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

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

Диссертация на соискание ученой степени
кандидата технических наук

Научный руководитель
д.т.н, профессор
Молдовян Александр Андреевич

Санкт-Петербург –2016

Оглавление

Введение 4

Глава 1. Анализ текущего состояния дел в области защищенной IP-телефонии 12

1.1 Принципы передачи голосовой информации в сетях с пакетной коммутацией 12

1.2 Обеспечение качества в IP-телефонии 17

1.3 Обеспечение информационной безопасности IP-телефонии 29

1.4 Постановка научных задач диссертационного исследования 39

Выводы по главе 1 41

Глава 2. Математическая модель активного нарушителя для защищенной IP-телефонии 43

2.1 Угрозы информационной безопасности в IP-телефонии 44

2.2 Обобщенная модель нарушителя 46

2.3 Частные модели нарушителей 52

2.4 Оценка вероятности успешного завершения атаки 67

Выводы по главе 2 70

Глава 3. Разработка предложений по совершенствованию протоколов распределения ключей 71

3.1 Метод повышения безопасности ZRTP за счет автоматической проверки аутентификационной строки 74

3.2 Метод выявления нарушителя протоколов распределения ключей, основанных на алгоритме Диффи-Хелмана 82

Выводы по главе 3 99

Глава 4. Исследование вероятностно-временных характеристик протоколов IP-телефонии 101

4.1 Методика оценки вероятностно-временных характеристик протоколов распределения ключей защищенной IP-телефонии 101

4.2 Исследование BBX DTLS 107

4.3 Исследование ВВХ ZRTP 112
4.4 Практическая оценка временных характеристик протокола ZRTP 123
4.5 Разработка предложений по улучшению вероятностно-временных характеристик протокола ZRTP 129
Выводы по главе 4 136
Заключение 139
Список сокращений и условных обозначений 142
Список литературы 144
Приложение А. Акты о внедрении 154
Приложение Б. Листинг программы – поиск пар и троек маршрутов 158
Приложение В. Общая характеристика протоколов распределения ключей IP-телефонии 169
Приложение Г. Протокол ZRTP 180
Приложение Д. Протокол DTLS 187
Приложение Е. Структура глобальной сети 193
Приложение Ж. Листинг программы – имитационное моделирование протокола ZRTP 204

Введение

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 [1]. 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 были разделены на три группы в зависимости от решаемых задач: обеспечение безопасности сигнализации, защита медиа трафика и распределение ключей для медиа трафика.

Стандартизация протоколов, а также распространенное использование персональных компьютеров в качестве терминалов пользователя для услуг IP-телефонии привели 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 программах.

Таким образом, диссертационная работа, посвященная исследованию протоколов обеспечения информационной безопасности IP-телефонии, а также разработке предложений по совершенствованию этих протоколов для повышения

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 информации, обеспечения качества при передаче голосовых и медиаданных, сжатия речи и видео, оценки качества предоставления услуг IP-телефонии. Исследования в области обеспечения безопасности данных в IP-телефонии приведены в работах Нопина С.В., Майстренко В. А, Шахова В.Г [2-4], Говор Т.А. [5], Докучаева В.А., Шведова А.В [6], Макаровой О.С. [7], Крюкова Ю.С. [8] и др.; исследования протоколов обеспечения безопасности IP-телефонии – в работах Оника Э. [9], Riccardo Bresciani и Andrew Butterfield, Charles V Wright, Vitaly Shmatikov, Prateek Gupta [10] 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., и др. [11 – 15]; исследование методов обеспечения безопасности протоколов – в работах Ф. Циммермана, Демьянчука А.А., Новикова Е.С., Молдовяна А.А, Молдовяна Д.Н,; обеспечение QoS (Quality of Service) и оценка качества, а также моделирование сетей IP-телефонии - в исследованиях Krzysztof Perlicki, Сухова А. М. [16], Мошака Н.Н., Рудинской С.Р. [17], Федосеевой О. С. [18] , Erol Gelenbe, Ricardo Lent [19], Rafik A. Goubran, P.Eng. [20] и др. Значительный вклад в исследование временных характеристик внесли Никитин В.Н. [21 - 22], а также Нсангу М. М. [24], Юркин Д. В., Винель А. В., Таранин В. В. [25], Галкин А.М., Яновский Г.Г. [26], Петрова М.Н. [27], Лосев Ю.И., Руккас К.М. [28].

Однако остается недостаточно освещенным вопрос обеспечения безопасности для сценария IP-телефонии точка-точка в случае, когда корреспонденты не имеют заранее выработанного ключевого материала. Также остаются малоизученными 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. [3], Макаровой О. С. [7], Докучаева В.А. [6], Миронова В.Г. [29 - 36] 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 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.

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 НСД 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 обеспечение – 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 источник, из них 35 иностранных. Приложения представлены на 58 страницах.

В первой главе описываются принцип передачи медиа информации в сетях с пакетной коммутацией, а также существующие пути обеспечения качества

сервисов и безопасности IP-телефонии. Сформулирована цель и задачи исследования.

Во второй главе описывается разработанная модель активного нарушителя для защищенной IP-телефонии. В качестве одной из самых опасных выделена атака активного нарушителя на протоколы распределения ключей защищенной IP-телефонии.

В третьей главе описан предлагаемый метод выявления нарушителя протоколов распределения ключей для защищенной IP-телефонии, а также представлены модификации протокола ZRTP, реализующие предложенный метод.

В четвертой главе представлена методика оценки вероятностно-временных характеристик протоколов распределения ключей защищенной IP-телефонии, а также описаны модификации протокола ZRTP с сокращенным временем успешного завершения.

Глава 1. Анализ текущего состояния дел в области защищенной IP-телефонии

1.1 Принципы передачи голосовой информации в сетях с пакетной коммутацией

1.1.1 Классификация протоколов IP-телефонии

Протоколы IP-телефонии разделяются на две большие группы, а именно протоколы передачи медиа информации по пакетным сетям, а также протоколы управления установлением соединения.

В первую группу входит протокол RTP (Real-time Transport Protocol) [37], работающий поверх UDP (User Datagram Protocol) протокола. Совокупность протоколов RTP/UDP/IP обеспечивает транспортный механизм для речевого трафика.

Протоколы второй группы обеспечивают управление при обслуживании вызова между абонентами. К этой группе относятся протоколы SIP (Session Initiation Protocol)[38], H.323, MGCP (Media Gateway Control Protocol) [39]. Протоколы установления соединения могут работать как поверх UDP транспорта, так и по TCP (Transmission Control Protocol). Таким образом, совокупность протоколов (SIP/H.323/MGCP)/(UDP/TCP)/IP формируют сигнальный механизм для передачи речевого и медиа трафика.

Исторически первым протоколом для IP-телефонии, получившим широкое распространение, стал H.323, представленный Международным союзом электросвязи в рекомендации H.323. Документ описывает несколько протоколов, которые совместно обеспечивают работу мультимедийных протоколов в сетях с негарантированным качеством обслуживания. Однако, H.323 имеет довольно сложную структуру, так как протокол изначально разрабатывался для интеграции телефонной сети общего пользования (ТфОП) с сетями передачи данных.

Управление вызовами может быть реализовано за счет использования протокола MGCP, архитектура которого состоит из нескольких элементов:

1)Шлюз – Media Gateway, выполняющий функции преобразования речевой информации из ТфОП в сеть с коммутацией пакетов;

2)Контроллер шлюзов – Call Agent, управляющий шлюзами;

3)Шлюз сигнализации – Signaling Gateway (SG), обеспечивающий передачу сигнализации, поступающей из ТфОП, к контроллеру шлюзов и в обратном направлении.

Особенностями MGCP являются сосредоточение всего интеллекта распределенного шлюза в контроллере и возможность разделения функций контроллера между несколькими вычислительными платформами.

Третьим протоколом, позволяющим осуществлять управление вызовами, является SIP [40]. SIP базируется на протоколе HTTP, имеет более простую структуру по сравнению с H.323 и MGCP. Задача протокола – сделать абонентские устройства и шлюзы более интеллектуальными, а также обеспечить расширяемость протокола для поддержки дополнительных услуг для пользователей. Подход к построению сетей IP-телефонии на базе протокола SIP намного проще, чем реализация на H.323 и MGCP. По этой причине – SIP протокол получил широкое распространение. Так, например, оператор Ростелеком, занимающий одно из первых мест на рынке предоставления услуг телефонной связи в России – переводит абонентов на VoIP с обновлением сети на GPON, используя при этом SIP протокол на сети и абонентские устройства GPON ONT.

Кроме приведенной выше классификации протоколов IP-телефонии, можно дополнительно выделить несколько подсистем, функционирующих для оказания услуг VoIP [1]:

- Подсистема обеспечения качества;
- Подсистема обеспечения безопасности IP-телефонии;
- Подсистема биллинга и менеджмента IP- телефонии;

- Подсистема дополнительных услуг;
- Подсистема обеспечения управлением вызовами и адресацией.

Подсистема обеспечения качества отвечает за поддержку качества телефонной связи и включает в себя совокупность протоколов, алгоритмов и механизмов, работающих для достижения этой цели.

Подсистема безопасности IP-телефонии отвечает за конфиденциальность телефонных переговоров корреспондентов, а так же передаваемой информации. Данная система включает в себя совокупность протоколов, механизмов и алгоритмов для обеспечения безопасности в сети IP-телефонии.

Подсистема биллинга и менеджмента применяется для учета вызовов пользователей, тарификации звонков и выполнения взаиморасчетов между пользователями (абонентами) и оператором, предоставляющим услугу.

Подсистема дополнительных услуг отвечает за оказание дополнительных сервисов абонентам сети IP-телефонии. К ним относятся: обеспечение роуминга и мобильности, предоставление дополнительных сервисов, таких как видео вызовы, информационные сервисы и т.д. Подсистема состоит из протоколов, применяемых для оказания дополнительных услуг.

Подсистема управления вызовами и адресации отвечает за выполнение базовых услуг VoIP, а именно:

- организация вызовов и маршрутизацию вызовов;
- передача голосового трафика.

1.1.2 Сценарии установления соединения в IP-телефонии

При описании системы IP-телефонии следует отдельно выделить возможные сценарии взаимодействия корреспондентов. В общем случае сценарием называется совокупность элементов, взаимодействующих при обработке звонка. В более широком смысле, сценарием может быть названа совокупность применяемых при обработке звонка протоколов, алгоритмов, механизмов, а также процедур их взаимодействия между собой для достижения конечной цели.

При составлении примера сценария введено допущение, что в качестве протокола сигнализации на сети IP-телефонии применяется протокол SIP. При составлении схемы взаимодействия учтено, что по закону о связи, запрещено присоединение операторов друг к другу с помощью VoIP. Соединение разных VoIP операторов разрешается выполнять только через сеть ТфОП [41].

На рисунке 1.1 представлена "Принципиальная схема подключения оператора VoIP". На ее примере рассмотрены возможные варианты сценариев обработки вызовов элементами сети IP-телефонии: пользователями (абонентами), IP-телефонными станциями (IP АТС, SoftSwitch), пограничными шлюзами E1. Для примера - приведено два поставщика услуг IP-телефонии, а также оператор традиционной телефонии.

Оператор 1 предоставляет VoIP сервисы абонентам, подключенным на сети 1. Оператор 1 может использовать несколько IP АТС, обозначенных SSx на рисунке, где x – порядковый номер IP АТС. Как правило, вероятность вызова от абонента А1 другому абоненту сети того же самого оператора (Б1 или В1) крайне мала для небольших и средних компаний. Наиболее распространены звонки абонентам, подключенным к другим операторам.

Возможны следующие сценарии соединения:

- А1-SS1-GW1-ТфОП-GW2-SS2-В2 (VoIP абонент одной компании через ТфОП звонит VoIP абоненту другого оператора)
- А1-SS1-GW1-ТфОП-Г (VoIP абонент одной компании через ТфОП звонит абоненту сети ТфОП другого оператора).
- А1-SS1-SS2-В1 (VoIP абонент одного оператора звонит другому абоненту этого же оператора, подключенному к дополнительной IP АТС оператора)
- А1-SS1-Б1 (VoIP абонент одного оператора звонит другому абоненту этого же оператора, при этом абоненты подключены к одной IP АТС)

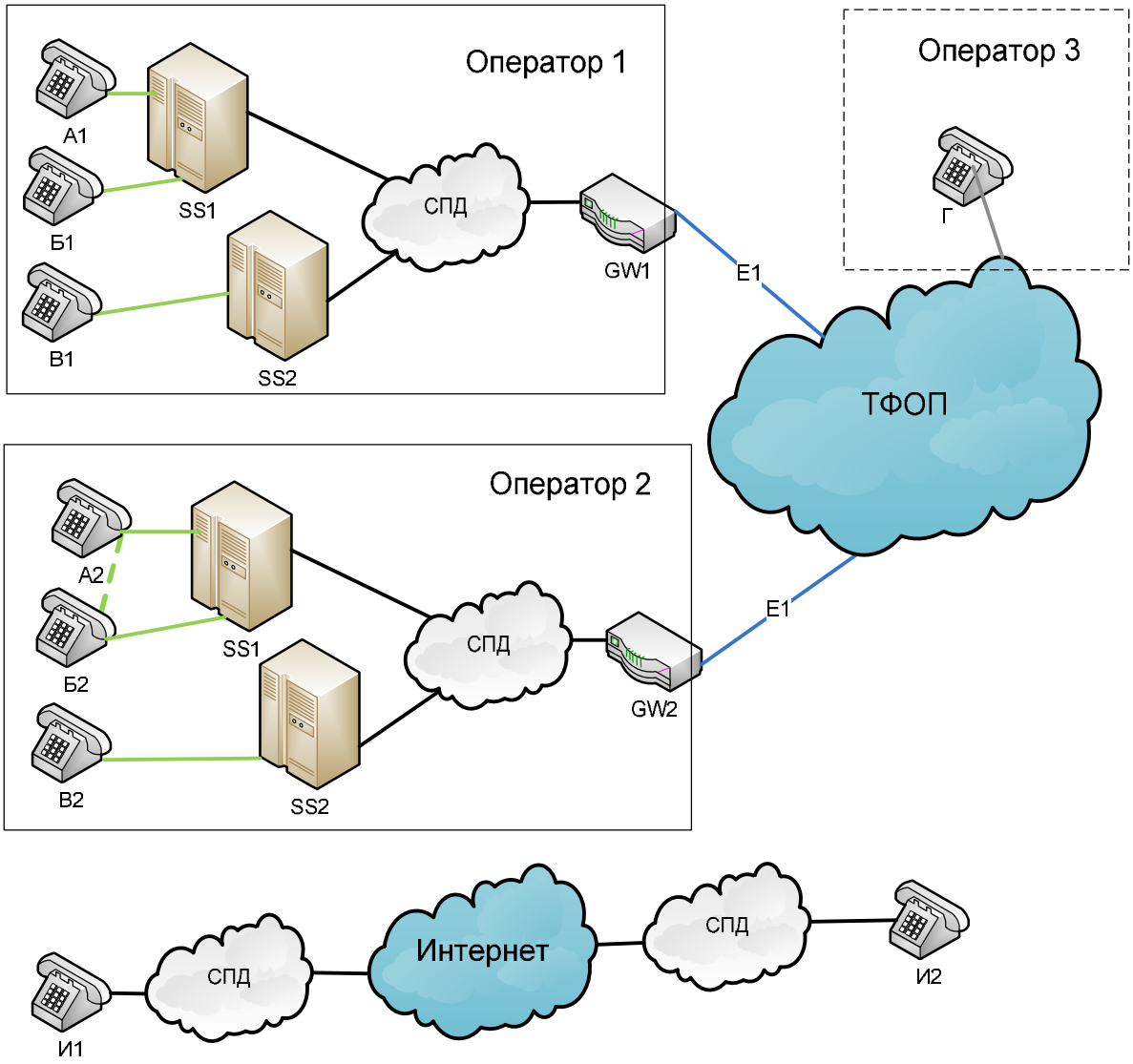


Рисунок 1.1 – Принципиальная схема подключения оператора VoIP

- А2-Б2 (VoIP абонент одного оператора звонит другому абоненту, при этом вызов осуществляется напрямую между корреспондентами, минуя IP АТС). Такой способ чаше всего используется, когда необходимо организовать передачу абонентской линии традиционной телефонии по сетям IP. Способ организации связи без АТС может применяться в корпоративных сетях для организации внутренней служебной связи, а также между отдельными корреспондентами глобальной сети, не имеющими подключения к одной

АТС, но имеющими потребность проведения сеансов телефонной связи в защищенном режиме.

Описанные сценарии приведены также на рисунке 1.2

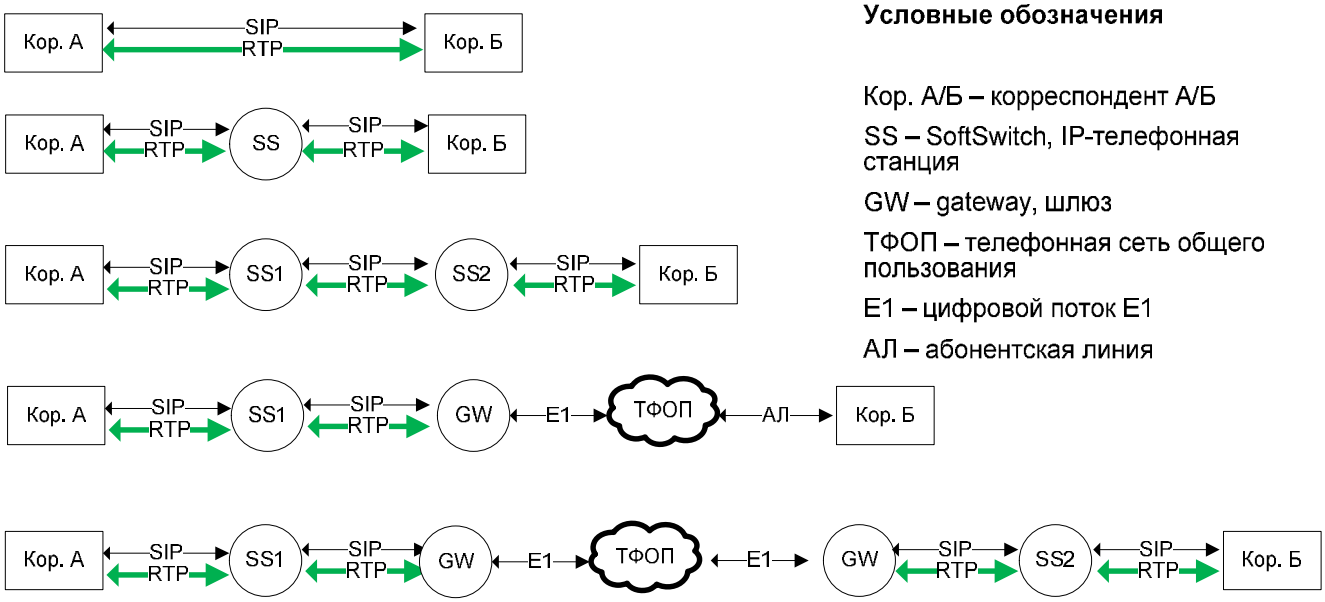


Рисунок 1.2 – Возможные сценарии установления соединения корреспондента VoIP

Во всех вышеприведенных сценариях при обработке вызовов должны выполняться нормы, определенные для телефонной связи. Однако, в сценариях могут применяться различные протоколы, алгоритмы обеспечения безопасности. Возможно использование различных механизмов поддержки качества обслуживания при установлении соединения между абонентами разных операторов. По этим причинам, подсистема обеспечения качества и подсистема обеспечения безопасности IP-телефонии [42] требуют более детального изучения.

1.2 Обеспечение качества в IP-телефонии

1.2.1 Показатели качества IP-телефонии

Международный Союз Электросвязи (МСЭ) определяет качество предоставляемых услуг как "суммарный эффект показателей качества услуги, который определяет степень удовлетворенности пользователя услуги" [43].

Наиболее популярным из показателей качества IP-телефонии является оценка MOS (Mean Opinion Schore), которая определяется как среднее значение оценок качества по пятибалльной шкале, полученных большой группой слушателей-экспертов [44].

Качество IP-телефонии определяется следующими двумя составляющими - качеством речи и качеством сигнализации [1]. Качество речи включает в себя:

- 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 включает:

- 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.

При использовании защищенной IP-телефонии дополнительно появляются показатели:

- время выполнения соединения т.е. время установление защищенного голосового канала между корреспондентами, использующими протоколы распределения ключей;
- вероятность успешной атаки нарушителя на IP-телефонию, работающую в защищенном режиме;
- время и вероятность успешного завершения протоколов обеспечения безопасности.

IP-телефония становится массовым явлением в наше время, поэтому на нее так же могут распространяться нормы, предъявляемые к традиционной телефонии.

Для контроля показателей качества IP-телефонии необходимо учитывать две совокупности норм: нормы, распространяющиеся на пакетные каналы связи, а также нормы, распространяющиеся на телефонию.

Для сети передачи данных выделяют следующие показатели:

Потери - отношение корректно принятых пакетов к общему числу переданных пакетов.

Задержки - время, которое требуется для передачи пакета от точки отправки до точки получения.

Пропускная способность - доступная для передачи между корреспондентами полоса пропускания.

Колебания задержки - разница между задержками, возникшими при передаче разных пакетов.

Для сети передачи данных для разных классов трафика в рекомендации МСЭ-Т Y.1541 [45] вводятся нормы на среднюю задержку, вариацию задержки, коэффициент потерянных пакетов, коэффициент ошибок в принятом пакете. Нормы представлены в таблице 1.1.

Таблица 1.1 – Нормы по рекомендации МСЭ-Т Y.1541

Характеристики сети	Классы качества обслуживания (QoS)					
	0	1	2	3	4	5
Задержка доставки пакета IP, IPTD (мс)	100	400	100	400	1000	--
Вариация задержки пакета IP, IPDV (джиттер)(мс)	50	50	--	--	--	--
Коэффициент потери пакетов IP, IPLR	10^{-3}	10^{-3}	10^{-3}	10^{-3}	10^{-3}	--
Коэффициент ошибок пакетов IP, IPER	10^{-4}	10^{-4}	10^{-4}	10^{-4}	10^{-4}	--

В рекомендации G.114 [46] для телефонной сети сформированы нормативы на одностороннюю задержку. Параметр не должен превышать 400 мс при сетевом планировании. В документе приведены некоторые значения задержек, которые

рекомендуется использовать в расчетах при использовании различных сред передачи и гибридных каналов передачи данных.

В Российском законодательстве в области связи следует выделить приказ Министерства информационных технологий и связи РФ от 27 сентября 2007 г. N113 “Об утверждении Требований к организационно-техническому обеспечению устойчивого функционирования сети связи общего пользования ” [47]. Документ описывает количественные требования к показателям качества для местных, международных и междугородних вызовов

В приказе нормируются и определяются показатели:

- доля несостоявшихся вызовов;
- время с начала передачи информации о занятии линии до получения ответа от станции - время отклика узла станции;
- время с момента окончания набора номера до получения сигнала о состоянии оборудования вызываемого абонента - время установления соединения;
- время с момента получения оборудованием вызывающего абонента от узла связи информации об ответе пользовательского оборудования вызываемого абонента до момента установления между пользователями соединения по голосовому каналу - время на выполнение соединения;
- время разъединения.

Показатели имеют различное значение в зависимости от охвата сети связи. В таблице 1.2 приведены значения нормируемых параметров, описанных в нормативном документе.

Для достижение высоких показателей качества применяют декомпозицию сети на несколько конструктивных блоков и используют дополнительные способы и алгоритмы в каждом из них. Далее они рассмотрены более подробно.

Таблица 1.2 – Технические нормы на показатели функционирования сетей телефонной сети связи в соответствии с приказом N113 Министерства информационных технологий и связи РФ от 27 сентября 2007 г.

N п/п	Наименование показателя	Норма (в час наибольшей нагрузки)
1.	Доля несостоявшихся вызовов из-за технических неисправностей или перегрузки сети связи в общем количестве попыток вызовов (потери вызовов) при установлении соединений:	
	в сети местной телефонной связи	не более 2%
	в сети зоновой телефонной связи	не более 2%
	в сети междугородной и международной телефонной связи	не более 2%
	в сети подвижной связи	не более 5%
	с узлом обеспечения вызова экстренных оперативных служб	не более 0,1%
2.	Время с начала передачи информации о занятии абонентской линии до момента получения пользовательским (оконечным) оборудованием от оконечного узла связи сети местной телефонной связи сигнала готовности к приему номера (время отклика узла связи)	не более 2 с
3.	Время с момента, когда пользовательское (оконечное) оборудование вызывающего абонента или пользователя услугой связи передало всю информацию, необходимую для установления соединения, до момента, когда это оборудование получило от узла связи сигнал о состоянии пользовательского (оконечного) оборудования вызываемого абонента или пользователя услугой связи (время установления соединения):	
	в сети местной телефонной связи	не более 6,6 с
	в сети зоновой телефонной связи	не более 2,7 с
	в сети междугородной и международной телефонной связи	не более 5,4 с
4.	Время с момента получения пользовательским (оконечным) оборудованием вызывающего абонента или пользователя услугой связи от узла связи сети местной телефонной связи информации об ответе от пользовательского (оконечного) оборудования вызываемого абонента или пользователя услугой связи до момента установления соединения между пользовательским (оконечным) оборудованием вызывающего и вызываемого абонента или пользователя услугой связи (время выполнения соединения):	
	в сети местной телефонной связи	не более 1,5 с
	в сети зоновой телефонной связи	не более 1 с
	в сети междугородной и международной телефонной связи	не более 1 с

1.2.2 Методы обеспечения качества в VoIP

В рекомендации ITU-T Y.1291 [48] выделяется несколько основных конструктивных блоков, распределенных по трем плоскостям (рисунок 1.3).

- Плоскость управления, содержащая механизмы управления трактами, через которые проходит трафик пользователя. В состав этих механизмов входит управление допуском, маршрутизация для QoS и резервирование ресурсов.
- Плоскость данных содержит механизмы, работающие непосредственно с трафиком пользователя. В состав этих механизмов входит управление буферами, предотвращение перегрузки, маркировка пакетов, организация очередей и диспетчеризация, классификация трафика, правила его обработки и моделирование.
- Плоскость административного управления, содержащая механизмы, относящиеся к эксплуатации, администрированию и административному управлению сетью. В состав этих механизмов входят: соглашение об уровне обслуживания (SLA), восстановление трафика, измерение и регистрация, а также заданные правила доставки информации

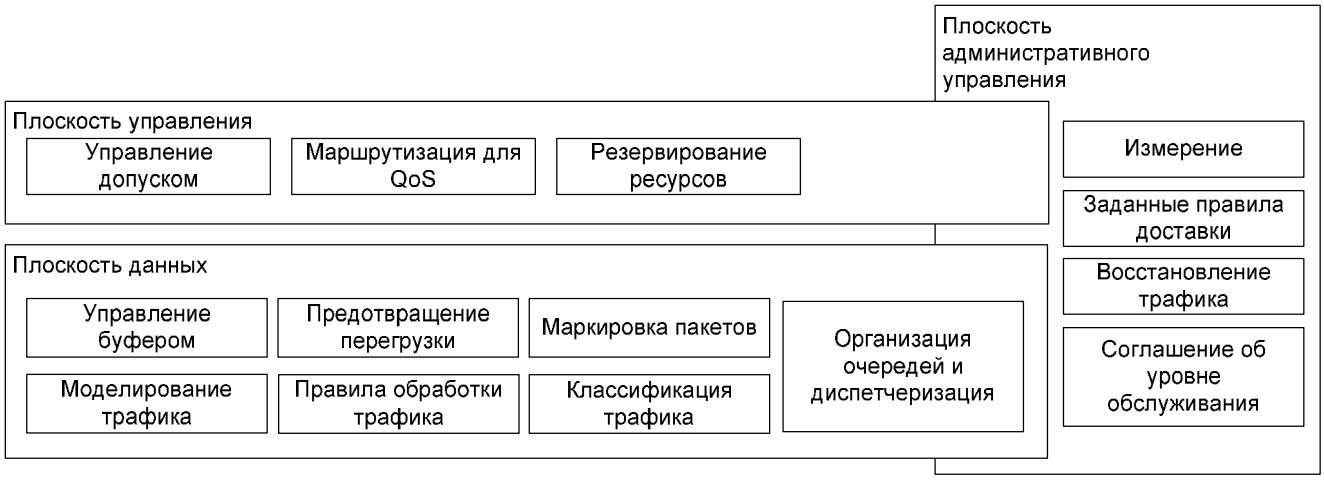


Рисунок 1.3 – Архитектурная модель для поддержки QoS по рекомендации ITU-T Y.1291

Далее будут рассмотрены протоколы и методы обеспечения качества, применяемые в различных плоскостях архитектурной модели для поддержки QoS.

