ЗАКЛЮЧЕНИЕ ДИССЕРТАЦИОННОГО СОВЕТА Д 002.199.01 НА БАЗЕ ФЕДЕРАЛЬНОГО ГОСУДАРСТВЕННОГО БЮДЖЕТНОГО УЧРЕЖДЕНИЯ НАУКИ САНКТ-ПЕТЕРБУРГСКОГО ИНСТИТУТА ИНФОРМАТИКИ И АВТОМАТИЗАЦИИ РОССИЙСКОЙ АКАДЕМИИ НАУК ПО ДИССЕРТАЦИИ НА СОИСКАНИЕ УЧЕНОЙ СТЕПЕНИ КАНДИДАТА НАУК

аттестационное дело № _____

решение диссертационного совета 09.02.2017 г. № 3

О присуждении Березину Андрею Николаевичу, гражданину Российской Федерации, ученой степени кандидата технических наук.

Диссертация «Методы повышения уровня безопасности защитных преобразований информации» по специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность» принята к защите 24 ноября 2016 г., протокол № 3 диссертационным советом Д 002.199.01 на базе Федерального государственного бюджетного учреждения науки Санкт-Петербургского института информатики и автоматизации Российской академии наук, 199178, Россия, Санкт-Петербург, 14 линия ВО, дом 39, утвержден приказом Рособрнадзора номер 2472-618 от 8 октября 2010 года.

Соискатель Березин Андрей Николаевич, 1988 года рождения, в 2012 г. с отличием окончил Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина) по специальности «Компьютерная безопасность» (диплом № ВСА 1120480), в 2016 г. окончил очную аспирантуру в Федеральном государственном автономном образовательном учреждении высшего образования «Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)» (СПбГЭТУ «ЛЭТИ»). Удостоверение о сдаче кандидатских экзаменов № 04-03, выдано в 2016 г. Федеральным государственным автономным образовательным учреждением высшего образования «Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)» (СПбГЭТУ «ЛЭТИ»). В настоящее время Березин Андрей Николаевич работает заведующим лабораторией на кафедре «Информационная безопасность» в Федеральном государственном автономном

образовательном учреждении высшего образования «Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)» (СПбГЭТУ «ЛЭТИ»).

Диссертация выполнена на кафедре автоматизированных систем обработки информации и управления Федерального государственного автономного образовательного учреждения высшего образования «Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)» (СПбГЭТУ «ЛЭТИ») Министерства образования и науки Российской Федерации.

Научный руководитель – доктор технических наук, профессор МОЛДОВЯН Николай Андреевич, основное место работы: Федеральное государственное бюджетное учреждение науки Санкт-Петербургский институт информатики и автоматизации Российской академии наук (СПИИРАН), заведующий лабораторией криптологии.

Официальные оппоненты:

КОРЖИК Валерий Иванович, доктор технических наук, профессор, Федеральное государственное образовательное бюджетное учреждение высшего профессионального образования «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича», Почётный профессор СПбГУТ;

ЛЕВИНА Алла Борисовна, кандидат физико-математических наук, доцент, Федеральное государственное образовательное бюджетное учреждение высшего образования «Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики», кафедра безопасных информационных технологий, доцент дали положительные отзывы на диссертацию.

Ведущая организация – акционерное общество «Научно-исследовательский институт «ВЕКТОР», г. Санкт-Петербург в своем положительном заключении, подписанном Емелиным Вадимом Ивановичем, доктором технических наук, старшим научным сотрудником, главным научным сотрудником АО «НИИ «Вектор», Морозовой Еленой Владимировной, кандидатом технических наук, доцентом, учёным секретарём Научно-технического Совета АО «НИИ «Вектор» и утвержденном Петкау Олегом Гергардовичем, кандидатом технических наук, доцентом, директором АО

«НИИ «Вектор», указала, что в целом диссертационная работа А.Н. Березина представляет собой завершенную научно-исследовательскую работу, выполненную на актуальную тему, отличается научной новизной и практической значимостью полученных результатов. Автором в диссертации сформулирована и решена важная научно-техническая задача разработки методов и алгоритмов защиты информации в процессе её сбора, хранения, обработки, передачи и распространения.

Соискателем предложен метод построения алгоритмов и протоколов защитных преобразований, повышенный уровень безопасности которых обеспечивается тем, что для их взлома требуется одновременно решить задачи дискретного логарифмирования и факторизации, разработаны протоколы локальной и удалённой аутентификации пользователей, объектов и субъектов информационных процессов, обладающие повышенным уровнем безопасности, предложены протоколы обеспечения конфиденциальности информации, передаваемой по открытым каналам связи, обладающие повышенным уровнем безопасности, разработаны протоколы обеспечения анонимности в открытых компьютерных сетях, обладающие повышенным уровнем безопасности. Текст автореферата полностью соответствует содержанию диссертации. Диссертационное исследование «Методы повышения уровня безопасности защитных преобразований информации» является научно-квалификационной работой и соответствует критериям, изложенным в п. 9 “Положения о присуждении ученых степеней”, утвержденного постановлением Правительства Российской Федерации № 842 от 24 сентября 2013 г., предъявляемых к кандидатским диссертациям, а его автор Березин Андрей Николаевич заслуживает присуждения ученой степени кандидата технических наук по специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность».

