УНИВЕРСИТЕТ ИТМО

МИНОБРНАУКИ РОССИИ

федеральное государственное автономное
образовательное учреждение высшего образования
«Санкт-Петербургский национальный
исследовательский университет
информационных технологий,
механики и оптики» (Университет ИТМО)

Кронверкский проспект, д. 49, г. Санкт-Петербург,
Российская Федерация, 197101
тел.: (812) 232-97-04 | факс: (812) 232-23-07
od@mail.ifmo.ru | www.ifmo.ru

19.07.2017 № 22.1/923

УТВЕРЖДАЮ
Прор те
Унив
д. т. н

ифоров

«19» 07 2017 г.

ЗАКЛЮЧЕНИЕ

Санкт-Петербургского национального исследовательского университета информационных технологий, механики и оптики (Университет ИТМО) Министерства образования и науки Российской Федерации

Диссертация « *Методы построения практичных протоколов групповой подписи и алгебраических алгоритмов защитных преобразований*» выполнена в Федеральном государственном автономном образовательном учреждении высшего образования «Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики».

В период подготовки диссертации соискатель *Синев Валерий Евгеньевич* работал в «Санкт-Петербургском национальном исследовательском университете информационных технологий механики и оптики» (Университет ИТМО) Министерства образования и науки Российской Федерации, международная научная лаборатория «Интеллектуальные технологии для социо-киберфизических систем», программист.

В 2008 г. окончил «Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» имени В.И. Ульянова(Ленина)» по специальности «Компьютерная безопасность» по диплому ВСГ № 2434551.

В настоящее время является аспирантом «Санкт-Петербургского национального исследовательского университета информационных технологий механики и оптики» (Университет ИТМО) Министерства образования и науки Российской Федерации, по направлению/специальности «Методы и системы защиты информации, информационная безопасность».

Справка об обучении № 34/2017, выдана в 2017 г. федеральным государственным автономным образовательным учреждением высшего образования «Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики»,

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, заведующий лабораторией.

По итогам рассмотрения принято следующее заключение:

1. Личное участие соискателя в получении результатов, изложенных в диссертации.

Содержание диссертации и основные положения, выносимые на защиту, отражают персональный вклад автора в опубликованных работах. Подготовка к публикации полученных результатов проводилась автором самостоятельно с консультациями с соавторами. Представленные к защите результаты получены лично автором.

2. Степень достоверности результатов проведенных исследований.

Достоверность подтверждена аналитическим обзором исследований и разработок в области алгоритмов и протоколов электронной цифровой подписи (ЭЦП) и защитных преобразований информации, положительными итогами практического применения результатов диссертационной, а также апробацией основных научно-практических положений в печатных трудах и докладах на всероссийских и международных конференциях.

3. Новизна и практическая значимость результатов исследования.

Новизна результатов исследования состоит в следующем:

– Метод построения и протокол утверждаемой групповой ЭЦП, обладающий повышенной безопасностью, отличающийся использованием вычислений по простому модулю со специальной структурой.

– Метод построения и протокол коллективной ЭЦП для произвольного числа групповых подписантов, отличающийся от известных протоколов тем, что коллективная ЭЦП формируется для групповых подписантов. В разработанном методе построения протоколов коллективной ЭЦП для групповых подписантов формируется единый рандомизирующий параметр с участием всех групповых подписантов.

– Метод построения и протокол коллективной ЭЦП для произвольного числа групповых и индивидуальных подписантов, использующий стандартную инфраструктуру открытых ключей, отличающийся тем, что единую коллективную подпись разделяют как групповые, так и индивидуальные подписанты. В разработанном методе построения протоколов коллективной ЭЦП для групповых и индивидуальных подписантов формируется единый рандомизирующий параметр с

участием всех групповых и всех индивидуальных подписантов.

– Результаты оценивания алгебраических защитных преобразований симметричного и асимметричного типа на основе операций матричного и векторного умножения.

– Способ снижения операции матричного умножения в алгоритмах защитных преобразований информации, отличающийся заданием матриц над конечными полями, представленными в явной векторной форме.

– Способ псевдовероятностного защитного преобразования информации, отличающийся реализацией вычислений в конечных полях, заданных в явной векторной форме, благодаря чему обеспечивается повышение производительности.

Применение полученных результатов позволяет расширить функциональность протоколов ЭЦП и обеспечивает возможность использования имеющейся на практике инфраструктуры открытых ключей при практическом использовании протоколов групповой ЭЦП, а также возможность реализации новых механизмов защиты информации на основе псевдоверояностных защитных преобразований информации.

4. Ценность научных работ аспиранта состоит в создании методов, протоколов и алгоритмов расширяющих области практического применения технологии ЭЦП и позволяющих создать и практически использовать новые защитные механизмы для современных средств обеспечения информационной безопасности информационно-телекоммуникационных систем. Научные результаты были представлены на 3 российских и 2 международных конференциях. Результаты диссертационных исследований имеют высокую научную значимость для теории и практики решения задач информационной безопасности.

