13.19 – Методы и системы защиты информации, информационная безопасность.

Заключение принято на заседании кафедры автоматизированных систем обработки информации и управления СПбГЭТУ «ЛЭТИ».

Присутствовали на заседании 35 чел. Результаты голосования: «за» - 35 чел., «против» – 0 чел., «воздержалось» - 0 чел., протокол № 7 от 14 июня 2016 г.

Сведения о составителях заключения

Цехановский Владислав Влади...