На правах рукописи

Ковцур Максим Михайлович

Методы повышения информационной безопасности IP-телефонии с учетом вероятностно-временных характеристик протоколов распределения ключей

Специальность 05.13.19 - Методы и системы защиты информации, информационная безопасность

Автореферат
диссертации на соискание ученой степени
кандидата технических наук

Санкт-Петербург – 2016

Работа выполнена в Федеральном государственном бюджетном учреждении науки Санкт-Петербургском институте информатики и автоматизации Российской академии наук (СПИИРАН).

Научный руководитель: доктор технических наук, профессор
Молдовян Александр Андреевич

Официальные оппоненты: Липатников Валерий Алексеевич,
доктор технических наук, профессор,
федеральное государственное казенное военное образовательное учреждение высшего профессионального образования "Военная академия связи имени Маршала Советского Союза С.М. Буденного" Министерства обороны Российской Федерации,
старший научный сотрудник

Кирюшкин Сергей Анатольевич,
кандидат технических наук,
ООО «Газинформсервис»,
советник генерального директора

Ведущая организация ПАО «Информационные телекоммуникационные технологии» (ПАО «Интелтех»), г. Санкт-Петербург.

Защита состоится ____ _____ 20__ года в __.__ на заседании диссертационного совета Д 002.199.01 при Федеральном государственном бюджетном учреждении науки Санкт-Петербургском институте информатики и автоматизации Российской академии наук (СПИИРАН) по адресу: 199178, Санкт-Петербург, В.О., 14 линия, 39.

С диссертацией можно ознакомиться в библиотеке и на сайте Федерального государственного бюджетного учреждения науки Санкт-Петербургского института информатики и автоматизации Российской академии наук (СПИИРАН), www.spiiras.nw.ru.

Автореферат разослан ___ _____ 20__ года.

Ученый секретарь
диссертационного совета Д 002.199.01,
канд. техн. наук, доцент Фаткиева Роза Равильевна

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы исследования. Современному периоду развития телекоммуникаций соответствуют возрастающие объемы трафика в корпоративных сетях, в частности, в сетях Интернет провайдеров. IP-телефонией называют технологию передачи речи по сетям с пакетной коммутацией на базе протокола IP. Как правило, под этим определением также подразумевают набор протоколов, методов и технологий, обеспечивающих голосовое общение по сети с коммутацией пакетов. Причинами распространения IP-телефонии послужили низкая стоимость в сравнении с аналоговой телефонией, вызванная применением недорогих сетей с коммутацией пакетов, а также универсальность и мобильность, позволяющая преобразовать речь в поток данных в любой точке сетевой инфраструктуры.

Развитие новых протоколов, а также передача голосовых пакетов в открытом виде через публичные сети привели к появлению и стандартизации протоколов обеспечения безопасности IP-телефонии. Протоколы разделены на группы в зависимости от решаемых задач: обеспечение безопасности сигнализации, защита медиа трафика и выработка ключей для медиа трафика.

Стандартизация протоколов, а также распространенное использование персональных компьютеров в качестве терминалов пользователя для услуг IP-телефонии привело к разработке большого числа программ для IP-телефонии, в том числе программного обеспечения (ПО) с открытым исходным кодом, позволяющего расширять возможности и использовать дополнительные алгоритмы в ПО.

Таким образом, диссертационная работа, посвященная исследованию протоколов обеспечения информационной безопасности IP-телефонии, а также разработке предложений по совершенствованию этих протоколов для обеспечения безопасности и эффективного функционирования при работе по каналам связи с различными параметрами, соответствует современной научной проблематике и является актуальной.

Степень разработанности темы. Проводятся научные исследования в областях обеспечения безопасной передачи голосовой информации, обеспечения качества при передаче голосовых и медиа данных, сжатия речи и видео, оценки качества предоставления услуг IP-телефонии. Исследования в области обеспечения информационной безопасности данных в IP-телефонии приведены в работах Нопина С.В., Майстренко В. А., Шахова В.Г., Говор Т.А., Докучаева В.А., Шведова А.В., Макаровой О.С., Крюкова Ю.С. и др.; исследования протоколов обеспечения информационной безопасности IP-телефонии – в работах Оника Э., Riccardo Bresciani и A. Butterfield, C. V. Wright, V. Shmatikov, Prateek Gupta и др.; исследования в области атак MITM и методов защиты от них описываются в работах Атрощенко В.А., Руденко М.В., Липатникова В.А., Дьяченко Р.А., Canteaut A., Sun H., Song J., Радивилова Т.А., Кирюшкина С. А., Карпухина Е.О.; обеспечение QoS (Quality of Service) и оценка качества, а также моделирование сетей IP-телефонии – в работах Krzysztof Perlicki, Сухова А. М., Федосеевой О. С., Меркулова А.Г., Erol Gelenbe, Ricardo Lent, Rafik A. Goubran, P.Eng. и др.; исследование методов обеспечения безопасности протоколов – в работах Ф. Циммермана, Демьянчука А.А., Новикова Е.С., Молдовяна Д.Н. Значительный вклад в иссле-

дование временных характеристик протоколов внесли Никитин В.Н., а также Нсангу М. М., Юркин Д.В., Винель А.В., Лосев Ю.И., Руккас К.М., Галкин А.М.;

Недостаточно освещенным остается вопрос обеспечения безопасности для сценария IP-телефонии точка-точка в случае, когда корреспонденты не имеют заранее выработанного ключевого материала. Также малоизученными являются вероятностно-временные характеристики протоколов безопасности IP-телефонии и вопрос о влиянии этих протоколов на выполнение установленных норм при использовании IP-телефонии.

В работах Нопина С.В., Макаровой О. С., Докучаева В.А., Миронова В.Г., Привалова А.А., Евглевской Н.В., Зубкова К.Н. приводятся описания моделей нарушителя безопасности информационных систем, в том числе нарушителя в IP-телефонии. Однако общим недостатком работ является то, что не описывается атака "человек посередине" на протоколы распределения ключей. Таким образом целесообразно разработать новую модель нарушителя, учитывающую эту атаку. Объектом исследования является защищенная IP-телефония, а предметом исследования – методы и протоколы обеспечения информационной безопасности IP-телефонии, а также вероятностно-временные характеристики этих протоколов.

Цель и задачи исследования. Целью является повышение уровня защищенности информации в сеансах безопасной IP-телефонии и сокращение времени установления защищенного соединения. Для достижения поставленной цели решены следующие задачи:

– исследование существующих протоколов безопасности IP-телефонии, их параметров, характеристик и особенностей, а также влияния протоколов на показатели качества;

– разработка модели нарушителя для оценки защищенности системы IP-телефонии;

– разработка методики оценки вероятностно-временных характеристик протоколов распределения ключей защищенной IP-телефонии;

– разработка предложений по модификации протокола распределения ключей для улучшения вероятностно-временных характеристик протокола;

– разработка метода выявления нарушителя протоколов распределения ключей, основанных на алгоритме Диффи-Хелмана;

– разработка предложений по модификации протокола Zimmermann Real-time Transport Protocol (ZRTP) для обеспечения безопасности корреспондентов при взаимодействии без сервера в топологии клиент-клиент.

