ОТЗЫВ ОФИЦИАЛЬНОГО ОППОНЕНТА

советника генерального директора ООО «Газинформсервис»

кандидата технических наук Кирюшкина Сергея Анатольевича

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».

Актуальность темы диссертации

IP-телефония нашла широкое применение в сетях сервис провайдеров на современном этапе развития телекоммуникационных систем. Согласно исследованиям и общедоступной статистике, наблюдается обширный рост числа пользователей IP-телефонии, а новые абоненты как правило присоединяются к ТФОП через сети с коммутацией пакетов. Однако, применение сети с коммутацией пакетов повлияло на процедуры обеспечения информационной безопасности пользователей. Теперь нарушителю, желающему получить доступ к передаваемой голосовой информации, не требуется физического присутствия рядом с линиями связи или оборудованием пользователя, так как нарушитель может реализовать удаленные атаки, а также прослушивать передаваемые голосовые данные с использованием широко распространенных анализаторов трафика.

Все это привело к созданию нескольких групп протоколов - SIPS / протоколы распределения ключей / SRTP. Существующие исследования рассматривают ИБ протоколов, при наличии предраспределенного секрета, однако недостаточное внимание уделено сценарию работы без предраспределенного секрета, а также дополнительным параметрам протоколов, таким как время выполнения при работе по КС с разными параметрами. По этой причине актуальность работы, посвященной исследованию существующих протоколов обеспечения безопасности IP-телефонии в топологии точка-точка при работе без предварительно распределенного ключевого материала не вызывает сомнения.

Соискателем решена важная 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, а также разработаны модель нарушителя для оценки защищенности системы IP-телефонии, методика оценки вероятностно-временных характеристик протоколов распределения ключей защищенной IP-телефонии, предложения по модификации протокола распределения ключей для улучшения вероятностно-временных характеристик протокола метод выявления нарушителя протоколов распределения ключей, основанных на алгоритме Диффи-Хелмана, предложения по модификации протокола Zimmermann Realtime Transport Protocol (ZRTP) для обеспечения безопасности корреспондентов.

Степень обоснованности научных положений, выводов и рекомендаций

Тема диссертации, направленность выполненных исследований, полученных результатов, соответствует пунктам № 3,6,10 паспорта специальности 05.13.19 «Методы и системы защиты информации, информационная безопасность».

На защиту вынесены следующие положения:

1. Математическая модель активного нарушителя для защищенной IP-телефонии позволяет получить аналитическую зависимость вероятности успешной атаки НСД с учетом вероятности атаки "человек посередине" на протоколы распределения ключей.

2. Метод выявления нарушителя протоколов распределения ключей, основанных на алгоритме Диффи-Хелмана, позволяет повысить безопасность IP-телефонии при отсутствии предраспределенного ключевого материала.

3. Методика оценки вероятностно-временных характеристик протоколов распределения ключей защищенной IP-телефонии позволяет рассчитать вероятность и среднее время успешного выполнения протоколов распределения ключей при работе по каналам связи с различными параметрами

Автор основывает свои результаты на базе широкого обзора работ в области защищенной IP-телефонии и информационной безопасности в целом. Для обоснования результатов Ковцур М.М. корректно применяет фундаментальные подходы и принципы, применяемые в теории вероятности, а также теорию вероятностных графов. Также автором проведена экспериментальная оценка времени работы протокола распределения

ключей по каналам связи с различными параметрами, выполнено имитационное моделирование исходного и модифицированного протоколов.

Оценка новизны и достоверности

Достоверность и обоснованность этих положений подтверждается:

- исследованием большого числа источников литературы и публикаций по теме диссертации, отраженных в списке литературы, как отечественных, так и зарубежных;

- применением корректного математического аппарата вероятностных графов и элементов теории вероятности;

- результатами теоретических расчетов подтверждаются экспериментальной оценкой и проведенным имитационным моделированием;

- апробацией результатов исследования в публикациях в отраслевых журналах по информационной безопасности, а также на тематических конференциях (российских и международных);

- непротиворечивостью результатов диссертационной работы с результатами других исследований.

Прежде всего, научная новизна определяется оценкой протоколов защищенной IP-телефонии с точки зрения вероятностно-временных характеристик, а также разработкой методов повышения ИБ для режима функционирования без предраспределенного ключевого материала.