5. Диссертация соответствует научной специальности: (05.13.19) « Методы и системы защиты информации, информационная безопасность», а также требованиям, установленным п. 14 Положения о присуждении ученых степеней, утвержденного Постановлением Правительства РФ № 842 от 24.09.2013 г. (ред. от 10.06.2017).

6. Полнота изложения материалов диссертации в работах, опубликованных соискателем (ниже приводится полный список и краткая характеристика научных работ соискателя, опубликованных по теме диссертации, с указанием вида, авторского вклада и объема научных изданий с указанием выходных данных).

Основные положения и результаты диссертации получили полное отражение в докладах на 3 российских и 2 международных конференциях, в 14 печатных работах, среди которых 5 работ в журналах, рекомендованных ВАК.

Основные публикации, в которых отражены результаты диссертации:

1. **Синев В.Е.** Протокол групповой подписи на основе двух вычислительно трудных задач / Синев В.Е. // Известия СПбГЭТУ «ЛЭТИ». 2016. № 6. С. 46-54 **(ВАК)** — 0.8 п.л (авторский вклад 100%).
2. **Синев В.Е.** Утверждаемая групповая подпись: новые протоколы / Молдовян А.А., Галанов А.И., Синев В.Е. // Вопросы защиты информации. 2016. № 2. С. 44-50 **(ВАК)** — 0.9 п.л (авторский вклад 60%).
3. **Синев В.Е.** Протоколы слепой подписи на основе двух вычислительно трудных задач / Галанов А.И., Захаров Д.В., Молдовян Д.Н., Синев В.Е. // Вопросы защиты информации. 2009. № 4. С.2-7 **(ВАК)** — 0.9 п.л (авторский вклад 40%).
4. **Синев В.Е.** Конечные расширенные поля для алгоритмов электронной цифровой подписи / Доронин С.Е., Молдовян Н.А., Синев В.Е. // Информационно-управляющие системы. 2009. № 1. С. 33-40 **(ВАК)** — 0.9 п.л (авторский вклад 60%).
5. **Синев В.Е.** Векторные конечные поля: задание умножения векторов большой четной размерности / Доронин С.Е., Молдовяну П.А., Синев В.Е. // Вопросы защиты информации. 2008. № 4(83). С.2-7 **(ВАК)** — 0.9 п.л (авторский вклад 60%).

Диссертационная работа соответствует требованиям п. 9 Положения о присуждении ученых степеней, п. 1 «Теория и методология обеспечения информационной безопасности и защиты информации», п. 5 «Методы и средства (комплексы средств) информационного противодействия угрозам нарушения информационной безопасности в открытых компьютерных сетях, включая Интернет» и п. 13 «Принципы и решения (технические, математические, организационные и др.) по созданию новых и совершенствованию существующих средств защиты информации и обеспечения информационной безопасности» специальности 05.13.19 «Методы и системы защиты информации, информационная безопасность».

Диссертация «*Методы построения практичных протоколов групповой подписи и алгебраических алгоритмов защитных преобразований*» Синева Валерия Евгеньевича 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 совместном заседании кафедры информационных систем и кафедры информационных технологий Санкт-Петербургского национального исследовательского университета информационных технологий, механики и оптики (Университет ИТМО).

Присутствовало на заседании 8 чел. в числе которых три доктора наук и четыре кандидата наук.

Результаты голосования: «за» - 8 чел., «против» - 0 чел., «воздержалось» - 0 чел., протокол № 6 от « 27 » июня 20 17 г.

Председательствующий,

д.т.н., проф., заведующий кафедрой информационных систем — Парфенов В.Г.

Секретарь заседания, к.т.н., доцент кафедры компьютерных технологий — Буздалов М.В.

Сведения о составителях заключения:
ФИО: Парфенов Владимир Глебович
Ученая степень: доктор технических наук
Ученое звание: профессор
Место работы: Федеральное государственное автономное образовательное учреждение высшего образования «Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики»
Должность: заведующий кафедрой информационных систем
Почтовый адрес: 197101, г. Санкт-Петербург, Кронверкский проспект, д.49.
Телефон: +7 (812) 233-42-98
Адрес электронной почты: parfenov@mail.ifmo.ru

ФИО: Буздалов Максим Викторович
Ученая степень: кандидат технических наук
Ученое звание: профессор
Место работы: Федеральное государственное автономное образовательное учреждение высшего образования «Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики»
Должность: доцент кафедры компьютерных технологий
Почтовый адрес: 197101, г. Санкт-Петербург, Кронверкский проспект, д.49.
Телефон: +7 (812) 233-42-98
Адрес электронной почты: mbuzdalov@corp.ifmo.ru