Научная новизна

1. Разработанная модель нарушителя отличается от известных аналогов учетом атаки “человек посередине” на протоколы обеспечения безопасности IP-телефонии.
2. 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.
3. Метод выявления нарушителя в отличие от существующих методов позво-

ляет 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.

4. Модифицированный протокол ZRTP, отличающийся меньшим временем успешного завершения, что снижает временные затраты при работе протокола по каналам связи с задержками и ошибками.

Теоретическая и практическая значимость работы. Теоретическая значимость: Модель позволяет получить аналитическую зависимость вероятности несанкционированного доступа (НСД) к информации 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: 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 НСД 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.

Результат работы используется в преподавании курсов “Безопасность IP-телефонии” в СПб ГУТ им М.А. Бонч-Бруевича на кафедре Защищенных Систем Связи, в Управлении Роскомнадзора по Северо-Западному федеральному округу, а также в ООО "Телкон".

Методология и методы исследования. Для решения поставленных задач использовались методы вероятностных графов, теории вероятности, комбинаторики. Для анализа данных разрабатывались дополнительные прикладные программы с использованием объектно-ориентированного программирования. Для экспериментальной оценки использовалось дополнительное программное обеспе-

чение – анализатор трафика, Zfone и программно-аппаратный маршрутизатор на базе платформы FreeBSD для эмуляции канала связи (КС).

Положения, выносимые на защиту:

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.

Степень достоверности и апробация результатов. Достоверность подтверждается корректностью применяемых математических методов исследования. Полученные теоретические и экспериментальные зависимости не противоречат результатам других исследований. Теоретические зависимости подтверждаются проведенными экспериментами, а также имитационным моделированием**.**

Основные положения работы докладывались на конференции «Современные экономические информационные системы: актуальные вопросы организации, методы и технологии защиты информации», Йошкар-Ола, 5 октября 2012, Межрегиональный открытый социальный институт; международной научно-технической и научно-методической конференции "Актуальные проблемы инфотелекоммуникаций в науке и образовании" 20 - 24 февраля 2012, Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича; II-й Международной научно-технической конференции «Актуальные проблемы инфотелекоммуникаций в науке и образовании” 26-27 февраля 2013, Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича; конференции Телекоммуникационные и вычислительные системы 28 ноября 2012 г, Московский технический университет связи и информатики; VI международной научно-практической конференции "Наука вчера, сегодня, завтра» 13 ноября 2013 г., Новосибирск;. IX Санкт-Петербургской межрегиональной конференции "Информационная безопасность регионов России (ИБРР-2015)" 28-30 октября 2015 г., Санкт-Петербург; IV Международной научно-технической и научно - методической конференции "Актуальные проблемы инфотелекоммуникаций в науке и образовании" 3-4 марта 2015, Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича.

Результат работы используется в преподавании курсов “Безопасность IP-телефонии” в СПб ГУТ им. М.А. Бонч-Бруевича на кафедре Защищенных Систем Связи, в Управлении Роскомнадзора по Северо-Западному федеральному округу, а также в ООО "Телкон", о чем получены акты внедрения.

Публикации. Результаты диссертации отражены в 16 публикациях, в том числе 5 публикациях в изданиях, входящих в перечень ВАК.

Личный вклад автора. Теоретические и практические выводы, результаты экспериментов, основные научные положения получены и сформулированы автором самостоятельно.

Структура и объем работы. Диссертация состоит из введения, четырех глав, заключения, списка источников литературы и приложений. Работа изложена на 153 страницах основного текста, содержит 54 рисунка, 14 таблиц, список литературы включает 122 источников, из них 35 иностранных. Приложения представлены на 58 страницах.

КРАТКОЕ СОДЕРЖАНИЕ РАБОТЫ

Во введении обоснована актуальность темы диссертации, представлены цель исследования, научная новизна, практическая ценность результатов диссертации.

В первой главе приведена классификация протоколов IP-телефонии и сценарии установления соединения. Представлены показатели качества защищенной IP-телефонии, а также описаны методы обеспечения качества. К показателям качества защищенной IP-телефонии относятся:

- качество речи (диалог - возможность пользователя связываться и разговаривать в реальном времени в полнодуплексном режиме с другим пользователем; разборчивость - чистота и тональность речи; эхо - слышимость собственной речи; уровень - громкость речи);
- качество сигнализации (задержки при установлении вызова - скорость успешного доступа и время установления соединения; завершение вызова - время отбоя и скорость разъединения; DTMF - определение и фиксация сигналов многочастотного набора номера);
- время выполнения защищенного соединения т.е. время установления речевого канала между корреспондентами, использующими протоколы распределения ключе (ПРК);
- вероятность успешной атаки нарушителя на IP-телефонию, работающую в защищенном режиме;
- время и вероятность успешного завершения протоколов обеспечения безопасности.

Приведена классификация протоколов обеспечения безопасности IP-телефонии. Выделяется три категории: протокол защиты сигнализации (Secured SIP), протокол защиты медиа информации (SRTP) и протоколы распределения ключей (ПРК) для защиты медиа информации (MIKEY, SDES, ZRTP, DTLS).

В диссертации разработаны требования, которым должен удовлетворять протокол распределения ключей, применяемый в топологии точка-точка между корреспондентам, не имеющими предраспределенного ключевого материала:

- Протокол должен поддерживать работу как в топологии клиент-сервер, так и в топологии клиент-клиент.
- Протокол должен быть самодостаточным и выполнять распределение ключей без применения дополнительных протоколов между корреспондентами.

- Протокол должен поддерживать механизм распределения ключей в топологии клиент-клиент без передачи ключа в явном виде по каналу связи (КС).
- Протокол должен иметь механизм обнаружения атаки человек посередине без заранее распределенного ключевого материала между корреспондентами.
- Протокол должен использовать TCP/UDP порты, применяемые для IP-телефонии, или TCP/UDP порты, использование которых согласовано в результате установления соединения.

Выполнена постановка научных задач диссертационного исследования.

Во второй главе описана математическая модель активного нарушителя, учитывающая атаку "человек посередине" (Man In The Middle, MITM) на ПРК и позволяющая определить вероятность успешной атаки НСД на систему защищенной IP-телефонии, работающую по схеме точка-точка. Модель опубликована в [1]. Для построения математической модели нарушителя выполнен анализ угроз и их источников. Используя уязвимости, активный нарушитель может выполнять комбинацию атак, которая может привести к достижению НСД.

В качестве основных возможных атак активного нарушителя выделены:

- перебор пароля для доступа к управлению оборудованием оператора или пользователя;
- организация проксирования или перенаправления всего или части трафика любым доступным способом;
- реализация атаки MITM на ПРК и другие протоколы безопасной IP-телефонии;
- атака на шифр – перебор ключа к перехваченному медиа трафику;
- установка закладки, модификация программного обеспечения (ПО) терминала пользователя;
- установка дополнительного оборудования на узле оператора связи;
- модификация настроек терминала пользователя для частичного отключения безопасности;
- перехват авторизационных данных для управления терминалом пользователя за счет прослушивания трафика управления шлюзом.