Соискатель имеет 48 опубликованных работ, в том числе по теме диссертации 25 работ, опубликованных в рецензируемых научных изданиях 10 работ, из них опубликованных в изданиях, рекомендуемых ВАК РФ – 8.

Основные научные результаты опубликованы в 25 научных трудах общим объемом 5,25 п.л., из которых 5 статей объемом 2,61 п.л., выполнены в соавторстве, а 1 статья объемом 0,56 п.л. – лично. Наиболее значимые работы по теме диссертации:

1. **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.

2. **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. *Личный вклад соискателя – 35%.*
3. **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. *Личный вклад соискателя – 65%.*
4. **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. *Личный вклад соискателя – 65%.*
5. **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. *Личный вклад соискателя – 35%.*
6. **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. *Личный вклад соискателя – 65%.*

Оригинальность содержания диссертации составляет не менее 85% от общего объёма текста; цитирование оформлено корректно; заимствованного материала, использованного в диссертации без ссылки на автора либо источник заимствования, не обнаружено; научных работ, выполненных соискателем учёной степени в соавторстве без ссылок на соавторов не выявлено.

На автореферат диссертации поступило 7 отзывов, все отзывы положительны:

1) Санкт-Петербургский филиал Федерального государственного бюджетного учреждения науки Института земного магнетизма, ионосферы и распространения радиоволн им. Н.В. Пушкова Российской академии наук. Отзыв составил заместитель директора по науке, д.т.н., профессор Коробейников А.Г. Замечания: Текст автореферата не позволяет полностью оценить все достоинства и недостатки разработанных протоколов. В частности протокол утверждаемой групповой подписи описан излишне кратко, хотя он представляется весьма интересным с практической точки зрения. Обозначения, используемые при описании разработанных протоколов, раскрыты недостаточно полно.

2) ФГБОУ ВО «Петербургский государственный университет путей сообщения Императора Александра I». Отзыв составил доцент кафедры «Информатика и информационная безопасность», к.т.н., доцент Глухарёв М. Л. Замечания: В Таблице 1 автореферата приведены оценки интегрального параметра безопасности, но нигде не поясняется, откуда берутся значения вероятности появления прорывных алгоритмов решения вычислительно задач, положенных в основу разработанных алгоритмов и протоколов.

3) ФГБОУ ВО ГУМРФ имени адмирала С.О. Макарова. Отзыв составил профессор кафедры «Комплексное обеспечение информационной безопасности», д.т.н., профессор Гаскаров В.Д. Замечания: недостаточно полно освещены потенциально возможные атаки на разработанные протоколы; некоторые из разработанных протоколов упомянуты в автореферате, но не описаны, например, протокол интерактивной аутентификации.

4) Федеральное государственное казённое военное образовательное учреждение высшего образования «Академия Федеральной службы охраны Российской Федерации». Отзыв составили сотрудники к.т.н., доцент Цибуля А.Н., к.т.н. Казачок А.В. Замечания: В автореферате в явном виде не представлена оценка степени достижения цели исследования – повышения уровня информационной безопасности информационно-телекоммуникационных технологий. При сравнении характеристик разработанных протоколов с аналогами основным критерием выступает трудоёмкость, что, в свою очередь, не в полной мере согласуется с темой диссертационного исследования. Возможно, следовало бы произвести оценку повышения уровня безопасности разработанных защитных преобразований. В таблице 1 автореферата при $P_{ЗФ}=P_{ЗДЛ}=10^{-32}$ по формуле должно быть равно$2*10^{-102}$.

5) ООО «СКАРТЕЛ». Отзыв составил директор по информационной безопасности и защите от мошенничества, к.т.н., Костин А.А. Замечания: В автореферате используются нестандартные обозначения, для которых не приводятся пояснения, что затрудняет разбор предложенных протоколов.

6) ООО «СофИТ лабс». Отзыв составил генеральный директор, к.т.н., Никехин А.А. Замечания: используемая формула интегрального показателя безопасности протоколов, поясняющая смысл понятия уровня безопасности использования

протоколов защитных преобразований, не учитывает вероятность появления в ближайшем будущем вычислительных технологий, реализуемых с помощью квантовых компьютеров.

