ЗАКЛЮЧЕНИЕ ДИССЕРТАЦИОННОГО СОВЕТА Д 002.199.01, СОЗДАННОГО 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 21.12.2017 г. № 2

О присуждении Синеву Валерию Евгеньевичу, гражданину Российской Федерации, ученой степени кандидата технических наук.

Диссертация «Методы построения и разработка практичных протоколов групповой подписи и алгебраических алгоритмов защитных преобразований» по специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность» принята к защите 19 октября 2017 г., протокол № 2, 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 Синев Валерий Евгеньевич, 1983 года рождения, в 2008 г. окончил Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина) по специальности «Компьютерная безопасность» (диплом № ВСГ 2434551), в 2017 г. окончил очную аспирантуру в федеральном государственном автономном образовательном учреждении высшего образования «Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики» (Университет ИТМО). Справка о сдаче кандидатских экзаменов № 34, выдана в 2017 г. федеральным государственным автономным образовательным учреждением высшего образования «Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики» (Университет ИТМО). В настоящее время Синев Валерий Евгеньевич работает ведущим инженером-программистом в ООО «Дримкас».

Диссертация выполнена в федеральном государственном автономном образовательном учреждении высшего образования «Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики» (Университет ИТМО)) 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:

АЛЕКСАНДРОВА Елена Борисовна доктор технических наук, доцент, профессор кафедры «Информационная безопасность компьютерных систем» ФГАОУ ВО «Санкт-Петербургский политехнический университет Петра Великого»;

ТАТАРНИКОВА Татьяна Михайловна доктор технических наук, доцент, профессор кафедры безопасности информационных систем ФГАОУ ВО «Санкт-Петербургский государственный университет аэрокосмического приборостроения», дали положительные отзывы на диссертацию.

Ведущая организация – акционерное общество «Научно-исследовательский институт «ВЕКТОР», г.Санкт-Петербург в своем положительном отзыве, 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 В.Е. Синева 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: разработка практических протоколов групповой подписи и алгебраических алгоритмов защитных преобразований.

Соискателем предложен метод построения протоколов групповой и слепой электронной цифровой подписи (ЭЦП), повышенный уровень безопасности которых обеспечивается тем, что для их взлома требуется одновременно решить вычислительно сложные задачи дискретного логарифмирования и факторизации, протоколов и алгоритмов групповой ЭЦП новых типов – коллективной ЭЦП для групповых подписантов и комбинированной коллективной ЭЦП, разработаны протоколы локальной и удалённой аутентификации пользователей, объектов и субъектов информационных процессов, обладающие повышенным уровнем безопасности, предложен метод построения производительных алгебраических алгоритмов псевдовероятностного защитного преобразования и алгоритм на его основе, обеспечивающий защищенность конфиденциальной информации к атакам с принуждением к раскрытию ключа защитного преобразования. Текст автореферата полностью соответствует содержанию диссертации. Диссертационное исследование «Методы построения и разработка практичных протоколов групповой подписи и алгебраических алгоритмов защитных преобразований» 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 Синев Валерий Евгеньевич заслуживает присуждения ученой степени кандидата технических наук по специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность».

Основные результаты диссертации изложены в 14 публикациях, в том числе, в 5 статьях, опубликованных в ведущих рецензируемых журналах, входящих в перечень ВАК («Известия СПбГЭТУ “ЛЭТИ”», «Вопросы защиты информации», «Информационно управляющие системы»).

Список работ, опубликованных автором по теме диссертации в журналах, входящих в перечень ВАК:

1. **Синев В.Е.** Повышение уровня безопасности протокола групповой цифровой подписи, основанного на механизме маскирования открытых ключей // Известия СПбГЭТУ «ЛЭТИ». 2016. № 6. С. 21-25.

2. Молдовян А.А., Галанов А.И., **Синев В.Е.** Утверждаемая групповая подпись: новые протоколы // Вопросы защиты информации. 2016. № 2. С. 44-50.

3. Галанов А.И., Захаров Д.В., Молдовян Д.Н., **Синев В.Е.** Протоколы слепой подписи на основе двух вычислительно трудных задач // Вопросы защиты информации. 2009. № 4. С.2-7.