При разработке модели нарушителя введено допущение, что если субъект атаки находится в одной сети с объектом атаки, то такой нарушитель является внутренним. В противном случае он является внешним. Тогда промежуточными целями нарушителей с точки зрения получения НСД являются:

$Ц_А$) захват оборудования оператора внешним нарушителем;

$Ц_Б$) захват терминала пользователя внешним нарушителем;

$Ц_В$) захват оборудования оператора внутренним нарушителем**;**

$Ц_Г$) захват терминала пользователя внутренним нарушителем.

Разработка модели начинается с анализа алгоритмов действий нарушителя по каждой из перечисленных целей. Алгоритмы представлены на рисунке 1. Используя алгоритмы действий нарушителя каждого типа, составляются вероятностные графы, представленные на рисунке 2. По каждому графу выполняется упрощение, выделяется ветвь, соответствующая успешному выполнению атаки

НСД, и составляется производящая функция $H(x)$ этой ветви. Вычисляется $P_{НСД} = H(x=1)$ для каждого из графов, в результате чего получается:

$$P_{нсдЦА} = p_{13A} p_{34A} (p_{45A} p_{57A} + p_{46A} p_{67A}), \quad (1)$$

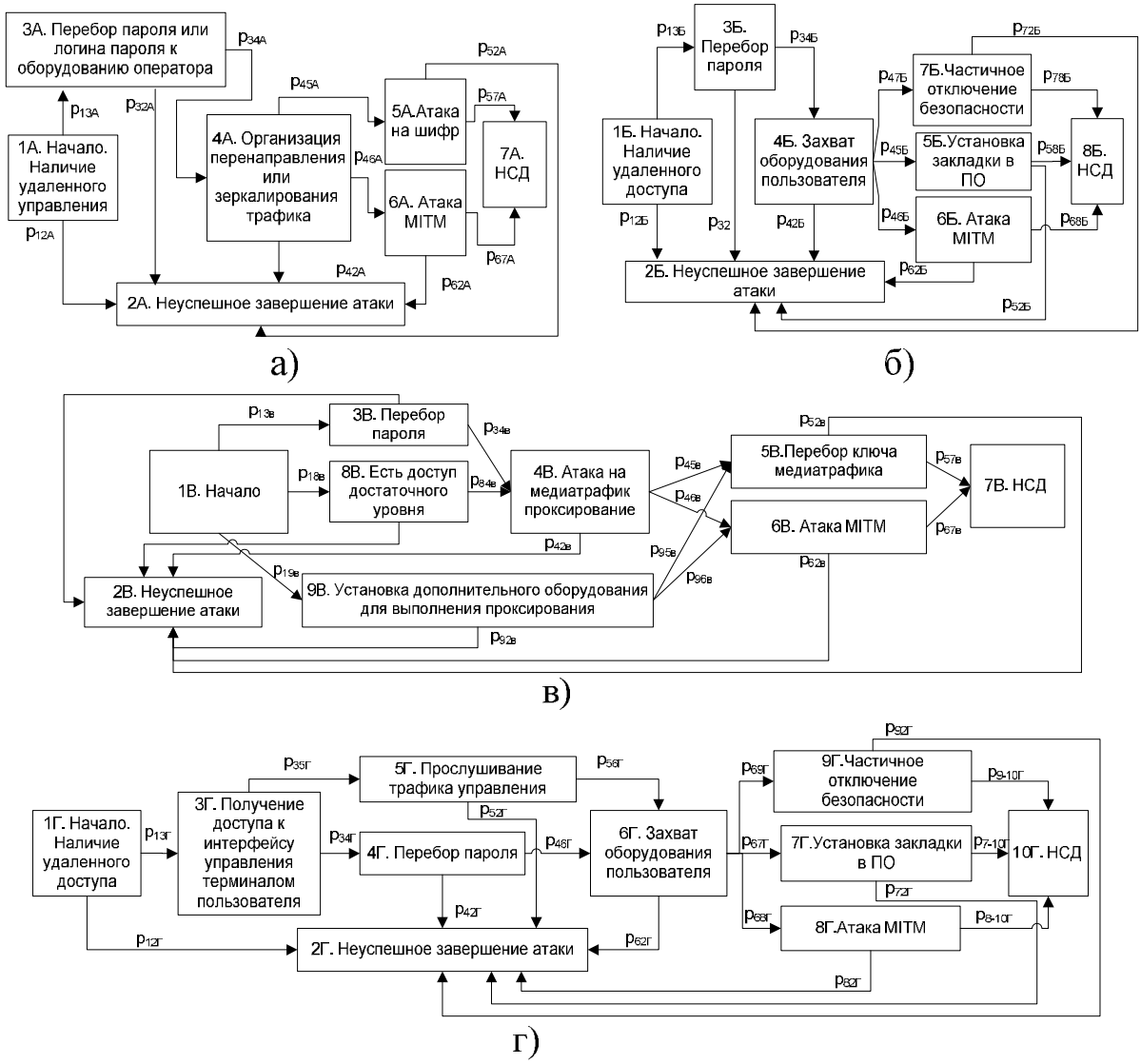

Рисунок 1 – Возможные алгоритмы действий при реализации различных целей: а)$Ц_А$, б)$Ц_Б$, в)$Ц_В$, г)$Ц_Г$

$$P_{нсдЦБ} = p_{13Б} p_{34Б} (p_{45Б} p_{58Б} + p_{46Б} p_{68Б} + p_{47Б} p_{78Б}), \quad (2)$$

$$P_{нсдЦВ} = ((p_{13В} p_{34В} + p_{18В} p_{84В}) p_{45В} + p_{19В} p_{95В}) p_{57В} + ((p_{13В} p_{34В} + p_{18В} p_{84В}) p_{46В} + p_{19В} p_{96В}) p_{67В}, \quad (3)$$

$$P_{нсдЦГ} = p_{13Г} (p_{34Г} p_{46Г} + p_{35Г} p_{56Г}) (p_{67Г} p_{7\text{-}10Г} + p_{68Г} p_{8\text{-}10Г} + p_{69Г} p_{9\text{-}10Г}), \quad (4)$$

где p_{ijX} – вероятность перехода из вершины i в вершину j для соответствующего графа.

Тогда вероятность успешной атаки нарушителя будет иметь вид:

$$P_{НСД} = max \{ P_{нсдЦА}, P_{нсдЦБ}, P_{нсдЦВ}, P_{нсдЦГ} \}. \quad (5)$$

Очевидно, в случае установления соединения в сценарии без сервера и при отсутствии предварительно распределенного ключевого материала, сам пользова-

тель является наиболее заинтересованным лицом для повышения безопасности и снижения $P_{НСД}$. Пользователь может использовать VoIP терминал, поддерживающий функцию отключения удаленного управления, что приведет к $p_{13Б}$=0, $p_{13Г}$=0, и, как следствие, $P_{НСДЦБ}$=0, $P_{НСДЦГ}$=0. Однако, пользователь не может оказывать влияние на вероятности *pijA*, *pijB*. В зависимости от промежуточных целей нарушителя можно выделить несколько частных моделей нарушителей:

В1) атака внутреннего нарушителя через перебор пароля на оборудование оператора путем организации MITM;

В2) атака внутреннего нарушителя при наличии у него доступа на оборудование путем организации MITM;

В3) атака внутреннего нарушителя через установку дополнительного оборудования на узле оператора для организации MITM;

А4) атака внешнего нарушителя через перебор пароля на оборудование оператора для организации MITM.