7) ЗАО «АСИС». Отзыв составил генеральный директор, к.т.н., доцент Солодянников А.В. Замечания: В автореферате используется термин «электронная цифровая подпись», на момент защиты диссертации являющийся устаревшим. Задачей исследования, как следует из автореферата, была разработка методов и алгоритмов защиты информации на этапах ее сбора, обработки, хранения, передачи и распространения. Далее в автореферате не рассмотрено: имеются ли отличия в применении разработанных алгоритмов на всех указанных этапах жизненного цикла информации. В цели работы в автореферате указано повышение уровня информационной безопасности информационно-телекоммуникационных технологий (ИТКТ), но не приведены критерии, в соответствии с которыми проводилась оценка. В автореферате наблюдается ряд ошибок орфографического и оформительского характера (неоднородное форматирование, использование формул в тексте, оформление таблиц и рисунков).

Выбор официальных оппонентов и ведущей организации обосновывается тем, что д.т.н., профессор Коржик В.И. является известным ученым в области методов кодирования и защиты информации, теории передачи сигналов, общей теории связи; к.ф.-м.н., доцент, Левина А.Б. – известный специалист в области математических методов защиты информации; ведущая организация, акционерное общество «Научно-исследовательский институт «ВЕКТОР», является известной как в России, так и за рубежом организацией в области разработки и создания систем защиты информации, составляющей государственную тайну, а также защиты конфиденциальной информации.

Диссертационный совет отмечает, что на основании выполненных соискателем исследований:

разработаны оригинальные протоколы обеспечения конфиденциальности, аутентификации и анонимности, отличающиеся использованием задачи дискретного логарифмирования по трудно факторизуемому модулю;

предложены:

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;

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;

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 стойкость протокола, для малых длин ключа;

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;

доказана перспективность использования предложенного метода для построения различного типа протоколов, безопасность которых основана на двух вычислительно трудных задачах факторизации и дискретного логарифмирования;

введены:

- новые типы протоколов обеспечения информационной безопасности, основанные на вычислительной сложности одновременного решения задачи факторизации и задачи дискретного логарифмирования;
- требования к выбору параметров протоколов защитных преобразований, основанных на вычислительной сложности задачи дискретного логарифмирования по трудно факторизуемому модулю;

Теоретическая значимость исследования обоснована тем, что:

доказаны сформулированные в работе теоретические утверждения с использованием формальных математических доказательств. Эти утверждения составляют основу процесса построения алгоритмов и протоколов, взлом которых требует одновременного решения двух независимых вычислительно трудных задач;

применительно к проблематике диссертации результативно (эффективно, то есть с получением обладающих новизной результатов)

использованы аппарат и методы алгебры, теории вероятности, дискретной математики, теории чисел, теории сложности и информационной безопасности;

изложены методологические и методические основы использования задачи дискретного логарифмирования по труднофакторизуемому модулю для построения алгоритмов и протоколов защитных преобразований информации;

раскрыты

проблемные аспекты применения имеющихся подходов в области синтеза алгоритмов и протоколов, безопасность которых основана на нескольких вычислительно трудных задачах;

основные вопросы, связанные с универсальностью и применимостью протоколов защитных преобразований различных типов, основанных одновременно на вычислительной трудности задачи факторизации и вычислительной трудности задачи дискретного логарифмирования;

сводимость решения задачи дискретного логарифмирования по трудно факторизуемому модулю к одновременному решению задачи факторизации и задачи дискретного логарифмирования как обоснование универсального метода построения протоколов защитных преобразований, основанных на двух вычислительно трудных задачах;

изучены существующие методы построения алгоритмов и протоколов защитных преобразований информации, безопасность которых основана на двух вычислительно трудных задачах факторизации и дискретного логарифмирования по простому модулю, при этом отдельное внимание уделено рассмотрению вопросов анализа безопасности их применения;

проведена модернизация существующих методов построения алгоритмов и протоколов защитных преобразований информации, основанных на задаче дискретного логарифмирования по простому модулю.

Значение полученных соискателем результатов исследования для практики подтверждается тем, что:

разработаны и внедрены (указать степень внедрения) следующие результаты диссертационной работы:

• метод построения алгоритмов и протоколов для применения в средствах защиты информации, обладающих повышенным уровнем безопасности, который позволит расширить виды алгоритмов и протоколов указанного типа;

• протоколы локальной и удалённой аутентификации пользователей, объектов и субъектов информационных процессов, обладающие повышенным уровнем безопасности;

• протоколы обеспечения конфиденциальности информации, передаваемой по открытым каналам связи, обладающие повышенным уровнем безопасности;

• протоколы обеспечения анонимности в открытых компьютерных сетях, обладающие повышенным уровнем безопасности;

