Акционерное общество
«Научно-исследовательский институт «Вектор»
(АО «НИИ «Вектор»)

ул. Академика Павлова, дом 14-а; г. Санкт-Петербург, 197376,
тел. (812) 295-10-97, 61, факс 591-72-74;
e-mail: nii@nii-vektor.ru www. nii-vektor.ru

ОКПО 07525192
ОГРН 1117847020400
ИНН 7813491943/ КПП 783450001

«УТВЕРЖДАЮ»
Генеральный директор акционерного
общества «Научно-исследовательский
ор» (АО «НИИ «Вектор»)
к.т.н., доцент
Петкау Олег Гергардович

ОТЗЫВ

ведущей организации – акционерного общества «Научно-исследовательский институт «ВЕКТОР» (АО «НИИ «Вектор») – на диссертационную работу Синева Валерия Евгеньевича «Методы построения и разработка практичных протоколов групповой подписи и алгебраических алгоритмов защитных преобразований», представленную на соискание ученой степени кандидата технических наук по специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность».

1. Актуальность темы исследования

Важными задачами, связанными с применением современных информационных технологий, являются задачи обеспечения требуемого уровня информационной безопасности и неотрекаемости (неотказуемости) от содержания электронных сообщений и документов. При решении последней задачи появляется возможность автоматизированной обработки электронных сообщений и документов, имеющих юридическую силу. Данная задача решается с помощью алгоритмов и протоколов электронной цифровой подписи (ЭЦП). В последнее время существенно расширился спектр прикладных информационных технологий, предполагающих обработку, распределение, передачу и хранение юридически значимых

документов и сообщений, представленных в электронном виде, что обусловило потребности практики по использованию протоколов ЭЦП, обладающих некоторыми дополнительными свойствами по сравнению с традиционным протоколом индивидуальной ЭЦП. Это привело к разработке и исследованию протоколов с участием нескольких подписантов (схемы коллективной ЭЦП) и протоколов, в которых подпись формируется некоторыми подмножествами сотрудников некоторого органа, выступающего в качестве группового подписанта (схемы групповой ЭЦП). Недостатками известных протоколов последнего типа является использование нестандартной инфраструктуры открытых ключей и нарушение базового положения о том, что закрытый ключ, связанный с открытым ключом, должен быть известен только единственному субъекту. Данные недостатки ограничивают области известных протоколов групповой подписи. Таким образом, разработка практичных протоколов групповой подписи, для функционирования которых может быть использована развернутая на практике стандартная инфраструктура открытых ключей, является актуальной научно-технической задачей.

В рамках задачи обеспечения информационной безопасности информационно-телекоммуникационных систем в последнее время исследователями значительное внимание уделяется псевдовероятностным защитным преобразованиям, позволяющим неоднозначное восстановление преобразованной информации и расширяющих спектр атак, которые могут быть отражены с помощью защитных преобразований. Однако известные решения обеспечивают сравнительно низкую производительность алгоритмов такого типа. Данный недостаток потенциально может быть устранен построением алгебраических алгоритмов псевдовероятностных защитных преобразований, что обусловливает актуальность поиска новых алгебраических алгоритмов защитных преобразований.

Таким образом, тема диссертационной работы Синева В.Е. «Методы построения и разработка практичных протоколов групповой подписи и алгебраических алгоритмов защитных преобразований» является актуальной.

2. Научная новизна результатов

Научная новизна работы заключается в разработке методов построения протоколов ЭЦП и алгоритмов защитных преобразований новых типов, а также в построении на основе предложенных методов новых протоколов ЭЦП и новых алгоритмов защитных преобразований. Основными новыми результатами являются следующие:

2.1. Разработан 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.

2.2. Разработан 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.

2.3. Разработан протокол коллективной ЭЦП для групповых подписантов, разделяющих единую цифровую подпись.

2.4. Разработан протокол комбинированной коллективной ЭЦП, позволяющий сформировать единую цифровую подпись, разделяемую несколькими индивидуальными и несколькими групповыми подписантами.

2.5. Разработан 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.

2.6. Разработан способ выполнения 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.

3. Достоверность и обоснованность результатов исследований

Достоверность результатов исследования обеспечивается корректным использованием математического аппарата, отсутствием противоречия результатов диссертационной работы и сделанных на их основании выводов известным научным фактам.

4. Значимость для науки и практики

Теоретическая значимость полученных результатов заключается в разработке методов построения протоколов цифровой подписи новых типов и новых алгебраических алгоритмов псевдовероятностного защитного преобразования.

Практическая значимость результатов диссертационного исследования определяется разработкой протоколов групповой ЭЦП с расширенной функциональностью, практическое внедрение которых реализуемо на базе существующей на практике инфраструктуры открытых ключей. Последнее обусловливает возможность расширения областей практического применения протоколов цифровой подписи в информационных технологиях.

Личный вклад автора присутствует в постановке задач, личном 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

- 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.

