ОТЗЫВ ОФИЦИАЛЬНОГО ОППОНЕНТА

старшего научного сотрудника федерального государственного казенного военного образовательного учреждения высшего профессионального образования "Военная академия связи имени Маршала Советского Союза С.М. Буденного" Министерства обороны Российской Федерации,

доктора технических наук, профессора Липатникова Валерия Алексеевича

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

Конфиденциальность и целостность являются обязательными требованиями для любой телефонной сети. Со временем удалось обеспечить определенный, хотя и далекий от совершенства, уровень безопасности в традиционных сетях. Распространение IP-телефонии и ее претензии на то, чтобы стать основной технологией передачи голоса в недалеком будущем, порождают ряд проблем, с которыми традиционная телефония либо ни когда не сталкивалась, либо давно о них забыла, либо уже научилась справляться.

Отчеты последних лет ведущих компаний из области информационной безопасности Symantec, Kaspersky, Positive Technologies показывают, что сети все чаще становятся объектом атаки.

В открытых источниках встречается значительное число исследований безопасности IP-телефонии, однако большинство из них либо рассматривают защищенную IP-телефонию при наличии предварительно распределенного ключевого материала, либо рассматривают нестандартизированные решения, либо не учитывают факт работы протоколов распределения ключей.

Однако проблематика обеспечения информационной безопасности при работе без предварительно распределенного ключевого материала исследована достаточно мало.

Актуальность темы диссертации обусловлена необходимостью исследования существующих протоколов обеспечения безопасности IP-телефонии в топологии точка - точка при работе без предварительно распределенного ключевого материала.

Объектом исследования является защищенная сеть IP-телефонии, а **предметом** исследования - методы и протоколы обеспечения информационной

безопасности IP-телефонии, а также вероятностно-временные характеристики этих протоколов.

Соискателем решена научно-техническая **задача** разработки методов повышения информационной безопасности IP-телефонии с учетом вероятностно-временных характеристик протоколов распределения ключей.

Степень обоснованности научных положений, выводов и рекомендаций

Тема диссертации, полученных результатов, направленность выполненных исследований соответствует пунктам №3 (Методы, модели и средства выявления, идентификации и классификации угроз нарушения информационной безопасности объектов различного вида и класса), №6 (Модели и методы формирования комплексов средств противодействия угрозам хищения (разрушения, модификации) информации и нарушения информационной безопасности для различного вида объектов защиты вне зависимости от области их функционирования), №10 (Модели и методы оценки эффективности систем (комплексов) обеспечения информационной безопасности объектов защиты) паспорта специальности 05.13.19 «Методы и системы защиты информации, информационная безопасность».

В результате проведенных исследований в диссертации сформулированы и выдвигаются автором для публичной защиты следующие основные научные результаты.

Первый научный результат базируется на установленной автором взаимосвязи учета возможности нарушителя реализовать атаку MITM на протокол распределения ключей и другие атаки. Математическая модель активного нарушителя для защищенной IP-телефонии позволяет получить аналитическую зависимость вероятности успешной атаки несанкционированного доступа с учетом вероятности атаки "человек посередине" на протоколы распределения ключей.

Сущность второго научного результата сформулированного в диссертации, заключается в дальнейшем развитии методологических принципов исследования вероятностно-временных характеристик и протоколов распределения ключей защищенной IP-телефонии. Разработанный метод выявления нарушителя протоколов распределения ключей, основанных на алгоритме Диффи-Хелмана, позволяет повысить безопасность IP-телефонии при отсутствии предраспределенного ключевого материала.

Третий научный результат основан на модель и метод выявления нарушителя протоколов распределения ключей представляет методику оценки вероятностно-временных характеристик протоколов распределения ключей защищенной IP-телефонии. Методика позволяет рассчитать вероятность и среднее

время успешного выполнения протоколов распределения ключей при работе по каналам связи с различными параметрами.

Оценка новизны и достоверности

Обоснованность и достоверность научных результатов, выводов и рекомендаций подтверждается:

- корректной постановкой задачи диссертационного исследования;
- анализом текущего состояния дел в IP-телефонии, а также определением влияния протоколов обеспечения безопасности на показатели качества IP-телефонии;
- анализом возможных действий нарушителя и сформированной на их основе модели нарушителя;
- разработкой методов повышения безопасности для IP-телефонии при работе без предварительного распределения ключевого материала, а также возможности применимости данных методов с учетом текущего уровня развития телекоммуникационных сетей;
- разработкой методики оценки вероятности и среднего времени успешного завершения с использованием известного математического аппарата;
- оценкой и сравнением экспериментальных результатов с теоретическими выводами;
- подтверждение теоретически полученных зависимостей результатами имитационного моделирования;
- непротиворечивостью результатов имитационного моделирования.