4. Доронин С.Е., Молдовян Н.А., **Синев В.Е.** Конечные расширенные поля для алгоритмов электронной цифровой подписи // Информационно-управляющие системы. 2009. № 1. С. 33- 40.

5. Доронин С.Е., Молдовяну П.А., **Синев В.Е.** Векторные конечные поля: задание умножения векторов большой четной размерности // Вопросы защиты информации. 2008. № 4(83). С.2-7.

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. Недостоверные сведения об опубликованных соискателем ученой степени работах в диссертации отсутствуют.

На автореферат диссертации поступило 7 отзывов, все отзывы положительные:

1) ФГБОУ ВО ГУМРФ имени адмирала С.О. Макарова. Отзыв составил профессор кафедры «Комплексное обеспечение информационной безопасности», д.т.н., профессор Ныркov А.П. Замечаний нет.

2) 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: недостатком диссертационной работы является отсутствие детального рассмотрения конкретных потенциальных приложений разработанных протоколов и связанных с ними моделей нарушителя.

3) 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: Судя по автореферату, к недостаткам диссертационной работы можно отнести следующее: отсутствие разработанного программного прототипа, с помощью которого

разработанные протоколы и алгоритмы могли быть протестированы экспериментально, и использование нестандартизованного термина «электронная цифровая подпись».

4) Федерального государственное бюджетное образовательное учреждение высшего образования «Калининградский государственный технический университет». Отзыв составил сотрудник доктор педагогических наук, кандидат технических наук, профессор Рудинский И.Д. Замечания: Недостаточное отражение условий и фактических данных экспериментальной проверки полученных результатов; Недостаточное внимание к вопросам программной реализации разработанных методов и алгоритмов.

5) Общество с ограниченной ответственностью научно-производственная фирма «Приборы» (ООО НПФ «Приборы»). Отзыв составил советник генерального директора по информационной безопасности, к.т.н, Гурьянов Д.Ю. Замечания: Отсутствие программного обеспечения, с помощью которого можно было бы провести тестирование разработанных протоколов и алгоритмов; по тексту автореферата имеются пропуски букв и опечатки.

6) ФГБОУ ВО «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А.Бонч-Бруевича». Отзыв составил почётный профессор кафедры защищённых систем связи СПбГУТ, д. т. н, профессор, Коржик В.И. Замечания:

- тема диссертации не раскрывает особенностей исследования, которые предполагается выполнить в работе;
- цель работы сформулирована нечетко — неясно, что такое «функциональность преобразований» и вообще, чем отличается данная работа от других многочисленных исследований по данным направлениям;
- объединение в одной диссертации различных улучшений цифровой подписи, а также защиты методов шифрования от атак с принуждением раскрытия действующего ключа, представляется чрезмерным — хватило бы и одной части, а вторую можно было бы оставить и для другого соискателя;

- в автореферате не раскрываются некоторые сокращения (например: ЗФ, ЗДЛ), а также не определены некоторые термины, которые нельзя признать общеизвестными даже специалистам по защите информации(алгебраические защитные преобразования — имеется в виду шифры, например, AES?; неотказуемость от электронных сообщений; псевдовероятностное шифрование — имеется в виду гомофонное шифрование?)
- Список публикаций достаточно впечатляющий, однако обращают на себя внимание следующие его особенности:

  — все работы из перечня ВАК, кроме одной, выполнены в соавторстве, а степень личного вклада автора диссертации в автореферате не отмечена;

  — три из пяти работ 8—9 летней давности;

  — в списке «Другие публикации» из восьми работ пять имеют объем одна страница — достаточно ли этого для изложения научного материала?

7) Акционерное общество «Научно-исследовательский институт «Рубин». Отзыв составили главный специалист отдела безопасности и защиты информации, к.т.н., Щукин А.Н. и главный научный сотрудник, к.т.н., доцент Добросельский М.А. Замечания: недостаточно полно рассмотрены сценарии практического применения предложенных протоколов; Отсутствует разработка программного прототипа, реализующий разработанный протокол.