В плоскости данных выполняются классификация и маркировка пакетов, применяются планировки к пакетам, а также используются дополнительные алгоритмы обработки пакетов.

Классификация может выполняться в зависимости от CoS, MPLS-EXP, номера порта подключения корреспондента к сетевому оборудованию или MAC адреса отправителя или получающего, Ethertype отправляемого пакета и других признаков. Основной задачей классификации является разделение пакетов на группы с целью их последующей маркировки с назначением параметров пакету:

- MPLS-EXP - три бита в MPLS для маркировки QoS;
- биты CoS 802.1p;
- IP Precedence байт (ToS) или DSCP.

Инструмент планировки применяется для определения какой кадр или пакет будет первым выходить из интерфейса сетевого узла. Задача решается за счет применения алгоритмов управления очередью, а также механизмов предотвращения переполнения очереди. Выделяют алгоритмы управления очередью: SP, WRR, WFQ, CBWFQ, MDRR, LLQ (PQ+CBWFQ), WRED.

Детальное рассмотрение каждого из алгоритмов выходит за рамки исследования. Описание алгоритмов приведено в [49]. Наиболее распространенным является применение приоритезации голосового трафика в низкоскоростных беспроводных каналах связи (КС) [50].

Для обеспечения качества VoIP могут применяться механизмы ограничения скорости – policing или shaping. Policing - ограничение скорости передачи данных без буфера. Shaping - ограничение скорости передачи данных с промежуточным буфером.

Дополнительно может применяться управление потоком Ethernet - механизм, позволяющий предупредить отправителя о необходимости остановить

передачу данных на указанном интервале времени по причине, что принимающий порт не может выполнить обработку.

Для низкоскоростных каналов дополнительно могут быть применены механизмы:

- Фрагментация и чередование пакетов;
- Механизмы компрессии (Compressed RTP - cRTP).

Так cRTP позволяет сжимать заголовок голосового пакета IP/UDP/RTP с 40 до 2-5 байт. Однако - данный механизм используется только в пределах одного физического канала связи.

К механизмам плоскости управления архитектурной модели для поддержания QoS относятся применение RSVP (резервирование ресурсов) на сети, а также использование алгоритмов маршрутизации с учетом QoS. В качестве входных данных алгоритмы могут использовать значение полей в промаркированных пакетах и таблицу маршрутизации, учитывающую различные параметры QoS для интерфейсов оборудования и для разных маршрутов. Часть такого функционала поддерживается, например, протоколом маршрутизации OSPF. Механизмы маршрутизации с учетом требований QoS и дополнительных возможностей протокола OSPF описаны в RFC 2676 [51].

К плоскости административного управления относятся механизмы изменения параметров для VoIP трафика, которые применяются на пользовательских терминалах, IP-телефонных станциях, а также на дополнительных элементах сети VoIP, таких, как RTP-прокси-серверы и пограничные контроллеры сессий (SBC, Session Border Controller).

1.2.3 Методы оценки качества VoIP и состояние исследований

В мире ведутся активные дискуссии о том, какие модели использовать для оценки качества предоставляемых сервисов, а также как оценить эффективность обработки пакетов в сети, какие методики использовать для оценки качества предоставляемых услуг.

Ведутся активные разработки в направлении оценки QoS и QoE VoIP трафика. QoS (Quality of Service - Качество Обслуживания) по определению ITU – это коллективный эффект работы сервисов, который определяет степень удовлетворения пользователя обслуживанием.

QoE (Quality Of Experience – Качество восприятия) субъективная мера оценки работы системы. QoE полагается на человеческое мнение и отличается от качества обслуживания QoS, которое может быть точно измерено. Например, реакция человека при прослушивание музыки через наушники базируется не только на частотной характеристике системы и спикеров, но и на комфорте единицы, чувствительности слуха человека.

Для IP-телефонии МСЭ стандартизировал математическую модель в рекомендации G.107 [52] для оценки QoE исходя из параметров качества терминала и сети. Эта модель получила название E-model и служит для расчета R-фактора.

Модель была широко использована для оценки QoE в сетях IP-телефонии в Японии. Такая же модель была необходима для видеотелефонных сервисов. В результате в лаборатории NTT был разработан набор параметров для оценки восприятия качества видеотелефонии, которые впоследствии использовались в новой модели МСЭ для видеотелефонии.

Используя Е-модель, а также параметры канала передачи данных и параметры применяемой системы IP-телефонии, можно оценить MoS (Mean Opinion Score) - субъективный уровень качества, воспринимаемый пользователем услуги IP-телефонии. В рекомендации [52] приводится соответствие R-фактора, описываемого и вычисляемого с использованием Е-модели, и параметра MoS (таблица 1.3).

На основании таблицы 1.3 выбрана нижняя граница MOS 3.6, которой соответствует R=70. Необходимо определить возможные параметры канала связи - задержку в канале связи (d) и % потери пакетов ($p.l.$) - при которых будет достигаться значение $R \geq 70$.

Таблица 1.3 – Связь R-фактор и MOS по рекомендации G.107

R-фактор	MoS (нижний порог)	Удовлетворенность пользователей
90	4,34	Высокая удовлетворенность
80	4,03	Удовлетворенность
70	3,60	Некоторые пользователи не удовлетворены
60	3,10	Многие пользователи не удовлетворены
50	2,58	Почти все пользователи не удовлетворены

В [53] рассматривается влияние параметров канала связи на предоставляемое качество услуг VoIP для разных кодеков: G.711, G.723 и G.729. Для этого выполняется расчет MOS с использованием E-модели для разных задержек канала связи в интервале задержек 0-1200 мс, а также для потери пакетов 0-12%. На рисунках 1.4-1.6 видно, как изменяется R в зависимости от *p.l.* и от *d*. Дополнительно на графиках отмечены условия, при которых обеспечивается значение R ≥ 70.

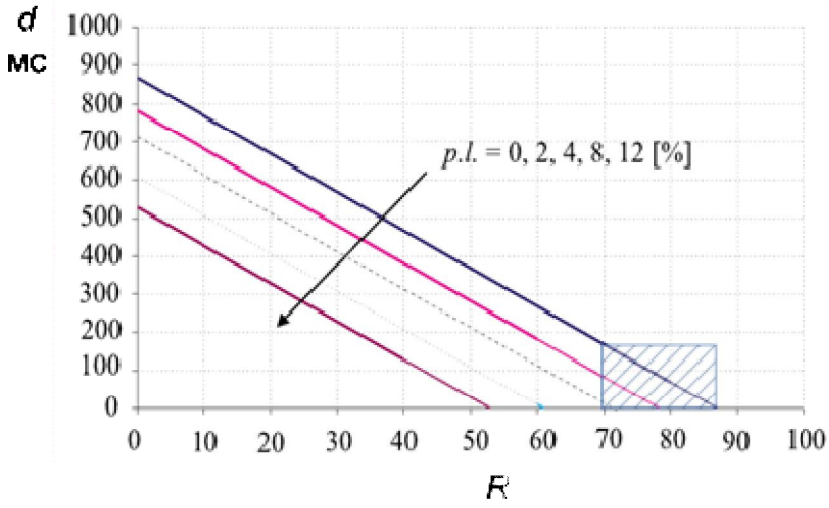


Рисунок 1.4 – Зависимость R-фактора от потери пакетов и задержки в канале связи для G.723 кодека

Из рисунков 1.4-1.6 видно, что кодек G.711 обеспечивает наибольшее значение MOS при наихудших условиях в канале связи: максимальной задержке и потере пакетов. При *p.l.*=0 условие *R*>=70 выполняется для *d*<=300 мс, при *p.l.*=12, *R*>=70 выполняется для *d*<=100 мс.

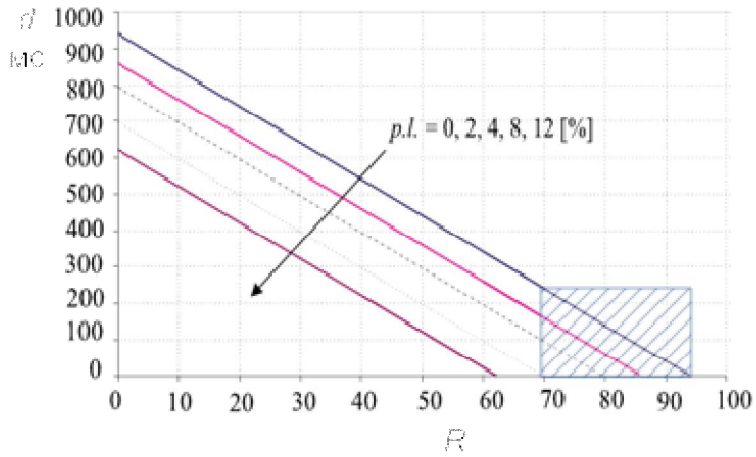


Рисунок 1.5 – Зависимость R-фактора от потери пакетов и задержки в канале связи для G.729 кодека

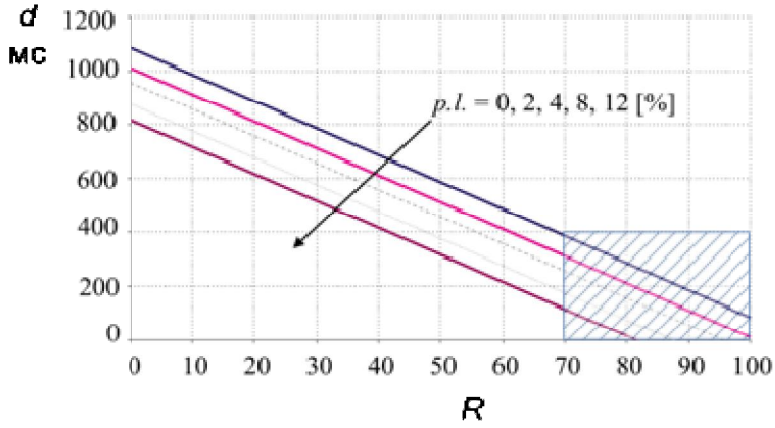


Рисунок 1.6 – Зависимость R-фактора от потери пакетов и задержки в канале связи для G.711 кодека

Дальнейший анализ протоколов обеспечения безопасности целесообразно проводить для канала связи с параметрами *d*<=300 и *p.l.*<=12 при использовании G.711 кодека. В последующих вычислениях также предпочтение отдается кодеку G.711, как самому устойчивому при работе по каналам связи с ошибками.

В качестве входного параметра при расчетах вместо параметра *p.l.* удобно использовать производный параметр - вероятность битовой ошибки в канале связи p_0. Для этого необходимо определить значение p_0, эквивалентное *p.l.*=12 для кодека G.711.

$$p.l.=1-(1-p_0)^{ps}\ , \qquad (1.1)$$

где *ps* - размер пакета, бит.

Для кодека G.711 допускаются размеры полезной нагрузки 80,160,240 байт. При этом размер пакета с учетом заголовков будет составлять соответственно 138,218,296 байт. p_0 определяется по формуле:

$$p_0 = 1 - 10^{\frac{\lg(1-p.l.)}{ps}} \qquad (1.2)$$

Рассчитанные значения приведены в таблице 1.4 Из таблицы видно, что максимальное значение вероятности битовой ошибки *ppl*=12% соответствует $p_0=1{,}16\cdot10^{-4}$. Соответственно, расчеты необходимо выполнять для значений $p_0 \le 1{,}16\cdot10^{-4}$.

Таблица 1.4 – Зависимость p_0 от *p.l.* для кодека G.711

Вероятность потери пакета, *p.l.*	Размер пакета, *ps* , бит	Вероятность битовой ошибки, p_0
0,12	138	$1{,}16\cdot10^{-4}$
0,12	218	$7{,}33\cdot10^{-5}$
0,12	298	$5{,}36\cdot10^{-5}$

В области исследования методов обеспечения качества при передаче медиа трафика в России ведутся разные исследования. Над проблемами качества обслуживания и анализом трафика в VoIP сетях также работали док. Сухов А. М. [16] , к.т.н Аль-Шрайдех Халед Садек [54], маг. Федосеева О. С. [18], маг. Каримжанова А.С [55], Малаховский А.А., Лычагин Н.И., Гузарев А.С. [56] и другие. Так упоминавшимся выше Суховым А.М была разработана аналитическая модель трафика на участке высокоскоростной сети (рисунок 1.7), согласно которой для сравнения качества соединений в глобальной сети достаточно

использовать единственный параметр: среднюю скорость потока. Вероятностные характеристики протокола SIP исследовались в работе Нсангу М. М. [24].

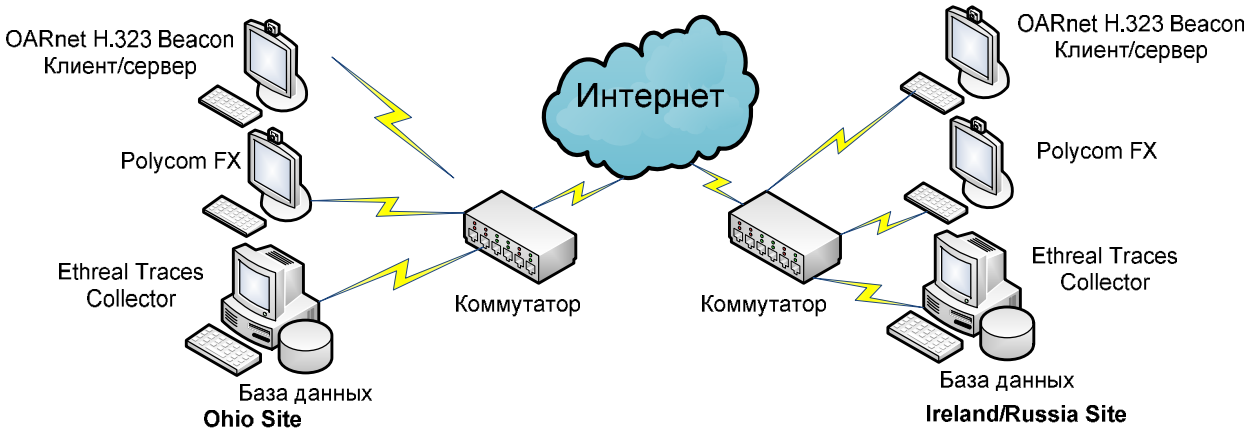


Рисунок 1.7 – Схема эксперимента в глобальной сети док. Сухова А. М.

Тема обеспечения QoS широко обсуждается за рубежом в университетах Центральной флориды (Erol Gelenbe, Chair Professor, Ricardo Lent, doctor и др) [19], Карленгтонском университете Канады (Lijing Ding, Ayman Radwan, Mohamed Samy El-Hennawey [20], Rafik A. Goubran, Ph.D., P.Eng) и др.

Вопрос обеспечения QoS рассматривается такими организациями как МСЭ, IETF, IEEE, ETSI, 3GPP. Были приняты ряд стандартов для качества QoS IP-телефонии и моделей по обеспечению качества IP-телефонии, но до настоящего времени не существует единого стандарта.

Однако, вопросы влияния протоколов обеспечения безопасности на качество изучены крайне слабо и требуют проработки и оценки.

1.3 Обеспечение информационной безопасности IP-телефонии

В силу общедоступности используемых каналов передачи голосовой информации в IP сетях особую актуальность приобретает обеспечение конфиденциальности VoIP-сервисов. Для решения этой задачи могут быть использованы разные подходы:

- обеспечение прямого защищенного канала между корреспондентами (например, VPN-туннель);
- применение специальных протоколов обеспечения безопасности для IP-сервисов.

Первый способ получил широкое распространение при построении виртуальных корпоративных сетей, но для его реализации корреспонденты должны поддерживать VPN-протокол. Однако, многие VoIP-устройства не поддерживают VPN (Таблица 1.4).

Поэтому, для обеспечения безопасности достаточно часто применяются специальные протоколы обеспечения безопасности IP-телефонии.

Таблица 1.4 – Продукты защищенной IP-телефонии

Производитель	Продукт	Реализация	протокол защиты			Поддержка VPN
			установления соединения	медиа-трафика	распределения ключей	
LinkSys	SPA8000	аппаратная	SIPS/TLS	SRTP	нет данных	нет
LinkSys	Cisco SPA112	аппаратная	SIPS/TLS	SRTP	нет данных	нет
Dlink	DVG-5008S	аппаратная	нет данных	нет данных	нет данных	PPTP
AddPack	AP200	аппаратная	SIPS/TLS	SRTP	нет данных	нет данных
Grandstream	GXW400x	аппаратная	SIPS/TLS	SRTP	SDES	нет
UM-Labs	RC-2100	аппаратная	SIPS/TLS	SRTP	ZRTP, SDES	нет данных
CounterPath	Eye-beam	программная	SIP/TLS	SRTP	TLS	нет
3XC	3CX softphone	программная	SIP/TLS	SRTP	нет данных	нет
Asterisk	IP PBX	программная	SIP/TLS	SRTP	ZRTP	нет
FreeSwitch	IP PBX	программная	SIP/TLS	SRTP	SDES	нет
Phoner	Phoner softphone	программная	SIP/TLS	SRTP	ZRTP	нет

1.3.1 Протоколы обеспечения безопасности IP-телефонии

К специальным протоколам обеспечения безопасности IP-телефонии относятся протоколы Secured SIP, SRTP, MIKEY, SDES, ZRTP, DTLS, S-MIME. Эти протоколы можно разделить на 3 категории [8, 57]:

- Протоколы защиты сигнализации (Secured SIP);
- Протокол защиты медиаинформации (SRTP);
- Протоколы генерации и распределения ключей для протоколов защиты медиаинформации (MIKEY, SDES, ZRTP, DTLS).

Необходимо рассмотреть подробнее эти категории.

Протоколы защиты сигнализации предназначены для обеспечения безопасности информации о телефонных номерах вызывающего и вызываемого абонента, поддерживаемых кодеках. Для решения этой задачи используется Secured SIP (SSIP, SIP/TLS) [38]. Этот протокол работает по аналогии с протоколом HTTPS, организовывая между корреспондентом и сервером SSL туннель с использованием сертификатов и открытого ключа. Все SIP-сообщения (сигнализация) передаются по этому туннелю. Недостатком протокола является необходимость применения инфраструктуры открытых ключей, используемой для организации TLS.

Для обеспечения конфиденциальности при передаче речи широко используется защищенный протокол реального времени – Secure Real-time Transport Protocol (SRTP)[58], который реализует функции криптографической защиты - шифрования и аутентификации речевых сообщений на основе алгоритма шифрования AES.

Криптографическая защита пакетов голосовой информации выполняется протоколом SRTP в режиме реального времени и не вносит изменений в вероятностно-временные характеристики протокола RTP. Но для его работы

необходимо предварительное формирование криптографических ключей. Эту задачу решает протокол распределения ключей (ПРК).

Рекомендация RFC 3711 описывает две составляющих – собственно протокол SRTP для переноса и криптозащиты медиа данных, а также протокол SRTCP (Secure Real-time Transport Control Protocol) для управления медиа сессией.

Основными задачами протокола SRTP является выполнение следующих функций:

- шифрование передаваемых голосовых данных;
- аутентификация передаваемых сообщений;
- защита от передачи повторных пакетов;
- сохранение полосы пропускания, сжатие RTP заголовков.

Основными задачами протокола SRTCP является выполнение следующих функций:

- шифрование передаваемых данных;
- аутентификация передаваемых сообщений.

Аутентификация и шифрование могут работать независимо друг от друга. Таким образом, возможен вариант, когда шифрование выключено и SRTP применяется только для целей аутентификации. Ограничением протокола является то, что аутентификация сообщения обязательна в SRTP и не может быть отключена.

1.3.2 Протоколы генерации и распределения ключей для защиты медиаинформации

Протоколы третьей группы, по аналогии с родственными протоколами распределения ключей в беспроводных сетях [59], предназначены для генерации и распределения между корреспондентами ключей шифрования медиаинформации. Для решения этой задачи могут использоваться протоколы MIKEY, SDES, ZRTP, DTLS.

Протокол обмена ключами MIKEY описан в рекомендациях RFC3830 [60] и RFC6309 [61]. MIKEY имеет несколько режимов работы, определяющих способ формирования секретного ключа сессии SRTP: режим предустановленного ключа, режим открытого ключа и режим Диффи–Хелмана. Причем второй и третий режимы не защищают от атаки вторжения в середину (MiTM, Man In the Middle) и требуют реализации механизма аутентификации сообщений. Транспортом для переноса сообщений протокола может выступать как SIP/SDP, так и протокол RTSP (Real Time Streaming Protocol).

SDES (Session Description Protocol Security) [62] описывается в RFC4568. Суть протокола состоит в том, что один из корреспондентов передает ключ в SIP сообщении по сигнальному каналу. Корреспондент получает его и использует для шифрования. Однако при этом обмен сигнальными сообщениями должен быть защищен от злоумышленника. По этой причине – SDES может использоваться только при наличии SIP/TLS защищенного соединения с цифровым сертификатом сервера. Также данный способ не обеспечивает безопасности из конца в конец. Это означает, что если соединение будет выполняться через IP АТС, SDES будет выполнять распределение ключей между корреспондентом А и IP PBX, между корреспондентом Б и IP-телефонной станцией, но не между корреспондентами А и Б напрямую.

Протокол DTLS [63] для SRTP описывается в RFC 5764. Протокол описывает формирование медиа-сессий точка-точка с двумя участниками с жестким фиксированием портов UDP корреспондента и респондента. Сообщения протокола передаются совместно с RTP пакетами. Каждая сессия содержит одну DTLS ассоциацию и два SRTP контекста (для SRTP и SRTCP). Для организации сессии (DTLS-ассоциации) корреспонденты выполняют обмен сообщениями, называемый DTLS handshake (Рисунок 1.8) Так как в основе протокола лежит TLS, использующий инфраструктуру открытых ключей (Public Key Infrastructure, PKI), то применение TLS возможно тоже только при наличии PKI.

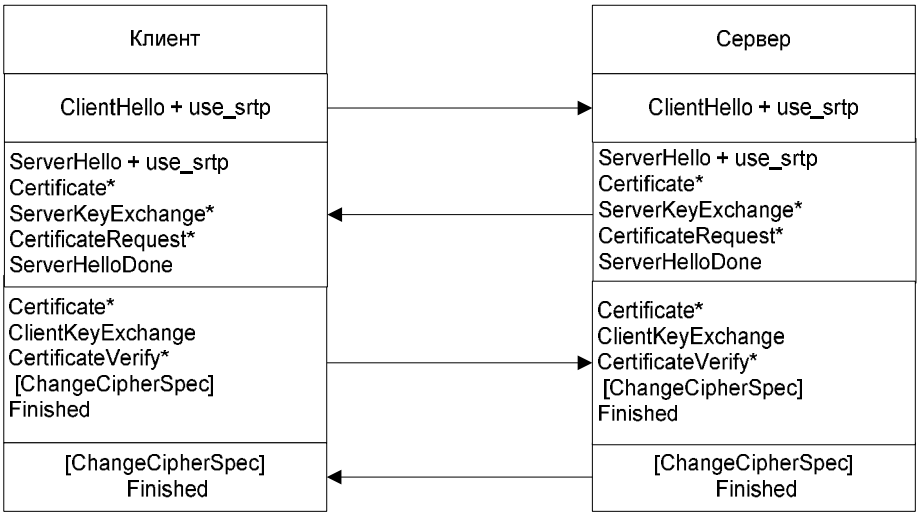


Рисунок 1.8 – Обмен сообщениями DTLS

Одним из наиболее перспективных протоколов генерации ключей является ZRTP [64, 65]. Протокол применяется в приложении для Android CsipSimple, программных телефонах Jitsi, Phoner, программных АТС FreeSwitch и Asterisk, аппаратных VoIP шлюзах компании UM-Labs. Отличительной особенностью ZRTP протокола является возможность обеспечения безопасности из конца в конец, от одного корреспондента до другого. Задачами протокола ZRTP являются:

- генерация ключевых параметров SRTP сессии;
- обеспечение конфиденциальности сообщений протокола;
- обеспечение аутентификации корреспондентов;
- защита от атаки вторжения посередине, как с использованием, так и без использования инфраструктуры открытых ключей.

Протокол предусматривает работу корреспондентов по топологии точка-точка, при этом отдельно выделяется возможность применении протокола при многопоточном режиме, когда необходимо организовать несколько защищенных медиа потоков. Кроме того, предусмотрен режим работы с легитимным посредником, которым может являться, например, корпоративная телефонная станция. Каждый из корреспондентов-участников протокола должен иметь предустановленный идентификатор (ZID), который должен быть уникален.

В основе протокола – обмен ключами по алгоритму Диффи-Хелмана. Особенностью протокола является передача параметров внутри RTP пакетов, оставляя пакеты совместимыми с RTP/AVP профилем. В этом случае, ZRTP-несовместимым устройством ZRTP-пакеты просто отклоняются и не влияют на установленное соединение.

Для аутентификации корреспондентов, а также исключения атаки вторжения в середину (MiTM, Man in The Middle), протокол ZRTP предусматривает использование короткой аутентификационной строки (SAS, Short Authentication String), а также части ключевого материала от предыдущих сессий между корреспондентами. Для контроля целостности передаваемых сообщений каждое сообщение ZRTP включает в себя проверочный код CRC, а также код аутентификации сообщения MAC (Message Authentication Code). MAC вычисляется, как ключевая хеш-функция, которая согласовывается на первой фазе протокола.

Обнаружение ошибки только в хеш-сообщении, как правило, означает обнаружение атаки MiTM, поскольку искажения за счет канальных ошибок проявляются и при проверке CRC ZRTP пакета.

Протокол выполняется последовательно в четыре фазы:

1. Обнаружение;
2. Подтверждение;
3. Вычисление ключей;
4. Завершение.

В общем случае, ZRTP работает в самом начале разговора корреспондентов, сразу после завершения работы протокола SIP, как начинает работать в стороны протокол RTP (Рисунок 1.9).

Более подробно протокол ZRTP описан в приложении Г.