Научная новизна определяется рассмотрением протоколов распределения ключей защищенной IP-телефонии касательно не только параметров информационной безопасности, но и вероятностно-временных параметров протоколов распределения ключей.

Разработанная модель нарушителя в отличие от аналогов позволяет учесть атаку “человек посередине” активного нарушителя на протоколы распределения ключей обеспечения безопасности IP-телефонии.

Методика оценки вероятностно-временных характеристик протоколов распределения ключей в отличие от существующих учитывает особенности протоколов распределения ключей, выраженные в наличии ограничения числа повторных передач сообщений с переменным таймером повторной передачи при работе по каналам с ошибками и задержками.

Метод выявления нарушителя в отличие от существующих методов позволяет выявить активного нарушителя протоколов в используемых каналах связи при отсутствии общего доверенного центра или ключа между корреспондентами, а также автоматически обнаружить нарушителя, владеющего

технологией синтеза голоса.

Предложенный модифицированный протокол ZRTP, отличается меньшим временем успешного завершения, что снижает временные затраты при работе протокола по каналам связи с задержками и ошибками.

Теоретическая значимость результатов исследования

Модель позволяет получить аналитическую зависимость вероятности несанкционированного доступа от вероятностей промежуточных атак.

Метод выявления нарушителя протоколов дополняет и развивает теорию информационной безопасности, в части свойств протоколов совместной выработки общего ключа, а именно: связывает число одновременно используемых каналов связи и устойчивость протоколов защищенной IP-телефонии к атаке активного нарушителя.

Методика оценки вероятностно-временных характеристик позволяет рассчитать вероятность и среднее время успешного выполнения протоколов распределения ключей при работе по каналам связи с различными значениями задержки и вероятности ошибки.

Практическая значимость результатов исследования

Модель нарушителя может быть использована при разработке методик контроля защищенных сетей электросвязи, а также в учебном процессе по дисциплине "Безопасность IP-телефонии".

Метод выявления нарушителя позволяет автоматически обнаружить вмешательство нарушителя протоколов в канал связи между корреспондентами для протокола ZRTP без участия пользователя.

Метод позволяет снизить вероятность успешной атаки несанкционированного доступа для нарушителя протоколов и может быть использован при проектировании, разработке и реализации решений защищенной IP-телефонии, имеющих режим работы без сервера, а также для усовершенствования существующих решений.

Методика может использоваться для оценки эффективности протоколов распределения ключей, в части времени выполнения и вероятности успешного завершения.

Методика оценки вероятностно-временных характеристик может применяться в расчетах при проектировании решений по защищенной IP-телефонии, использующих в своем составе протоколы распределения ключей.

В целом полученные соискателем результаты, выводы и рекомендации представляются в достаточной степени обоснованными и апробированными, обладают необходимой научной новизной и достоверностью.

Замечания по представленной на оппонирование диссертационной работе

К недостатками диссертационной работы, на мой взгляд, следует отнести:

1. Постановка задачи исследования произведена только на вербальном уровне, без математической формализации условий, ограничений и требуемого результата (целевой функции).
2. Выдвинутые автором идеи и положения не доведены до уровня технических и программно-алгоритмических решений в виде результатов интеллектуальной деятельности (изобретений, полезных мод и др.), обладающих свойствами новизны и промышленной применимости.
3. Метод выявления нарушителя не предусматривает возможность многоэтапность информационного противоборства сети IP-телефонии и нарушителя, а также предварительных действий нарушителя по подготовке к атаке.

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.

Диссертация имеет важное прикладное значение для разработки, проектирования и внедрения защищенных сетей электросвязи, а также в учебном процессе по дисциплине "Безопасность IP-телефонии".

В целом диссертация представляет собой научную квалификационную работу, в которой на основании выполненных автором исследований решена научная задача разработки методов повышения информационной безопасности IP-телефонии с учетом вероятностно-временных характеристик протоколов распределения ключей имеющей важное научно-техническое значение.

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
доктор технических наук, профессор