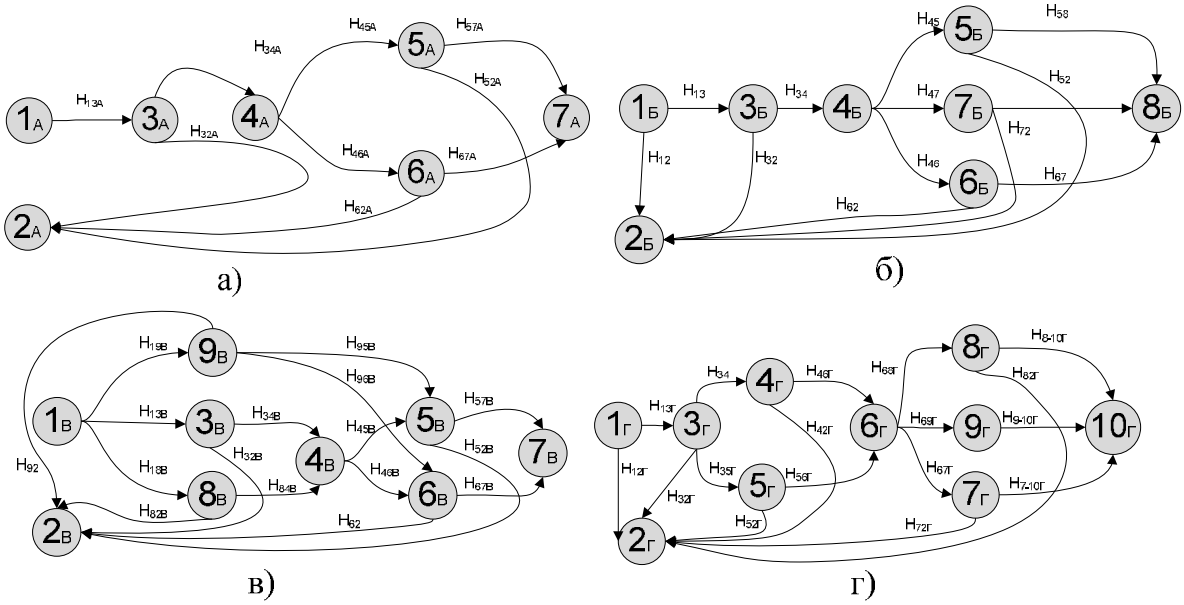

Рисунок 2 – Вероятностный граф по соответствующим алгоритмам действий нарушителя при реализации целей: а) $Ц_А$, б) $Ц_Б$, в) $Ц_В$, г) $Ц_Г$

Для нарушителей В1,В2,В3,А4 представлены $P_{НСД}$:

$$P_{нсдВ1}=p_{34В}p_{67В}, \quad (6)$$

$$P_{нсдВ2}=p_{84В}p_{67В}, \quad (7)$$

$$P_{нсдВ3}=p_{67В}, \quad (8)$$

$$P_{нсдА4}=p_{34А}p_{67А}, \quad (9)$$

где: $p_{34А}$, $p_{34В}$ – вероятность успешного завершения атаки перебор пароля для доступа к оборудованию оператора; $p_{84В}$ – вероятность использования нарушителем имеющегося доступа достаточного уровня на оборудование оператора; $p_{67А}$, $p_{67В}$ – вероятность успешного завершения “атаки на механизм распределения ключей”.

Очевидно, что $P_{нсдВ3}$ больше или равна $P_{нсдВ1}$, $P_{нсдВ2}$, $P_{нсдА4}$. Следовательно, $P_{НСД}$ будет определяться величиной $p_{67В}$, которая будет соответствовать атаке НСД внутреннего нарушителя на узле оператора связи посредством установки дополнительного оборудования для организации MITM. Поэтому, целесообразно

сократить p_{67B}, обеспечивая защиту от нарушителя, нацеленного на MITM.

В третьей главе выполнена оценка вероятности существования непересекающихся пар и троек маршрутов в глобальной сети, предложены и обоснованы методы модернизации ПРК с целью повышения безопасности ПРК.

Предложены методы повышения безопасности ПРК, не требующие заранее распределенного ключевого материала у корреспондентов, опубликованные в [2]. Однако, для реализации методов важно, чтоб используемые каналы связи были независимыми, то есть не имели общих точек. При наличии общей точки, захватив ее, активный нарушитель может выполнить атаку MITM в двух КС одновременно.

Поэтому необходимо оценить вероятность наличия независимых КС в глобальной сети при подключении к разным операторам связи. Методика оценки вероятности совпадения маршрутов состоит в следующем:

- Выполняется теоретическая оценка, показывающая количество пар и троек маршрутов между пунктами.
- Осуществляется выбор узлов глобальной сети для сбора статистики. Фактически узлами являются IP-адреса, принадлежащие разным операторам и доступные в населенном пункте каждого из корреспондентов.
- Выполняется проверка выбранного удаленного IP-адреса к населенному пункту соответствующего респондента и к оператору связи.
- Выполняется сбор статистики при подключении к разным операторам и до каждого из удаленных узлов. Сбор выполняется с использованием команды tracert Windows и результат сохраняется в файл.
- Полученные результаты загружаются в базу данных MySQL и выполняется алгоритм поиска совпадения пар и троек маршрутов.

В ходе эксперимента для проверки наличия независимых маршрутов между корреспондентами выбраны города Санкт-Петербург, Москва и др. Итоговый результат приведен в таблице 1. Таким образом, только 4,9% из всех возможных пар маршрутов имели общие точки между собой. В результате практического эксперимента также не было обнаружено ни одного из крупных городов, с которым не было бы хоть одной пары маршрутов без общих точек. Можно сделать вывод, что применение двух и более КС, предоставляемых разными операторами связи, между абонентами позволяет организовать с большой вероятностью два независимых канала связи, не имеющих общей точки.

Общее количество возможных сочетаний маршрутов Way_count_i для i-го направления также определяется по формуле 10 и позволяет получить число пар и троек для дальнейшего сравнения с результатом эксперимента:

$$Way\_count_i = \frac{\prod_{i=0}^{Ipw-1}(N_S - i)\prod_{i=0}^{Ipw-1}(N_D - i)}{Ipw!}, \qquad (10)$$

где N_S – число независимых точек выполнения трассировки;

N_D – число IP-адресов в удаленной точке маршрута;

Ipw – количество маршрутов, сравниваемых при оценке совпадений.

С распространением интернет многие имеют в распоряжении несколько подключений к разным операторам связи с использованием разных технологий (WiFi, 3G, 4G и т.д.). Как правило, эти подключения являются открытыми каналами общего пользования, могут подвергаться атакам нарушителей или содержать нарушителя, выполняющего атаку человек посередине. В данных условиях – методы повышения безопасности состоят в использовании нескольких независимых КС одновременно. Методы позволяют повысить безопасность за счет внедрения механизма обнаружения нарушителя и для некоторых случаев – исключения нарушителя из КС. Предлагается несколько модификаций метода выявления нарушителя протоколов распределения ключей, основанных на алгоритме Диффи-Хелмана, при использовании нескольких независимых КС:

- двухканальный метод, когда корреспонденты имеют два независимых КС (2К);
- трехканальный метод в режиме обнаружения нарушителя (3-ОН);
- трехканальный метод в режиме исключения нарушителя(3-ИН).