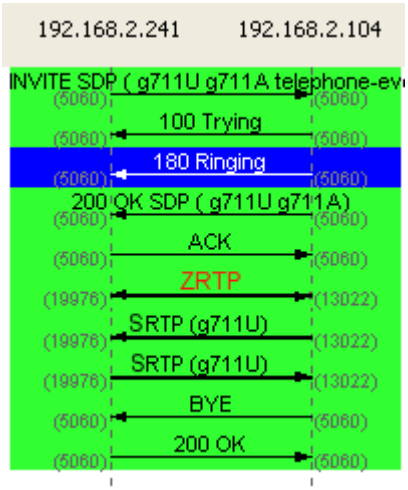


Рисунок 1.9 – Схема обмена сообщениями между корреспондентами с использованием SIP/SRTP/ZRTP

1.3.3 Требования к протоколам распределения ключей

Для дальнейшего исследования также необходимо сформулировать требования, которым должны отвечать ПРК:

1. Протокол должен поддерживать работу как в топологии клиент-сервер, так и в топологии клиент-клиент.
2. Протокол должен являться самодостаточным и выполнять функцию распределения ключевого материала без применения дополнительных протоколов между корреспондентами.
3. Протокол должен поддерживать механизм распределения ключей в топологии клиент-клиент без передачи ключа в явном виде по каналу связи.
4. Протокол должен иметь механизм обнаружения MITM без заранее распределенного ключевого материала между корреспондентами.
5. Протокол должен использовать TCP/UDP порты, применяемые для IP-телефонии, или TCP/UDP порты, использование которых согласовано в результате установления соединения.

Первое требование обосновано необходимостью обеспечения безопасности в топологии клиент-клиент, так как в топологии клиент-сервер корреспонденты уже имеют пред распределенный общий секрет, который используется для защиты сообщений протокола распределения ключей для SRTP

Второе требование обосновано требованиями по простоте интеграции в существующие системы связи, программные терминалы. В случае одновременной работы нескольких протоколов, каждый из которых передает свои сообщения по каналу связи, это усложнит интеграцию протокола в программный VoIP терминал пользователя.

Третье требование обосновано принципом обеспечения безопасности, оговаривающим, что ключ шифрования никогда не должен передаваться по каналу связи в явном виде.

Четвертое требование вызвано возможностью использования протокола распределения ключей между равноправными корреспондентами, не имеющими предварительно распределенного ключевого материала и общих сертификатов, а также общего доверенного центра сертификации.

Пятое требование вызвано упрощением интеграции протокола безопасности в существующие сети с целью препятствия блокировки сообщений протокола распределения межсетевыми экранами при использовании TCP или UDP портов, не предусмотренных протоколами SIP / RTP.

1.3.4 Состояние исследований по защите голосовых связей при использовании IP-телефонии

Существующие исследования в области работ по защите голосовых связей можно разделить на несколько категорий, а именно:

- Разработка безопасных систем IP-телефонии;
- Анализ безопасности, обеспечиваемый системами IP-телефонии;
- Анализ безопасности, обеспечиваемый отдельными протоколами VoIP, а также анализ самих протоколов.

К работам первой категории относятся работы Нопина С.В. и Шахова В.Г. [3]. Они занимались разработкой программ защищенной IP-телефонии, а также изучением особенностей защиты голосовой информации. В работах [2, 3] основным направлением исследования являлось применение средств ОС Windows

для организации безопасной IP-телефонии, при этом для распределения ключей предлагалось использовать центры распределения ключей.

Вторая категория посвящена работам по анализу уровня безопасности, который обеспечивают современные системы безопасности IP-телефонии. К этой категории относятся работы, в которых рассматриваются общие вопросы по обеспечению безопасности в системах IP-телефонии: “Обеспечение безопасности современных VoIP сетей”[5], “Защита информации на корпоративных сетях VoIP” [6]. Некоторые работы направлены на формирование требований по обеспечению безопасности в сетях IP-телефонии. К этим работам относиться, например, работа “Методика формирования требований по обеспечению информационной безопасности сети IP-телефонии от угроз среднестатистического «хакера»”[7] Макаровой О. С., где предложен подход по формированию требований, которым должна отвечать безопасная VoIP сеть.

К работам третьей категории относятся исследования, направленные на анализ протоколов обеспечения безопасности VoIP. К этим работам относятся исследования Эммануэля Оника из университета Александру Иоана Куза (Румыния). В работе “Securing the Media Stream Inside VoIP SIP Based Sessions”[9] проводиться исследование SRTP протокола и протоколов обмена ключами, приводятся возможные атаки на протоколы, а также описывается реализация интеграции протокола ZRTP в программу “SIP Communicator”. Известно несколько работ [66], [10] по анализу протоколов на наличие уязвимостей, например в «ProVerif Analysis of the ZRTP Protocol» проводиться анализ протокола ZRTP на наличие уязвимостей с помощью моделирования в программе ProVerif. В исследовании [67] приводится описание нескольких атак на VoIP протоколы, в том числе атак на MIKEY и SDES протоколы.

В работе "Spot me if you can:Uncovering spoken phrases in encrypted VoIP conversations" [68] исследуется применение протокола SRTP при работе с кодеками с переменной скоростью кодирования. Показано, что информация о длине зашифрованных VoIP пакетов может быть использована для

идентификации фраз, произносимых в разговоре. Исследование показало, что пассивный противник может идентифицировать фразы из стандартного диалога, в зашифрованном телефонном вызове, со средней точность 50%, и с точностью более чем 90% для некоторых отдельных фраз.

Исследования в области атак MITM и методов защиты от них приводятся в работах Атрощенко В.А., Руденко М.В., Дьяченко Р.А., Багдасарян Р.Х. [11], Canteaut A. [12], Sun H., Song J., Chen Z. [13], Радивиловой Т.А., Бушманова В.С. [14], Карпухина Е.О., Михайлова В.Ю. [15]. При этом опасность и распространенность данной атаки наиболее активно отмечается в различных источниках массовой информации [77 - 80].

Однако ни одна из работ не исследует вероятностно-временных характеристики протоколов обеспечения безопасности VoIP.

1.4 Постановка научных задач диссертационного исследования

При оценке влияния протоколов обеспечения безопасности на качество требуется учитывать особенности IP-телефонии по сравнению с традиционной телефонией. Так, в традиционной телефонии время отклика узла связи, т.е. время с начала передачи информации о занятии абонентской линии до момента получения оконечным оборудованием сигнала готовности к приему номера, определяется готовностью станции обслужить вызов. В IP-телефонии это время определяется оконечным оборудованием и не зависит от текущего состояния телефонной станции. Однако, параметр “время установления соединения” для IP-телефонии включает в себя время отклика узла IP-телефонной станции, а также время, требуемое для взаимодействия между корреспондентами, или корреспондентом и телефонной станцией. Отсчет этого времени начинается после окончания набора номера пользователем и заканчивается получением сигнала ожидания ответа или занятости от респондента.

Необходимо оценить, как протоколы безопасности IP-телефонии могут влиять на нормируемые показатели функционирования сетей телефонной сети связи.

Применение SIP-S может влиять на норму “потери вызовов” в случае, если при сценарии абонент-абонент один из корреспондентов использует политику безусловного использования SIP-S, а второй не поддерживает SIP-S протокол. Некоторая задержка дополнительно может возникать за счет времени, требуемого на организацию TLS канала между корреспондентами, необходимого для работы SIP-S протокола.

Протоколы распределения ключей влияют на время установления соединения или на время организации защищенного речевого канала, в зависимости от места срабатывания протокола в сценарии соединения. Так протокол ZRTP может работать после установления соединения, начиная с этапа, когда один из корреспондентов снял трубку. В этом случае, протокол влияет на норму “Время установления соединения”. Другие протоколы также требуют передачу дополнительных сообщений, что может увеличивать значение нормируемых параметров.

В соответствии с вышеизложенным, целью диссертационной работы является оценка вероятностно временных характеристик протоколов безопасности IP-телефонии, как влияющих на параметры качества IP-телефонии, а также повышение безопасности IP-телефонии при работе корреспондентов в топологии клиент-клиент без сервера.

Для достижения цели необходимо решить следующие научные задачи:

1. Исследование существующих протоколов безопасности IP-телефонии, их параметров, характеристик и особенностей, а также влияния протоколов на показатели качества;
2. Разработка модели нарушителя для оценки защищенности системы IP-телефонии. Разрабатываемая модель позволит учесть атаки, которые может

выполнить нарушитель при использовании декомпозиции безопасности IP-телефонии на составляющие протоколы.

3. Разработка методики оценки вероятностно-временных характеристик протоколов обеспечения безопасности IP-телефонии, позволяющей оценить такие характеристики протокола, как время успешного завершения и вероятность успешного завершения при работе по каналам связи с ошибками и задержками с учетом особенностей протоколов
4. Разработка предложений по модификации протокола распределения ключей для улучшения вероятностно-временных характеристик протокола. Модификация позволит ПРК работать по каналам с большими задержками, чем оригинальные ПРК, при этом выполняя установленные нормы.
5. Разработка метода выявления нарушителя протоколов распределения ключей, основанных на алгоритме Диффи-Хелмана, который позволит снизить вероятность успешной атаки НСД;
6. Разработка предложений по модификации протокола Zimmermann Real-time Transport Protocol (ZRTP) для обеспечения безопасности корреспондентов при взаимодействии без сервера в топологии клиент-клиент. Модифицированный ПРК позволит уменьшить вероятность успешной атаки нарушителя, контролирующего канал связи, и может использоваться для повышения безопасности в случаях, когда корреспонденты не имеют защищенного канала связи, или срок действия существующего ключевого материала закончился, или общий секрет компрометирован нарушителем.

В соответствии с вышеизложенными целями и задачами исследования диссертационная работа имеет название "Методы повышения информационной безопасности IP-телефонии с учетом вероятностно-временных характеристик протоколов распределения ключей ".

Выводы по главе 1

В первой главе рассмотрены актуальные проблемы и существующие подходы их решения в области защищенной IP-телефонии. В частности,

рассмотрены основные компоненты и протоколы IP-телефонии, а также возможные сценарии установления соединений. Описаны механизмы и алгоритмы, применяемые для обеспечения нормируемого показателя MOS, а также значений других нормированных показателей. Показаны значения параметров канала связи, при которых имеет смысл выполнять анализ работы протоколов IP-телефонии.

Приведен набор протоколов обеспечения безопасности IP-телефонии, а также классификация протоколов и их сокращенное описание. Выполнен обзор исследований в области обеспечения безопасности IP-телефонии, и выявлено отсутствие исследований о влиянии протоколов безопасности на нормируемые параметры функционирования сети телефонии. Показано влияние протоколов безопасности на параметры функционирования сети телефонии, выраженное в возникновении задержки при установлении защищенного соединения между корреспондентами.

Глава 2. Математическая модель активного нарушителя для защищенной IP-телефонии

Нарушитель может выбрать различные способы атаки на систему IP-телефонии, работающую в защищенном режиме, исходя из особенностей протоколов обеспечения безопасности IP-телефонии, описанных в разделе 1.3. Существуют несколько моделей нарушителя в IP-телефонии. Вероятностная модель нарушителя описана в [3] и описывает действия нарушителя, а также основные атаки при реализации безопасной IP-телефонии на ОС Windows. Модель учитывает различные типы атак, в том числе, характерные именно для Windows при использовании криптографических средств операционной системы. Однако, данная модель не учитывает, что ключи распространяются с помощью протоколов распределения ключей IP-телефонии, и предполагает только предварительную установку секрета у обоих корреспондентов. При атаке, направленной на несанкционированный доступ к информации (НСД), рассматривается только вероятность дешифрования передаваемого контента методом перебора, а атака модификация пакетов рассматривается только в случае успешной атаки получения пароля при дешифрации перехваченных пакетов.

В стандарте Российской Федерации, подготовленном Федеральной службой по техническому и экспортному контролю [69], описывается общая модель нарушителя. Модель также не учитывает особенностей работы безопасной IP-телефонии, состоящих в применении нескольких протоколов для обеспечения безопасности: защита сигнализации, защита медиа трафика, распределение ключевого материала,- а также не описывает атаки непосредственно на эти протоколы. В работе [7] предложена совокупность требований, предъявляемых к сети IP-телефонии, а также описываются основные общие типы атак на систему IP-телефонии от среднестатистического хакера. Однако, в работе отсутствует декомпозиция протоколов безопасности IP - телефонии на составляющие и отсутствует описание атак конкретно на эти протоколы. В работе [6] описываются

общие принципы обеспечения безопасности , а также возможные действия нарушителей при атаках на систему IP-телефонии. При этом не рассматриваются атаки на протоколы распределения ключевого материала, используемые в IP-телефонии. Так как в существующих моделях нарушителя [29 - 36], не описывается декомпозиция протоколов безопасности IP-телефонии, целесообразно разработать новую модель нарушителя, учитывающую описанные выше особенности.

Существующие модели [3, 7, 69, 29, 30, 6, 31, 36, 70] не позволяют определить вероятность успешной атаки НСД на систему защищенной IP-телефонии, работающую по схеме корреспондент-корреспондент, не учитывают атаку человек посередине (MITM) на ПРК. Вследствие этого целесообразно разработать такую модель нарушителя, которая позволила бы решить данную задачу.

2.1 Угрозы информационной безопасности в IP-телефонии

Угроза безопасности информации в IP-телефонии возникает в результате образования канала между источником угрозы и носителем (источником) информации, что создает условия для нарушения безопасности информации.

Актуальность угрозы безопасности информации будет определяться, в том числе, видом источника угрозы безопасности информации, наличием уязвимости источника информации и средой распространения информационного сигнала.

По виду источника угрозы воздействий на информацию можно выделить:

- угрозы, связанные с деятельностью организаций, обладающих высоким потенциалом, оснащенностью и мотивацией, обусловленной политическими, экономическими, военными и другими целями иностранных государств;
- угрозы, связанные с деятельностью организаций, обладающих мотивацией, обусловленной их экономическими, информационными и другими целями;

- угрозы, связанные с деятельностью отдельных физических лиц (преступных элементов).

Способы воздействия на информацию определяются возможностями источника угроз. Источник угроз, предпринимающий действия или осуществляющий подготовку к действиям по несанкционированному воздействию на информацию является нарушителем информационной безопасности.

Далее в качестве нарушителя рассматривается физическое лицо, случайно или преднамеренно совершающее действия в своих интересах или в интересах организаций, следствием которых является нарушение безопасности информации при ее обработке техническими средствами в информационных системах.

Целесообразно рассматривать нарушителей с точки зрения наличия права постоянного или разового доступа в контролируемую зону (КЗ) [71]. Выделяется два типа нарушителей:

- нарушители, не имеющие права доступа в КЗ – внешние нарушители;
- нарушители, имеющие право доступа в КЗ – внутренние нарушители.

Внешними нарушителями могут быть:

- представители разведывательных служб иностранных государств;
- представители террористических и криминальных структур;
- посторонние лица.

Внутренними нарушителями могут быть:

- работники оператора;
- работники сторонних организаций – разработчиков или поставщиков программного обеспечения и технических средств, обеспечивающие сопровождение этих средств на защищаемом объекте.

Обеспечение безопасности передачи речи в IP-телефонии осуществляется с применением криптографических протоколов: защищенного протокола реального времени – SRTP, реализующего функции криптографической инкапсуляции

данных, а также протоколов, выполняющих функцию автоматического распределения ключей для сессий SRTP, и протоколов защиты сигнализации.

Учитывая, что передача данных IP-телефонии осуществляется по сетям общего доступа, а VoIP терминалы доступны любому физическому лицу, как и легальный доступ к сетям - можно сделать вывод об актуальности угроз удаленного доступа и возможности их реализации как внешними нарушителями, так и отдельными категориями внутренних нарушителей.

2.2 Обобщенная модель нарушителя

Под моделью нарушителя понимается описание совокупности практических и теоретических возможностей, знаний, времени, места действия, а также прочих характеристик, свойственных нарушителю.

Под вероятностной моделью [stochastic, probabilistic model] — понимают модель, которая в отличие от детерминированной модели содержит случайные элементы [72]. При задании на входе модели некоторой совокупности значений, на ее выходе могут получаться различающиеся между собой результаты в зависимости от действия случайного фактора.

Под математической моделью нарушителя понимается модель, содержащая случайные элементы в виде вероятностей успешного выполнения отдельных атак, формирующих одну общую атаку, и определяющая вероятность достижения конечной цели этой атаки нарушителем.

Чтобы модель нарушителя была максимально полезной – она должна ориентироваться на конкретный объект защиты. Поэтому модель не может быть универсальной и синтезируется исходя из анализа структуры системы, ресурсов и способов их использования.

Существующие модели нарушителя не учитывает особенностей работы безопасной IP-телефонии, состоящих в применении нескольких протоколов для обеспечения безопасности, а также не описывают атаки непосредственно на эти протоколы.

Следовательно, целесообразно разработать модель нарушителя, учитывающую эти особенности. Для этого необходимо рассмотреть схему взаимодействия корреспондентов защищенной IP-телефонии для прямого соединения клиент – клиент, при отсутствии предварительно распределенного ключевого материала, и возможные варианты действия нарушителя в схеме (рисунок 2.1).

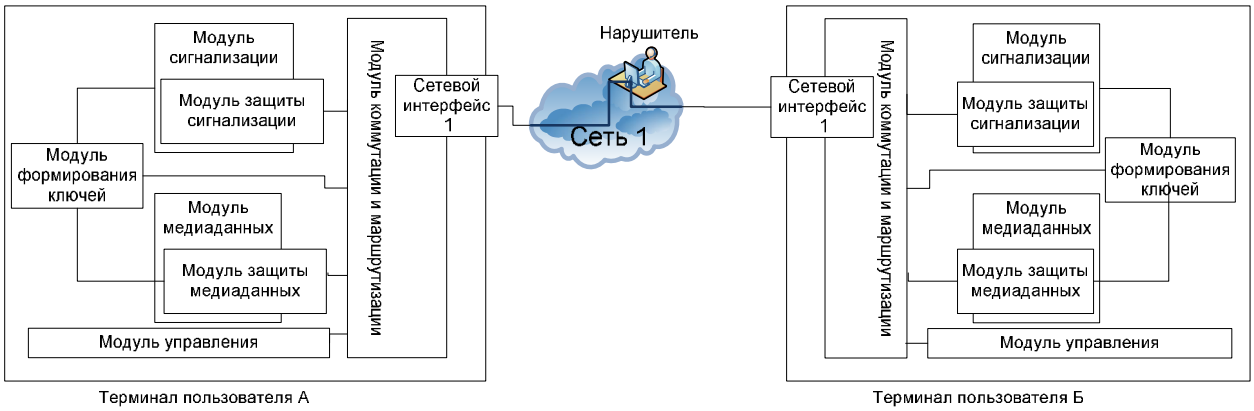


Рисунок 2.1 – Структурная схема соединения в сценарии клиент-клиент

Нарушитель может использовать следующие стратегии:

- Пассивную, используя только перехват передаваемых данных.
- Активную, используя штатные средства системы защиты и ее недостатки для проведения атаки или дополнительные средства для воздействия на систему с целью выполнения атаки.

В дальнейшем рассматривается нарушитель, использующий активную стратегию атаки, эксплуатирующую уязвимость протокола Диффи-Хелмана, лежащего в основе большинства протоколов распределения ключей (ПРК) IP-телефонии. Этот протокол защищает от атаки пассивного нарушителя. Однако, он неустойчив к атаке Man In The Middle (MITM) активного нарушителя [5, 73].

При осуществлении противоправных действий нарушитель может:

- находиться в одной подсети с объектом атаки, в том числе иметь права доступа какого-либо уровня в сеть или к оборудованию, на которое выполняется атака;

- не находиться в одной подсети с объектом атаки или не иметь прав доступа какого-либо уровня в сеть или к оборудованию, на которое выполняется атака.

VoIP терминалом пользователя, как правило, является IP-телефон, шлюз IP-телефонии, или иное вычислительное устройство (стационарный компьютер или мобильный терминал: ноутбук, планшетный компьютер, смартфон и т.д.) с установленным специализированным программным обеспечением IP-телефонии. Это устройство позволяет пользователю получать услуги IP-телефонии и выполнять аудио или видео вызовы других пользователей.

При рассмотрении атак на терминал пользователя введено допущение, что в одной подсети с жертвой может находиться только внутренний нарушитель. Соответственно, некоторые типы атак будут доступны только для этой категории нарушителей.

Для достижения целей НСД нарушитель при проведении атаки может использовать следующие существующие угрозы безопасности:

1. Преднамеренный несанкционированный доступ на оборудование оператора или пользователя, полученный за счет атаки перебора пароля или другой атаки на механизмы обеспечения безопасности информационной системы (ИС), со стороны внутренних или внешних нарушителей, обладающих правами и полномочиями на доступ к оборудованию более низкого уровня, или не имеющих доступа к нему,.
2. Преднамеренное воздействие на таблицу маршрутизации со стороны внешних или внутренних нарушителей, а также использование штатных средств оборудования для частичного перенаправления трафика пользователями, обладающими правами и полномочиями на доступ к информации в информационной системе.
3. Преднамеренное специализированное воздействие на обмен сообщениями ПРК, а также на другие передаваемые данные корреспондентов, направленное на нарушение конфиденциальности и целостности

передаваемых данных, со стороны внутренних и внешних нарушителей, обладающих правами и полномочиями на доступ к информации в ИС.

4. Специальное воздействие в виде атаки на шифр на перехваченную информацию, передаваемую между корреспондентами, со стороны внутренних и внешних нарушителей, обладающих правами и полномочиями на доступ или перехват зашифрованной информации в информационной системе, с целью нарушения конфиденциальности и дешифрования данных.
5. Преднамеренное несанкционированное специальное воздействие на программное обеспечение одного или нескольких корреспондентов со стороны внутренних или внешних нарушителей, обладающих правами и полномочиями на доступ к оборудованию и используемому программному обеспечению пользователя.
6. Преднамеренная несанкционированная установка дополнительного оборудования на узле оператора для целей специального воздействия на передаваемую от пользователей информацию со стороны внутренних нарушителей, обладающих правами и полномочиями доступа на узел оператора.
7. Преднамеренное несанкционированное воздействие на конфигурационные файлы терминала со стороны внутренних и внешних нарушителей, обладающих правами и полномочиями доступа к терминалу пользователя, с целью изменения настроек безопасности.
8. Преднамеренный несанкционированный перехват авторизационных данных для управления оборудованием пользователя со стороны внутренних нарушителей, обладающих правами и полномочиями на доступ к данным, передаваемым между компьютером пользователя и терминалом пользователя.

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 [74] выделены:

- Перебор пароля для доступа к управлению оборудованием оператора или пользователя;
- Организация проксирования или перенаправления всего или части трафика любым доступным способом;
- Выполнение 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;
- Изменение настроек терминала пользователя для частичного отключения безопасности;
- Перехват авторизационных данных для управления терминалом пользователя за счет прослушивания трафика управления шлюзом.

Атака перебор пароля к оборудованию [75] позволяет получить нелегитимному пользователю контроль над атакуемым оборудованием для дальнейшей организации атаки НСД. Сложность атаки зависит от протокола управления, на который выполняется атака (telnet, ssh, snmp, web и т.д.), от длины используемых паролей, вычислительных ресурсов нарушителя, и дополнительных ограничений и защитных механизмов атакуемого оборудования, а также от ширины канала связи между нарушителем и жертвой. Атака выполняется с использованием специализированного программного обеспечения при наличии канала связи для удаленного доступа к интерфейсу управления оборудованием.

Атака “организация проксирования или перенаправления трафика” позволяет нарушителю частично или полностью пропускать через свое

оборудование трафик легитимного корреспондента. Это может быть достигнуто за счет использования функции зеркалирования портов на оборудовании оператора, за счет использования маршрутизации на основе политик (policy based routing) , а также за счет других механизмов, доступных на оборудовании оператора связи с коммутацией пакетов.

Атака на ПРК заключается в организации MITM и выработки ключей поочередно с каждым из корреспондентов [76]. Она позволяет нарушителю становиться промежуточным элементом между корреспондентами и прослушивать или модифицировать передаваемую информацию. При этом опасность и распространенность данной атаки наиболее активно отмечается в различных источниках массовой информации [77 - 80].

Атака на шифр заключается в получении ключа шифрования при наличии зашифрованного сообщения. Атака может выполняться с помощью специализированного программного обеспечения, осуществляющего перебор пароля на основании частичной информации о передаваемых данных.

Установка закладки, модификация программного обеспечения терминала пользователя позволяет нарушителю получать контроль над оборудованием пользователя и любой информацией, проходящей через терминал, а также выполнять отвод информации на свой сервер с целью выполнения атаки НСД.

Установка дополнительного оборудования на узле оператора связи, позволяет нарушителю выполнять модификацию данных, передаваемых между корреспондентами, без необходимости изменения маршрутизации на сетевом оборудовании оператора. Атака выполняется за счет включения между оборудованием оператора и корреспондента оборудования нарушителя, или подключение этого оборудования в сеть передачи данных оператора.

Атака “изменение настроек терминала пользователя для снижения уровня безопасности” может выполняться за счет изменения таблицы маршрутизации на терминале пользователя, частичного отключения механизмов безопасности,

например, изменение режима работы протокола SRTP на аутентификацию сообщений без шифрования, модификации данных телефонной книжки и т.д.

Атака “перехват авторизационных данных пользователя, применяемых для управления VoIP-терминалом”, может быть выполнена внутренним нарушителем, находящимся в одной подсети с легитимным пользователем, и достигается путем перехвата трафика в момент авторизации пользователя на VoIP терминале за счет атаки на MAC-таблицу оборудования, или перенастройки сетевого оборудования.

2.3 Частные модели нарушителей

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 [81]:

$Ц_А$) 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.

Конечной целью каждой атаки является НСД.

2.3.1 Внешний нарушитель

Разработка модели начинается с анализа алгоритмов действий нарушителя по каждой из перечисленных целей.

2.3.1.1 Захват оборудования оператора внешним нарушителем

Рассмотрена модель для внешнего нарушителя, задачей которого является достижение НСД, а решается задача через захват оборудования оператора. Алгоритм действий нарушителя приведен на рисунке 2.2.

Для начала атаки нарушитель должен определить, на какой ресурс или какое устройство оператора начать выполнять атаку. Одной из возможностей получить эту информацию является использование команды tracert для определения промежуточных узлов между нарушителем и жертвой. Соответственно – с

большой вероятностью эти узлы могут принимать участие в обмене пакетами между двумя корреспондентами.

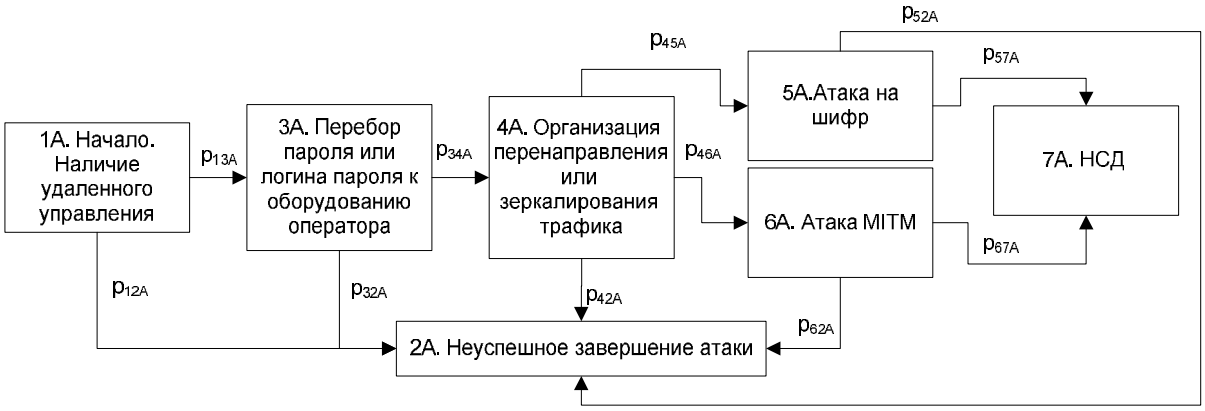


Рисунок 2.2 – Возможный алгоритм действий при выполнении захвата оборудования оператора внешним нарушителем

После выбора узла нарушитель может попытаться захватить управление этим узлом, выполняя, например, атаку перебор пароля. Однако – технически удаленное управление может быть запрещено для нарушителя с использованием списков доступа ACL (Access Control List).

