Федеральное государственное бюджетное учреждение науки Санкт-Петербургский институт информатики и автоматизации Российской академии наук (СПИИРАН)

199178, Санкт-Петербург, 14 линия, 39
Телефон: (812)328-33-11 Факс: (812)328-44-50
E-mail: spiiran@iias.spb.su
http://www.spiiras.nw.ru
ОКПО 04683303, ОГРН 1027800514411
ИНН/КПП 7801003920/780101001

10.02.2016 № 073-09/65/84

УТВЕРЖДАЮ
Директор СПИИРАН
член-корреспондент РАН

_____ Юсупов Р.М.

ЗАКЛЮЧЕНИЕ

Федерального государственного бюджетного учреждения науки Санкт-Петербургского института информатики и автоматизации Российской академии наук

Диссертация Ковцура Максима Михайловича «Методы повышения информационной безопасности IP-телефонии с учетом вероятностно-временных характеристик протоколов распределения ключей» выполнена в Федеральном государственном бюджетном учреждение науки Санкт-Петербургском институте информатики и автоматизации Российской академии наук.

В период подготовки диссертации соискатель Ковцур Максим Михайлович работал в ООО "Дилер" техническим директором.

Ковцур М.М. в 2008г. окончил Санкт-Петербургский государственный университет телекоммуникаций им. М. А. Бонч-Бруевича по специальности Многоканальные телекоммуникационные системы.

В 2011г. окончил очную аспирантуру Санкт-Петербургского государственного университета телекоммуникаций им. М. А. Бонч-Бруевича.

Справка о сдаче кандидатских экзаменов № 5/195, выдана в 2016г. Федеральным государственным бюджетным учреждением науки Санкт-Петербургским институтом информатики и автоматизации Российской академии наук.

Научный руководитель– Молдовян Александр Андреевич, доктор технических наук, профессор, заместитель директора по информационной безопасности СПИИРАН.

По результатам рассмотрения диссертации «Методы повышения информационной безопасности IP-телефонии с учетом вероятностно-временных характеристик протоколов распределения ключей» принято следующее заключение:

Оценка выполненной соискателем работы.

В диссертационной работе Ковцура Максима проведен анализ основных угроз в защищенной IP-телефонии, а также изучены существующие модели нару-

шителей для IP-телефонии. На основании исследования предложена новая математическая модель активного нарушителя, учитывающая возможность нарушителя выполнить атаку на протокол распределения ключей(ПРК) в защищенной IP-телефонии. Изучены существующие ПРК IP-телефонии и их влияние на время установления защищенного соединения. На основе исследования выбраны основные пути совершенствования протоколов распределения ключей: повышение информационной безопасности и сокращение времени успешного завершения ПРК. Для времени выполнения протоколов распределения ключей предложена методика оценки вероятностно-временных характеристик ПРК защищенной IP-телефонии. Для повышения безопасности разработан метод выявления нарушителя ПРК.

Проведена апробация предложенной модели, методики и метода.

Актуальность и востребованность данной тематики обусловлена тем, что направление "3. Информационно-телекоммуникационные системы", утвержденное указом Президента Российской Федерации N 899 от 7 июля 2011 г, является одним из приоритетных направлений развития науки, технологий и техники в Российской Федерации. IP-телефония является одним из элементов информационно-телекоммуникационной системы и нашла широкое применение в сетях связи операторов в России и всего мире. Распространено использование IP-телефонии по открытым каналам передачи данных, что привело к появлению и стандартизации протоколов обеспечения безопасности IP-телефонии и делает вопросы информационной безопасности IP-телефонии еще более актуальным.

Личное участие соискателя в получении результатов, изложенных в диссертации.

Содержание диссертации и основные положения, выносимые на защиту, отражают персональный вклад автора в 16 опубликованных работах. Подготовка к публикации полученных результатов проводилась совместно с соавторами, причем вклад диссертанта был значительным. Представленные к защите результаты получены лично автором:

- Математическая модель активного нарушителя для защищенной IP-телефонии.
- Метод выявления нарушителя протоколов распределения ключей, основанных на алгоритме Диффи-Хелмана.
- Методика оценки вероятностно-временных характеристик протоколов распределения ключей защищенной IP-телефонии.

Степень достоверности результатов проведенных исследований.

Достоверность подтверждена корректностью используемых математических методов исследования, экспериментальными и теоретическими зависимостями, полученными в ходе исследования, а также апробацией основных научно-практических положений в печатных трудах и на научно-практических конференциях. Теоретические зависимости подтверждаются также результатами имитационного моделирования. Результаты диссертационной работы использованы в Управлении Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций по Северо-Западному федеральному окру-

гу при разработке методики контроля защищенных сетей электросвязи, а также в Санкт-Петербургский государственный университет телекоммуникаций им. М.А. Бонч-Бруевича и ООО «ТелКон».

Научная новизна.