Таблица 1. Результаты оценки числа независимых пар и троек маршрутов между выбранными городами

Страна	Город	Число точек в городе	Для пар маршрутов				Для троек маршрутов			
			Общее число маршрутов	Число маршрутов без общих точек	Число маршрутов с общей точкой	% совпадения маршрутов	Общее число маршрутов	Число маршрутов без общих точек	Число маршрутов с общей точкой	% совпадения маршрутов
Россия	Барнаул	3	60	59	1	1,67%	60	57	3	5,00%
Россия	Москва	3	60	60		0,00%	60	60		0,00%
Россия	Новосибирск	3	60	60		0,00%	60	60		0,00%
Германия	Берлин	3	60	57	3	5,00%	60	51	9	15,00%
Германия	Мюнхен	3	60	60		0,00%	60	60		0,00%
США	Нью-Йорк	4	120	119	1	0,83%	240	234	6	2,50%
США	Эддиссон	3	60	59	1	1,67%	60	57	3	5,00%
Австралия	Сидней	3	60	58	2	3,33%	60	57	3	5,00%
Австралия	Мельбурн	5	200	157	43	21,5%	600	116	484	81,07%
Россия	Санкт-Петербург	12	1320	1320		0,00%	13200	13200		0,00%
США	Даллас	3	60	51	9	15,00%	60	33	27	45,00%
Япония	Фукуока	3	60	34	26	43,33%	60		60	100,00%
Япония	Токио - Чийода	7	420	384	36	8,57%	2100	1576	524	24,95%
Всего				2478	122	4,9%		15561	1119	7,2%

В качестве показателей для оценки безопасности выбраны вероятность успешной атаки MITM $P_{УА}$, вероятность обнаружения нарушителя $P_{ОН}$, вероятность успешной генерации общего секрета $P_{УК}$. В качестве входного параметра при анализе используется $P_{НIК}$ – вероятность нахождения активного нарушителя, способного выполнить атаку MITM, в одном КС.

Для реализации 2К метода повышения безопасности корреспондент А отправляет одинаковое сообщение Диффи-Хелмана (ДХ) корреспонденту Б по двум каналам связи. Если присутствует активный нарушитель в одном из каналов связи, он изменяет сообщение ДХ для участия в протоколе выработки ключа. Корреспондент Б получает сообщения от корреспондента А, сравнивает их. Если сообщения одинаковые, значит либо отсутствует активный нарушитель в двух КС, либо присутствует один и тот же нарушитель в обоих каналах. Если сообщения разные, значит присутствует нарушитель в одном канале связи или два независимых нарушителя в двух каналах связи. Корреспондент Б отправляет два ответных сообщения ДХ по двум КС. Корреспондент А получает сообщения и сравнивает их. $P_{УА}$, $P_{ОН}$, $P_{УК}$ определяются по формулам:

$$P_{УА2К} = (P_{Н1К})^2, \quad (11)$$

$$P_{ОН2К} = 2(1- P_{Н1К})\, P_{Н1К}, \quad (12)$$

$$P_{УК2К} = (1- P_{Н1К})^2, \quad (13)$$

где $P_{Н1К}$ – вероятность, что нарушитель может выполнить успешную атаку MITM в одном из КС.

Для трехканального протокола в режиме ОН:

$$P_{УА3\text{-}ОН} = (P_{Н1К})^3, \quad (14)$$

$$P_{ОН3\text{-}ОН} = 3(1- P_{Н1К})^2\, P_{Н1К} + 3(1- P_{Н1К})\, P_{Н1К}^2, \quad (15)$$

$$P_{УК3\text{-}ОН} = (1- P_{Н1К})^3. \quad (16)$$

Для трехканального протокола в режиме ИН:

$$P_{УА3\text{-}ИН} = (P_{Н1К})^3 + 3(1- P_{Н1К})\, P_{Н1К}^2, \quad (17)$$

$$P_{ОН3\text{-}ИН} = 3(1- P_{Н1К})^2\, P_{Н1К}, \quad (18)$$

$$P_{УК3\text{-}ИН} = (1- P_{Н1К})^3 + 3(1- P_{Н1К})^2\, P_{Н1К}. \quad (19)$$

Итоговые графики зависимостей показателей для оценки безопасности приведены на рисунке 3.

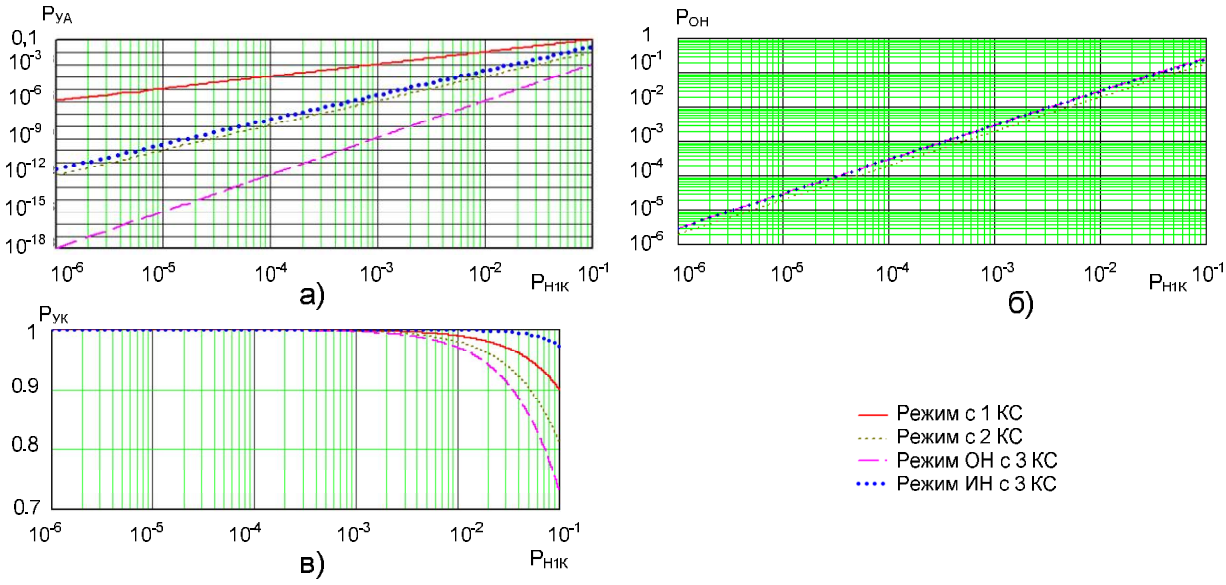

Рисунок 3 – Сравнительные характеристики ПРК в четырех режимах: а) вероятность успешной атаки MITM; б) вероятность обнаружения нарушителя; в) вероятность успешной выработки ключа

Из всех представленных реализаций трехканальная в режиме ОН имеет наименьшую вероятность успешной атаки MITM и наивысшую вероятность обнаружения нарушителя. Трехканальная реализация в режиме ИН имеет наивысшую вероятность успешной выработки ключа. Двухканальная реализация может использоваться в случае наличия у корреспондентов не более двух КС.