Вероятность p_{12} отражает событие, что удаленное управление со стороны нарушителя отключено или у оператора установлены ACL.

Вероятность p_{13} отражает событие, обратное p_{12}, что существует возможность удаленного подключения к устройству оператора.

Нарушитель выбирает доступный протокол (telnet, SNMP, ssh, http/https или др.) удаленного управления, на который будет выполнять атаку перебором пароля. Вероятность успешного перебора пароля за ограниченное время определяется, как

$$p_{34A}=F(l, D, T, C), \quad (2.1)$$

где l – длина логина/пароля;

T – время, в течении которого требуется выполнить перебор;

D – дополнительные ограничения протокола, затрудняющие выполнение перебора пароля, а так же технические возможности нарушителя;

c – скорость канала связи, по которому выполняется перебор.

Вероятность p_{34A} отражает событие, что перебор пароля выполнен успешно и нарушитель получил доступ на оборудование оператора. Вероятность p_{32} отражает событие, что перебор пароля за ограниченное время закончился неуспешно.

В случае успешного захвата удаленного управления, нарушитель может достичь НСД двумя путями: выполнить перебор пароля к передаваемому медиа трафику и прослушивать данные, или выполнить атаку на механизм распределения ключей и дешифровать трафик с использованием полученного ключевого материала. Однако – успешное выполнение этих двух атак может не привести к положительному результату по достижению НСД, если не существует возможности выполнить атаку MITM на медиа трафик, создав правила на оборудовании оператора, которые позволят нарушителю пропускать трафик пользователя через свое оборудование. По этой причине – событие “атака на медиа трафик” в модели нарушителя перенесено ранее, чем “перебор ключа медиа трафика”, или “атака на механизм распределения ключей”.

Вероятность успешной атаки на медиа трафик (MITM, организация проксирования) можно определить по формуле:

$$1 - p_{42A} = \begin{cases} 1, & \text{если существует техническая возможность на оборудовании оператора} \\ & \text{создать правило для перенаправления трафика пользователя в сторону} \\ & \text{нарушителя для выполнения целей "проксирования" MITM} \\ 0, & \text{если не существует такой технической возможности} \end{cases} \quad (2.2)$$

Под атакой понимается изменение маршрута передачи пакетов медиаданных, чтобы они проходили через оборудование нарушителя. В случае успешного проведения атаки нарушитель пытается выполнить одну из двух возможных атак.

- перебор ключа медиа трафика;
- атака на механизм распределения ключей.

При этом вероятности отражают:

p_{45A} – вероятность, что нарушитель начал выполнять перебор пароля к медиа трафику.

p_{46A} – вероятность, что нарушитель начал атаку на механизм распределения ключей VoIP.

Вероятность p_{57} означает успешную атаку по перебору пароля. В этом случае – нарушителю становиться доступно прослушивание медиа трафика одного конкретного разговора, а также модификации данных при наличии проксирования и быстрого дешифрования ключа.

Вероятность p_{52} отражает неуспешное окончание атаки по перебору пароля за ограниченное время. Перехваченные данные могут храниться у нарушителя сколько угодно долго, однако актуальность перехваченных данных может устаревать со временем. Так расшифрованные через 100 лет переговоры могут не принести никакой пользы нарушителю, так как за это время данные устареют. T_{NAR_AKT} – время, в течении которого данные являются актуальными – зависит от характера данных. T_{NAR_SRTP} – время, требуемое на перебор пароля, зависит от технических мощностей нарушителя – Nar_{TH}, применяемых для защиты медиаданных криптографических примитивов и криптоалгоритмов – Nar_K, длины ключа – Nar_L, а также от усложняющих элементов (применение инициализирующего вектора, дополнительных счетчиков и т.д.) – Nar_D.

$$p_{57A}=f(T_{NAR\_AKT,}\ T_{NAR\_SRTP})=f\ (T_{NAR\_AKT},\ Nar_{TH},\ Nar_K,\ Nar_L,\ Nar_D) \quad (2.3)$$

$$p_{52A}=1-p_{57A} \quad (2.4)$$

Вероятность p_{67} определяет успешную атаку на механизм распределения ключей. Под атакой понимается вторжение нарушителя в середину канала связи в момент обмена ключами между корреспондентами. Это позволяет нарушителю выработать два ключа – один для работы с первым корреспондентом и второй для работы со вторым корреспондентом. Тем самым, во время разговора двух корреспондентов нарушитель выполняет шифрование и дешифрование медиаданных с использованием своих ключей. Вероятность атаки зависит от

наличия у нарушителя технических и программных средств для проведения MITM на протокол распределения ключей.

Следует отметить, что для проведения данной атаки требуется разработка специализированного программного обеспечения, но не требуются большие вычислительные мощности.

Вероятность p_{62} отражает неуспешное выполнение атаки и может быть определена, как:

$$p_{62A}=1-p_{67A} \quad (2.5)$$

Для анализа алгоритма используется математический аппарат вероятностных графов [82], который позволяет получить для исследуемого алгоритма оценки среднего времени выполнения и вероятность успешного завершения.

На рисунке 2.3 представлен вероятностный граф, соответствующий приведенному ранее алгоритму. Вероятностный граф используется для получения производящей функции, соответствующей переходу системы из начального состояния в конечное.

Каждой ветви графа соответствует производящая функция вида:

$$H_{zy}=p_{zy}x^{Tzy}, \quad (2.6)$$

где p_{zy} – вероятность перехода в состояние y из состоянии z,

T_{zy} – время, необходимое для перехода из состояния z в состояние y.

Используя возможный алгоритм действий нарушителя, составлен вероятностный граф, представленный на рисунке 2.3.

По графу выделена ветвь, соответствующая успешному выполнению атаки НСД и составлена производящая функция $H(x)$ этой ветви.

Для графа в соответствии с методикой, приведенной в [82], представлены $P_{НСД} = H(x=1)$:

$$P_{нсдЦА}= p_{13A}p_{34A}(p_{45A}p_{57A}+p_{46A}p_{67A}), \quad (2.7)$$

где p_{ijA} – вероятность перехода из вершины i графа в вершину j.

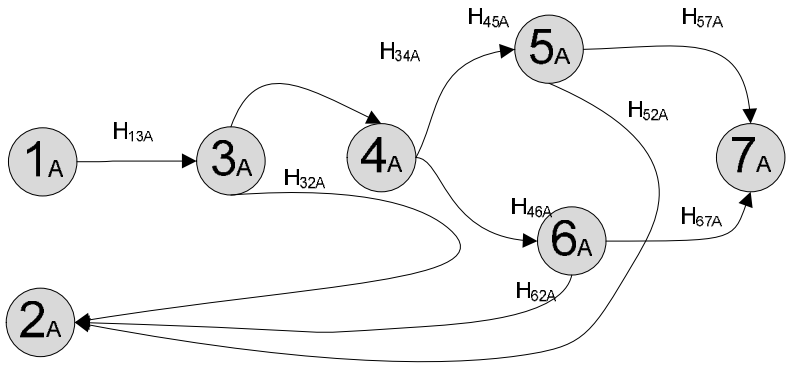


Рисунок 2.3 – Вероятностный граф - захват оборудования оператора внешним нарушителем

2.3.1.2 Захват терминала пользователя внешним нарушителем

Рассмотрена модель для внешнего нарушителя, задачей которого является достижение НСД, а решается задача через захват терминала пользователя. Алгоритм действий нарушителя приведен на рисунке 2.4.

Рассмотрены детальнее атаки, которые может предпринять нарушитель, в зависимости от использования у одного из корреспондентов шлюза или персонального компьютера со специализированным программным обеспечением.

При использовании шлюза наиболее вероятной является атака с проксированием всего трафика через оборудование нарушителя. Атака выполняется по схеме, указанной на рисунке 2.5, где IP1, IP2 – шлюзы пользователей, а Sн – сервер нарушителя со специализированным ПО.

Для проведения этой атаки нарушителю требуется в первую очередь захватить управление VoIP терминалом пользователя и выполнить его перенастройку. Например – если у корреспондента в режиме точка-точка в телефонной книжке шлюза введены сочетания номер – IP-адрес, то нарушитель может подменить IP – адрес корреспондента Б в записной книжке корреспондента А на свой, тем самым звонки с телефона корреспондента А будут приходить на Sн. Далее – сервер нарушителя выполняет протоколы безопасности между собой и корреспондентом Б от имени корреспондента А. Протоколы безопасности тоже выполняются между корреспондентами Б и сервером нарушителя. В результате –

нарушитель получает доступ ко всей информации, передаваемой от корреспондента А к корреспонденту Б, в открытом виде и при необходимости может не только прослушивать, но и изменять данные, передаваемые между корреспондентами. Перенаправление трафика от корреспондента А на Sн можно осуществлять не только за счет подмены записи в адресной книжке, но и за счет изменения настроек на шлюзе корреспондента А, установив адрес своего Sн в качестве прокси-сервера или основного сервера IP-телефонии.

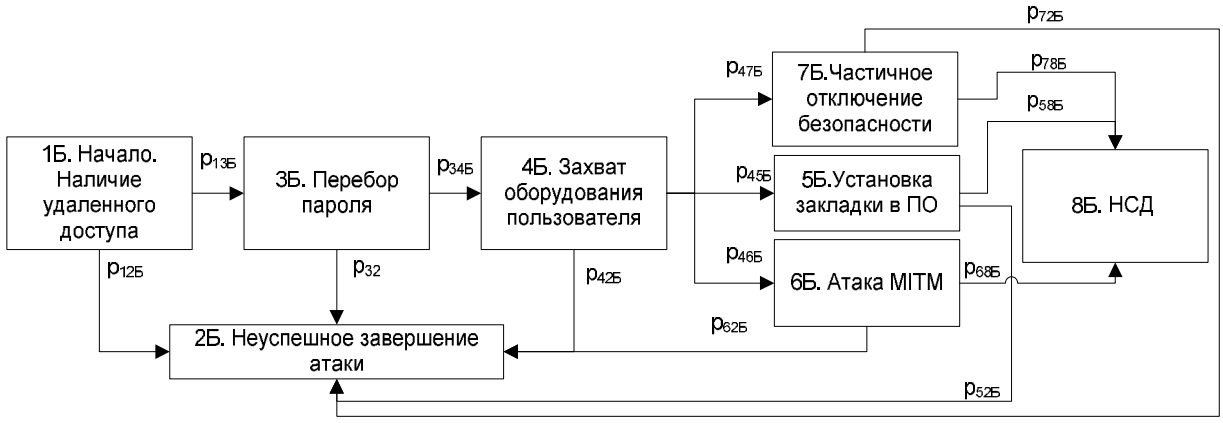


Рисунок 2.4 – Возможный алгоритм действий при захвата терминала пользователя внешним нарушителем

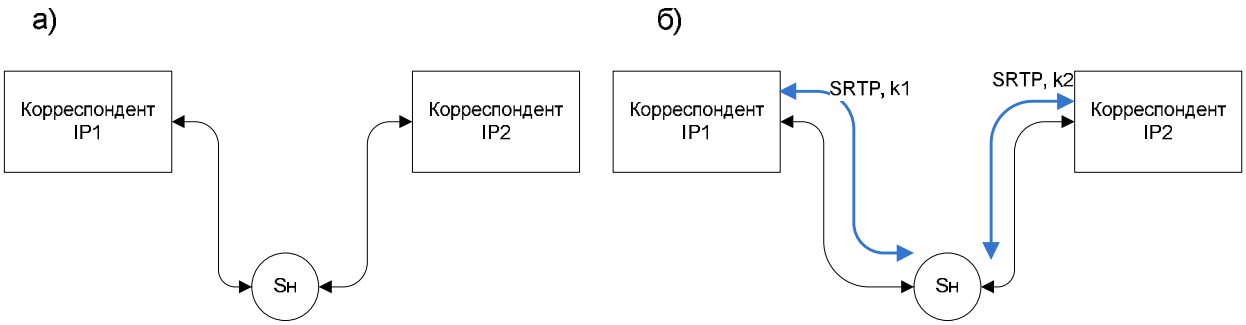


Рисунок 2.5 – Атака с проксированием а)выполнение ПРК, б)установленный защищенный речевой канал

При использовании компьютера с установленным программным шлюзом IP-телефонии наиболее реализуемыми являются атаки:

- атака с проксированием всего медиарафика корреспондентов через Sн;
- внедрение программы-шпиона на компьютер.

Первый вид атаки был описан ранее. Атака с внедрением программы-шпиона состоит в установке на терминал пользователя программного обеспечения, которое отправляет голосовые данные в открытом виде с терминала или передает все исходящие и входящие пакеты с сетевого интерфейса терминала пользователя на Sn для дальнейшей обработки. Тогда для доступа к передаваемой информации нарушителю может потребоваться выключить применяемые на терминале пользователя А протоколы безопасности IP-телефонии, или, как минимум, изменить режим работы SRTP, выключив шифрование передаваемых медиаданных.

Как правило, IP-телефоны и шлюзы имеют возможность удаленного управления, которая используется самими пользователями для их настройки. Вычислительные устройства также могут иметь удаленное управление, организованное внутренними средствами применяемой операционной системы, или с использованием дополнительного программного обеспечения. Однако, удаленное управление может быть также отключено пользователем, или возможности удаленного управления могут быть ограничены за счет применения списков доступа.

Для успешного выполнения атаки нарушитель должен захватить удаленное управление пользовательским терминалом. В первую очередь – успех атаки зависит от многих факторов. Вероятность успешного проведения этого этапа атаки рассматривается, как

$$p_{34Б} = \begin{cases} 1, \text{ если у пользовательского терминала включено удаленное управление} \\ \quad \text{и нет настоенных списков доступа на все удаленные протоколы} \\ 0, \text{ если у пользовательского терминала включено удаленное управление} \\ \quad \text{и есть настоенные списки доступа на все удаленные протоколы} \\ 0, \text{ если у пользовательского терминала выключено удаленное управление} \end{cases} \quad (2.8)$$

При наличии удаленного управления, нарушителю для проведения атаки требуется подобрать пароль или пару логин-пароль для авторизации на терминале пользователя [83]. Предполагается, что IP адрес жертвы известен нарушителю заранее. Подбор пароля или логина-пароля зависит от протокола удаленного

управления, на который выполняется атака. Вероятность успешного перебора пароля имеет смысл оценивать за конечный интервал времени T, так как вероятность успешного перебора пароля за бесконечное время будет равна 1.

Вероятность успешного перебора пароля можно определить как:

$$p_{45Б}=F(l, D, T, C), \quad (2.9)$$

где l – длина логина-пароля;

T – время, в течении которого требуется завершить перебор;

D – дополнительные ограничения протокола, затрудняющие выполнение перебора пароля, а так же технические возможности нарушителя;

C – скорость канала связи, по которому выполняется перебор.

После успешного перебора пароля и получения доступа к терминалу пользователя, нарушитель с некоторой вероятностью может выбрать один из двух возможных путей:

- установка закладки, модификация ПО терминала;
- изменение настроек терминала пользователя;
- MITM для всех протоколов IP-телефонии.

Вероятность выбора одной из двух атак определяется технической оснащенностью нарушителя, а также наличием у него специализированных инструментов и средств.

Смысл первой атаки состоит в захвате голосовой информации в обход протоколов IP-телефонии, или в выключении протоколов безопасности IP-телефонии, или смене режимов работы протоколов безопасности IP-телефонии, чтобы можно было выполнять прослушивание.

Смысл второй и третьей атаки состоит в изменении настроек пользовательского терминала для реализации атаки MITM, при которой все данные протоколов безопасности проходят через нарушителя, что позволяет ему контролировать передаваемые голосовые пакеты, а также при необходимости выполнять модификацию передаваемых данных. Фактически, при данной атаке нарушитель выполняет соединение по очереди с каждым из корреспондентов,

используя протоколы обеспечения безопасности IP-телефонии, реализуя схему, представленную на рисунке 2.6.

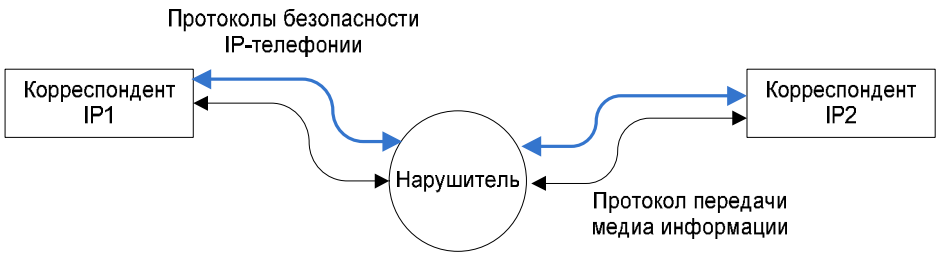


Рисунок 2.6 – Реализация атаки MITM для всех протоколов обеспечения безопасности VoIP

Выбрав одну из атак, нарушитель попытается выполнить ее для получения несанкционированного доступа к передаваемой информации. Однако существует вероятность неуспешного выполнения выбранной атаки, которая отражается вероятностями p_{72} и p_{62} соответственно. Например – атака “изменение настроек терминала пользователя” может кончиться неуспешно, если пользователь заметит измененные настройки и восстановит свои настройки, сменив пароли доступа к терминалу или отключив удаленное управление.

Используя возможные алгоритмы действий нарушителя, составлен вероятностный граф, представленный на рисунке 2.7.

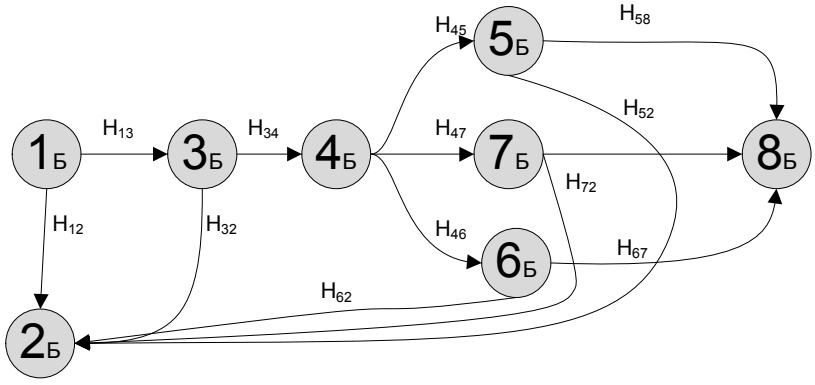


Рисунок 2.7 – Вероятностный граф захват терминала пользователя внешним нарушителем

Из графа выделена ветвь, соответствующая успешному выполнению атаки НСД, и составлена производящая функция *H(x)* этой ветви.

Для графа в соответствии с методикой, приведенной в [82], представлены $P_{НСД} = H(x=1)$:

$$P_{нсдЦБ} = p_{13Б}p_{34Б}(p_{45Б}p_{58Б}+p_{46Б}p_{68Б}+p_{47Б}p_{78Б}) , \quad (2.10)$$

где $p_{ijБ}$ – вероятность перехода из *i*-й в *j*-ую вершину графа.

2.3.2 Внутренний нарушитель

2.3.2.1 Захват оборудования оператора внутренним нарушителем

Рассмотрена модель внутреннего нарушителя, задачей которого является достижение НСД, а решается задача через захват оборудования оператора.

По сравнению с внешним нарушителем, внутренний относительно оператора нарушитель обладает рядом преимуществ. Он изначально имеет некоторый уровень доступа на оборудование оператора связи, а также может иметь возможность установки и подключения дополнительного оборудования к существующему оборудованию на сети оператора.

Если нарушитель не имеет достаточного уровня доступа на оборудование оператора, он может попытаться получить доступ, выполняя атаку перебора паролей для получения более высокого уровня.

Алгоритм действий нарушителя приведен на рисунке 2.8.

$p_{18В}$ характеризует вероятность, что у внутреннего нарушителя изначально есть доступ достаточного уровня для проведения последующих действий для достижения НСД.

Вероятность $p_{18В}$ может быть определена, как:

$$p_{18В} = \begin{cases} 1, & \text{если нарушитель имеет достаточный уровень доступа;} \\ 0, & \text{если нарушитель не имеет достаточный уровень доступа.} \end{cases} \quad (2.11)$$

$p_{19В}$ отражает вероятность события , что нарушителю удалось подключить свое дополнительное оборудование в сети оператора на узел, через который проходит медиа трафик жертвы.

$$p_{19B} = \begin{cases} 1, & \text{если нарушитель смог установить дополнительное оборудование} \\ & \text{на узле оператора;} \\ 0, & \text{если нарушитель не смог установить дополнительное оборудование} \\ & \text{на узле оператора.} \end{cases} \quad (2.12)$$

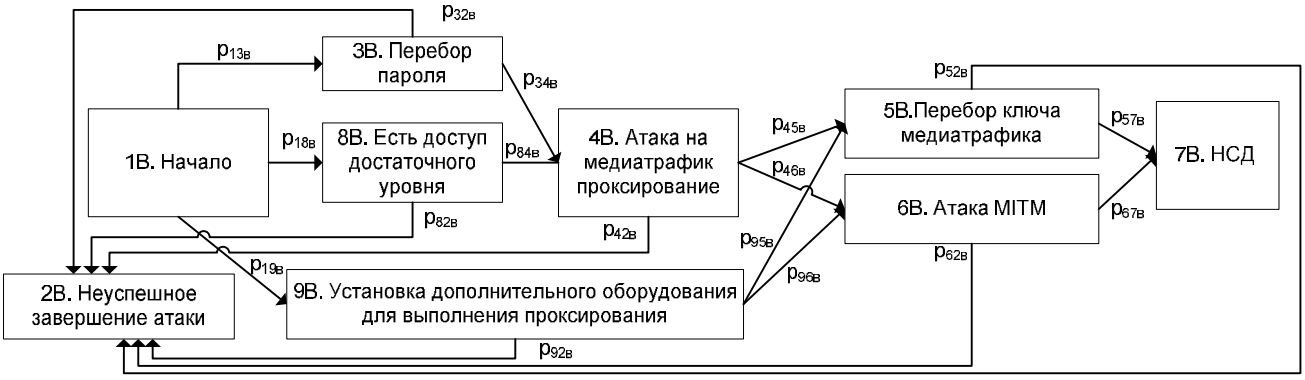


Рисунок 2.8 – Возможный алгоритм действий при выполнении захвата оборудования оператора внутренним нарушителем

Устанавливаемое оборудование изначально должно иметь функционал модификации или зеркалирования пакетов. С этого шага нарушитель может выбирать один из двух путей для дальнейшего проведения атаки. Выбор зависит от технических возможностей установленного оборудования. Однако, даже при установке оборудования нарушителя есть некоторая вероятность, что атака может быть проведена неуспешно. Например – это может произойти в том случае, если клиенты начнут применять дополнительные механизмы для отслеживания вторжения или дополнительные протоколы, использование которых может быть не учтено в оборудовании нарушителя.

Используя возможные алгоритмы действий нарушителя, составлен вероятностный граф, представленный на рисунке 2.9.

В графе выделена ветвь, соответствующая успешному выполнению атаки НСД и составлена производящая функция *H(x)* этой ветви. Для графа в соответствии с методикой, приведенной в [82], представлены $P_{НСД.}$

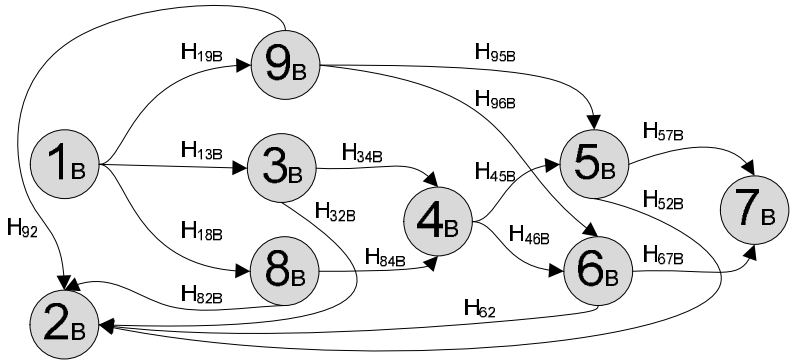


Рисунок 2.9 – Вероятностный граф - Захват оборудования оператора внутренним нарушителем

$$P_{нсдЦВ}=((p_{13B}p_{34B}+p_{18B}p_{84B})p_{45B}+p_{19B}p_{95B})p_{57B}+$$
$$((p_{13B}p_{34B}+p_{18B}p_{84B})p_{46B}+p_{19B}p_{96B})p_{67B}\ , \qquad (2.13)$$

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

Тогда вероятность защиты от атаки НСД будет иметь вид:

$$P_{защ\_нсд\_B}=1-P_{нсдЦВ}=$$
$$=1-((p_{13B}p_{34B}+p_{18B}p_{84B})p_{45B}+p_{19B}p_{95B})p_{57}+((p_{13B}p_{34B}+p_{18B}p_{84B})p_{46B}+p_{19B}p_{96B})p_{67B} \qquad (2.14)$$

где p_{13B} – вероятность выбора атаки перебор пароля для доступа к оборудованию оператора;

p_{18B} – вероятность наличия доступа достаточного уровня на оборудование оператора;

p_{19B} – вероятность наличия у нарушителя возможности установки дополнительного оборудования для выполнения атаки;

p_{34B} – вероятность успешного завершения атаки перебор пароля для доступа к оборудованию оператора;

p_{45B} – вероятность выбора атаки “взлом шифра”;

p_{46B} – вероятность выбора “атака на механизм распределения ключей”;

p_{57B} – вероятность успешного завершения атаки “взлом шифра”;

p_{67B} – вероятность успешного завершения атаки “атака на механизм распределения ключей”;

$p_{95В}$ – вероятность выбора атаки “взлом шифра”;

$p_{96В}$ – вероятность выбора “атака на механизм распределения ключей”.

2.3.2.2 Захват терминала пользователя внутренним нарушителем

Рассмотрена модель для внутреннего нарушителя, задачей которого является достижение НСД, а решается задача через захват терминала пользователя. Алгоритм действий нарушителя приведен на рисунке 2.10.

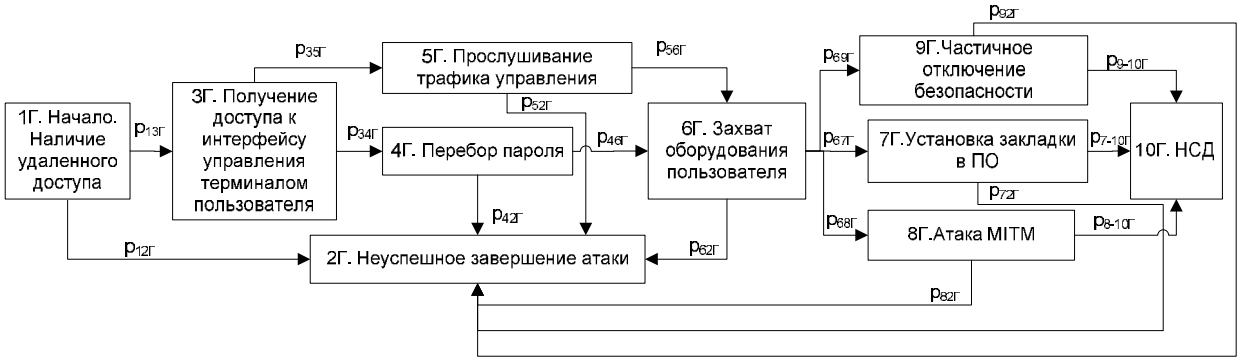


Рисунок 2.10 – Возможный алгоритм действий при выполнении захвата терминала пользователя внутренним нарушителем

Используя возможный алгоритм действий нарушителя, составлен вероятностный граф, представленный на рисунке 2.11. Из графа выделена ветвь, соответствующая успешному выполнению атаки НСД, и составлена производящая функция *H(x)* этой ветви. Для графа в соответствии с методикой [82] представлена вероятность успешного завершения атаки НСД - $P_{НСД}$:

$$P_{нсдЦГ}= p_{13Г}(p_{34Г}p_{46Г}+p_{35Г}p_{56Г})(p_{67Г}p_{7\text{-}10Г}+p_{68Г}p_{8\text{-}10Г}+p_{69Г}p_{9\text{-}10Г}) \quad (2.15)$$

где $p_{ijГ}$ – вероятность перехода из вершины *i* графа в вершину *j*.

