Экз. № 1

УТВЕРЖДАЮ

Заместитель начальника Академии ФСО России

доктор социологических наук, профессор

В.И. Козачок

"13" января 2017 г.

ОТЗЫВ

на автореферат диссертации Березина Андрея Николаевича на тему «Методы повышения уровня безопасности защитных преобразований информации», представленной на соискание ученой степени кандидата технических наук по специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность».

Актуальность темы. В настоящее время большое значение приобретает направление, связанное с обеспечением компьютерной безопасности. Это обусловлено постоянным ростом объёмов обрабатываемой информации, совершенствованием средств её хранения, передачи и обработки. Вопросу обеспечения безопасности субъектов информационных отношений, а также хранящейся и обрабатываемой в них информации уделяется всё большее внимание.

Работа Березина А. Н.. посвящена решению актуальной научной задачи – разработки методов и алгоритмов защиты информации в процессе её сбора, хранения, обработки, передачи и распространения.

Научная новизна работы определяется разработкой нового метода построения алгоритмов и протоколов, нарушение безопасности которых требует одновременного решения двух вычислительно сложных задач, отличающегося использованием задачи дискретного логарифмирования по трудно факторизуемому модулю, размер множителей которого выбирается

таким образом, что, по крайней мере, решение задачи дискретного логарифмирования по модулю одного из делителей модуля имеет вычислительную сложность не ниже заданного уровня стойкости.

Теоретическая и практическая значимость работы определяется тем, что предложен метод построения алгоритмов и протоколов, имеющих повышенный уровень безопасности, свободный от недостатков существующих аналогов, а разработанные протоколы аутентификации, обеспечения конфиденциальности и анонимности имеют широкое применение в информационно-телекоммуникационных технологиях.

Представленные в автореферате научные положения являются обоснованными, что подтверждается апробацией основных результатов работы на четырнадцати конференциях различного уровня и пятью публикациями в рецензируемых изданиях, рекомендованных ВАК.

Результаты диссертационного исследования внедрены в деятельность СПИИРАН, в учебный процесс Санкт-Петербургского государственного электротехнического университета «ЛЭТИ» им. В.И. Ульянова (Ленина) и государственного университета морского и речного флота имени адмирала С.О. Макарова.

В то же время по работе можно сделать следующие замечания.

1. В автореферате в явном виде не представлена оценка степени достижения цели исследования – повышения уровня информационной безопасности информационно-телекоммуникационных технологий.

2. 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 информации.

3. В таблице 1 автореферата при $P_{\text{ЗФ}} = P_{\text{ЗДЛ}} = 10^{-32}\ l$ по формуле должно быть равно $2 \cdot 10^{-102}$.

Однако высказанные замечания не снижают ценности полученных автором научных результатов и не влияют на общую положительную оценку.

Заключение. Содержание автореферата позволяет сделать вывод о том, что диссертация представляет собой законченное научное исследование, результаты которого обладают научной новизной, теоретической и практической значимостью. Работа Березина Андрея Николаевича соответствует паспорту специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность» и отвечает требованиям, предъявляемым к кандидатским диссертациям, установленным Положением о порядке присуждения учёных степеней, утвержденным постановлением Правительства Российской Федерации от 24.09.2013 г. № 842, а её автор заслуживает присуждения учёной степени кандидата технических наук.

Отзыв обсужден и одобрен на заседании кафедры Безопасности сетевых технологий (протокол № 16 от 23 декабря 2016 года).

Отзыв подготовили:

Сотрудник Академии ФСО России
кандидат технических наук, доцент — Цибуля А.Н.

Сотрудник Академии ФСО России
кандидат технических наук — Козачок А. В.

«12» января 2017 года

Сведения о составителях отзыва:

Фамилия, имя, отчество: Цибуля Алексей Николаевич

Ученая степень: кандидат технических наук

Ученое звание: доцент

Место работы: Федеральное государственное казенное военное образовательное учреждение высшего образования «Академия Федеральной службы охраны Российской Федерации»
Должность: сотрудник
Телефон: 8 (4862) 54-99-33
Почтовый адрес: 302034, Орёл, ул. Приборостроительная, д. 35
Электронная почта: tsibul@mail.ru

Фамилия, имя, отчество: Козачок Александр Васильевич
Ученая степень: кандидат технических наук
Место работы: Федеральное государственное казенное военное образовательное учреждение высшего образования «Академия Федеральной службы охраны Российской Федерации»
Должность: сотрудник
Телефон: 8 (4862) 54-99-33
Почтовый адрес: 302034, Орёл, ул. Приборостроительная, д. 35
Электронная почта: totrin@mail.ru