Протокол ZRTP по сравнению с другими ПРК – DTLS, SDES, MIKEY – имеет встроенный механизм защиты от активного нарушителя, выраженный в вербальной проверке Short Authentication String (SAS) обоими корреспондентами по второму, установившемуся защищенному голосовому каналу связи. Однако, данный механизм не устойчив против атаки MITM активного нарушителя, владеющего технологией синтеза голоса, а также модификацией передаваемых голосовых данных.

Схема возможной атаки нарушителя представлена на рисунке 4. В качестве метода повышения безопасности ZRTP предлагается внедрить механизм автоматической проверки SAS в протокол с использованием дополнительного канала связи. В качестве данного КС может выступать SMS, отправленное корреспонденту А от корреспондента Б для автоматического анализа, пакет с данными, отправленный по сети с пакетной коммутацией, и т.д. Схема взаимодействия корреспондентов показана на рисунке 5,а. Для схемы также вычислены $P_{УА}$, $P_{ОУ}$, $P_{ИН}$.

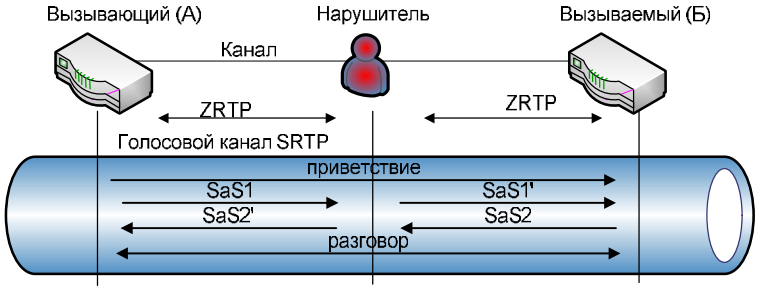

Рисунок 4 – Нарушитель, выполняющий замену SAS в голосовом канале связи

Схема взаимодействия корреспондентов для двухканального и трехканального режима ZRTP показана на рисунке 5, б и 5, в соответственно.

В четвертой главе описывается методика оценки вероятностно-временных характеристик (ВВХ) ПРК защищенной IP-телефонии, позволяющая оценить среднее время и вероятность успешного завершения протоколов обеспечения информационной безопасности IP-телефонии в зависимости от параметров КС с учетом особенностей ПРК и опубликованная в [5].

Для оценки ВВХ ПРК представляется в виде вероятностного графа, каждая ветвь которого соответствует передаче какого-либо сообщения протокола. Особенностью ПРК является наличие ограниченного числа повторных передач сообщений в случае недоставки, а также переменное значение задержки при повторной передаче сообщений. Из составленного вероятностного графа в соответствии с методикой выделяется ветвь успешного завершения ПРК. Выполняется упрощение вероятностного графа, для ветви успешного завершения определяется производящая функция $H(x)$:

$$H(x) = f(p_i x^{ti}), \quad (20)$$

где $p_i = (1 - p_0)^{ni}$;

n_i - длина i-го сообщения, бит;

p_0 - вероятность битовой ошибки в КС;

t_i - время передачи i-го сообщения, с.

С использованием производящей функции вычисляется среднее время успешного завершения протокола T_{CP} и вероятность успешного завершения протокола P в зависимости от задержки и битовой ошибки в КС. Используется модель КС – дискретный канал без памяти. T_{CP} и P будут иметь вид:

$$T_{CP} = \frac{dH(x)}{dx}(x = 1). \quad (21)$$

$$P = H(x = 1). \quad (22)$$

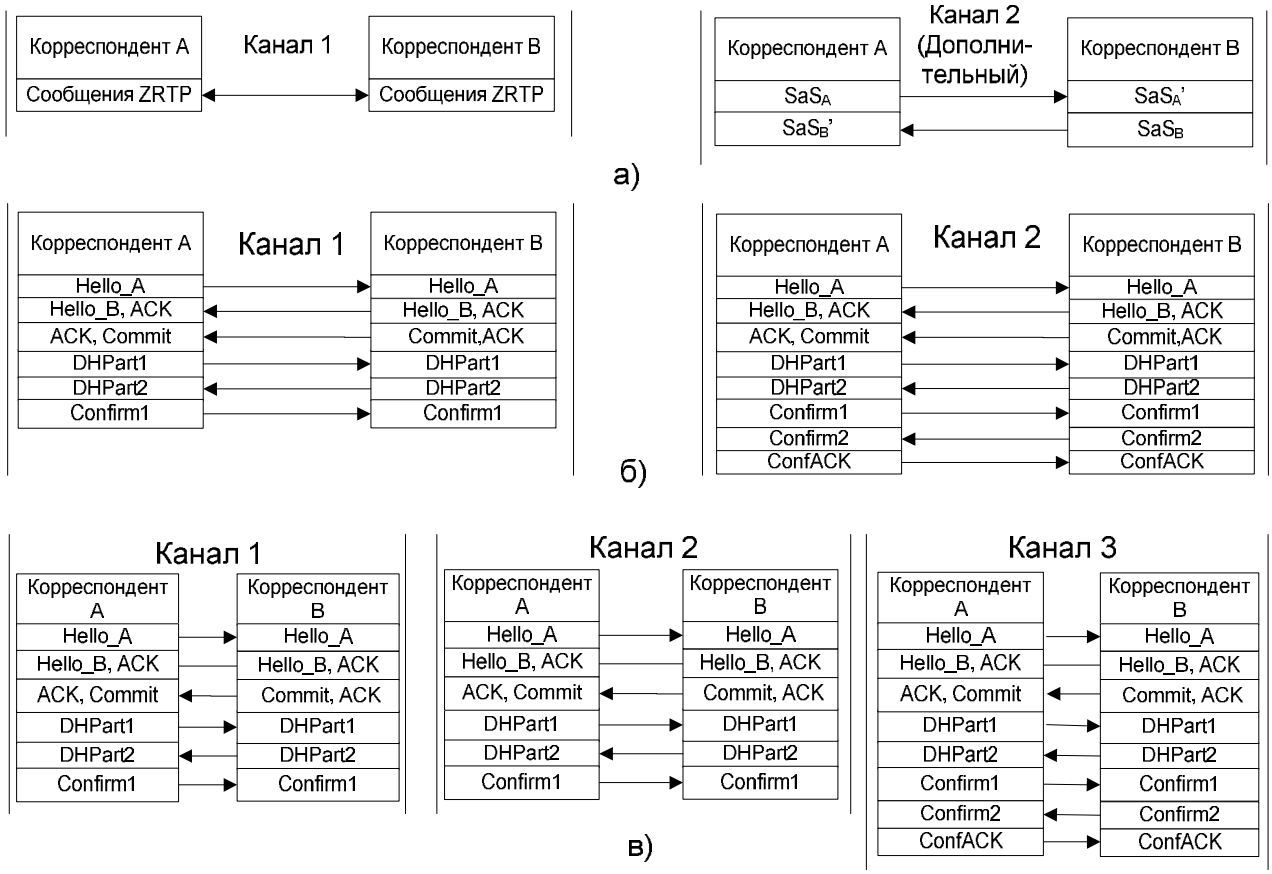

Рисунок 5 – Вариант взаимодействия корреспондентов при использовании а) механизма автоматической проверки SAS для протокола ZRTP; б) двухканального режима ZRTP; в) трехканального режима ZRTP

Полученные зависимости для протокола ZRTP и DTLS для разных задержек d в КС и разных значений битовой ошибки p_0, приведены на рисунке 6. Насколько видно из графика для ZRTP, при $d \geq 300$ мс, p_0=10^{-5} T_{CP} ZRTP составляет 2,5 сек и превышает норму на 60%. Целесообразно сокращать T_{CP} для уменьшения времени, необходимого на организацию защищенного соединения.