Вероятность защиты от атаки будет иметь вид:

$$P_{защ\_нсд\_Г}=1- P_{нсдЦГ} =1-p_{13}(p_{34}p_{46}+p_{35}p_{56})(p_{67}p_{7\text{-}10}+p_{68}p_{8\text{-}10}+p_{69}p_{9\text{-}10}) \quad (2.16)$$

где $p_{13Г}$ – вероятность наличия удаленного подключения;

$p_{34Г}$ – вероятность выбора атаки “перебора пароля к оборудованию пользователя”;

$p_{46Г}$ – вероятность успешного перебора пароля к оборудованию пользователя за ограниченное время;

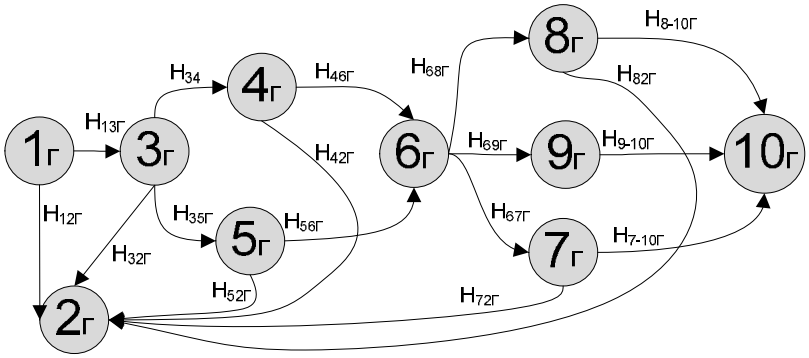


Рисунок 2.11 – Вероятностный граф - захват терминала пользователя внутренним нарушителем

$p_{35Г}$ – вероятность выбора атаки “получение пароля к оборудованию пользователя за счет прослушивания трафика пользователя”;

$p_{56Г}$ – вероятность успешного завершения атаки “перехват пароля к оборудованию пользователя за счет прослушивания трафика управления”;

$p_{68Г}$ – вероятность выбора атаки MITM для всех протоколов VoIP;

$p_{8\text{-}10Г}$ – вероятность успешного завершения атаки MITM для всех протоколов VoIP;

$p_{67Г}$ – вероятность выбора атаки “установка закладки на терминале пользователя”;

$p_{7\text{-}10Г}$ – вероятность успешного завершения атаки “установка закладки на терминале пользователя или отключение безопасности”.

$p_{6\text{-}9Г}$ – вероятность выбора атаки “полное или частичное отключение безопасности”;

$p_{9\text{-}10Г}$ – вероятность успешного завершения атаки “полное или частичное отключение безопасности”.

Значения многих вероятностей, входящих в формулу, требуют экспертной оценки и не могут быть вычислены. Также значения этих вероятностей зависят от нарушителя, его возможностей, а также дополнительных обстоятельств.

2.4 Оценка вероятности успешного завершения атаки

Для каждого из рассматриваемых графов в соответствии с методикой, приведенной в [82], приведены $P_{НСД}$:

$$P_{нсдЦА} = p_{13А} p_{34А}(p_{45А}p_{57А} + p_{46А}p_{67А}) \quad (2.17)$$

$$P_{нсдЦБ} = p_{13Б}p_{34Б}(p_{45Б}p_{58Б} + p_{46Б}p_{68Б} + p_{47Б}p_{78Б}) \quad (2.18)$$

$$P_{нсдЦВ} = ((p_{13В}p_{34В} + p_{18В}p_{84В})p_{45В} + p_{19В}p_{95В})p_{57В} +$$

$$+((p_{13В}p_{34В} + p_{18В}p_{84В})p_{46В} + p_{19В}p_{96В})p_{67В} \quad (2.19)$$

$$P_{нсдЦГ} = p_{13Г}(p_{34Г}p_{46Г} + p_{35Г}p_{56Г})(p_{67Г}p_{7\text{-}10Г} + p_{68Г}p_{8\text{-}10Г} + p_{69Г}p_{9\text{-}10Г}) \quad (2.20)$$

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

$$P_{нсд} = max\ \{ P_{нсдЦА}, P_{нсдЦБ}, P_{нсдЦВ}, P_{нсдЦГ}\} \quad (2.21)$$

Очевидно, в случае установления соединения в сценарии корреспондент-корреспондент без сервера и при отсутствии предварительно распределенного ключевого материала, сам пользователь является наиболее заинтересованным лицом для повышения безопасности и снижения $P_{НСД}$. При этом пользователь может применять 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 pij_A, pij_B. В зависимости от промежуточных целей нарушителя выделяется несколько частных моделей нарушителей, представленных в таблице 2.1.

Следует заметить, что $p_{57А}$, $p_{57В}$ зависят от применяемого алгоритма шифрования. Существующие рекомендации SRTP предусматривают применение алгоритма AES с ключом 128 или 256 бит. Взлом такого алгоритма является крайне маловероятным [84]. Поэтому наиболее вероятным будет выбор атаки MITM на ПРК со стороны нарушителя. Следовательно, можно ввести допущение,

что вероятность выбора атаки на шифр p_{45A}=0, p_{45B}=0 , а вероятность выбора атаки MITM p_{46A}=1, p_{46B}=1.

Таблица 2.1. Вероятности атак в зависимости от целей нарушителя

Обозначение и определение вероятности	Возможные значения вероятностей	Цели нарушителей			
		B1) Атака внутреннего нарушителя через захват оборудования оператора за счет перебора пароля и организация MITM	B2) Атака внутреннего нарушителя при наличии у него доступа на оборудование путем организации MITM	B3) Атака внутреннего нарушителя через установку дополнительного оборудования на узле оператора путем организации MITM	A4) Атака внешнего нарушителя через захват оборудования оператора за счет перебора пароля и организация MITM
p_{13B} – вероятность выбора атаки "перебор пароля для доступа к оборудованию оператора"	0..1	1	0	0	-
p_{18B} – вероятность наличия доступа достаточного уровня на оборудование оператора	0..1- p_{13B}	0	1	0	-
p_{19B} – вероятность наличия у нарушителя возможности установки дополнительного оборудования на узле оператора связи для выполнения атаки	0..1- p_{18B}- p_{13B}	0	0	1	-
p_{34A},p_{34B} – вероятность успешного завершения атаки перебор пароля для управления оборудованием оператора	0..1	0..1	-	-	0..1
p_{84B} – вероятность использования нарушителем имеющегося доступа достаточного уровня на оборудование оператора	0..1	-	0..1	-	-
p_{46A}, p_{46B} – вероятность выбора "атаки MITM на ПРК и другие протоколы безопасной IP-телефонии"	0..1- p_{45A} 0..1- p_{45B}	1	1	-	1
p_{67A},p_{67B} – вероятность успешного завершения “атаки MITM на ПРК и другие протоколы безопасной IP-телефонии”	0..1	0..1	0..1	0..1	0..1
p_{96B} – вероятность выбора "атаки MITM на ПРК и другие протоколы безопасной IP-телефонии"	0..1- p_{95B}	-	-	1	-
p_{13A} – вероятность наличия возможности удаленного подключения к оборудованию оператора	0 или 1	-	-	-	1

Тогда вероятность успешной атаки НСД будет иметь вид:

$$P_{нсд} = max \{ P_{нсдЦА}, P_{нсдЦВ} \} \quad (2.22)$$

$$P_{нсдЦА}=p_{13A}p_{34A}p_{46A}p_{67A} \quad (2.23)$$

$$P_{нсдЦВ}=((p_{13B}p_{34B}+p_{18B}p_{84B})p_{46B}+p_{19B}p_{96B})p_{67B} \quad (2.24)$$

В зависимости от промежуточных целей и возможностей также выделяется несколько нарушителей (В1, В2, В3,А4), представленных в таблице 2.1.

Подставив значения p_{ijX} из таблицы в формулы 2.23,2.24 получаем:

$$P_{нсдВ1}=p_{34B}p_{67B} \quad (2.25)$$

$$P_{нсдВ2}=p_{84B}p_{67B} \quad (2.26)$$

$$P_{нсдВ3}=p_{67B} \quad (2.27)$$

$$P_{нсдА4}=p_{34A}p_{67A} \quad (2.28)$$

$$P_{НСД}=max\{P_{нсдВ1}, P_{нсдВ2}, P_{нсдВ3}, P_{нсдА4}\} \quad (2.29)$$

Очевидно, что $P_{нсдВ3}$ больше или равна $P_{нсдВ1}$, $P_{нсдВ2}$, $P_{нсдА4}$. Следовательно, $P_{НСД}$ будет определяться величиной p_{67B}, 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. График зависимости $P_{НСД}$ для модели захват оборудования оператора внешним нарушителем приведен на рисунке 2.12.

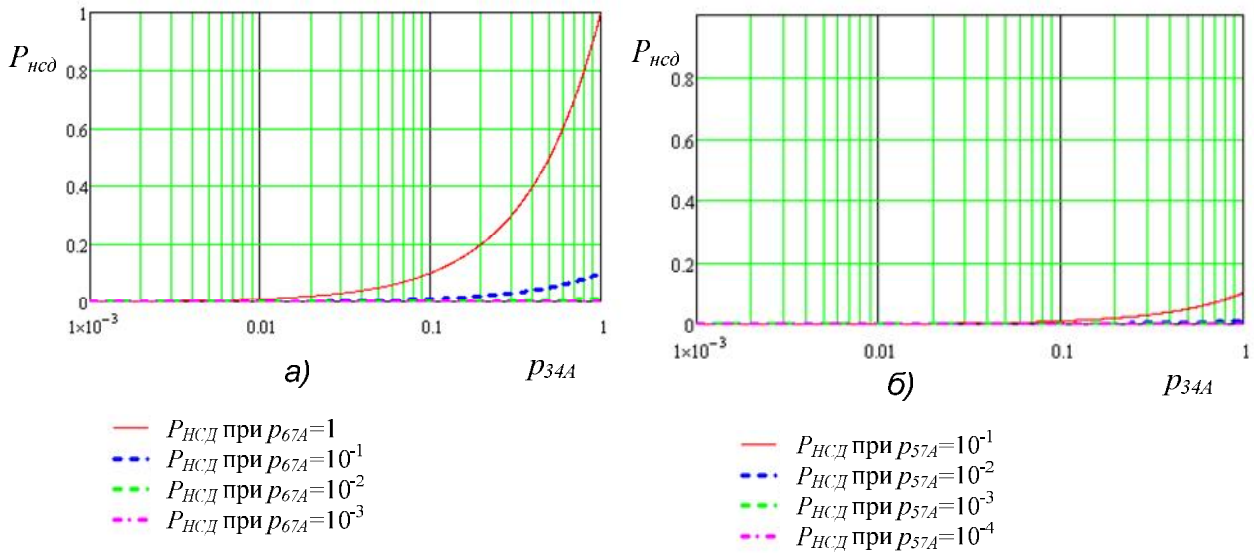


Рисунок 2.12 – Зависимость $P_{НСД}$ для модели - захват оборудования оператора внешним нарушителем а) при выборе MITM б)при выборе атаки на шифр

Выводы по главе 2

Приведено определение нарушителя и описание терминала пользователя. Показана совокупность атак, которые может выполнять нарушитель для достижения НСД. Представлена математическая модель активного нарушителя для защищенной IP-телефонии, учитывающая возможности этого нарушителя реализовать атаку MITM на ПРК и другие атаки. Модель позволяет рассчитать вероятность успешной атаки, нацеленной на НСД, в зависимости от значений вероятностей промежуточных атак и опубликована в [74]. Приведены частные модели нарушителей в зависимости от выбранных целей, возможностей и местоположения нарушителя.

Для борьбы с нарушителем, поставившим цель захватить управление оборудованием пользователя, необходимо выполнять все рекомендации по обеспечению безопасности при настройке оборудования, а именно, блокировать удаленное управление из нелегитимных и прочих сетей, или отключать удаленное управление.

Приведена оценка вероятности выбора каждым из частных нарушителей определенных промежуточных целей при реализации атаки. Показаны возможные действия пользователя для защиты от атак, а также определена наиболее опасная для пользователя атака MITM на протокол обеспечения безопасности IP-телефонии, которая также является наиболее предпочтительной для нарушителя.

Показано, что особую опасность представляет внешний и внутренний нарушители, выполняющие атаку на оборудование оператора. Представлена вероятностная модель такого нарушителя. Показано, что наиболее опасной является атака MITM на протоколы распределения ключевого материала.

Глава 3. Разработка предложений по совершенствованию протоколов распределения ключей

Для исследования вероятностно-временных характеристик необходимо рассмотреть протоколы распределения ключей защищенной IP-телефонии, отвечающие требованиям к ПРК, описанным в первой главе:

$К_1$. Поддержка топологий клиент-сервер и клиент-клиент;

$К_2$. Самодостаточность (функционирование без применения дополнительных протоколов между корреспондентами для реализации функции распределения ключей);

$К_3$. Работа без передачи ключа в открытом виде по каналу связи;

$К_4$. Наличие механизма обнаружения MITM без заранее распределенного ключевого материала между корреспондентами, а также без использования сертификатов;

$К_5$. Использование TCP/UDP портов, применяемых для IP-телефонии (SIP/RTP), или TCP/UDP портов, использование которых согласовано в результате установления соединения;

В случае выполнения требования, K_i=1. В противном случае K_i=0.

Сравнение протоколов приведено в таблице 3.1.

Таблица 3.1 – Оценка ПРК на соответствие требованиям

Описание требования к ПРК	Протоколы			
	DTLS	ZRTP	SDES	MIKEY
K_1	1	1	0	1
K_2	1	1	0	0
K_3	1	1	0	1
K_4	0	1	0	0
K_5	1	1	1	1
$Q_{ПРК}$	4	5	1	3

Оценка каждого из протоколов производится в соответствии с функцией $Q_{ПРК}$:

$$Q_{ПРК} = \sum_{i=1}^{5} K_i \qquad (3.1)$$

Протокол DTLS не отвечает четвертому требованию, представленному в таблице 3.1, так как разрабатывался для работы в топологии клиент - сервер и использует предустановленные сертификаты для защиты от MITM у обоих корреспондентов. Поэтому для DTLS $К_4$=0.

В отличие от прочих протокол ZRTP имеет встроенный механизм SAS (Short Authentication String)для защиты от MITM. Потому для ZRTP $К_4$=1. Для SDES и MIKEY $К_4$=0.

Протокол MIKEY не удовлетворяет второму требованию из таблицы 3.1, так как сообщения протокола могут передаваться либо в SIP/SDP-сообщения, либо поверх RTSP (Real Time Streaming Protocol), но в последнем случае корреспонденты должны дополнительно поддерживать протокол RTSP. Поэтому K_2=0 для MIKEY.

Пятое требование при работе поверх RTSP протокола не выполняется, но при этом выполняется второе требование. При работе MIKEY поверх в SIP/SDP-сообщения пятое требование выполняется, но не выполняется второе требование. Так как при оценке $Q_{ПРК}$ используется K_2=0, то K_1=1 для MIKEY.

Протокол SDES не удовлетворяет первому и третьему требованию (K_1=0 и K_3=0), так как ключ передается между корреспондентами в явном виде в сообщениях SDP и требует их дополнительной защиты. Для защиты как правило используется дополнительный протокол SIPS. Однако, при соединении клиент-клиент, когда у корреспондентов нет заранее распределенного ключевого материала, SIPS соединение с защитой от MITM организовать невозможно. Протокол SDES не удовлетворяет второму требованию, так как для передачи данных протокола SDES используются сообщения SIP/SDP. Соответственно $К_2$=0 для SDES.

Исходя из таблицы 3.1, в большей степени приведенным требованиям соответствуют протоколы ZRTP и DTLS, имеющие наибольшее значение $Q_{ПРК}$. Оценка ВВХ характеристик выполняется для этих протоколов.

Результаты проведенных исследований показывают, что известные протоколы распределения ключей необходимо совершенствовать в двух направлениях [85]:

1) повышение безопасности;
2) улучшение ВВХ характеристик протоколов.

В главе 2 показано, что наиболее опасной атакой является атака MITM на протокол распределения ключей. Задача формирования ключей в условиях вторжения нарушителя в середину канала связи является актуальной и ее решению посвящен ряд научных работ [86 - 90]. Особенностью данных работ является то, что для формирования ключей между корреспондентами используется эффект независимости случайных процессов в различных точках среды передачи сигнала. В протоколах формирования ключей для IP-телефонии обмен сообщениями реализуется на сетевом уровне и эффекты случайных процессов в среде передачи данных одинаковы во всех точках на трассе передачи пакетов, поэтому предложенные подходы крайне затруднительно использовать для распределения ключей в IP-телефонии. Проводятся исследования по повышению безопасности протоколов [91- 92], однако общностью данных работ является необходимость наличия общего секрета между корреспондентами. Однако, данное условие не всегда может быть выполнено.

Одним из путей повышения безопасности протокола является снижение вероятности вторжения нарушителя в протокол выработки ключевого материала за счет использования нескольких независимых каналов связи. Таким образом, используемые в протоколе каналы связи должны отвечать требованию - не иметь общих точек, контролируя которые, нарушитель может одновременно атаковать используемые каналы.

В данном разделе проводится исследование вероятности, что в выбранном направлении найдется хотя бы два независимых маршрута передачи данных, а также оценка вероятностей обнаружения атаки при использовании нескольких маршрутов одновременно, успешного вторжения нарушителя в каналы связи, используемые при выполнении протокола, а также успешного распределения общего ключа. Предлагаются методы повышения безопасности, основанные на использовании нескольких каналов связи одновременно. В частности, описываются метод повышения безопасности ZRTP за счет автоматической проверки аутентификационной строки и метод выявления нарушителя протоколов распределения ключей, основанных на алгоритме Диффи-Хелмана.

3.1 Метод повышения безопасности ZRTP за счет автоматической проверки аутентификационной строки

Протокол Диффи-Хелмана может быть полностью скомпрометирован активным злоумышленником. Поэтому при работе протокола необходимо обеспечить подлинность исходных данных [104]. По этой причине протокол обмена ключами Диффи-Хелмана обычно применяют по защищенному каналу передачи данных [105], в котором невозможно выполнить подмену передаваемых сообщений, или при использовании сертификатов [106] или доверенного центра сертификации, которому доверяют оба корреспондента для целей аутентификации.

В случае необходимости установить защищенное соединение между двумя корреспондентами, они, во-первых, могут не иметь общих сертификатов (т.е. сертификатов, имеющих один и тот же корневой доверенный центр), не иметь общего доверенного центра сертификации или распределения ключей, а также могут не иметь защищенного канала связи между собой.

При наличии у корреспондентов сертификатов, подписанных разными центрами сертификации, невозможно проверить подлинность сертификата, так

как каждый из корреспондентов может не доверять центру сертификации респондента.

Для организации защищенного соединения между корреспондентами также требуется выполнить распределение ключевого материала для этого соединения. Корреспонденты могут использовать симметричное или ассиметричное шифрование. При использовании симметричного шифрования – один из корреспондентов должен передать другому секретный ключ. Если этот ключ станет известным нарушителю – переданные в процессе сеанса связи сообщения будут расшифрованы нарушителем. При использовании ассиметричного шифрования – информация не будет прочитана нарушителем даже в случае перехвата сообщений. Однако – при обмене ключами для организации защищенного соединения у корреспондентов не будет возможности удостовериться – что открытый ключ передается между ними без модификации нарушителем, как представлено на рисунке 3.1.

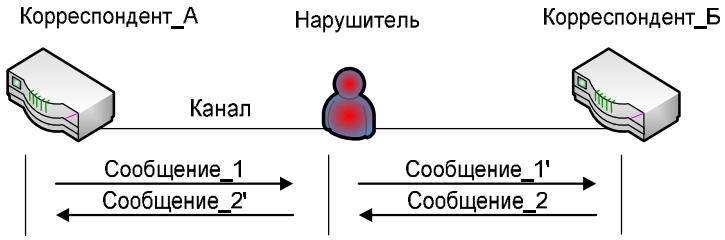


Рисунок 3.1 – MITM при использовании ассиметричного шифрования

Также стоит отметить, что открытый и закрытый ключи имеют большую длину и их передача между корреспондентами в словесном или письменном виде затруднена.

Для повышения безопасности предлагается использовать два метода:

- повышение безопасности за счет автоматизации проверки аутентификационной строки по второму каналу связи;
- использование двух и более каналов связи для выполнения протокола распределения ключей.

Защита от нарушителя в режиме клиент-клиент выполняется за счет проверки аутентификационной строки, которая передается по голосовому каналу в ручном режиме. Голосовой канал в этом случае является дополнительным каналом связи по отношению к IP-каналу. Целесообразно автоматизировать процесс проверки SAS. Существующий метод не безопасен, так как используется один канал связи, а современные средства анализа и синтеза речи позволяют выполнять автоматическое вырезание строки и замену на строку, синтезированную нарушителем.

Проведенное практическое исследование показало, что существует высокая вероятность наличия между корреспондентами независимых непересекающихся маршрутов при использовании нескольких каналов связи. В основе предлагаемых протоколов использовано преимущество легитимных корреспондентов над нелегитимными, заключающееся в том, что только легальные корреспонденты могут получать сообщения по двум и более каналам связи одновременно, обладая знаниями об IP-адресах корреспондентов, при этом эта информация не является секретной для нарушителя. Следует отметить, что метод модернизации протоколов распределения ключей рассматривается, как повышение безопасности, но при этом не обеспечивает 100% достоверность.

Рассматриваются несколько возможных вариантов модернизации протокола распределения ключей при использовании двух или трех каналов связи. В качестве критериев оценки используются величины следующих вероятностей:

- вероятность успешной атаки MITM $P_{УА}$;
- вероятность обнаружения атаки MITM $P_{ОН}$;
- вероятность успешной генерации общего секрета $P_{УК}$.

Протокол ZRTP имеет механизм защиты от MITM, выраженный в вербальной проверке короткой аутентификационной строки SAS по речевому каналу между обоими корреспондентами. Это означает, что после выполнения протокола ZRTP и установления речевого канала в топологии клиент-клиент без

сервера корреспонденты получают значение SAS – вычисленную текстовую строку из комбинации символов.

SAS= f(hash(Hello респондента||Commit||DHPart1||DHPart2).

Один из корреспондентов произносит аутентификационную строку по установившемуся речевому канал. Второй корреспондент сверяет SAS на своем терминале со значением, полученным по речевому каналу. Если SAS совпадают, значит, не имеет место атака MITM, или имеет место атака с подделкой SAS по речевому каналу связи. Если SAS различаются - значит, имеет место атака MITM в канале передачи данных. Таким образом, при соединении двух корреспондентов без участия сервера - аутентификация выполняется за счет знания корреспондентом голоса второго корреспондента, а также за счет неискаженной передачи информации по двум каналам - по речевому каналу SRTP и каналу передачи данных.

Современные технологии достаточно просто позволяют выполнять как анализ голоса корреспондентов, так и синтез речи, в том числе, синтез речи для целей подделки голоса. Рассматриваются два варианта:

1. Корреспонденты знают голос друг друга.
2. Корреспонденты не знают голос друг друга.

В первом случае, при соединении вызывающий корреспондент, как правило, произносит приветствие и имя вызываемой стороны. После этого выполняется вербальная проверка SAS. Собранных голосовых данных может быть достаточно для синтеза речи корреспондента для замены одних слов на другие с целью подмены SAS в голосовом канале. В этом случае - проверка SAS пройдет успешно даже при наличии атаки MITM (Рисунок 3.2).

Во втором случае, когда корреспонденты не знают голоса друг друга, не требуется сбора данных, так как синтез можно выполнять с использованием любого голоса.

В качестве модернизации протокола ZRTP предлагается добавление автоматизированной проверки аутентификационной строки SAS. При

использовании двух и более каналов связи, проверка позволит обнаружить нарушителя.

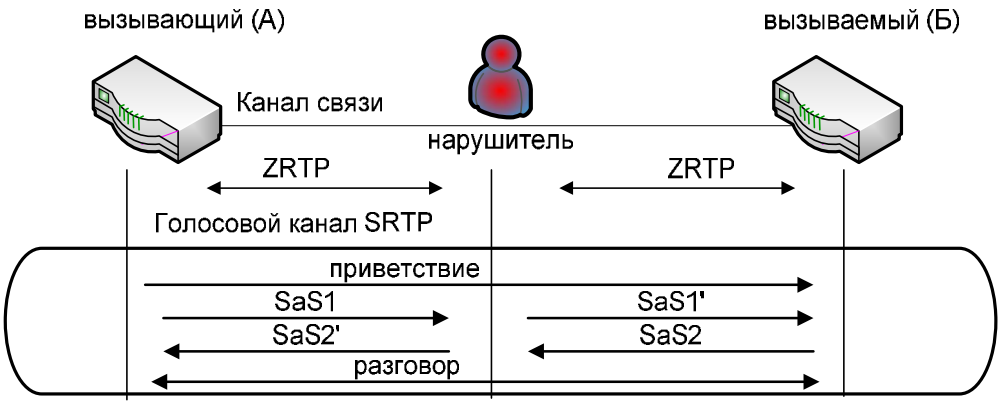


Рисунок 3.2 – Нарушитель, выполняющий замену SAS в голосовом канале связи

Информация об IP-адресах может быть передана между корреспондентами по телефону, по электронной почте, при личной встрече, письмом и другими доступными способами. Отличительной особенностью является то, что информация об IP-адресах не является секретной информацией для нарушителя и может быть передана по открытым каналам связи, в то время, как пароль для симметричного шифрования является секретным и разглашение приведет к возможности нарушителя дешифровать передаваемую информацию. По сравнению с длиной ассиметричного ключа, общая длина двух IPv4 или IPv6 адресов гораздо меньше. При перехвате ассиметричного ключа – нарушитель может отправлять данные легитимному респонденту так же, как и легитимный корреспондент.

При использовании IP-адресов дополнительной мерой для повышения безопасности является проверка IP-адресов отправителя сообщений респондентом, а также возможность получения всех сообщений, отправленных по двум каналам связи, только легитимными респондентами при отсутствии атаки MITM одновременно в нескольких каналах.

Данный метод повышения безопасности ZRTP требует передачи всего одного сообщения от каждого из корреспондентов по дополнительному каналу

связи. В качестве второго канала связи может выступать не обязательно канал передачи данных, но и SMS, MMS транспорт.

Особенностью подхода также является невысокая сложность разработки программной реализации протокола за счет использования существующих библиотек [93, 94]. Значение SAS передается в приложение по результатам выполнения протокола ZRTP. Достаточно дополнительно передать этот параметр корреспонденту по второму каналу связи в открытом или зашифрованном виде для реализации автоматической проверки.

Недостатком метода повышения безопасности в виде автоматизации проверки SAS является обнаружение нарушителя в канале связи непосредственно после успешного выполнения протокола, а не во время выполнения.

Для оценки возможности применения нескольких каналов связи для целей повышения безопасности необходимо решить следующие задачи:

- оценить вероятность наличия общей точки в двух и более каналах связи при использовании разных операторов связи между корреспондентами;
- разработать алгоритм принятия решения о наличии нарушителя и оценка вероятности ошибки возможных решений.

Оценка вероятности выполнена в разделе 3.2.2 текущей главы и показывает высокое значение вероятности наличия двух и более независимых каналов связи между корреспондентами, подключенными к разным операторам связи.