Научная новизна состоит в развитии теории информационной безопасности в части исследования протоколов распределения ключей защищенной IP-телефонии:

1. Разработана модель активного нарушителя, которая учитывает особенности защищенной IP-телефонии, состоящие в использовании нескольких протоколов обеспечения безопасности одновременно, что приводит к возможности реализации атаки "человек посередине" на протоколы распределения ключей.
2. Разработана методика оценки вероятностно-временных характеристик протоколов распределения ключей защищенной IP-телефонии, учитывающая особенности этих протоколов, выраженные в наличии таймера повторной передачи сообщений с переменным временем ожидания.
3. Предложен метод выявления нарушителя для защищенной IP-телефонии, позволяющий выявить нарушителя при выполнении протоколов распределения ключей между корреспондентами, не обладающими общим ключевым материалом. Показана возможность применения данного метода на современных сетях связи, с учетом текущего технического развития.
4. Представлены модификации протокола распределения ключей с сокращенным временем успешного завершения протокола при функционировании по каналам связи с различными параметрами.

Практическая значимость результатов исследования.

Практическая значимость результатов диссертационной работы заключается в их использования при разработке методики контроля защищенных сетей электросвязи, а также в учебном процессе. Предлагаемые модель, методика и метод могут быть использованы при проектировании и разработке защищенных решений IP-телефонии, а также для модернизации существующих решений.

Модель активного нарушителя позволяет рассчитать вероятность НСД в зависимости от вероятностей промежуточных атак. Методика оценки вероятностно-временных характеристик ориентирована на расчет вероятности успешного завершения и среднего времени успешного выполнения протоколов распределения ключей при работе по каналам связи с различными значениями задержки и вероятности ошибки. Метод выявления нарушителя делает возможным количественно оценить вероятность успешной атаки активного нарушителя, вероятность обнаружения нарушителя, а также вероятность успешной выработки общего секрета между корреспондентами в зависимости от используемого числа каналов и выбранного режима работы, а также автоматически обнаружить вмешательство

нарушителя в канал связи для протокола ZRTP.

Специальность, которой соответствует диссертация.

Диссертационная работа полностью соответствует критериям «Положения о присуждении ученых степеней», предъявляемым к диссертациям на соискание ученой степени кандидата технических наук.

Диссертационная работа Ковцура М.М. представляет собой завершенную научно-квалификационную работу, выполненную лично автором, в которой решена актуальная научно-техническая задача повышения уровня защищенности информации в сеансах безопасной IP-телефонии и сокращения времени установления защищенного соединения за счет улучшения вероятностно-временных характеристик протоколов.

Диссертационная работа рекомендуется к защите по специальности 05.13.19 Методы и системы защиты информации, информационная безопасность.

Полнота изложения материалов диссертации в работах, опубликованных соискателем.

Соискатель имеет 22 научных труда. Материалы, отражающие основные результаты диссертационной работы, опубликованы в научных журналах, а также в сборниках докладов научно-технических конференций, в том числе международных. Всего по теме диссертации опубликовано 16 работ, из них: 5 работ в изданиях, входящих в перечень рецензируемых научных изданий, рекомендованных ВАК Российской Федерации, 11 статей в других изданиях и материалах конференций. Основные результаты диссертации изложены в следующих работах в необходимой полноте:

ОСНОВНЫЕ ПУБЛИКАЦИИ ПО ТЕМЕ ДИССЕРТАЦИИ

В изданиях, рекомендованных ВАК Минобрнауки РФ:

1. Ковцур, М. М. Исследование путей совершенствования протоколов распределения ключей в защищенной IP-телефонии / Ковцур М.М. // Фундаментальные исследования.–2014–№ 8(часть 6). – С. 1300-1308. –статья – 0,99/0,99 п.л., авторский вклад 100%
2. Ковцур, М. М. Повышение защиты протоколов распределения ключей от атак вторжения в середину канала связи / М. М. Ковцур, В.Н. Никитин, Д. В. Юркин // Информационно – управляющие системы. – 2014. – №1(68) – С. 70-75. – статья – 0,67/0.22 п.л., авторский вклад 33%
3. Ковцур, М. М. Анализ пропускной способности сети радиосвязи стандарта IEEE 1609 / М.М. Ковцур, В.А.Григорьев, В.Н. Никитин, В.И. Кузнецов, С.А. Тараканов, //Электросвязь.–2014– №1.–С. 10-12. –статья – 0.34/0.07 п.л., авторский вклад 20%

4. Ковцур, М. М. Обеспечение информационной безопасности ИТС / М.М. Ковцур, В.Н. Никитин, О.И. Лагутенко//Электросвязь.–2014. – №1.–С. 29-31. – статья – 0,34/0,11 п.л., авторский вклад 33%

5. Ковцур, М. М. Исследование вероятностно-временных характеристик протокола распределения ключей защищенной IP-телефонии / М.М. Ковцур, В.Н. Никитин, А.В. Винель // Информационно – управляющие системы. –2013 №1(62), С. 54-63. –статья – 1.1/0.37 п.л., авторский вклад 33%

В других изданиях:

6. Ковцур, М. М. Исследование ВВХ протоколов обеспечения безопасности VoIP телефонии при работе по каналам связи с ошибками / М.М. Ковцур // Сборник материалов Международной научно-технической и научно-методической конференции "Актуальные проблемы инфотелекоммуникаций в науке и образовании". – СПб.: СПбГУТ – 2012. – С. 235 – 236–статья – 0,14/0,14 п.л., авторский вклад 100%

