ИНТЕЛТЕХ INTELTECH

Публичное акционерное общество «Информационные телекоммуникационные технологии» (ПАО «Интелтех»)

ул. Кантемировская д. 8, Санкт-Петербург, Россия, 197342 Тел. (812) 295-50-69, Факс (812) 542-18-49

www.inteltech.ru E-mail: inteltech@inteltech.ru ИНН 7803503490, ОГРН 1027801525608, КПП 780201001/781401001

21.04.2016 № 9Н06-211

На № _____ от _____

УТВЕРЖДАЮ
Первый заместитель
генерального директора
ПАО «Интелтех»
по научной работе,
кандидат военных наук

ОТЗЫВ

ведущей организации – Публичного акционерного общества «Информационные телекоммуникационные технологии (ПАО «ИНТЕЛТЕХ») на диссертационную работу КОВЦУРА Максима Михайловича «Методы повышения информационной безопасности IP-телефонии с учетом вероятностно-временных характеристик протоколов распределения ключей», представленную на соискание ученой степени кандидата технических наук по специальности 05.13.19 «Методы и системы защиты информации, информационная безопасность»

1. Актуальность темы диссертации

Согласно исследованиям в различных открытых источниках, IP-телефония нашла широкое применение в современных сетях передачи данных. Причинами роста сегмента IP-телефонии являются невысокая стоимость сервисов, возможность получать услуги без установки дополнительного оборудования, используя программные клиенты на терминале пользователя. Для обеспечения защиты информации применяется совокупность протоколов обеспечения безопасности IP-телефонии. При этом

нарушение информационной безопасности в сетях IP-телефонии приносит ущерб как пользователям услуги, так и операторам связи.

Таким образом, диссертационная работа Ковцура М.М., посвященная повышению защищенности информации в сеансах безопасной IP-телефонии и сокращению времени установления защищенного соединения, соответствует решению актуальной научной задачи, имеющей существенное значение для развития науки и практики.

2. Научная новизна и основные результаты исследования

Научную новизну диссертации характеризуют следующие положения:

математическая модель активного нарушителя для защищенной IP-телефонии, отличающаяся от известных аналогов учетом атаки “человек посередине” на протоколы обеспечения безопасности IP-телефонии;

методика оценки вероятностно-временных характеристик протоколов распределения ключей защищенной IP-телефонии, отличающаяся от существующих учетом особенностей протоколов распределения ключей, выраженных в наличии ограничения числа повторных передач сообщений с переменным таймером повторной передачи при работе по каналам с ошибками и задержками;

разработанный метод выявления нарушителя протоколов распределения ключей, основанных на алгоритме Диффи-Хелмана, отличающийся от существующих методов возможностью выявить активного нарушителя протоколов в используемых каналах связи при отсутствии общего доверенного центра или ключа между корреспондентами, а также позволяющий автоматически обнаружить нарушителя, владеющего технологией синтеза голоса;

модификация протокола ZRTP, отличающаяся сокращенным временем успешного выполнения, что уменьшает временные затраты при работе протокола по сравнению с исходной реализацией.

3. Практическая ценность результатов исследований

Практическая ценность диссертационного исследования состоит в том, что представленная математическая модель активного нарушителя для защищенной IP-телефонии может быть использована при разработке методик

контроля защищенных сетей электросвязи, в учебном процессе по дисциплине "Безопасность IP-телефонии". Метод выявления нарушителя протоколов распределения ключей обеспечивает автоматическое обнаружение вмешательства нарушителя в канал связи между корреспондентами при использовании протокола ZRTP. Метод снижает вероятность успешной атаки НСД нарушителя и может применяться при разработке, проектировании и реализации решений защищенной IP-телефонии, а также для модернизации существующих решений.

Методика оценки вероятностно-временных характеристик протоколов распределения ключей может применяться для оценки времени выполнения и вероятности успешного завершения этих протоколов при проектировании решений защищенной IP-телефонии.

Результаты диссертации использованы в учебном процессе и при разработке методик контроля защищенных сетей электросвязи. Результаты внедрены в Управлении Роскомнадзора по Северо-Западному федеральному округу, в СПб ГУТ им М.А. Бонч-Бруевича на кафедре Защищенных Систем Связи, а также в ООО "Телкон".

