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**»
Директор акционерного общества
«Научно-исследовательский институт
«ВЕКТОР» (АО «НИИ «Вектор»)

к.т.н., доцент

Петкау Олег Гергардович

16 января 2017 г.

ОТЗЫВ

ведущей организации – акционерного общества «Научно-исследовательский институт «ВЕКТОР» (АО «НИИ «Вектор») – на диссертационную работу Березина Андрея Николаевича «Методы повышения уровня безопасности защитных преобразований информации», представленную на соискание ученой степени кандидата технических наук по специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность».

1. Актуальность темы исследования

Защитные преобразования информации обеспечивают целостность, конфиденциальность, подотчётность, неотказуемость, аутентичность и достоверность информации при её передаче и хранении с использованием открытых систем, что обусловливает их существенную роль и важное место в области информационной безопасности. Разработка корректных моделей и сопровождающих их методов в форме программного и программно-аппаратного инструментария для обеспечения перечисленных свойств информационных ресурсов является актуальным направлением развития наукоемких информационных технологий. Важной частью защитных преобразований являются протоколы аутентификации и электронной цифровой подписи, обеспечивающие работу юридически значимого электронного документооборота.

В настоящее время опубликовано большое количество работ, посвящённых тематике повышения безопасности защитных преобразований информации путем такого построения разрабатываемых технологий и систем, при котором их стойкость основывается на вычислительной трудности одновременного решения задач факторизации и дискретного логарифмирования в конечном поле. Однако опубликованные решения позволяют строить только некоторые частные алгоритмы защитных преобразований информации.

Последнее обстоятельство обусловлено тем, что существующие подходы весьма сложно применить для построения алгоритмов защитных преобразований других типов. Дальнейшее развитие как теории, так и практики построения защищенных систем, потенциально связано с рядом современных достижений в области применения вычислительно сложных задач для построения алгоритмов защитных преобразований информации. Тема диссертации связана с получением новых результатов в указанном направлении, что определяет ее актуальность.

2. Научная новизна результатов

Научная новизна работы заключается в следующем.

- 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 простых делителей 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 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.

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.

Значимость полученных результатов заключается в том, что, при использовании метода построения алгоритмов и протоколов, нарушение безопасности которых требует одновременного решения двух вычислительно сложных задач, были проанализированы все основные типы алгоритмов и протоколов защитных преобразований информации, применяемых на практике. В частности, в диссертации предлагаются алгоритмы аутентификации, обмена секретом и электронной цифровой подписи. При этом в случае появления прорывного алгоритма решения по одной из используемых вычислительно сложных задач, высокая стойкость алгоритма или протокола сохранится.

Полученные в диссертационной работе результаты рекомендуется использовать для создания систем защиты информации, передаваемой в открытых компьютерных сетях, с повышенным уровнем безопасности.

Личный вклад автора присутствует в постановке задач, личном участии в проведении исследований, обработке и интерпретации 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 алгоритмов и протоколов, 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.

4. Полнота опубликованных результатов работы, их соответствие паспорту специальности

Диссертационная работа состоит из введения, списка сокращений, пяти глав, заключения, списка литературы. Объем работы составляет 134 страницы без учета приложений, 35 рисунков и 13 таблиц.

По теме диссертации опубликовано 6 статей в научно-технических журналах и 2 доклада в трудах конференций. Из них 5 статей опубликованы в журналах, которые входят в перечень ВАК («Вопросы защиты информации», «Информационно управляющие системы» и «Известия СПбГЭТУ “ЛЭТИ”»).

Основные результаты данной диссертационной работы докладывались и обсуждались на 4 международных и 4 всероссийских конференциях:

- IX Санкт–Петербургской межрегиональной конференции «Информационная безопасность регионов России (ИБРР–2015)» (Санкт-Петербург, 2015);
- XIV Санкт–Петербургской международной конференции «Региональная информатика – 2014» (Санкт-Петербург, 2014);
- VIII Санкт–Петербургской межрегиональной конференции «Информационная безопасность регионов России (ИБРР–2013)» (Санкт-Петербург, 2013);
- XIX международной научно–методической конференции «Современное образование: содержание, технологии, качество» (Санкт-Петербург, 2013);
- всеармейской научно–практической конференции «Инновационная деятельность в Вооружённых силах Российской Федерации» (Санкт-Петербург, 2013);
- XIII Санкт–Петербургской международной конференции «Региональная информатика – 2012» (Санкт-Петербург, 2012);
- XVIII международной научно–методической конференции «Современное образование: содержание, технологии, качество» (Санкт-Петербург, 2012);
- VII Санкт–Петербургской межрегиональной конференции «Информационная безопасность регионов России (ИБРР–2011)» (Санкт-Петербург, 2011).

Это позволяет 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.

5. 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.

6. Замечания по диссертации и автореферату:

1. Формула на странице 26, выбранная для оценивания уровня безопасности не раскрывает полноты исследуемого вопроса, поскольку не учитывает вероятность появления прорывных вычислительных технологий, которые могут быть применены для решения использованных вычислительно сложных задач (например, появление квантового вычислителя способного выполнить алгоритм Шора).

2. Приводимые в диссертации оценки появления прорывного решения задачи дискретного логарифмирования и задачи факторизации носят условный характер.

3. В разделе 2.5 на стр. 49 автор ссылается на конкретную методику выбора разрядности параметров задач факторизации и дискретного логарифмирования для обеспечения заданного уровня стойкости, однако не приводится обоснование выбранной методики.

4. Автор использует термины «защитные преобразования информации», «алгоритмические средства защиты информации» но не приводит их определение.

5. При сравнении характеристик разработанных протоколов с аналогами на страницах 68, 73, 78, 83, 100, 108, не приводятся оценки основных технических характеристик при реализации на реальных устройствах.

6. На рисунках 2.1, 2.2, 2.3 (стр. 38, 44, 46 соответственно) не показаны деления шкал и соответствующие им конкретные значения величин.

7. Общая оценка диссертационной работы

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

Диссертация Березина Андрея Николаевича «Методы повышения уровня безопасности защитных преобразований информации» на соискание ученой степени кандидата технических наук является научно-

квалификационной работой, в которой изложены научно обоснованные алгоритмические решения и разработки, важные для дальнейшего развития защитных преобразовании информации. 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».

Отзыв на диссертацию и автореферат обсужден на заседании научно-технического отдела 11 января 2017 г., протокол № 1.

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, доцент
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