Для протокола ZRTP была выполнена экспериментальная оценка ВВХ T_{CP}. Схема эксперимента представлена на рисунке 7. Полученные точки нанесены на

график, показанный на рисунке 6. Эксперимент подтверждает теоретически полученную зависимость.

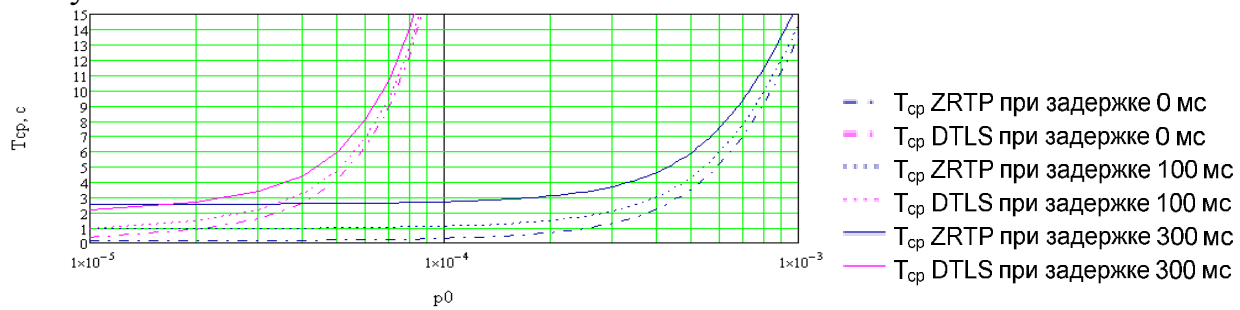

Рисунок 6 – Зависимость среднего времени выполнения протоколов ZRTP и DTLS от p_0 при разных значениях d

Сценарий обмена сообщениями в протоколе ZRTP представлен на рисунке 4,б, второй канал. Сам протокол разделяется на четыре фазы. Протокол ZRTP выполняется после установления соединения между корреспондентами, что влияет на время установления защищенного речевого канала связи.

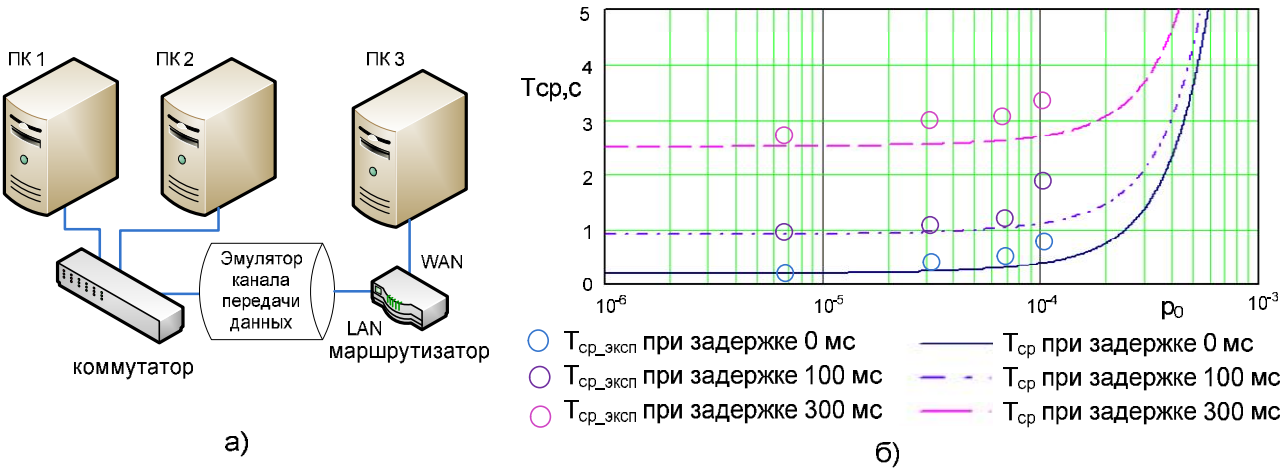

Рисунок 7 – Экспериментальная оценка среднего времени выполнения ZRTP
а) схема эксперимента б) сравнение теоретической зависимости и экспериментально полученных значений $T_{ср}$

Оценка среднего времени выполнения протокола при d=0, 100, 300 мс представлены на рисунке 6. Целесообразным является сокращение среднего времени успешного выполнения протокола T_{CP} для соблюдения $T_{CP} \leq 1{,}5$ с при работе по каналам с задержками до 300 мс.

Сокращение времени установления защищенного соединения достигается за счет объединения нескольких фаз с потерей некоторого функционала, который не используется в топологии точка-точка. В первой модификации протокола улучшение среднего времени достигается за счет отказа от существующего механизма выбора инициатора и респондента за счет отправки отдельного сообщения. Инициатором в этом случае предлагается выбирать корреспондента, который первым отправил сообщение протокола DHPart1. Также дополнительно выполняется объединение информационных данных о поддерживаемых криптографических наборах и информационных блоков протокола Диффи-Хелмана. Обмен сообще-

ниями протокола во второй модификации, а также соответствующий вероятностный граф приведен на рисунке 8.

Сравнение графиков среднего времени успешного завершения исходного протокола ZRTP $T_{прот}$, первой $T_{мод1}$ и второй $T_{мод2}$ модификации представлено на рисунке 9. Выигрыш во времени T_{B2}, характеризующий сэкономленное время за счет применения модифицированного протокола по сравнению с исходным, и относительный выигрыш B_{B2} , отражающий отношение сэкономленного времени к $T_{прот}$, определены по формулам:

$$T_{B2} = T_{прот} - T_{мод2}, \quad (23)$$

$$B_{B2} = T_{B2} / T_{прот} \ . \quad (24)$$

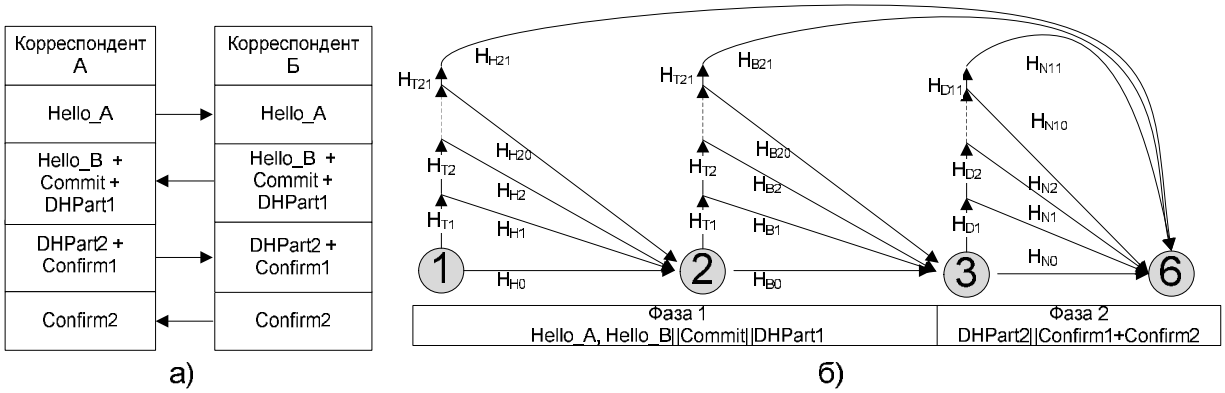

Рисунок 8 – Вторая модификация протокола; а) сценарий обмена сообщениями; б) вероятностный граф

Сравнение графиков представлено на рисунке 9 и в таблице 2.

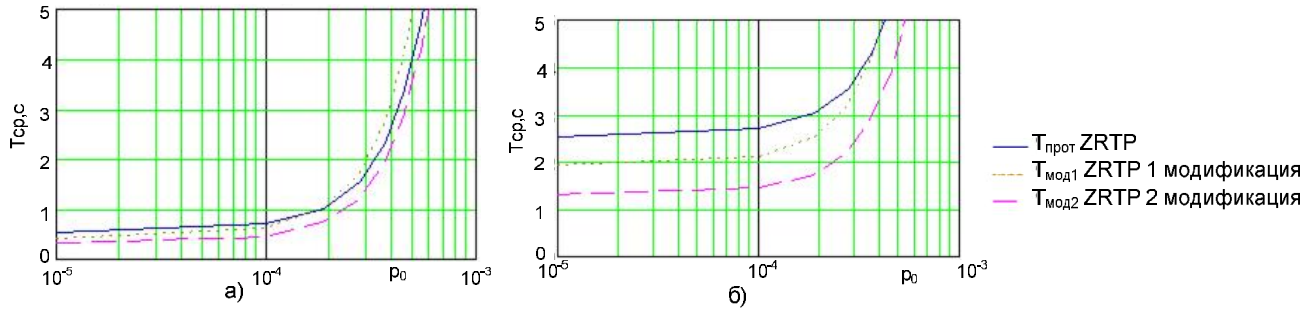

Рисунок 9 – Сравнение среднего времени успешного завершения оригинального ZRTP, первой и второй модификаций ZRTP а) при d=50мс; б) при d=300мс

Таблица 2. Оценка выигрыша среднего времени успешного завершения модифицированного ZRTP

Задержка	50мс			150мс			300мс			400мс		
p_0	10^{-5}	$5{\cdot}10^{-5}$	10^{-4}	10^{-5}	$5{\cdot}10^{-5}$	10^{-4}	10^{-5}	$5{\cdot}10^{-5}$	10^{-4}	10^{-5}	$5{\cdot}10^{-5}$	10^{-4}
$T_{прот}$, с	0,52	0,58	0,7	1,3	1,38	1,5	2,5	2,59	2,7	3,32	3,38	3,51
$T_{мод2}$, с	0,315	0,36	0,451	0,715	0,76	0,851	1,315	1,36	1,45	1,715	1,76	1,851
T_{B2}, выигрыш, с	0,205	0,22	0,249	0,585	0,62	0,649	1,185	1,23	1,24	1,605	1,62	1,659
B_{B2}, выигрыш, %	39,42	37,93	35,57	45,0	44,93	43,27	47,4	47,49	46,26	48,34	47,93	47,26

Выигрыш B_{B2} по сравнению с исходным ZRTP составил от 39,42% до 48,34%, позволив при задержке до 300 мс сократить время успешного выполнения протокола до 1,45 с, что менее установленной нормы 1,5 с, что позволяет выполнять эту норму. Поставленная задача считается решенной. Применение модифицированного протокола совместно с предложенным методом выявления нарушителя в режиме ОН позволяет значительно снизить вероятность успешной атаки MITM, тем самым повышая информационную безопасность.

ЗАКЛЮЧЕНИЕ

В диссертационной работе 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, в том числе получены следующие основные результаты:

1. Предложена математическая модель активного нарушителя для защищенной IP-телефонии, учитывающая возможность этого нарушителя реализовать атаку человек посередине на протокол распределения ключей, которая позволяет рассчитать вероятность успешной атаки, нацеленной на несанкционированный доступ к информации (НСД), в зависимости от значений вероятностей промежуточных атак.

2. Предложена методика оценки вероятностно-временных характеристик протоколов распределения ключей защищенной IP-телефонии, учитывающая особенности протоколов, выраженные в наличии ограничения числа повторных передач сообщений и переменного таймера повторной передачи.

3. Представлена модификация протокола распределения ключей ZRTP, которая позволяет выполнять протокол за меньшее время по сравнению с исходной реализацией. Выигрыш достигается за счет улучшения временных характеристик протокола распределения ключей ZRTP, состоящего в исключении алгоритма распределения ролей инициатора и респондента, а также в объединении информационных данных о поддерживаемых криптографических наборах и блоков протокола Диффи - Хелмана.

4. Разработан метод выявления нарушителя протоколов распределения ключей, применяемый при работе по сценарию клиент-клиент для корреспондентов, не имеющих заранее распределенного ключевого материала. Метод позволяет с более высокой вероятностью установить защищенное соединение между двумя корреспондентами по сравнению с существующими методами, а также обнаружить наличие активного нарушителя в канале связи.

5. Предложены модификации протокола ZRTP, реализующие разработанный метод выявления нарушителя. Модификации по сравнению с исходным протоколом позволяют выявить активного нарушителя, реализующего атаку человек посередине на протокол распределения ключей.

Полученные результаты соответствуют пунктам "3. Методы, модели и средства выявления, идентификации и классификации угроз нарушения информа-

ционной 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" и "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.

Перспективными задачами исследования является разработка программной реализации модифицированного протокола с применением общедоступных библиотек, разработка программного клиента IP-телефонии, реализующего протокол, а также доработка решения за счет внедрения элементов стеганографии в предлагаемые методы повышения безопасности.

СПИСОК РАБОТ 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.
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.
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.
4. Ковцур, М. М. Обеспечение информационной безопасности ИТС / М.М. Ковцур, В.Н. Никитин, О.И. Лагутенко//Электросвязь.–2014. – №1.–С. 29-31.
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.

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
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
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
9. Ковцур, М.М. Экспериментальная оценка временных характеристик протокола ZRTP/ М.М. Ковцур, В.Н. Никитин // сборник материалов всероссийской

конференции «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
10. Ковцур, М. М. Протоколы обеспечения безопасности IP-телефонии/ М. М. Ковцур // Первая миля – 2012. – №5. – С.18-26
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
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
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
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.
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
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

Подписано к печати __.__.2016
Объем 20 печ. л. Тираж 80 экз.
Отпечатано в _____