4. Достоверность и обоснованность результатов исследований

Основные выводы и положения, представленные в диссертации, обоснованы и аргументированы. Обозначенная в диссертации научная задача исследована и решена на основе корректного использования фундаментальных принципов, концепций и подходов, используемых в теории вероятности, комбинаторики, теории вероятностных графов.

Достоверность основных результатов диссертации подтверждается:

- обстоятельным сравнительным анализом достоинств и недостатков предшествующих научных разработок по исследуемой проблематике и преемственностью основных научных положений;

- корректностью предложенных методов, методики и модели и апробированных результатов диссертации в печатных трудах, докладах на конференциях;

- теоретически полученные зависимости подтверждаются результатами экспериментальной оценки и результатами имитационного моделирования;

- положительными результатами внедрения основных результатов диссертации.

5. Апробация и публикации

Результаты исследований прошли апробацию на 7 международных и всероссийских конференциях. По теме диссертации опубликовано 16 научных работ, в том числе 5 в журналах, входящих в перечень рецензируемых научных изданий.

6. Рекомендации по использованию результатов и выводов диссертации

Результаты диссертационной работы целесообразно использовать в организациях, занимающихся исследованием и разработкой технических систем защищенной IP-телефонии и решений на базе данных разработок. Результаты рекомендуется использовать для доработки существующих программных клиентов IP-телефонии, применяемых, в том числе, в сценарии корреспондент-корреспондент.

7. Замечания по диссертации

1. Не приведен алгоритм выбора параметров информационной безопасности модернизированного протокола ZRTP, в том числе алгоритма шифрования и хеширования.

2. В автореферате не описан подробно механизм формирования и проверки аутентификационной строки SAS, встроенный в протокол ZRTP.

3. Из текста работы непонятно, учитывался ли различный размер сообщений протокола ZRTP при имитационном моделировании.

4. В диссертации не приведены аналитические формулы расчета среднего времени успешного завершения транзакций работы протоколов распределения ключей.

5. При исследовании вероятносто-временных характеристик протоколов IP-телефонии автор приводит формулу для расчета вероятности успешной передачи пакета длины (4.2) только для биномиального канала, при этом канал с соответствующей ему частью памяти маршрутизаторов не рассматривается как система массового обслуживания и в формуле (4.4) для

расчета времени передачи пакета по каналу не учитывается интенсивность поступления пакетов в систему, интенсивность их обслуживания и приоритет.

6. В тексте диссертации присутствуют стилистические ошибки, так на стр.121 приведены формулы для расчета среднего времени (4.55) и вероятности (4.56) успешного завершения ПРК, которые автор называет функциями; переходную (производящую) функцию вероятностей переходов по ребру вероятностного графа по тексту автор называет «производящей функцией вероятностного графа…» (стр.104), «производящая функция ветви…» (стр.109), «производящей функцией элемента….» (стр.115) и др.

Перечисленные замечания не снижают высокий научный уровень проведенных исследований и не влияют на общий положительный вывод о качестве представленной к защите диссертации. Замечания носят рекомендательный характер и могут быть учтены автором в дальнейших публикациях по теме диссертации.

8. Общая оценка диссертационной работы

Диссертационная работа Ковцура М.М. представляет собой завершенную научно-квалификационную работу, выполненную на актуальную тему и обладающую практической и теоретической значимостью полученных результатов, научной новизной.

Автором сформулирована и решена важная научная задача повышения защищенности информации в сеансах безопасной IP-телефонии и сокращения времени установления защищенного соединения.

Основные этапы работы, результаты и выводы представлены в автореферате, который достаточно полно отражает содержание диссертации.

Диссертационная работа «Методы повышения информационной безопасности IP-телефонии с учетом вероятностно-временных характеристик протоколов распределения ключей» соответствует паспорту научной специальности и отвечает критериям, предъявляемым к кандидатским диссертациям и установленным Положением о присуждении ученых степеней, утвержденным постановлением Правительства РФ № 842 от 24.09.2013 г., а ее автор - Ковцур Максим Михайлович по уровню профессиональных, общенаучных, специальных знаний заслуживает присуждения учёной степени

кандидата технических наук по специальности 05.13.19 «Методы и системы защиты информации, информационная безопасность».

Диссертационная работа и отзыв на диссертационную работу КОВЦУРА Максима Михайловича рассмотрены и одобрены на заседании теоретической секции НТС ПАО «Интелтех» (протокол № 8 от 27 апреля 2016 года).

Главный научный сотрудник
ПАО «Интелтех»,
доктор технических наук,
профессор