7. Ковцур, М. М. Протоколы обеспечения безопасности VoIP-телефонии / М. М. Ковцур, В. Н. Никитин, Д. В. Юркин. // Защита информации.Инсайд.– 2012– №3.– С. 74-81–статья – 0.92/0.308 п.л., авторский вклад 33%

8. Ковцур, М. М. Оценка вероятностно-временных характеристик защищенной IP-телефонии / М. М. Ковцур, В. Н. Никитин, Д. В. Юркин. // Защита информации. Инсайд. – 2012.– №4. – С. 64–71–статья – 0.92/0.31 п.л., авторский вклад 33%

9. Ковцур, М.М. Экспериментальная оценка временных характеристик протокола ZRTP/ М.М. Ковцур, В.Н. Никитин // сборник материалов всероссийской конференция «Современные экономические информационные системы: актуальные вопросы организации, методы и технологии защиты информации». Йошкар-Ола, 5 октября 2012 : Межрегиональный открытый социальный институт (МОСИ). – 2012. – С. 30–35–статья – 0.33/0.16 п.л., авторский вклад 50%

10. Ковцур, М. М. Протоколы обеспечения безопасности IP-телефонии/ М. М. Ковцур // Первая миля – 2012. – №5. – С.18-26–статья – 1.1/1.1 п.л., авторский вклад 100%

11. Ковцур, М.М. О вероятностно-временных характеристиках синхронизации систем передачи с широкополосными сигналами / М.М.Ковцур, А.В. Красов, В.Н. Никитин //Труды конференции Телекоммуникационные и вычислительные системы 28 ноября 2012 г. Московский технический университет связи и информатики–статья – 0.06/0.02 п.л., авторский вклад 33%

12. Ковцур, М.М. Пути совершенствования протоколов распределения ключей для IP-телефонии / М.М. Ковцур, В.Н. Никитин// Актуальные проблемы инфотелекоммуникаций в науке и образовании. II-я Международная научно-техническая конференция: сб. научных статей / под. ред. С.М. Доценко, сост. А.Г. Владыко, Е.А. Аникевич, Л.М. Минаков. - СПб.: Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, 2013. - 1291 с. С 852 - 855–статья – 0.35/0.17 п.л., авторский вклад 50%

13. Ковцур, М. М. Исследование непересекающихся маршрутов глобальной сети / М.М. Ковцур // "Наука вчера, сегодня, завтра. №6 (6)" сборник статей по материалам VI международной научно-практической конференции .-

Новосибирск:Изд."СибАК" – 2013 – С. 19-24 –статья – 0.33/0.33 п.л., авторский вклад 100%

14. Ковцур, М. М. / Оптимизация вероятностно-временных характеристик криптографического протокола распределения ключей IP-телефонии // М.М. Ковцур Universum: технические науки. – 2014. –№ 2 (3). –С. 2. –статья – 0.23/0.23 п.л., авторский вклад 100%

15. Ковцур, М. М. Оценка скоростных характеристик реализации атаки типа перебор пароля на IP-АТС при использовании FAIL2BAN / М.М. Ковцур, А.А. Молдовян// Информационная безопасность регионов России (ИБРР-2015). IX Санкт-Петербургская межрегиональная конференция. Санкт-Петербург,28-30 октября 2015 г.: Материалы конференции / СПОИСУ. – СПб., 2015. – 418 с. – С. 171 –статья – 0.06/0.03 п.л., авторский вклад 50%

16. Ковцур М. М. Математическая модель активного нарушителя для защищенной IP-телефонии / М.М. Ковцур, В.Н. Никитин // Актуальные проблемы инфотелекоммуникаций в науке и образовании. IV Международная научно-техническая и научно - методическая конференция, Санкт-Петербург, 3-5 марта 2015: сб. научных статей в 2 т. / под. ред. С.В. Бачевского, сост. А.Г. Владыко, Е.А. Аникевич, Л.М. Минаков. - СПб.: Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, 2015. - 920 с. С 330-335 –статья – 0.56/0.56 п.л., авторский вклад 50%

Диссертация «Методы повышения информационной безопасности IP-телефонии с учетом вероятностно-временных характеристик протоколов распределения ключей» Ковцура Максима Михайловича рекомендуется к защите на соискание ученой степени кандидата технических наук по специальности 05.13.19 Методы и системы защиты информации, информационная безопасность.

Заключение принято на расширенном совместном семинаре лабораторий информационно-вычислительных систем и технологий программирования, безопасности информационных систем СПИИРАН.

Присутствовало на заседании 9 чел.

Результаты голосования: «за»-9 чел., «против» - 0 чел., «воздержалось» - 0 чел., протокол № 1 от «23» декабря 2015 г.

Заведующий лабораторией информационно-вычислительных систем и технологий программирования, д.т.н. В.Ю. Осипов

Заведующий лабораторией безопасности информационных систем, к.т.н. Р.Ш. Фахрутдинов