Предлагается использовать следующий алгоритм автоматической проверки SAS. Корреспонденты A и B выполняют предварительный обмен информацией об IP-адресах IP_{A1}, IP_{A2}, IP_{B1}, IP_{B2}, где IP_{A1}, IP_{A2} – адреса корреспондента A, IP_{B1}, IP_{B2} – адреса корреспондента B, а также настраивают таблицу маршрутизации. Для установки защищенного соединения, корреспонденты A и B, выполняют протокол ZRTP через канал связи IP_{A1} - IP_{B1} , в результате чего каждый вычисляет значение SAS (рисунок 3.3). Корреспондент A отправляет SAS_A по каналу связи IP_{A2} - IP_{B2} корреспонденту B. Корреспондент B получает SAS_A'. Корреспондент B

отправляет SAS_B по каналу связи IP_{A2} - IP_{B2} корреспонденту А. Корреспондент А получает SAS_B'.

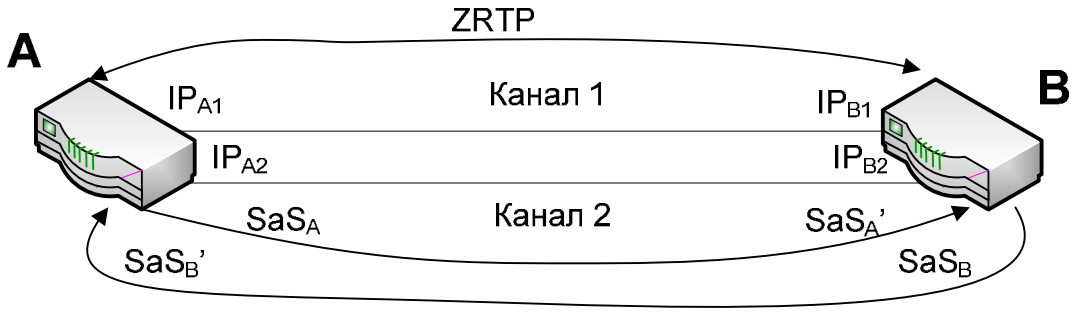


Рисунок 3.3 – Механизм автоматической проверки SAS

Корреспондент В выполняет сравнение SAS_A' и SAS_B. Если они совпадают – значит отсутствует активный нарушитель в двух каналах связи, либо присутствует один и тот же активный нарушитель одновременно в двух каналах связи. Если значения SAS не совпадают, корреспондент В получает уведомление от терминала о наличии нарушителя в канале связи.

Корреспондент А выполняет сравнение SAS_A и SAS_B'. Если они совпадают – значит отсутствует активный нарушитель в двух каналах связи, либо присутствует один и тот же активный нарушитель одновременно в двух каналах связи. Если значения SAS не совпадают, корреспондент А получает уведомление от терминала о наличии нарушителя в канале связи.

Фактически – протокол позволяет выявить наличие активного нарушителя, работающего в одном из двух каналов связи.

Выполняется расчет вероятностей событий: $P_{УА,}$ $P_{ОН,}$ $P_{УК.}$

Под успешной атакой понимается событие, что нарушитель успешно реализовал атаку MITM, выполнив обмен ключами с обоими корреспондентами при использовании нескольких каналов связи, не обнаружив себя при проведении атаки. Это возможно лишь в одном случае, если один и тот же нарушитель может контролировать все используемые корреспондентами каналы связи и выполнять синхронную модификацию передаваемых сообщений в каждом из каналов связи.

Вероятность успешной атаки $P_{УА\_SAS}$ для протокола с автоматической проверкой SAS соответствует вероятности события, что нарушитель может прослушивать и выполнять модификацию сообщений в двух каналах связи одновременно.

$$P_{УА2\_SAS} = (P_{НІК})^2 \quad (3.1)$$

Под событием обнаружения нарушителя определяется событие, что нарушитель обнаружен корреспондентами в одном из используемых каналов связи. Обнаружение нарушителя позволяет пользователям определить, что может быть выработан компрометированный ключ, который позволит нарушителю дешифровать и прослушивать передаваемую информацию, а также выполнять модификацию передаваемых сообщений

Вероятность обнаружения нарушителя $P_{ОН\_SAS}$ для протокола с автоматической проверкой SAS соответствует вероятности нахождения нарушителя в одном канале связи при отсутствии нарушителя в другом канале связи.

Пусть сеанс ZRTP выполняется по первому каналу связи.

Вероятность наличия нарушителя в первом канале связи при отсутствии нарушителя во втором канале связи будет иметь вид:

$$P_{НАР1К\_НЕТ\_НАР2К} = (1 - P_{НІК}) P_{НІК} \quad (3.2)$$

Вероятность наличия нарушителя во втором канале связи при отсутствии нарушителя в первом канале связи будет определяться по аналогии с 3.2.

$$P_{ОН\_SAS} = 2(1 - P_{НІК}) P_{НІК} \quad (3.3)$$

Под событием успешной выработки ключа понимается, что нарушитель не обнаружен ни в одном из каналов связи и корреспонденты вырабатывают ключ для дальнейшей работы и шифрования передаваемых данных. Событие возможно только в случае, если нарушителя нет ни в одном канале связи.

Вероятность успешной выработки ключа $P_{УК\_SAS}$ для протокола с автоматической проверкой SAS соответствует вероятности отсутствия

нарушителя в обоих каналах связи. Вероятность отсутствия нарушителя в одном канале связи $P_{НЕТ\_НАР}$ имеет вид:

$$P_{НЕТ\_НАР}=1- P_{НІК} \quad (3.4)$$

Тогда:

$$P_{УК\_SAS} = P_{НЕТ\_НАР}^2 = (1- P_{НІК})^2 \quad (3.5)$$

Однако, протокол с автоматической проверкой SAS не позволяет определить, какой именно из каналов связи атакует нарушитель. Также наличие нарушителя определяется только в результате полного выполнения протокола и не может быть детерминировано в течении выполнения протокола. По этой причине - следует рассмотреть дополнительные варианты модернизации протокола ZRTP, в том числе варианты, лишенные выше описанных недостатков.

3.2 Метод выявления нарушителя протоколов распределения ключей, основанных на алгоритме Диффи-Хелмана

3.2.1 Структура глобальной сети

Структура глобальной сети детально описана в [95 -96]. Выделяют 4 класса (tier) операторов связи. Каждый оператор и участник глобальной сети имеет свою автономную систему (AS). Под автономной системой понимают систему IP – сетей и маршрутизаторов, управляемых одним оператором и имеющую единую политику маршрутизации с другими автономными системами.

К операторам первого класса (tier-1) относят межконтинентальных операторов связи, формирующих основу глобальной сети. Как правило, эти операторы соединяются друг с другом по принципу каждый с каждым на безвозмездной основе. Кроме этого, они присоединяют к себе операторов второго уровня, но уже на платной основе. Число операторов первого класса 10-15 штук и постоянно меняется. В соответствии с разными источниками [97 - 99] в список операторов первого класса входят компании Verizon, AT&T, Level 3, MCI EMEA, Tata Communications и др. Список компаний приведен в приложении Е.

В соответствии с исследованиями компании The Cooperative Association for Internet Data Analysis [100] также можно выделить список основных провайдеров, формирующих структуру глобальной сети. В приложении Е приведен список самых крупных операторов связи и пример взаимодействия оператора Level 3 с другими операторами как первого, так и более низких классов.

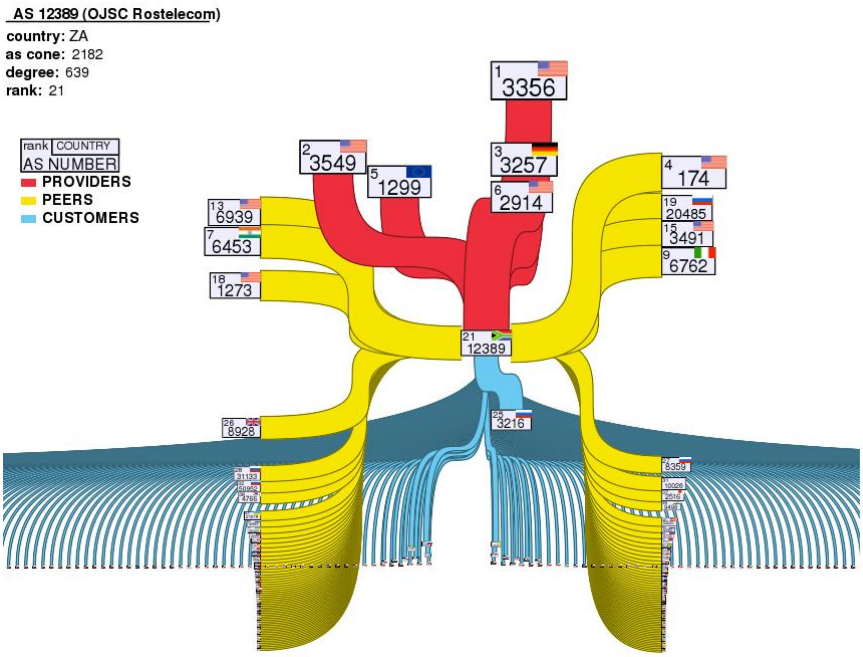
Ко второму классу относятся национальные операторы связи, которые присоединяются к операторам первого класса на платной основе. Как правило, такие операторы имеют несколько точек подключения к операторам первого уровня. Также операторы соединяются с другими операторами второго класса для взаимного обмена трафиком.

Операторы второго класса могут охватывать несколько стран одного континента, а также крупные территории внутри стран. К операторам этого класса в России относят Ростелеком, Транстелеком. На рисунке 3.4 по данным [101] приведена схема взаимодействия Ростелеком (AS 12389) с другими 639 автономными системами.

К операторам третьего класса относятся региональные операторы, присоединяющиеся к операторам второго уровня несколькими подключениями. Как правило – это 3 – 5 точек подключения. Также операторы могут обмениваться трафиком между собой через организованные точки пирринга. К операторам третьего уровня относят: УралСвязьИнформ, ДальСвязь, МТС, Мегафон, Билайн и прочих операторов.

К четвертому классу относят провайдеров услуг, присоединяющихся к операторам второго и третьего класса. Из известных компаний в Петербурге к операторам четвертого класса относятся ИнтерЗет/Z-Телеком, ТКТ, Эртелеком, МТУ-Интел, Комстар (Стрим), Комкор (Акадо) и другие. Взаимодействие оператора четвертого уровня с операторами других уровней на примере провайдера ИнтерЗет приведено в приложении Е.

а)



б)

Рисунок 3.4 – Схема взаимодействия оператора Ростелеком (AS 12389) с другими операторами связи а) на карте б) по странам [101]

Следует отметить, что в случае построения полносвязной сети из существующих автономных систем нельзя определить точный маршрут, по которому пакеты будут передаваться между корреспондентами, подключенными к разным автономным системам. Маршрутизация пакетов в сети любого оператора связи зависит от загрузки каналов связи, возникающих аварий на

оборудовании, а также от действующих дополнительных соглашений между операторами, определяющих ценовую политику и параметры SLA.

Таким образом, возможный маршрут передачи пакета в глобальной сети, а также структура глобальной сети является случайной и выполнить теоретическую оценку числа непересекающихся маршрутов между разными точками не представляется возможным. Для оценки наличия непересекающихся маршрутов необходимо проводить практическую проверку.

3.2.2 Экспериментальная оценка вероятности совпадения маршрутов

Для оценки вероятности совпадения маршрутов при использовании каналов передачи данных от двух разных операторов связи проводится следующий эксперимент [102]. Выбирается несколько стран: США, Россия, Германия, Австралия, Япония, – в каждой из которых также выбирается два города. С использованием базы IP-адресов в каждом из городов подбирается по 3-4 IP-адреса, которые становятся удаленными точками. Для них проводится проверка с использованием сервисов Whois [103] для уточнения, что адрес действительно принадлежит к выбранному городу, и определяется оператор, обслуживающий IP-адрес. Важным условием является обслуживание выбранных удаленных точек различными операторами связи. Также выбираются несколько городов России и несколько IP-адресов в каждом из них. С использованием нескольких точек, подключенных к разным операторам связи, проводится исследование маршрутов на предмет наличия общих узлов (Таблица 3.1). Всего в эксперименте участвовало двенадцать городов из пяти стран мира.

Проверка маршрутов проводилась при подключении к сети интернет с использованием провайдеров Санкт- Петербурга: Петерстар (Мегафон), Interzet, Ростелеком, МТС, Tele2. Для проверки маршрута и составляющих точек маршрута от начальной точки до удаленной точки использовалась команда tracert, показывающая промежуточные узлы - маршрутизаторы, через которые проходит пакет. Команда запускалась отдельно до каждого IP-адреса с использованием

BAT-программы, а результат вывода сохранялся в текстовые файлы статистики. В дальнейшем, полученные исходные данные маршрутов загружались в базу данных для обработки и анализа маршрутов.

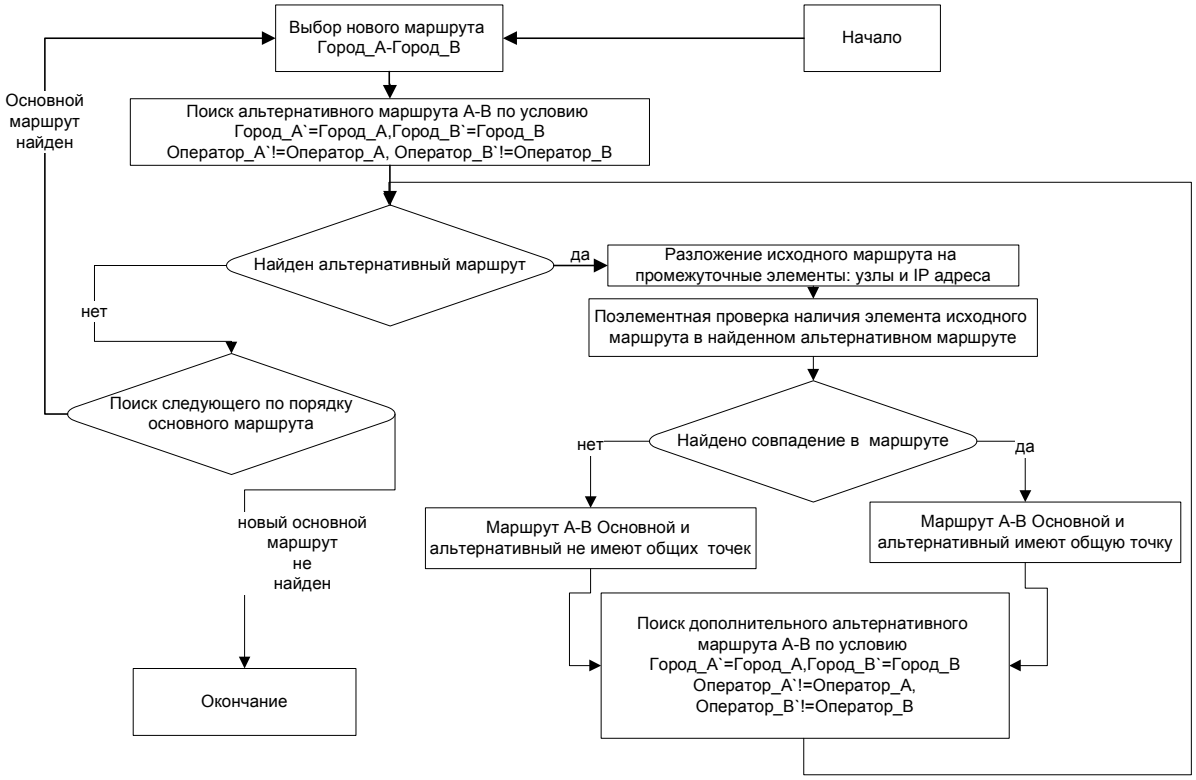
Таблица 3.1 – Страны и города для проверки совпадения маршрутов

Страна	Города
Россия	Москва, Санкт-Петербург, Барнаул, Новосибирск
Австралия	Сидней, Мельбурн
Германия	Берлин, Мюнхен
США	Эддисон, Нью-Йорк, Даллас
Япония	Чийода-Токио, Фокуока

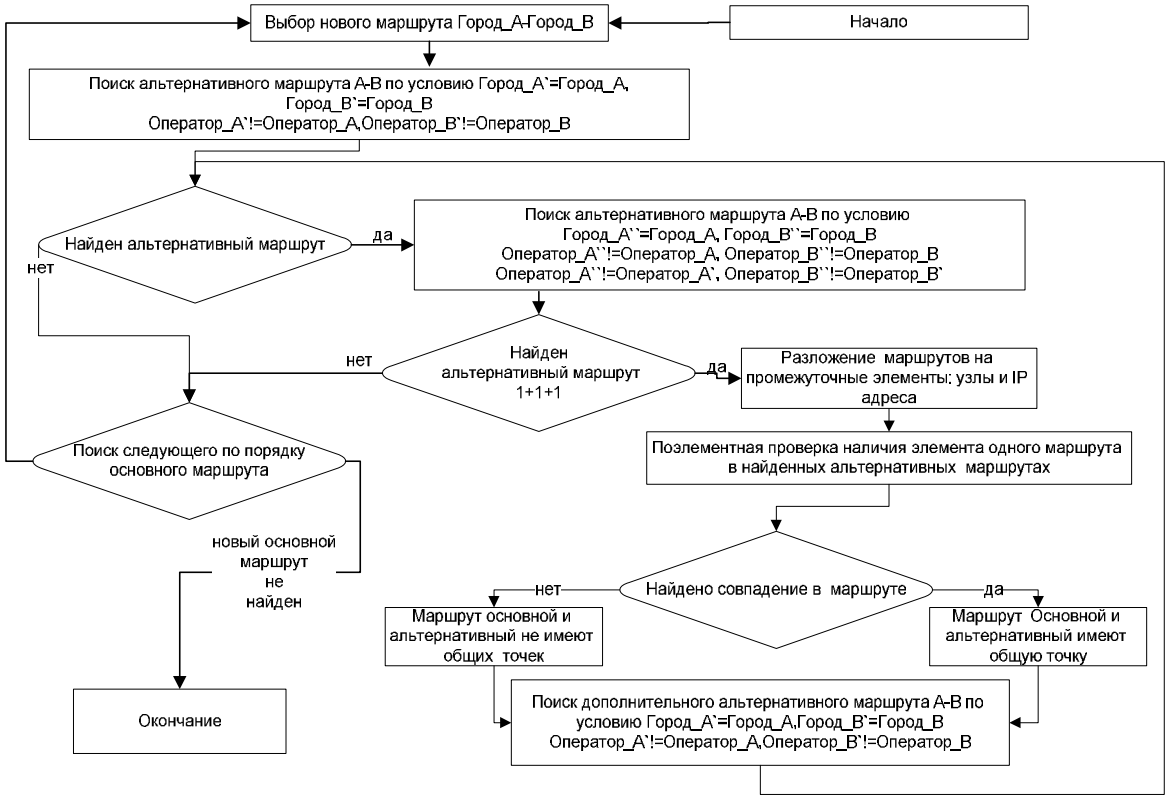
Для целей анализа разработано 2 приложения на языке программирования PHP, выполняющих анализ маршрутов в соответствии с приведенными алгоритмами на рисунке 3.5а и 3.5б.

В результате работы алгоритма по-парного сравнения маршрутов получено число маршрутов и сами маршруты, на которых встречались общие точки. В результате работы алгоритма сравнения троек маршрутов получено число маршрутов без общих точек, а также число с одной и двумя общими точками.

Обнаружено, что общие узлы у некоторых из выбранных операторов существуют на трассе между Санкт-Петербургом и Сиднеем, Мельбурном, Берлином и т.д. Следует отметить, что по этим направлениям число пар маршрутов с общими точками, как правило, гораздо меньше, чем число пар маршрутов без общих точек. Так при общем количестве пар маршрутов Санкт-Петербург-Берлин общие точки были обнаружены у трех пар маршрутов из 60 возможных, что эквивалентно вероятности 0.05 при выбранном числе удаленных точек. По направлениям Мюнхен, Санкт-Петербург, Новосибирск, Москва общих узлов обнаружено не было.



а)



б)

Рисунок 3.5 – Алгоритм поиска маршрутов с совпадающими промежуточными узлами: а) пары маршрутов; б) тройки маршрутов

В таблице 3.2 приведен пример сравнения пары маршрутов между точками Санкт-Петербург – Берлин. Итоговый подсчет маршрутов, полученный в результате работы алгоритма (Рисунок 3.5), приведен в таблице 3.3.

Таблица 3.2 – Пример сравнения пары маршрутов Санкт-Петербург - Берлин

Основной маршрут		Дополнительный маршрут		Наличие общих узлов, названия узлов
Петерстар	SysEleven GmbH	МТС	PROJECT-A-INFRA	Нет
Петерстар	PROJECT-A-INFRA	МТС	SysEleven GmbH	Нет
Interzet	SysEleven GmbH	Петерстар	PROJECT-A-INFRA	Нет
Interzet	PROJECT-A-INFRA	Петерстар	SysEleven GmbH	Нет
Ростелеком	SysEleven GmbH	Tele2	PROJECT-A-INFRA	Нет
Ростелеком	PROJECT-A-INFRA	Tele2	SysEleven GmbH	Нет
Interzet	SysEleven GmbH	МТС	PROJECT-A-INFRA	Есть, bei-b1-link.telia.net, hbg-bb1-link.telia.net, s-bb3-link.telia.net, s-b2-link.telia.net,
Interzet	PROJECT-A-INFRA	МТС	SysEleven GmbH	Есть, bei-b1-link.telia.net, hbg-bb1-link.telia.net, s-bb3-link.telia.net, s-b2-link.telia.net,

Число маршрутов Way_count_i для i-го направления определяется из следующих данных:

$$Way\_count_i = \frac{\prod_{i=0}^{Ipw-1}(N_S - i)\prod_{i=0}^{Ipw-1}(N_D - i)}{Ipw!}, \quad (3.6)$$

где N_S - число независимых точек выполнения трассировки;

N_D - число IP-адресов в удаленной точке маршрута;

Ipw - количество независимых маршрутов, сравниваемых для анализа числа совпадений.

Таблица 3.3 – 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	15,0%
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	81,1%
Россия	Санкт-Петербург	12	1320	1320		0,00%	13200	13200		0,00%
США	Даллас	3	60	51	9	15,00%	60	33	27	45,0%
Япония	Фукуока	3	60	34	26	43,33%	60		60	100%
Япония	Токио - Чийода	7	420	384	36	8,57%	2100	1576	524	24,9%
Всего				2478	122	4,9%		15561	1119	7,2%

Так, например для пар маршрутов получено

$$Way\_count_{Новосибирск} = \frac{5(5-1)3(3-1)}{2!} = 60$$

для Санкт-Петербурга получено

$$Way\_count_{Санкт-Петербург} = \frac{5(5-1)12(12-1)}{2!} = 1320$$

для Берлина для трех маршрутов получено

$$Way\_count_{Берлин} = \frac{5(5-1)(5-2)3(3-1)(3-2)}{3!} = 60$$

Следует отметить, что из общего числа пар маршрутов (2524) только для 113 были найдены совпадения. Таким образом, только 4,4% из всех возможных

маршрутов имели общие точки между собой. В результате практического эксперимента также не было обнаружено ни одного из городов, с которым не было бы хотя бы одной пары маршрута без общих точек. Исходя из этого, можно сделать вывод, что применение двух каналов связи, предоставляемых разными операторами связи, между абонентами позволяет организовать с большой вероятностью два независимых канала связи, не имеющих общей точки.

При заданной вероятности наличия нарушителя в одном из каналов связи, применение двухканального протокола одновременно в обоих каналах позволит снизить вероятность атаки MITM в 22,7 раз.

При использовании трехканального режима – в среднем 7.2% из всех сочетаний троек маршрутов имеют общую точку. Соответственно, в 13 раз уменьшается вероятность какого-либо влияния нарушителя на трехканальный протокол. При наличии одной общей точки в трехканальном режиме – возможно использовать метод выявления нарушителя для уменьшения влияния нарушителя на протокол распределения ключей.

3.2.3 Оценки вероятностей исходов распределения ключей при использовании нескольких каналов связи

Для повышения безопасности предлагается применять метод выявления нарушителя протоколов распределения ключей, основанных на алгоритме Диффи-Хелмана, позволяющий выполнять распределение ключей с использованием нескольких каналов связи одновременно (Рисунок 3.6) и выявлять активного нарушителя.

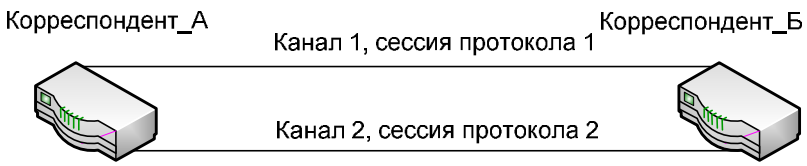


Рисунок 3.6 – Использование несколько каналов связи для распределения ключей

В настоящее время наличие двух и более подключений у одного корреспондента достаточно распространено. Частным случаем может послужить

пользователь, имеющий беспроводное подключение через 3G / 4G модем и одновременно имеющий подключение к сети интернет от оператора проводной широкополосной сети передачи данных.

Пусть существуют два корреспондента, имеющие каждый по два и более подключений в глобальную сеть Интернет. Каждое подключение выполняется через разных операторов связи. Оба корреспондента имеют публичный IP-адрес в каждом используемом канале связи. Каждый из корреспондентов передает другому свои IP-адреса, которые будут использоваться для установления связи между корреспондентами. Данные могут быть переданы в словесной беседе, при встрече, с помощью электронной почты или почтового отправления и т.д., а также с использованием комбинации вышеописанных средств связи.

Реализация работы протокола ZRTP по двум и более каналам связи требует интеграцию многоканального протокола с протоколами SIP / RTP для решения следующих технических задач:

- определение дополнительных IP-адресов, а также UDP портов для выполнения второй сессии протокола, а также передачу этих параметров в сам протокол, класс протокола или функцию протокола;
- реализация проверки полученных сообщений Диффи-Хелмана по разным каналам связи и выполнение дальнейших действий по результатам проверки;
- интеграцию с SIP и RTP протоколом, так как оригинальный ZRTP протокол использует согласованные IP и UDP порты из этих протоколов.

В то же время - реализация одновременного обмена сообщениями ZRTP по двум каналам связи, а также реализация логики проверки совпадающих сообщений может потребовать гораздо больших ресурсов.

Для реализации двухканального метода (2К) повышения безопасности по двум каналам связи будут передаваться одинаковые сообщения обмена Диффи-Хелмана. Инициатор (вызывающий корреспондент, желающий установить

защищенное соединение) отправляет по двум каналам связи два одинаковых сообщения. Респондент получает сообщения, производит необходимые вычисления, а также проверяет, что получены одинаковые сообщения. В случае, если получены разные сообщения – имеет место наличие активного нарушителя в одном из каналов, выполняющего атаку MITM. Респондент отвечает, отправляя по двум каналам связи ответные сообщения Диффи-Хелмана. Инициатор получает сообщения и проверяет – являются ли сообщения одинаковыми. Если сообщения одинаковые – значит, либо отсутствует активный нарушитель в обоих каналах связи, либо существует один и тот же активный нарушитель в обоих каналах связи. Взаимодействие корреспондентов при использовании модификации ZRTP представлена на рисунке 3.7.