Выбор официальных оппонентов и ведущей организации обосновывается тем, что д.т.н., доцент Александрова Е.Б. является специалистом в области информационной безопасности, в частности математических методов защиты информации, протоколов аутентификации; д.т.н., доцент, Татарникова Т. М. – известный специалист в области информационной безопасности и информационных технологий, 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:

протокол утверждаемой групповой ЭЦП, основанный на вычислениях по простому модулю и отличающийся выполнением вспомогательной операции возведения в целочисленную степень по трудно разложимому модулю и вычислением рандомизирующих экспонент, маскирующих открытые ключи подписантов, как значения однонаправленной функции в зависимости от открытых ключей подписантов и секретного ключа руководителя группы подписантов, за счет чего обеспечивается повышение уровня безопасности, обеспечиваемого протоколом;

метод построения протоколов коллективной ЭЦП, отличающийся тем, что рандомизирующий параметр подписи формируется несколькими групповыми подписантами, благодаря чему обеспечивается возможность выработки единой ЭЦП, разделяемой несколькими групповыми подписантами, что дает практически важное расширение функциональности протоколов коллективной подписи;

метод построения протоколов комбинированной коллективной ЭЦП, отличающийся тем, что рандомизирующий параметр подписи формируется несколькими групповыми подписантами и несколькими индивидуальными подписантами, благодаря чему обеспечивается возможность выработки единой ЭЦП, разделяемой несколькими групповыми подписантами и несколькими индивидуальными подписантами, что дает практически важное дополнительное расширение функциональности протоколов групповой подписи;

способ повышения производительности алгебраических псевдовероятностных алгоритмов защитных преобразований, отличающийся представлением блоков преобразуемых данных в виде элементов конечного расширенного поля, заданного в явной векторной форме, благодаря чему обеспечивается повышение производительности алгоритма защитного преобразования.

предложены:

протокол слепой ЭЦП, основанный на вычислениях по простому модулю и отличающийся выполнением вспомогательной операции возведения второго элемента

подписи в целочисленную степень по трудно разложимому модулю, за счет чего обеспечивается повышение уровня безопасности, обеспечиваемого протоколом;

метод построения протоколов с нулевым разглашением секрета на основе вычислительно трудной задачи дискретного логарифмирования в скрытой циклической подгруппе конечной некоммутативной группы и протокол на его основе;

протокол строгой взаимной аутентификации удаленных пользователей, вычислительно трудной задачи дискретного логарифмирования в скрытой циклической подгруппе конечной некоммутативной группы.

доказана перспективность использования разработанных методов для построения протоколов групповой ЭЦП новых типов и протокола аутентификации с нулевым разглашением, основанным на вычислениях в конечных некоммутативных группах;

введены:

- новые типы протоколов, расширяющие класс протоколов групповой подписи;
- новые типы протоколов групповой ЭЦП 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 в скрытой подгруппе конечной некоммутативной группы.

Теоретическая значимость исследования обоснована тем, что:

предложенные методы позволяют построить новые типы протоколов групповой подписи,

расширен класс протоколов защитных преобразований, реализуемых на основе вычислительно сложной задачи дискретного логарифмирования в скрытой циклической подгруппе конечной некоммутативной группы;

предложен новый механизм формирования маскирующих коэффициентов в протоколах утверждаемой групповой ЭЦП;

доказаны корректность работы построенных протоколов и выполнимость требования вычислительной неотличимости по шифртексту разработанного алгоритма псевдовероятностного защитного преобразования от вероятностного;

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 основные требования к разрабатываемым протоколам групповой ЭЦП для обеспечения возможности их внедрения в практику на основе существующей инфраструктуры открытых ключей;

раскрыты

проблемные аспекты применения в области построение протоколов групповой ЭЦП, безопасность которых основана на нескольких вычислительно трудных задачах;

основные вопросы, связанные с применимостью протоколов коллективной групповой ЭЦП и комбинированной групповой ЭЦП.

изучены существующие методы построения алгоритмов и протоколов коллективной и групповой ЭЦП, при этом отдельное внимание уделено рассмотрению вопросов анализа безопасности их применения;

проведена модернизация существующих методов построения алгоритмов и протоколов групповых ЭЦП новых типов – коллективной ЭЦП для групповых подписантов и комбинированной коллективной ЭЦП.

