Отзыв официального оппонента
на диссертационную работу
Березина Андрея Николаевича
«Методы повышения уровня безопасности защитных преобразований информации» по специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность»
на соискание ученой степени кандидата технических наук

1. Актуальность темы диссертационной работы

Актуальность темы диссертационной работы определяется повсеместным использованием алгоритмов и протоколов защитных преобразований для решения задач обеспечения информационной безопасности современных информационных технологий, а также тем фактом, что уровень безопасности, определяемый защитными преобразованиями, зависит от лучшего известного алгоритма решения вычислительно сложной задачи, положенной в их основу, и вероятностью скорого появления ее решения. На практике используются только те протоколы, которые основаны на хорошо изученных и апробированных вычислительно сложных задачах. Предположение о достаточно низкой вероятности появления прорывных решений лежит в основе принятия решения о безопасности протоколов защитных преобразований. Ввиду отсутствия доказательства, что решение вычислительно сложных задач не появится в ближайшее время, вопрос о безопасности алгоритмов, использующих их, является актуальным. Для достижения более надежных гарантий развивается подход к построению протоколов и алгоритмов, основанных на двух различных вычислительно сложных задачах, что делает данную работу актуальной.

2. Степень обоснованности научных положений, выводов и рекомендаций

Автором проведён анализ современного состояния исследований в области математических способов защиты, взлом которых требует

решения нескольких вычислительно сложных задач, что позволило ему корректно определить направление дальнейшего исследования.

Автор основывает свои результаты на хорошо апробированном математическом аппарате, в частности задачах факторизации и дискретного логарифмирования, корректно применяет математические методы и фундаментальные подходы.

В работе представлены следующие научные результаты:

1. Новый метод построения алгоритмов и протоколов защитных преобразований информации, основанных на задачах факторизации и дискретного логарифмирования. Автором проведено достаточно подробное обоснование корректности метода.

2. На основе предложенного метода, автором разработаны три группы протоколов для обеспечения конфиденциальности, аутентичности, анонимности, подотчётности, неотказуемости и целостности. Для каждого из предложенных протоколов доказана корректность его работы.

3. Автором предложены рекомендации по выбору безопасных длин параметров протоколов, разработаны вспомогательные алгоритмы генерации с использованием апробированных научных результатов в данной области.

3. Научная новизна и достоверность результатов исследования

На защиту вынесены следующие результаты:

- Метод построения алгоритмов и протоколов, повышенный уровень безопасности которых обеспечивается тем, что для их взлома требуется одновременно решить задачи дискретного логарифмирования и факторизации.

- Протоколы локальной и удалённой аутентификации пользователей, объектов и субъектов информационных процессов, обладающие повышенным уровнем безопасности.

- Протоколы обеспечения конфиденциальности информации, передаваемой по открытым каналам связи, обладающие повышенным уровнем безопасности.

- Протоколы обеспечения анонимности в открытых компьютерных сетях, обладающие повышенным уровнем безопасности.

Новизна полученных результатов определяется новым методом, применённым автором для построения протоколов обеспечения информационной безопасности. Схожие идеи встречались в литературе ранее, но автор смог реализовать свою идею в протоколах самого разного назначения.

Полученные научные результаты прошли апробацию на 14 конференциях различного уровня, в том числе на 4 международных и 4 всероссийских.

4. Теоретическая и практическая значимость результатов

Предложенный метод успешно использован автором для разработки семейства протоколов защитных преобразований информации, обладающих повышенным уровнем безопасности.

Разработанные протоколы иллюстрируют состоятельность нового метода и могут применяться в средствах защиты информации для обеспечения конфиденциальности, аутентичности, анонимности, подотчётности, неотказуемости и целостности.

Автором представлены акты внедрения результатов при выполнении работ по гранту РФФИ (№14-07-00061 А) на базе 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.

5. Соответствие защищаемых положений паспорту специальности

Тема диссертации, полученные научные результаты соответствуют пунктам №5, 11, 13 раздела 2 «Области исследования» паспорта

специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность».

6. Полнота изложения материалов диссертации в автореферате, работах, опубликованных автором

Полученные результаты представлены в 6 журнальных статьях, 5 из которых опубликованы в журналах, рекомендованных ВАК, 1 статья опубликована в открытом зарубежном журнале.

Диссертация содержит 134 страницы, включает введение, 5 глав, заключение, список литературы (143 наименования), 35 рисунков и 13 таблиц. Оформление диссертации и автореферата соответствует требованиям предъявляемым ВАК. Содержание автореферата соответствует основным результатам диссертации.

7. Общая оценка диссертационной работы

Диссертационная работа хорошо структурирована, имеет внутреннее единство и свидетельствует о личном вкладе автора в науку. Научные результаты, представленные в диссертации, обоснованны, апробированы и достоверны. Данные результаты имеют важное значение для создания новых средств защиты информации и расширения существующих протоколов обеспечения информационной безопасности, а также для учебного процесса.

8. Возражения и замечания

1. В работе используется «интегральный параметр безопасности», который, как пишет автор, «учитывает вероятность появления в ближайшем будущем вычислительно эффективного алгоритма решения вычислительно сложной задачи», на чем основывает автор свои предположения о данной вероятности?

2. Отсутствует математическое доказательство обоснованности формулы «интегрального параметра безопасности», не представлено в чем измеряется данный показатель.
3. В выводах ко второй главе автор пишет, что «предложены ограничения на выбор параметров, используемых в новом методе», но не рассмотрен вопрос, при вводе данных ограничений на сколько снизится пространство ключей, и не станет ли это критичным для предложенных методов?
4. В главе 3 при генерации ключа предлагается после проверки уничтожить делители p_i и q_i, но при их «уничтожении» данные все равно какое-то время будут хранится в памяти ПК, не спровоцирует ли это возможность проведения успешных атак на предлагаемые алгоритмы?
5. В главе 4 при создании ЭЦП автор пишет, что использует «специальную хэш-функцию», но какая именно хэш-функция используется не написано.
6. Предложенные автором протоколы ЭЦП выдают подписи намного меньшего размера, чем у существующих алгоритмов, что вызывает сомнения в их стойкости.
7. Выбор автором задач факторизации и дискретного логарифмирования по простому модулю опирается на интуитивно признанное предположение о независимости этих задач, хотя существует общий метод решения для этих двух задач (общий метод решета числового поля).
8. В работе не представлено, на сколько, предложенный метод даст выигрыш/проигрыш во времени/мощности относительно алгоритмов использующих одну вычислительно сложную задачу, тем самым остался открытым вопрос целесообразности данного метода.

Указанные недостатки не снижают ценность полученных научных результатов.

9. Заключение

Диссертация представляет собой законченную научно-квалификационную работу, в которой решена научная задача разработки универсального метода построения протоколов защитных преобразований, основанных на задачах факторизации и дискретного логарифмирования по простому модулю, для обеспечения информационной безопасности в информационно-телекоммуникационных системах.

Диссертационная работа «Методы повышения уровня безопасности защитных преобразований информации» отвечает требованиям п.9 Положения о присуждении учёных степеней, утверждённого постановлением Правительства Российской Федерации от 24 сентября 2013, предъявляемых к кандидатским диссертациям, а её автор – Березин Андрей Николаевич заслуживает присуждения учёной степени кандидата технических наук по специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность».

Официальный оппонент _____