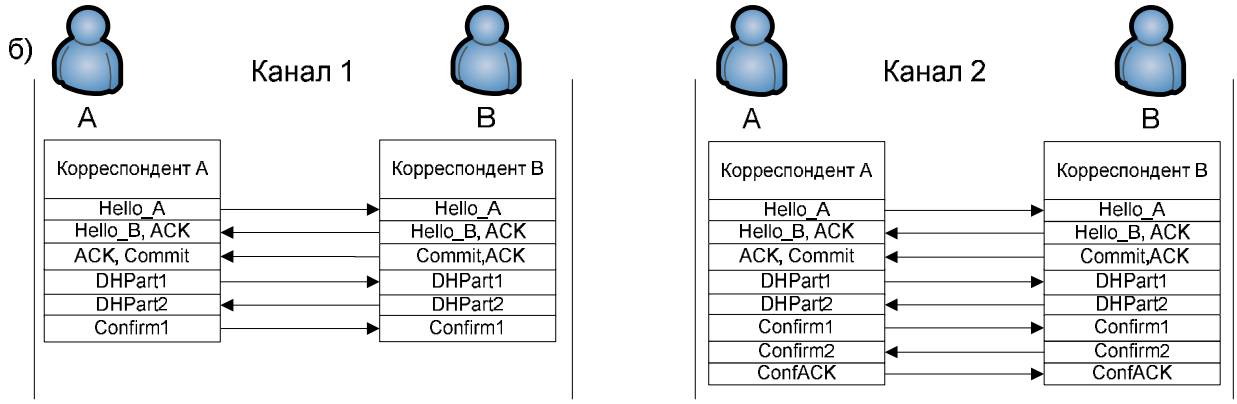


Рисунок 3.7 – Вариант взаимодействия корреспондентов при использовании модернизированного протокола ZRTP в режиме двухканального обмена.

Вводится вероятность $P_{Н1К}$, что нарушитель может выполнять атаку MITM в одном из каналов связи[107]. Эта же вероятность будет соответствовать неудачной попытке выполнения атаки MITM, так как обнаруживается приведенным выше протоколом [108].

Выполняется расчет вероятностей событий: $P_{УА,}$ $P_{ОН,}$ $P_{УК.}$

Под успешной атакой понимается событие, что нарушитель реализовал атаку MITM, выполнив обмен ключами с обоими корреспондентами по нескольким каналам связи. При этом, нарушитель не обнаружил себя при проведении атаки. Это становится возможным лишь в случае, когда один и тот же

нарушитель может контролировать все используемые корреспондентами каналы связи и выполнять синхронную модификацию передаваемых сообщений в каждом из каналов связи.

Вероятность успешной атаки $P_{УА2}$ для двухканального протокола соответствует $P_{Н2К}$ - вероятности события, что нарушитель может прослушивать и выполнять модификацию сообщений в 2 каналах связи одновременно.

$$P_{УА2}= P_{Н2К} = (P_{Н1К})^2 \quad (3.7)$$

Обнаружение нарушителя позволяет пользователям определить, что может быть выработан компрометированный ключ, позволяющий дешифровать и прослушивать передаваемую информацию, а также выполнять модификацию сообщений. Вероятность обнаружения нарушителя зависит от числа используемых каналов связи, а также от способности алгоритма распределения ключей определить существование нарушителя в конкретном или конкретных каналах связи из совокупности используемых.

Вероятность обнаружения нарушителя $P_{ОН2}$ для двухканального метода соответствует вероятности нахождения нарушителя в одном канале связи при отсутствии нарушителя в другом канале связи.

Вероятность наличия нарушителя в первом канале связи при отсутствии нарушителя во втором канале связи будет иметь вид:

$$P_{НАР1К\_НЕТ\_НАР2К}=(1- P_{Н1К}) P_{Н1К} \quad (3.8)$$

Вероятность наличия нарушителя во втором канале связи при отсутствии нарушителя в первом канале связи будет иметь вид:

$$P_{НЕТ\_НАР1К\_НАР2К}=(1- P_{Н1К}) P_{Н1К}= P_{Н1К}- (P_{Н1К})^2 \quad (3.9)$$

$$P_{ОН2}= P_{НАР1К\_НЕТ\_НАР2К} + P_{НЕТ\_НАР1К\_НАР2К=}=2(1- P_{Н1К}) P_{Н1К} \quad (3.10)$$

Под успешной выработкой ключа понимается событие, что нарушитель не обнаружен ни в одном канале связи и корреспондентами выработан ключ для шифрования передаваемых данных. Это возможно только в случае отсутствия нарушителя в применяемых каналах связи, или при использовании способности

алгоритма распределения ключей определять точное нахождение нарушителя в конкретном или конкретных каналах связи из совокупности используемых.

Вероятность успешной выработки ключа $P_{УК2}$ для двухканального протокола соответствует вероятности отсутствия нарушителя в обоих каналах связи. Вероятность отсутствия нарушителя в одном канале связи $P_{НЕТ\_НАР}$:

$$P_{НЕТ\_НАР}=1- P_{Н1К} \quad (3.11)$$

Тогда:

$$P_{УК2}= P_{НЕТ\_НАР}^{2} = (1- P_{Н1К})^{2} \quad (3.12)$$

Рассматривается другой вариант метода выявления нарушителя с использованием трех каналов передачи данных.

Пусть по трем каналам связи передаются одинаковые сообщения обмена Диффи-Хелмана. Пример взаимодействия корреспондентов при использовании модернизированного протокола ZRTP приведен на рисунке 3.8.

Инициатор отправляет по трем каналам связи три одинаковых сообщения. Респондент получает сообщения, производит необходимые вычисления, а также проверяет, что получены одинаковые сообщения по всем трем каналам связи. В случае, если получены разные сообщения, имеет место наличие активного нарушителя, выполняющего атаку MITM, или нарушитель контролирует одновременно все три канала связи.

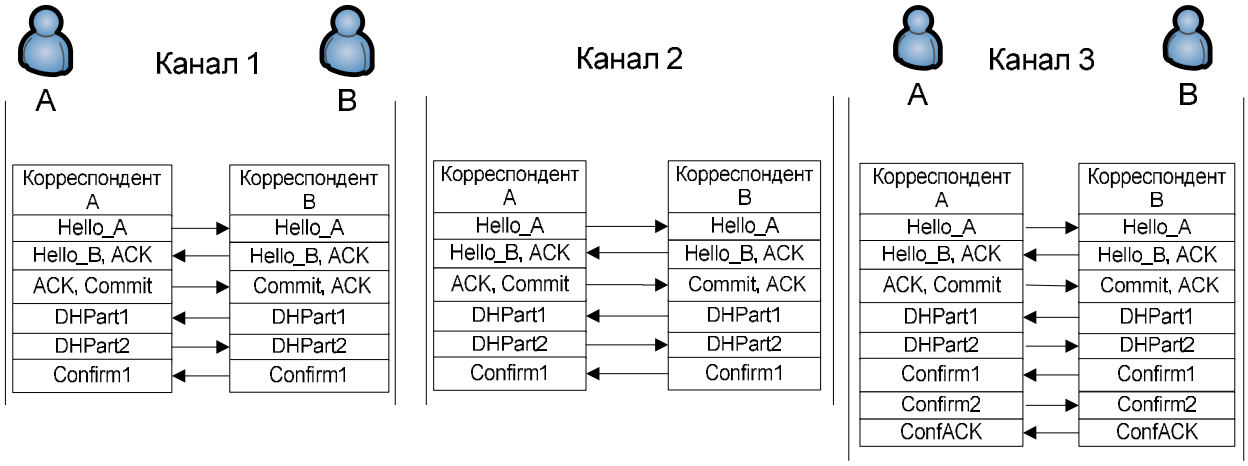


Рисунок 3.8 – Вариант взаимодействия корреспондентов при использовании модернизированного протокола ZRTP при работе одновременно по трем каналам связи.

Респондент отвечает, отправляя по трем каналам связи ответные сообщения Диффи-Хелмана. Инициатор получает сообщения и проверяет – являются ли сообщения одинаковыми.

Возможны несколько вариантов работы протокола при использовании метода выявления нарушителя:

- Если сообщения одинаковые – значит, либо отсутствует активный нарушитель во всех каналах связи, либо существует активный нарушитель во всех трех каналах связи.
- Если одно сообщение отличается от других, значит либо присутствует один активный нарушитель в этом канале связи, либо присутствуют два нарушителя в двух других каналах связи.
- Если все сообщения разные, значит, присутствуют два отдельно работающих нарушителя, не имеющих между собой канала связи.

Таким образом, протокол позволяет:

- при наличии одного нарушителя в одном из трех каналов связи определить канал с нарушителем;
- при наличии нарушителя в двух каналах связи выявить наличие нарушителя, без определения каналов связи, содержащих нарушителя.

Однако, протокол не позволяет при нахождении нарушителя в трех каналах связи определить наличие нарушителя. Соответственно, возможно выделить два режима работы метода повышения безопасности:

- ОН: режим работы с обнаружением нарушителя (3-ОН);
- ИН: режим работы с исключением нарушителя (3-ИН).

При работе в режиме ОН в случае обнаружения отличия хотя бы одного из трех сообщений - протокол завершается с ошибкой, уведомляя пользователя о наличии нарушителя в канале связи.

В случае работы в режиме ИН при обнаружении отличия одного из трех сообщений - формируется уведомление пользователя о наличии нарушителя в конкретном канале связи, при этом протокол продолжает работу и учитывает

сообщения лишь из тех каналов связи, где не обнаружен нарушитель. Так обеспечивается правильное исключение нарушителя. Вероятность правильного исключения нарушителя $P_{ПрИ}$ для трехканального протокола соответствует событию нахождения нарушителя в одном из каналов связи при его отсутствии в двух других каналах.

$$P_{ПрИ} = 3\ P_{Н1К}\ (1- P_{Н1К})^2 \qquad (3.13)$$

Однако, при наличии активного нарушителя одновременно в двух каналах связи из трех возможных, а также синхронной модификации сообщений в двух каналах связи нарушителем, механизм исключения может вызвать некорректное определение канала с нарушителем, что приведет к ошибочному выбору двух каналов, содержащих нарушителя, в качестве надежных. Это позволит нарушителю успешно выполнить обмен ключами с корреспондентами, осуществив успешную атаку MITM.

Вероятность ошибочного исключения соответствует вероятности события, что нарушитель находится одновременно в двух каналах связи.

$$P_{ОшИ} = 3\ P_{Н1К}^2\ (1- P_{Н1К}) \qquad (3.14)$$

Эта вероятность будет также являться составляющей частью вероятности успешной атаки MITM.

Выполняется расчет вероятностей для протокола трехканального обмена в режиме ОН $P_{УА,}\ P_{ОН,}\ P_{УК}$.

Вероятность успешной атаки $P_{УАЗ\_ОН}$ для трехканального протокола в режиме ОН соответствует $P_{Н3К}$ - вероятности события, что нарушитель может прослушивать и выполнять модификацию сообщений в трех каналах связи одновременно.

$$P_{УАЗ\_ОН=}\ P_{Н3К} = (P_{Н1К})^3 \qquad (3.15)$$

Вероятность обнаружения нарушителя $P_{ОНЗ\_ОН}$ для трехканального протокола в режиме ОН соответствует вероятности нахождения нарушителя в одном или двух каналах связи при отсутствии нарушителя в другом канале связи.

Вероятность наличия нарушителя в одном из каналов связи при отсутствии нарушителя в двух других каналах связи будет иметь вид:

$$P_{НАР1К\_НЕТ\_НАР23К}=3(1- P_{Н1К})^2 P_{Н1К} \quad (3.16)$$

Вероятность наличия нарушителя в двух из трех каналов связи при отсутствии нарушителя в одном из каналов связи будет иметь вид:

$$P_{НЕТ\_НАР1К\_НАР23К}=3(1- P_{Н1К}) P_{Н1К}^2 \quad (3.17)$$

$$P_{ОНЗ\_ОН} = P_{НАР1К\_НЕТ\_НАР23К} + P_{НЕТ\_НАР1К\_НАР23К} =$$

$$=3(1- P_{Н1К})^2 P_{Н1К} + 3(1- P_{Н1К}) P_{Н1К}^2 \quad (3.18)$$

Вероятность успешной выработки ключа $P_{УКЗ\_ОН}$ для трехканального протокола в режиме ОН соответствует вероятности отсутствия нарушителя в трех каналах связи:

$$P_{УКЗ\_ОН}= P_{НЕТ\_НАР}^3 = (1- P_{Н1К})^3 \quad (3.19)$$

Выполняется расчет вероятностей $P_{УА,}$ $P_{ОН,}$ $P_{УК}$ для протокола трехканального обмена в режиме ИН.Вероятность успешной атаки $P_{УАЗ\_ИН}$ для трехканального протокола соответствует вероятности события, что нарушитель может прослушивать и выполнять модификацию сообщений в двух или трех каналах связи одновременно.

$$P_{УАЗ\_ИН}= (P_{Н1К})^3 +3(1- P_{Н1К}) P_{Н1К}^2 \quad (3.21)$$

Вероятность обнаружения нарушителя $P_{ОНЗ\_ИН}$ для трехканального протокола в режиме ИН соответствует вероятности нахождения нарушителя в одном канале связи при отсутствии нарушителя в двух других каналах связи и будет иметь вид:

$$P_{ОНЗ\_ИН} = 3(1- P_{Н1К})^2 P_{Н1К} \quad (3.22)$$

Вероятность успешной выработки ключа $P_{УКЗ\_ИН}$ для трехканального протокола в режиме ИН соответствует вероятности отсутствия нарушителя в двух или трех каналах связи:

$$P_{УКЗ\_ИН}=(1- P_{Н1К})^3 + 3(1- P_{Н1К})^2 P_{Н1К} \quad (3.22)$$

Для сравнения, для простого протокола Диффи-Хелмана, работающего по одному каналу, вероятности будут иметь вид:

$P_{УА1} = P_{Н1К}$

$P_{ОН2} = 0$

$P_{УК} = 1 - P_{Н1К}$

Полученные зависимости для вероятностей представлены на рисунках 3.9а-3.9в.

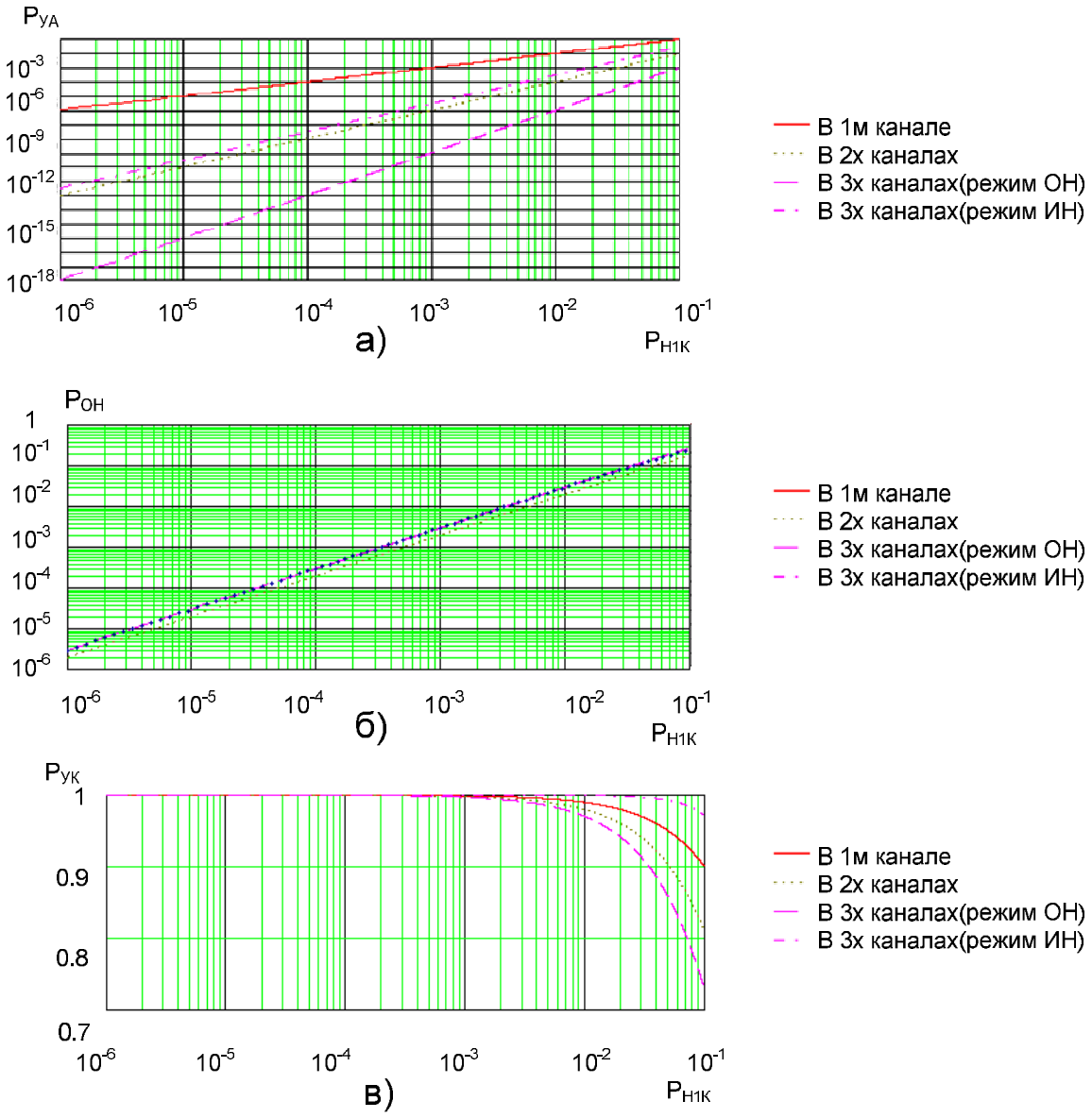


Рисунок 3.9 – Сравнительные характеристики ПРК в четырех режимах: а) вероятность успешной атаки MITM б) вероятность обнаружения нарушителя в) вероятность успешной выработки ключа

Модификация протокола для работы по нескольким независимым каналам существенно уменьшает вероятность успешной атаки MITM. Эффективность защиты возрастает с увеличением числа независимых каналов. Модификация в режиме обнаружения нарушителя с использованием трех каналов связи имеет наибольшую вероятность обнаружения нарушителя, а также наименьшую вероятность успешной атаки нарушителя. Модификация в режиме исключения нарушителя с применением трех каналов имеет наибольшую вероятность успешной выработки общего секрета между корреспондентами. Для реализации выбирается одна из модификаций в зависимости от целей и доступных ресурсов, выраженных в числе доступных каналов связи.

Исследования показывают, что при подключении корреспондентов к нескольким операторам связи независимые двойки и тройки маршрутов имеются всегда. Вероятность успешного формирования общего ключа в многоканальной схеме с обнаружением нарушителя уменьшается незначительно. В схеме с исключением нарушителя данная вероятность увеличивается, но при использовании трасс большой протяженности возможно совпадение узлов прохождения маршрутов, что может снизить эффективность работы модифицированного протокола.

Выводы по главе 3

Предложен метод выявления нарушителя протоколов распределения ключей, основанных на алгоритме Диффи-Хелмана, заключающийся в использовании нескольких открытых каналов связи и опубликованный в [108]. Метод отличается от существующих пониженной вероятностью успешной атаки MITM, а также наличием механизма определения активного нарушителя в канале связи даже при отсутствии заранее распределенного общего секрета. Однако, данный метод накладывает ограничения на используемые каналы связи, выраженное в том, что каналы связи должны быть независимые.

Разработана методика оценки вероятности совпадения маршрутов в глобальной сети. Методика позволяет количественно оценить вероятность

существования общих точек у пар и троек имеющихся маршрутов. Показано, что вероятность наличия двух независимых каналов связи достаточно велика, но ее значение уменьшается при увеличении расстояния между точками подключения.

Предложен метод повышения безопасности ПРК, отличающийся от существующего метода вербальной проверки SAS автоматизацией процесса обнаружения нарушителя, не требующей участия пользователей.

Глава 4. Исследование вероятностно-временных характеристик протоколов IP-телефонии

4.1 Методика оценки вероятностно-временных характеристик протоколов распределения ключей защищенной IP-телефонии

Обзор протоколов безопасности VoIP, выполненный в Приложении В, показывает, что практически любой протокол можно представить в виде совокупности сообщений и совокупности фаз, направленных для выполнения конечной цели протокола. Выделяются два возможных варианта завершения протокола - успешное завершение и неуспешное завершение.

Успешным называется такое завершение протокола, при котором достигается цель инициализации протокола. Например - для протоколов распределения ключей IP-телефонии успешным считается завершение, если корреспонденты в результате выполнения протокола получили ключевой материал для работы SRTP. Неуспешным называется завершение протокола, при котором не достигается конечная цель протокола. Применительно к ПРК IP-телефонии - неуспешным считается завершение, если корреспонденты не согласовали ключи для работы SRTP.

Как правило, любой протокол можно разделить на логические части – фазы. Фазы различных протоколов можно описать с использованием примитивов. Следует заметить, что для многих протоколов безопасности IP-телефонии предусмотрена повторная передача сообщений в тех случаях, когда сообщение не доставлено до респондента, или не получено ответное подтверждающее прием сообщение. Данную особенность необходимо учитывать при оценке вероятностно-временных характеристик [109].

При анализе протокола имеет смысл оценивать такие вероятностно-временные характеристики (ВВХ) [110], как среднее время выполнения протокола

и вероятность успешного завершения [111, 112]. Данные характеристики оцениваются при заданных начальных условиях, при которых выполняется протокол.

Для анализа ВВХ полагается, что сообщения протокола передаются в дискретном канале без памяти (ДКБП), параметром которого является скорость c, вероятность бытовой ошибки p_0, а также задержка d. Для количественной оценки ВВХ характеристик протоколов предлагается использовать метод вероятных графов [113 - 115].

Суть метода состоит в том, что любой процесс с конечным числом состояний можно описать вероятностным графом, ветви которого характеризуются производящими функциями (ПФ), аргументом которых является p_{ij} – вероятность перехода из i-й в j-ую вершину, а время t – параметром, определяющим процесс.

Рассматривается простой процесс передачи сообщения от одного корреспондента к другому. Пусть n – длина пакета в битах. Тогда вероятность успешной передачи пакета $p_{pkt\_success}$, будет иметь вид:

$$p_{pkt\_success} = (1-p_0)^n \tag{4.2}$$

Вероятность, что пакет из n бит передан с ошибкой, будет иметь вид:

$$p_{pkt\_loss} = 1-(1-p_0)^n \tag{4.3}$$

Приведенный выше процесс описывается вероятностным графом, представленным на рисунке 4.1, где f_1, f_2 – производящие функции ветвей.

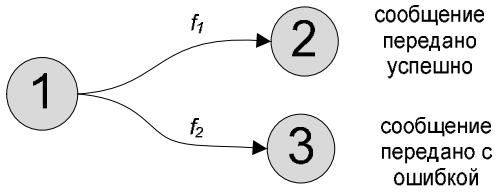


Рисунок 4.1 – Граф передачи сообщения от одного корреспондента к другому

Пусть t – время передачи пакета по каналу связи. Оно определяется формулой 4.4:

$$t = \frac{n}{c} + d \quad , \tag{4.4}$$

где c – скорость канала связи, бит/с;

d – задержка в канале связи, с.

ПФ для ветви 1-2 будет иметь вид:

$$f_1(x) = (1 - p_0)^n x^{n/c+d} \tag{4.5}$$

ПФ для ветви 1-3:

$$f_2(x) = (1 - (1 - p_0)^n) x^{n/c+d} \tag{4.6}$$

Производящая функция далее применяется для расчета $T_{ср}$ - среднего времени выполнения протокола:

$$T_{ср} = \frac{df_1(x)}{dx}(x = 1) \tag{4.7}$$

ПФ также используется для расчета вероятности успешного завершения, которая определяется, как значение производящей функции в точке $x=1$:

$$P = f_1(x = 1) \tag{4.8}$$

4.1.1 ВВХ примитивных протоколов

Следует рассмотреть методику для таких примитивных протоколов, как “протокол с бесконечной повторной передачей сообщений неограниченное число раз”, “протокол с повторной передачей сообщений ограниченное число раз”, а также “протокол с повторной передачей сообщений ограниченное число раз с переменным временем задержки между повторами”.

Рассматривается применение методики на примитивном протоколе с бесконечной повторной передачей сообщений неограниченное число раз, задачей которого является передача одного сообщения длинной n от корреспондента к респонденту, и выполнение повторной отправки сообщения в случае, если сообщение доставлено не было.

Граф, описывающий протокол при неограниченном числе передач одного сообщения, приведен на рисунке 4.2.

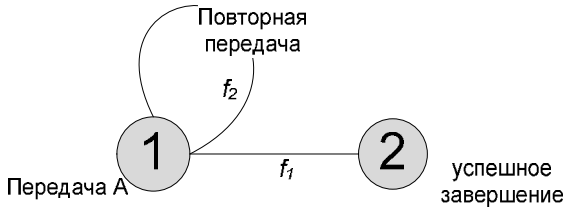


Рисунок 4.2 – Граф, описывающий протокол при бесконечном числе повторов

Производящая функция такого вероятностного графа в общем случае имеет вид:

$$f(x)=\sum_{i=0}^{v} p_i x^{t_i} \tag{4.9}$$

где p_i - вероятность перехода из первого состояния во второе;

t_i- время, необходимое для этого перехода;

v - число повторных передач сообщения.

Производящая функция далее применяется для расчета среднего времени выполнения протокола:

$$T_{cp}=\frac{df(x)}{dx}(x=1) \tag{4.10}$$

Также ПФ используется для вычисления вероятности успешного завершения, определяемой, как значение производящей функции в точке *x=1*

$$P = f(x=1) \tag{4.11}$$

Так как исследуемый протокол имеет всего два состояния – начала и завершения, показанных на графе на рисунке 4.2, то протокол всегда будет заканчиваться успешно.

Представленный выше протокол усложняется введением дополнительного параметра – времени ожидания перед повторной передачей сообщения. Тогда при расчете времени перехода от одной вершины графа к другой необходимо учитывать как время передачи сообщения протокола в канале связи, так и задержки, вызванные ожиданием перед повторной передачей, которые так же могут зависеть от номера итерации. Тогда:

$$f_1 = p_1 x^{a1}$$

$$f_2 = p_2 x^{a2} \qquad (4.12)$$

где p_1 - вероятность успешного приема сообщения респондентом;

a_1 - время передачи сообщения, с;

p_2 - вероятность неуспешного приема сообщения респондентом;

a_2 - время ожидания перед повторной передачей сообщения, одинаковое для всех повторов, с.

Производящая функция графа f_{12p} будет иметь вид:

$$f_{12p} = p_1 x^{a1} + p_1 x^{a1} p_2 x^{a2} + ... + p_1 x^{a1} (p_2 x^{a2})^i + ... = f_1 + f_1 f_2 + ... + f_1 f_2^i + ... = \frac{f_1}{1 - f_2} \qquad (4.13)$$

Дополнительно вводится усложнение начального протокола, выраженное в ограничении k числа повторов сообщений, приводящих к успешному завершению. В этом случае, в протоколе с конечным числом повторных передач появляется третье состояние неуспешного завершения (Рис 4.3).