Научной новизной обладают следующие результаты диссертационной работы:

- предложенная математическая модель активного нарушителя для защищенной IP-телефонии в отличие от моделей Докучаева В.А., Нопина С.В., Макаровой О. С. учитывает возможность реализации атаки человек посередине на протоколы обеспечения информационной безопасности IP-телефонии;

- разработанная методика оценки вероятностно-временных характеристик протоколов распределения ключей защищенной IP-телефонии в отличие от известных учитывает ограничение на количество повторных передач сообщений в протоколе, а также изменение значения задержки при каждом повторении;

- предложенный Метод выявления нарушителя протоколов распределения ключей, основанных на алгоритме Диффи-Хелмана, позволяет в отличие от других известных методов определить присутствие активного нарушителя в канале связи при отсутствии общего ключа между корреспондентами IP-телефонии;

- разработанная модификация протокола распределения ключей ZRTP, отличается от оригинального протокола сокращенным временем работы, что позволяет выполнять распределение ключей по каналам связи с задержкой до 300 мс, обеспечивая норму на время установления соединения в 1,5 секунды, определенную в приказе Министерства информационных технологий и связи РФ от 27 сентября 2007 г. №113.

Теоретическая и практическая значимость результатов исследования

Теоретическая значимость

Модель позволяет связать вероятность успешной атаки НСД активного нарушителя с вероятностями успешного завершения промежуточных атак.

Метод выявления нарушителя протоколов распределения ключей позволяет связать количество применяемых каналов связи при реализации метода повышения информационной безопасности в выбранном режиме и вероятность атаки нарушителя на протокол.

Методика оценки вероятностно-временных характеристик позволяет количественно оценить такие параметры, как вероятность успешного выполнения протокола и среднее время успешного завершения.

Практическая значимость

Модель, метод и методика могут быть использованы при проектировании, разработке, модернизации защищенных систем IP-телефонии, имеющих режим работы без предварительного ключевого материала.

В частности, метод выявления нарушителя позволяет сохранить конфиденциальность передаваемых медиаданных, сокращая вероятность успешной атаки человек посередине активного нарушителя.

Методика может использоваться для оценки таких показателей протокола распределения ключей, как среднее время работы и вероятности успешного завершения при функционировании по каналам связи с различными параметрами.

Практическая значимость подтверждается внедрением предлагаемых результатов диссертационного исследования в Санкт-Петербургском государственном университете телекоммуникаций им. проф. М.А. Бонч-Бруевича, в ООО "Телкон", а также в Управлении Роскомнадзора по Северо-Западному федеральному округу, о чем соответствуют акты в приложении диссертации.

Замечания по представленной на оппонирование диссертационной работе

К диссертационной работе имеется ряд замечаний:

1. В подразделе 1.3 представлен обзор и некоторый анализ решений по обеспечению информационной безопасности протоколов IP –телефонии. При этом в ряде случаев указано на необходимость использования инфраструктуры открытых ключей (PKI) (например, в протоколе SIP/TLS). При этом автор отмечает, что необходимость использования PKI в данном случае является недостатком, не приводя аргументации этого вывода.
2. Из пункта 3.2.2 непонятно, каким образом проверялась принадлежность удаленных IP-адресов к разным операторам связи при экспериментальной оценке вероятности совпадения маршрутов.
3. В подразделе 4.4 не указаны характеристики физических интерфейсов применяемых коммутатора и маршрутизатора.
4. Из диссертации не следует, изучалась ли автором в ходе исследований возможность стандартизации предложенных доработок протокола ZRTP через профильные Российские органы по стандартизации, взаимодействующие с IETF.

Однако указанные недостатки никаким образом не снижают положительной оценки работы и не влияют на качество полученных теоретических и практических результатов.

Заключение о соответствии регламентируемым требованиям

Полученные автором основные результаты достаточно полно опубликованы в научных изданиях. Оформление диссертации соответствует требованиям, предъявляемым к работам, направляемым в печать. Содержание автореферата соответствует основным результатам диссертации.

Диссертация имеет внутреннее единство, свидетельствует о личном вкладе автора в науку. Предложенные им новые решения аргументированы и критически оценены по сравнению с известными аналогами.

Диссертация имеет важное прикладное значение для разработки, проектирования и внедрения защищенных сетей электросвязи, а также может быть весьма полезна в учебном процессе при изучении вопросов информационной безопасности IP-телефонии.

Диссертация Ковцура М.М. представляет собой законченное научное исследование, результаты которого обладают научной новизной.

Диссертационная работа Ковцура Максима Михайловича отвечает требованиям, установленным п. 9 Положения о присуждении ученых степеней, утвержденного постановлением Правительства Российской Федерации от 24 сентября 2013 № 842, предъявляемым к кандидатским диссертациям, а ее автор заслуживает присуждение ученой степени кандидата технических наук по специальности - 05.13.19 «Методы и системы защиты информации, информационная безопасность»

официальный оппонент
советника генерального директора ООО «Газинформсервис»
кандидат технических наук
Кирюшкин Сергей Анатольевич