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

функциональность разработанных протоколов групповой ЭЦП новых типов отвечает потребностям практики;

разработанные протоколы новых типов могут быть внедрены в практику на основе имеющейся инфраструктуры открытых ключей;

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

Результаты диссертационной работы использованы в производственной деятельности ООО «Удостоверяющий центр ГАЗИНФОРМСЕРВИС» и внедрены в учебный процесс кафедры информационной безопасности Санкт- Петербургского государственного электротехнического университета «ЛЭТИ» имени В.И.Ульянова

(Ленина) на старших курсах обучения студентов по специальности «090900 – Информационная безопасность».

определены возможности и перспективы практического использования полученных результатов диссертации при исследовании протоколов групповых ЭЦП;

созданы способ построения протоколов групповых ЭЦП, обладающих повышенным уровнем безопасности, способы, позволяющие существенно расширить круг таких протоколов и устранить недостатки известных в литературе протоколов-аналогов;

представлены перспективы исследования, состоящие в разработке протоколов групповой ЭЦП, коллективной ЭЦП для групповых подписантов, в которых подпись свободна от включения третьего дополнительного параметра, что упростит строение этих протоколов, их реализацию и использование имеющейся на практике инфраструктуры открытых ключей при практическом применении протоколов данных типов.

Оценка достоверности результатов исследования выявила:

Обоснованность научных положений, выводов и практических рекомендаций, полученных в диссертационной работе, обеспечивается анализом состояния исследований в данной области на сегодняшний день, формальными доказательствами, вычислительным экспериментом и апробацией результатов на всероссийских научно-практических конференциях с международным участием: VI Санкт- Петербургская межрегиональная конференция «Информационная безопасность регионов России (ИБРР-2009)» (Санкт-Петербург, 28-30 октября 2009), XI Санкт-Петербургская международная конференция «Региональная информатика-2008 (РИ-2008)» (Санкт-Петербург, 22-24 октября 2008), XII Санкт-Петербургская международная конференция Региональная информатика «РИ-2010» (Санкт-Петербург, 20-22 октября 2010г), IX Санкт-Петербургская межрегиональная конференция (Санкт-Петербург, 28-30 октября 2015 г);

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 протоколов групповой ЭЦП, в том числе протоколов, основанных на двух вычислительно сложных задачах, а также в области алгоритмов защитных преобразований и протоколов аутентификации удаленных пользователей информационно-телекоммуникационных систем;

использованы полученные характеристики для сравнения с данными, приведенными в современной научной литературе по протоколам групповых ЭЦП и алгебраическим алгоритмам защитных преобразований.

Личный вклад соискателя состоит в:

участии в проведении исследований, обработке, интерпретации и формулировке полученных результатов, подготовке материалов к публикации, апробации их на конференциях, представляется значительным и, безусловно, является обоснованием для их использования в диссертации. В частности, автором лично:

- предложен метод построения и разработан протокол коллективной ЭЦП для групповых подписантов;
- предложен метод построения и разработан протокол комбинированной коллективной ЭЦП для групповых и индивидуальных подписантов;
- предложен метод построения и разработан алгоритм псевдовероятностного защитного преобразования алгебраического типа;
- разработан протокол групповой ЭЦП повышенной безопасности, основанный на вычислительной трудности одновременного решения задачи дискретного логарифмирования по простому модулю и задачи факторизации;
- разработаны протоколы строгой аутентификации удаленных абонентов, основанные на вычислительной трудности задачи дискретного логарифмирования в скрытой циклической подгруппе конечной некоммутативной группы;
- выполнена подготовка основных публикаций по работе.

Диссертационный совет считает, что Синев В.Е. в своей диссертационной работе решил научную задачу разработки методов и алгоритмов практических протоколов

групповой подписи, обладающих повышенным уровнем безопасности и устойчивости к атакам, что имеет важное социально-экономическое и хозяйственное значение.

На заседании 21.12.2017 г. диссертационный совет принял решение присудить Синеву В.Е. 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 техниче
член-корреспон Юсупов Рафаэль Мидхатович

Ученый секрета
кандидат технич Зайцева Александра Алексеевна
21.12.2017 г.