внедрены в учебный процесс на кафедрах «Информационная безопасность» СПбГЭТУ «ЛЭТИ» при подготовке специалистов по специальности 09.03.01 "Компьютерная безопасность", «Комплексное обеспечение информационной безопасности» государственного университета морского и речного флота имени адмирала С.О. Макарова при подготовке бакалавров по направлению 10.03.01 — «Информационная безопасность» для чтения лекций, проведения лабораторных работ и практических занятий, связанных с методами и средствами защиты информации;

• метод построения алгоритмов и протоколов, повышенный уровень безопасности которых обеспечивается тем, что для их взлома требуется одновременно решить задачи дискретного логарифмирования и факторизации;

• протоколы локальной и удалённой аутентификации пользователей, объектов и субъектов информационных процессов, обладающие повышенным уровнем безопасности;

• протоколы обеспечения конфиденциальности информации, передаваемой по открытым каналам связи, обладающие повышенным уровнем безопасности;

использованы при выполнении работ по теме «Новые способы, алгоритмы и применения отрицаемого шифрования для защиты информации в информационно-телекоммуникационных системах», выполненных по гранту РФФИ № 14-07- 00061 А в СПИИРАН;

определены возможности и перспективы практического использования полученных результатов диссертации при исследовании конкретных технологий обеспечения конфиденциальности, аутентификации и анонимности;

создан единый способ построения протоколов защитных преобразований информации, обладающих повышенным уровнем безопасности, позволяющий существенно расширить круг таких протоколов и устранить недостатки известного в литературе способа-аналога;

представлены предложения и направления для дальнейших научных исследований, в основу которых могут быть положены разработанные метод, алгоритмы и протоколы.

Оценка достоверности результатов исследования выявила:

достоверность полученных результатов подтверждена проведением всестороннего анализа работ по исследуемой проблеме, корректным применением научно-методического аппарата в виде использованных методов и теорий, апробацией основных результатов диссертации в печатных трудах и докладах на международных и всероссийских конференциях, положительными итогами практической реализации результатов работы;

теория построена на известных принципах, проверенных данных и фактах с использованием современных известных и апробированных методов исследования, согласуется с опубликованными частными результатами других исследователей;

идея базируется на анализе работ отечественных и зарубежных исследователей в области защитных преобразований информации, основанных на некоторых вычислительно сложных задачах;

использованы полученные характеристики для сравнения с данными, приведенными в современной научной литературе по защитным преобразованиям информации;

установлено качественное и количественное соответствие результатов решения задачи разработки методов и алгоритмов защиты информации в процессе её сбора, хранения, обработки, передачи и распространения. При этом подтверждено преимущество предложенного подхода перед результатами, полученными другими авторами.

Личный вклад соискателя состоит в:

- анализе современного состояния дел в области защитных преобразований информации, безопасность которых основана на двух вычислительно трудных задачах;
- исследовании и классифицировании существующих методов построения защитных преобразований информации, безопасность которых основана на двух вычислительно трудных задачах;
- постановке задачи разработки универсального метода построения защитных преобразований информации, безопасность которых основана на двух вычислительно трудных задачах факторизации и дискретного логарифмирования;
- разработке и обосновании универсального метода построения защитных преобразований информации, безопасность которых основана на двух вычислительно трудных задачах, с использованием задачи дискретного логарифмирования по трудно факторизуемому модулю;
- рассмотрением возможных атак на алгоритмы и протоколы, разработанные с использованием предложенного метода;
- разработке протоколов обеспечения конфиденциальности;
- разработке протоколов аутентификации;
- разработке протоколов обеспечения анонимности;
- исследовании предложенных методов и алгоритмов с использованием возможностей атакующих по решению вычислительно сложных задач и проведении расчёта основных показателей разработанных алгоритмов и протоколов;

- подготовке основных публикаций по выполненной работе.

Диссертационный совет считает, что Березин А.Н. в своей диссертационной работе решил научную задачу разработки методов и алгоритмов защиты информации в процессе её сбора, хранения, обработки, передачи и распространения, обладающих повышенным уровнем безопасности, имеющую важное социально-экономическое и хозяйственное значение.

На заседании 09.02.2017 г. диссертационный совет принял решение присудить Березину А.Н. ученую степень кандидата технических наук.

При проведении тайного голосования диссертационный совет в количестве 21 человека, из них 5 докторов наук по специальности рассматриваемой диссертации, участвовавших в заседании, из 26 человек, входящих в состав совета, проголосовали: за 21, против нет, недействительных бюллетеней нет.

Председатель диссертационного совета
доктор технических наук,
член-корреспондент РАН Юсупов Рафаэль Мидхатович

Ученый секретарь диссертационного совета
кандидат технических наук, доцент Фаткиева Роза Равильевна
09.02.2017 г.