5. Полнота опубликованных результатов работы, их соответствие паспорту специальности

Диссертационная работа состоит из введения, пяти глав, заключения, списка литературы. Объем работы составляет 166 страниц, 11 рисунков, 4таблицы и список литературы из 126 наименований.

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»).

Основные результаты данной диссертационной работы докладывались и обсуждались на следующих конференциях:

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),

Всеармейская научно-практическая конференция «Инновационная деятельность в Вооруженных силах Российской Федерации» (Санкт-Петербург 25-26 ноября, 2010 г.).

IX Санкт-Петербургская межрегиональная конференция (Санкт-Петербург, 28-30 октября 2015 г)

В целом можно сделать вывод, что апробация результатов исследований, представленных в диссертации, среди учёных и специалистов по разработке методов защиты информации и средств обеспечения информационной безопасности проведена в достаточной мере.

Тема диссертации, направленность проведенных исследований и полученных результатов соответствует паспорту специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность» по п. 5. «Методы и средства (комплексы средств) информационного противодействия угрозам нарушения информационной безопасности в открытых компьютерных сетях, включая Интернет», п. 11. «Технологии идентификации и аутентификации пользователей и субъектов информационных процессов. Системы разграничения доступа», п. 13. «Принципы и решения (технические, математические, организационные и др.) по созданию новых и совершенствованию существующих средств защиты информации и обеспечения информационной безопасности».

Содержание автореферата соответствует основным положениям диссертационной работы. В нем изложены все основные результаты, выносимые на защиту, дано достаточно полное представление о научно-практической значимости работы.

6. Рекомендации по использованию результатов и выводов

Полученные в диссертационной работе результаты рекомендуется использовать в организациях, деятельность которых связана с

исследованием и разработкой систем и средств защиты информации, передаваемой в открытых компьютерных сетях, в том числе в ФГБУН Санкт-Петербургский институт информатики и автоматизации Российской академии наук (СПИИРАН), ФГБОУВО Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» имени В.И. Ульянова (Ленина) (СПбГЭТУ «ЛЭТИ»), ПАО "Информационные телекоммуникационные технологии" (ПАО Интелтех).

7. Замечания по диссертации и автореферату:

7.1. Недостаточно внимания уделено рассмотрению сценариев практического применения разработанных протоколов коллективной и групповой ЭЦП.

7.2. Практические применения протоколов коллективной и групповой подписи являются сравнительно редкими случаями.

7.3. Термин «практичные протоколы» в названии диссертации несколько расплывчат и для понимания его смысла требуется обратиться к содержанию диссертации.

7.4. Разработанные протоколы коллективной ЭЦП для групповых подписантов могут быть рассмотрены как частный случай разработанных протоколов комбинированной коллективной ЭЦП.

7.5. Наличие параметра ЭЦП, обозначенного как U, в протоколе групповой подписи приводит к увеличению размера групповой ЭЦП по сравнению с протоколом индивидуальной ЭЦП.

7.6. В диссертационной работе упоминается о функциональности расширении стандарта ЭЦП ГОСТ Р 4.10–2012, однако любое модифицирование криптосхемы, регламентируемой стандартом, выходит за рамки стандарта.

7.7. В работе присутствуют опечатки и неточности изложения материала, затрудняющие ознакомление с результатами диссертационной работы.

8. Общая оценка диссертационной работы

Отмеченные недостатки носят частный характер и не снижают научной ценности и практической значимости проведенного исследования.

Диссертация Синева Валерия Евгеньевича «Методы построения и разработка практичных протоколов групповой подписи и алгебраических алгоритмов защитных преобразований» на соискание ученой степени кандидата технических наук является завершенной научно-квалификационной работой, в которой решена задача повышения производительности процедур псевдовероятностного защитного

преобразования и построения протоколов групповой ЭЦП, практическое внедрение которых реализуемо на базе существующей инфраструктуры открытых ключей, имеющая существенное значение для развития области информационной безопасности. 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».

Отзыв на диссертацию и автореферат обсужден на заседании научно-технического отдела 24 ноября 2017 г., протокол № 4.

Главный научный сотрудник АО «НИИ «Вектор»,
доктор технических наук, старший научный сотрудник
Емелин Вадим Иванович

Ученый секретарь Научно-технического Совета АО «НИИ «Вектор»
кандидат технических наук, доц
Морозова Елена Владимировна

Сведения о составителях отзыва:
Емелин Вадим Иванович
доктор технических наук
старший научный сотрудник
АО «НИИ «Вектор»
Главный научный сотрудник
ул. Академика Павлова, дом 14-а; г. Санкт-Петербург, 197376
тел. (812) 295-27-24
e-mail: nii@nii-vektor.ru
Морозова Елена Владимировна
кандидат технических наук
доцент
АО «НИИ «Вектор»
ул. Академика Павлова, дом 14-а; г. Санкт-Петербург, 197376
тел. (812) 295-27-24
e-mail: nii@nii-vektor.ru