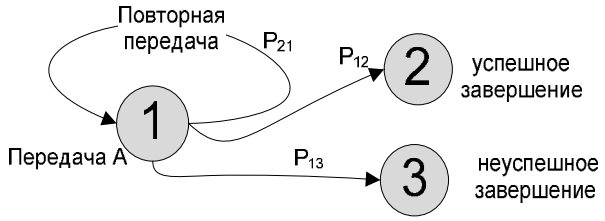


Рисунок 4.3 – Граф первого этапа первой фазы при конечном числе повторов

Упрощение графа [116,117] приведено на рисунке 4.4. Производящая функция f_{12k}, учитывающая конечное число повторов, равное k, и соответствующая ветви успешного завершения будет иметь вид:

$$f_{12k}(x) = p_1 x^{a1} + p_1 x^{a1} p_2 x^{a2} + ... + p_1 x^{a1} (p_2 x^{a2})^k \qquad (4.14)$$

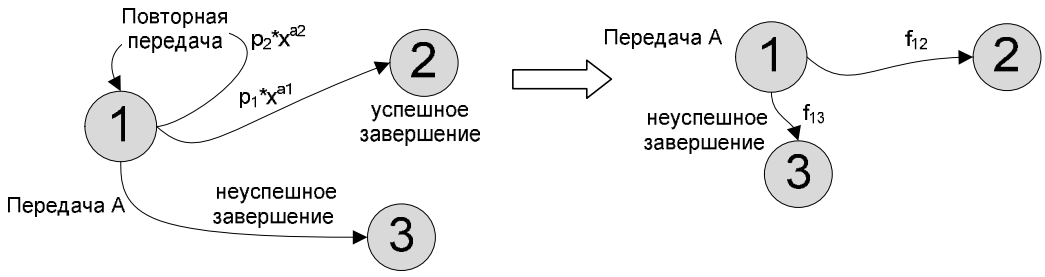


Рисунок 4.4 – Граф протокола повторных сообщений
при конечном *k*-числе повторов

В случае с одинаковым временем задержки повтора производящая функция f_{12k}, соответствующая успешному завершению, будет иметь вид:

$$f_{12k} = px^{a1}\sum_{i=0}^{k}(p_2x^{a2})^i \tag{4.15}$$

Сумма $k+1$ -первых членов может быть также определена, как:

$$f_{12k} = \frac{f_1(f_2^{k+1}-1)}{(f_2-1)}. \tag{4.16}$$

Производящая функция $f_{13\text{к}}$ перехода из точки 1 в точку 3, соответствующая ветви неуспешного завершения, имеет вид:

$$f_{13k} = p_1x^{a1}(p_2x^{a2})^{k+1}+...+p_1x^{a1}(p_2x^{a2})^i+....=p_1x^{a1}(p_2x^{a2})^{k+1}(1+...+1(p_2x^{a2})^{i-(k+1)}+.....)=$$
$$=p_1x^{a1}\frac{(p_2x^{a2})^{k+1}}{1-p_2x^{a2}}=\frac{f_2^{k+1}\cdot f_1}{(1-f_2)} \tag{4.17}$$

Тогда среднее время перехода из точки 1 в точку 2

$$T_{CP} = \frac{df_{12k}}{dx}(x=1) \tag{4.18}$$

Введено допущение, что времена ожидания при повторе сообщения a_{2i} будут разными. Эта особенность характерна для протокола с повторной передачей сообщений k число раз с переменным временем задержки между повторами. Тогда ПФ будет иметь вид:

$$f_{12k} = p_1x^{a1}+p_1x^{a1}p_2x^{a21}+...+p_1x^{a1}(p_2x^{a2\bullet k})^k+p_1x^{a1}(p_2x^{a2(k+1)})^{k+1}...p_1x^{a1}(p_2x^{a2(k+i)})^{k+i}$$
$$\frac{(p_2x^{a22})^2}{p_2x^{a21}}=p_2\frac{(x^{a22})^2}{x^{a21}}$$

$$\frac{(p_2 x^{a23})^3}{(p_2 x^{a22})^2} = p_2 \frac{(x^{a23})^3}{(x^{a22})^2}$$

$$\frac{(x^{a22})^2}{x^{a21}} = \frac{(x^{a23})^3}{(x^{a22})^2} \Rightarrow (x^{a22})^4 = x^{a21}(x^{a23})^3 \quad (4.19)$$

Из 4.19 следует, что при разном времени последовательность не является геометрической прогрессией и к ней не может быть применена ранее приведенная формула (4.16) и производящая функция f_{12k} ветви успешного завершения будет иметь вид:

$$f_{12k} = p_1 x^{a1}(1 + p_2 x^{a21} + (p_2)^2 x^{a21+a22} + ... + (p_2)^k x^{a21+a22+..+a2k}) \quad (4.20)$$

Выполнена оценка протокола с конечным k-числом повторных передач с переменной задержкой a_{2i} между повторами, когда a_{2i} удовлетворяет следующему условию:

a_{21} .. $a_{2(m-1)}$ – имеют разное значение;

a_{2m}...a_{2k} – имеют одинаковое значение.

Тогда ПФ f_{12v} будет иметь вид:

$$f_{12v} = p_1 x^{a1} + p_1 x^{a1} p_2 x^{a21} + p_1 x^{a1} (p_2)^2 x^{a21+a22} + .. p_1 x^{a1} (p_2)^k x^{a21+..+a2k}$$

$$f_{12v} = p_1 x^{a1} + p_1 x^{a1} p_2 x^{a21} + p_1 x^{a1} (p_2)^2 x^{a21+a22} + .. + p_1 x^{a1} (p_2)^{m-1} x^{a21+..+a2(m-1)} +$$
$$+ p_1 x^{a1} (p_2)^m x^{a21+..+a2m} + p_1 x^{a1} (p_2)^{m+1} x^{a21+..+a2m+a2m} + .. + p_1 x^{a1} (p_2)^k x^{a21+..+a2(m-1)+(k-m)a2m}$$

$$f_{12v} = \sum_{i=0}^{m-1} (p_1 x^{a1} {p_2}^i \prod_{j=1}^{i} (x^{a2j})) + p_1 x^{a1} (\frac{(p_2 x^{a2m})^{k-m+1} - 1}{p_2 x^{a2m} - 1}) \prod_{j=1}^{m-1} (x^{a2j}) {p_2}^m x^{a2m} \quad (4.21)$$

4.2 Исследование ВВХ DTLS

4.2.1 Анализ параметров протокола DTLS, определяющие вероятностно- временные характеристики

DTLS – один из протоколов обмена ключевым материалом между корреспондентами в IP-телефонии. DTLS [118] является адаптацией другого протокола обеспечения безопасности – TLS. В отличии от предшественника, DTLS адоптирован для работы по сети с негарантированной доставкой

сообщений с использованием протокола UDP. Главной задачей DTLS протокола является согласование между корреспондентами главного секретного ключа, применяемого впоследствии для SRTP протокола. Описание протокола приведено в приложении Д.

В общем виде – схема обмена сообщениями протокола DTLS для генерации ключей SRTP представлена на рисунке 4.5.

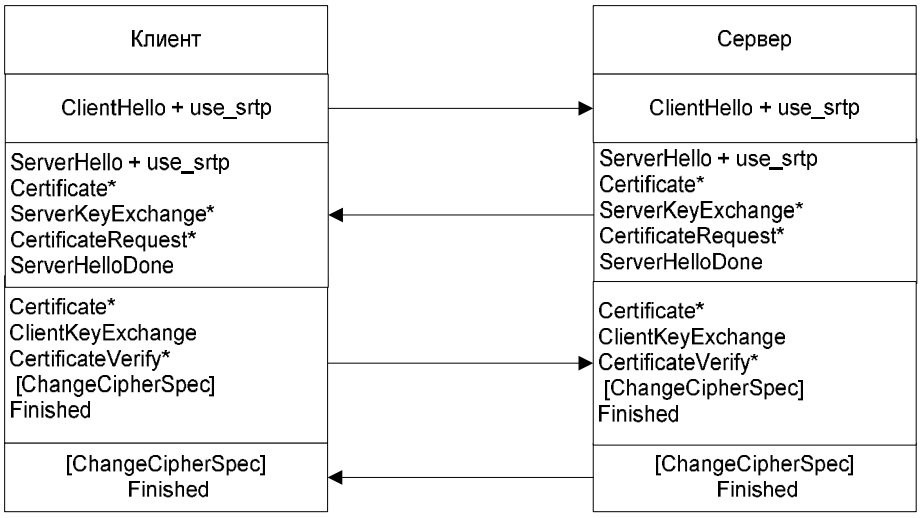


Рисунок 4.5 – Обмен сообщениями по протоколу DTLS

При расчете вероятностно-временных характеристик протокола DTLS следует учесть особенность повторной передачи сообщений. Согласно [118], значения таймеров повторной передачи сообщения выбираются реализацией протокола, несогласованность таймеров может привести к возникновению очередей сообщений. Начальное значение таймера повторной передачи рекомендуется установить в 1 секунду (минимальное значение, определенное в [119]), и удваивать значение таймера каждый раз до достижения значения в 60 секунд. Значение таймера обнуляется каждый раз, как имеет место успешная передача сообщения.

После долгого периода бездействия, например, после осуществленной передачи данных, значение таймера может быть сброшено на начальное значение.

Протокол DTLS не регламентирует ограничение по числу повторов. В соответствии с рекомендацией RFC 6298 значения таймера повторной передачи

сообщения должно изменяться в диапазоне от одной секунды до шести десяти секунд. Таймер будет принимать значения: 1 с., 2 с., 4 с., 8 с., 16 с., 32 с., 60с. Значения таймера обеспечивают семь повторов. При передаче – несколько сообщений протокола, как правило, группируются в комплексные сообщения.

В соответствии с вышеописанным, при расчете ВВХ протокола вводятся следующие допущения:

- Повторные сообщения отправляет только клиент, не получивший следующего по сценарию сообщения в течении времени, равного текущему значению таймера повторной передачи.
- При передаче одного сообщения максимальное число повторов составляет семь, после чего протокол завершает работу.

Протокол DTLS может работать в разных режима, в зависимости от которых может меняться длина передаваемых сообщений. Расчет выполняется для режима Диффи-Хелмана с аутентификацией, в котором участвуют все сообщения. Список сообщений, а также их длины, приведены в приложении Д.

4.2.2 Оценка и расчет ВВХ протокола DTLS

Для составления вероятностного графа учитываются описанные ранее особенности этого ПРК и вводятся следующие переменные:

NH – размер сообщений Client Hello + Hello Verify Request, бит;

NC – размер сообщения Client Hello with COOKIE, бит;

ND – размер сообщений Server Hello, Certificate, Server Hello Done, бит;

NF – размер сообщений Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message, бит;

NK – размер сообщений Change Cipher Spec, Encrypted Handshake Message, бит;

H_{XX} – производящая функция ветви, где *xx* – обозначение соответствующей ветви.

Вероятностный граф всего протокола DTLS, приведен на рисунке 4.6.

Выполняется упрощение графа. Производящая функция ветви успешного завершения $H\_success$ будет иметь вид:

$$H\_success = H_{AS} \cdot H_{BS} \cdot H_{QS}, \tag{4.22}$$

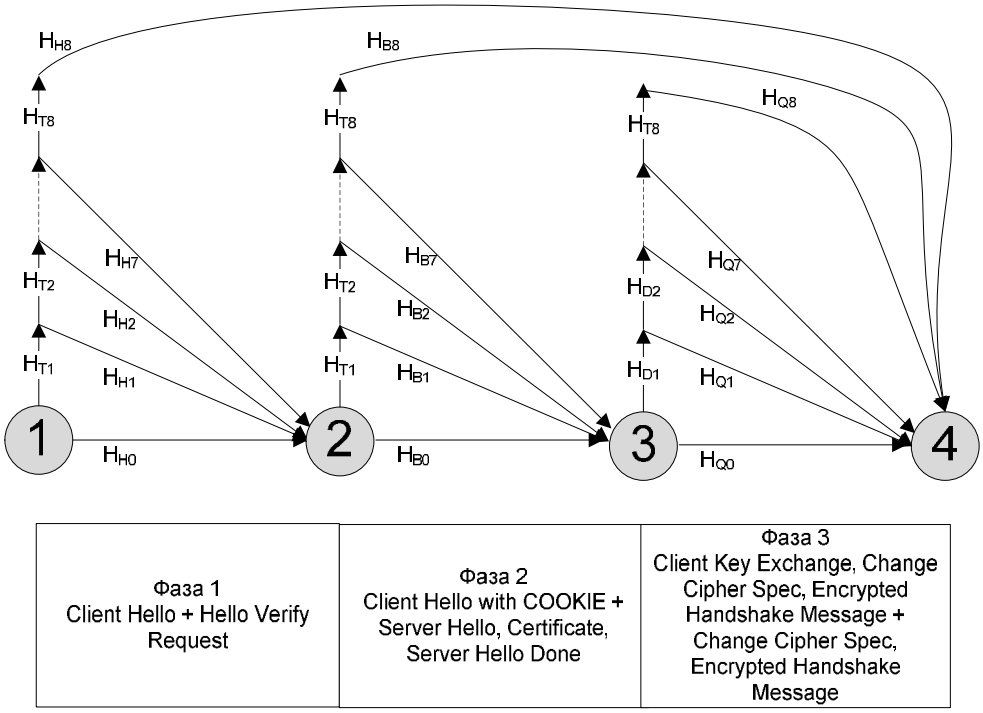


Рисунок 4.6 – Вероятностный граф протокола DTLS

где $H_{AS} = (\sum_{y=0}^{6}(H_A(y) \cdot \prod_{i=1}^{y} H_T(i))) + H_{A\_ост.} \prod_{i=0}^{7} H_T$ (4.23)

$$T_{Hi}(i) = \begin{cases} 0, \text{ при } i = 0 \\ 1, \text{ при } i = 1 \\ 2, \text{ при } i = 2 \\ 4, \text{ при } i = 3 \\ 8, \text{ при } i = 4 \\ 16, \text{ при } i = 5 \\ 32, \text{ при } i = 6 \\ 60, \text{ при } i \geq 7 \end{cases} \tag{4.24}$$

$$H_A(y) = [1 - p_0]^{NH} \cdot x^{\frac{NH}{c}+2d} \cdot ((1-(1-p_0)^{NH}) x^{T_{Hi}})^y \tag{4.25}$$

$$H_{A\_ост.} = 1 - (\sum_{r=0}^{6}((1-p_0)^{NH}) \cdot (1-(1-p_0)^{NH})^r) \tag{4.26}$$

$$H_T(i)=x^{T_{Hi}(i)} \tag{4.27}$$

Производящие функции H_{BS}, H_{QS} определяются по аналогии с производящей функцией H_{AS}:

$$H_{BS}=(\sum_{y=0}^{6}(H_B\cdot\prod_{i=1}^{y}H_T))+H_{B\_ост.}\prod_{i=0}^{7}H_T \tag{4.28}$$

$$H_B=\left[1-p_0\right]^{NC+ND}\cdot x^{\frac{NC+ND}{c}+2d}\cdot((1-(1-p_0)^{NC+ND})x^{T_{Hi}})^y \tag{4.29}$$

$$H_{B\_ост.}=1-(\sum_{y=0}^{6}((1-p_0)^{NC+ND})\cdot(1-(1-p_0)^{NC+ND})^y) \tag{4.30}$$

$$H_{QS}=(\sum_{y=0}^{6}(H_Q\cdot\prod_{i=1}^{y}H_T))+H_{Q\_ост.}\prod_{i=0}^{7}H_T \tag{4.31}$$

$$H_Q=\left[1-p_0\right]^{NF+NK}\cdot x^{\frac{NF+NK}{c}+2d}\cdot((1-(1-p_0)^{NF+NK})x^{T_{Hi}})^y \tag{4.32}$$

$$H_{Q\_ост.}=1-(\sum_{y=0}^{6}((1-p_0)^{NF+NK})\cdot(1-(1-p_0)^{NF+NK})^y) \tag{4.33}$$

Среднее время завершения протокола DTLS, а также вероятность успешного завершения, определяется по методике, описанной ранее.

$$T_{ср}=\frac{dH\_success}{dx}(x=1) \tag{4.34}$$

$$P=H\_success(x=1) \tag{4.35}$$

Полученные зависимости представлены на рисунках 4.7, 4.8.

Очевидно, что в каналах хорошего качества ($p_o < 10^{-5}$) время успешного выполнения протокола существенно зависит от величины задержки сообщений в канале связи и практически не зависит от вероятности ошибки. При этом в каналах с задержкой более 150 мс время выполнения протокола DTLS становится соизмеримым с величинами, определяющими полное время установления соединений в сетях телефонной связи общего пользования.

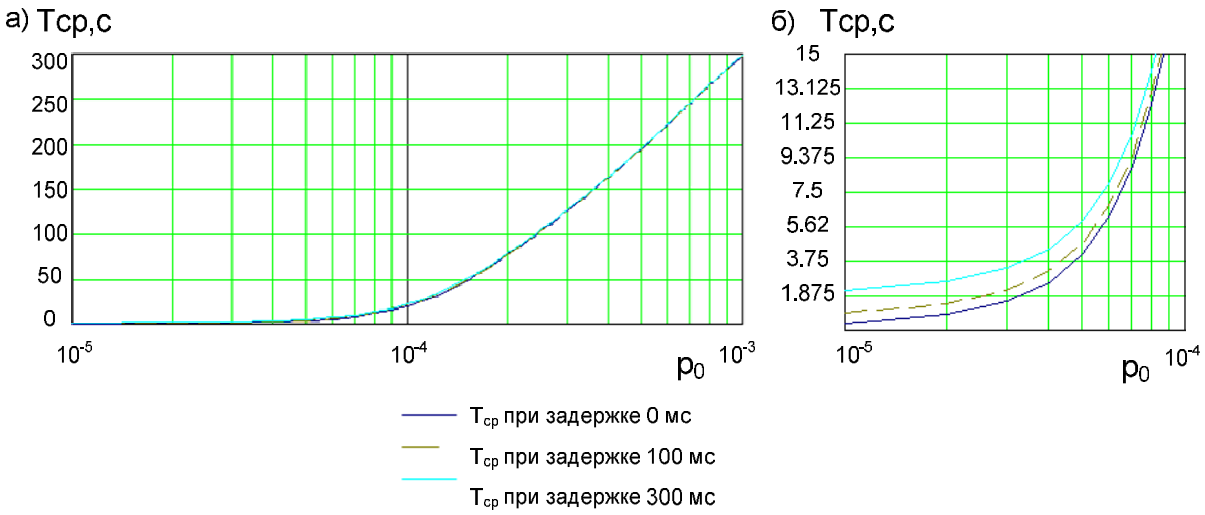


Рисунок 4.7 – Среднее время успешного завершения протокола DTLS от p_0

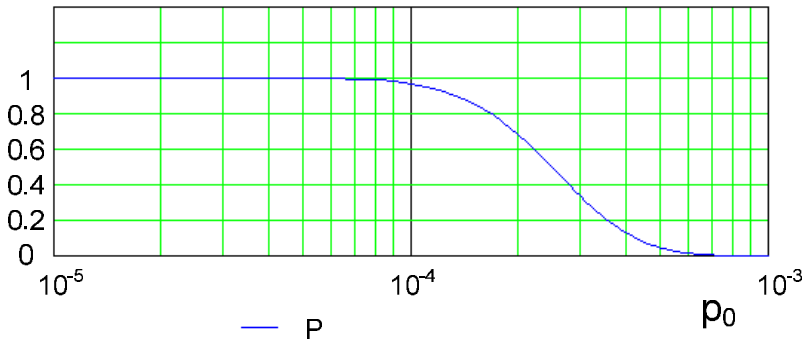


Рисунок 4.8 – Зависимость вероятности успешного завершения протокола DTLS от p_0 при $10^{-5} \le p_0 \le 10^{-3}$

С ухудшением качества канала при $p_o \geq 10^{-5}$ среднее время выполнения протокола резко возрастает, а зависимость от задержки пакетов в канале связи нивелируется.

4.3 Исследование ВВХ ZRTP

4.3.1 Анализ параметров протокола ZRTP, определяющих вероятностно- временные характеристики

Протокол ZRTP описан в приложении Г. В основу протокола ZRTP положен алгоритм Диффи-Хелмана [120].

Протокол выполняется последовательно в четыре фазы: обнаружение, подтверждение, вычисление ключей и завершение.

Корреспонденты отправляют друг другу сообщения *Hello* на первой фазе протокола. Они содержат данные о поддерживаемых криптографических наборах для определения возможности применения SRTP: алгоритмы хеширования, алгоритмы шифрования, типы аутентификационных тегов, протоколы согласования ключей, типы SAS. Также передается информация о версии ZRTP, набор флагов и параметров для различных операций. Протоколом определяется повторная отправка сообщения *Hello* до 20 раз, после чего протокол завершается неуспешно и сессия не устанавливается в защищенном режиме. Повторная передача *Hello* выполняется с переменной задержкой, величина которой имеет значения: 50, 100, 200 мс. Начиная с четвертого повтора, задержка имеет постоянное значение 200 мс. Каждое из полученных сообщений *Hello* подтверждается ответным *HelloACK* сообщением, после приема которого повторная отправка *Hello* прекращается.

Для перехода в следующую фазу сообщение *Hello* должны получить оба корреспондента, а сообщение *HelloACK* должен получить хотя бы один из них.

На второй фазе протокола корреспонденты согласуют между собой, кто будет инициатором для выполнения алгоритма Диффи-Хелмана. Инициатор первым отправляет *“Commit”*сообщение. Если оба корреспондента выбирают роль инициатора и отправляют сообщение *“Commit”* одновременно , сравниваются значения хеша *hvi* из этих сообщений. Тот, чье значение *hvi* окажется больше – сохраняет роль инициатора.

Протокол предусматривает повторную передачу сообщения *“Commit”*до 10 раз, после чего протокол завершается неуспешно и сессия не устанавливается в защищенном режиме. Повторная передача *Commit* сообщения выполняется с переменной задержкой, величина которой имеет значения: 150, 300, 600, 1200 мс. Начиная с четвертого повтора, задержка имеет постоянное значение 1200 мс. Каждое полученное по каналу связи сообщение *Commit* подтверждается ответным

сообщением *DHPart1* третьей фазы, после приема которого повторная передача *Commit* прекращается.

На третьей фазе в результате обмена открытыми сообщениями *DHPart1* и *DHPart2* производится формирование секретных ключей для SRTP сессии.

Протокол предусматривает повторную передачу *DHPart2* сообщения до 10 раз, после чего протокол завершается неуспешно и сессия не устанавливается в защищенном режиме. Повторная отправка *DHPart2* сообщения выполняется с переменной задержкой, величина которой имеет значения: 150, 300, 600, 1200 мс. Начиная с четвертого повтора задержка имеет постоянное значение 1200 мс. Каждое полученное сообщение *DHPart2* подтверждается ответным сообщением *Confirm1*четвертой фазы, после приема которого повторная передача *DHPart2* прекращается.

На четвертой фазе для подтверждения успешного формирования общего ключа осуществляется обмен *Confirm2* и *ConfACK* сообщениями. Последовательность обмена сообщениями между взаимодействующими корреспондентами в процессе выполнения протокола ZRTP показана на рисунке 4.13. Для *Confirm2* предусмотрена повторная отправка сообщений с параметрами, аналогичными сообщению *DHPart2*.

Протокол считается завершенным, когда инициатор получает сообщение *ConfACT* или первый SRTP пакет с верным тегом аутентификации.

4.3.2 Оценка ВВХ протокола ZRTP

На рисунке 4.9. представлен обмен сообщениями протокола ZRTP между взаимодействующими корреспондентами.

Используя описанные ранее особенности ПРК, составляется полный вероятностный граф и описываются производящие функции для первой фазы протокола ZRTP, в ДКБП с равномерным распределением ошибок в сообщениях. Для этого определяются следующие параметры:

T_{HA} - время формирования и передачи сообщения *Hello* корреспондентом А, с;

$T_{ож}$ - время ожидания при передаче сообщения *Hello*, которое выжидает корреспондент между повторными передачами сообщения, с;

l - размер пакета, передаваемого по каналу связи, бит;

p_0 - вероятность битовой ошибки в канале связи;

NH – размер сообщения *Hello*, (*Hello_A, Hello_B*), бит;

NA - размер в битах сообщения *HelloACK*, бит.

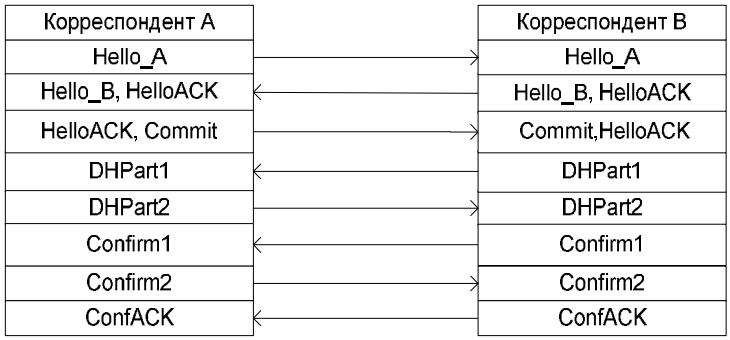


Рисунок 4.9 – Обмен сообщениями по протоколу ZRTP

При определении производящей функции элемента для первой фазы протокола, а именно передачи одного сообщения Hello, необходимо учесть особенности, что повтор сообщения Hello производится только 20 раз, после чего протокол завершает работу. Для каждого повтора $T_{ож}=T_{Hi}(i)$:

$$T_{Hi}(i)=\begin{cases}0, \text{ при } i=0\\0.05, \text{ при } i=1\\0.1, \text{ при } i=2\\0.2, \text{ при } i\geq 3\end{cases} \tag{4.35}$$

$$H_{Ti}(i)=x^{T_{Hi}(i)}$$

При оценке ВВХ вводиться допущение, что доставка сообщения *Hello* не подтверждается сообщением *HelloACK*.

В данных условиях, производящая функция первой фазы протокола (рисунок 4.10) при передаче сообщения *Hello* будет иметь следующий вид:

$$H_{HELLO} = H_0 + H_1 + ... + H_{20} + H_{21} \ , \tag{4.36}$$

где $H_i = H_{H(i)} \prod_{k=1}^{i} H_T(k)$

$H_{H0} = (1-(1-p_0)^l) x^{T_{HA}}$ - производящая функция, определяющая ветвь безошибочной передачи сообщения *Hello* при единичной передаче сообщения.

$H_{H1} = (1-(1-p_0)^l)^2 x^{T_{HA}}$ - производящая функция, определяющая ветвь безошибочной передачи сообщения *Hello* при одной повторной передаче сообщения.

$H_{H(i)} = (1-(1-p_0)^l)^i x^{T_{HA}}$ - производящая функция, определяющая ветвь безошибочной передачи сообщения *Hello* при *i*-й повторной передаче сообщения, *i*=1..20.

H_{21} - производящая функция, определяющая ветвь недоставки сообщения за 20 повторных передач сообщения:

$$H_{21} = P_{ост} x^{T_{HA} + \sum_{i=1}^{20} T_{Hi}(i)}, \tag{4.37}$$

где $P_{ост}$ - вероятность, что сообщение *Hello* не было передано за 20 попыток;

$$T_{HA} = l / c, \tag{4.38}$$

где *c* – скорость канала связи, бит/с.

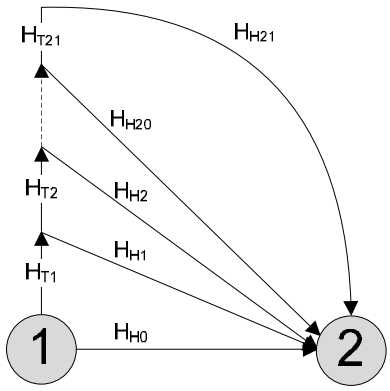


Рисунок 4.10 – Вероятностный граф передачи сообщения Hello

Для составления вероятностного графа всего протокола ZRTP необходимо воспользоваться ранее описанными особенностями ПРК. Введены следующие переменные:

NC - размер сообщения *Commit*, бит;

ND - размер сообщения *DHPart1*, бит;

NP - размер сообщения *DHPart2*, бит;

NO - размер сообщения *Confirm1*, бит;

NF - размер сообщения *Confirm2*, бит;

NK - размер сообщения *ConfACK*, бит;

H_{XX} – производящая функция ветви, где xx – обозначение соответствующей ветви.

Вероятностный граф всего протокола ZRTP представлен на рисунке 4.11.

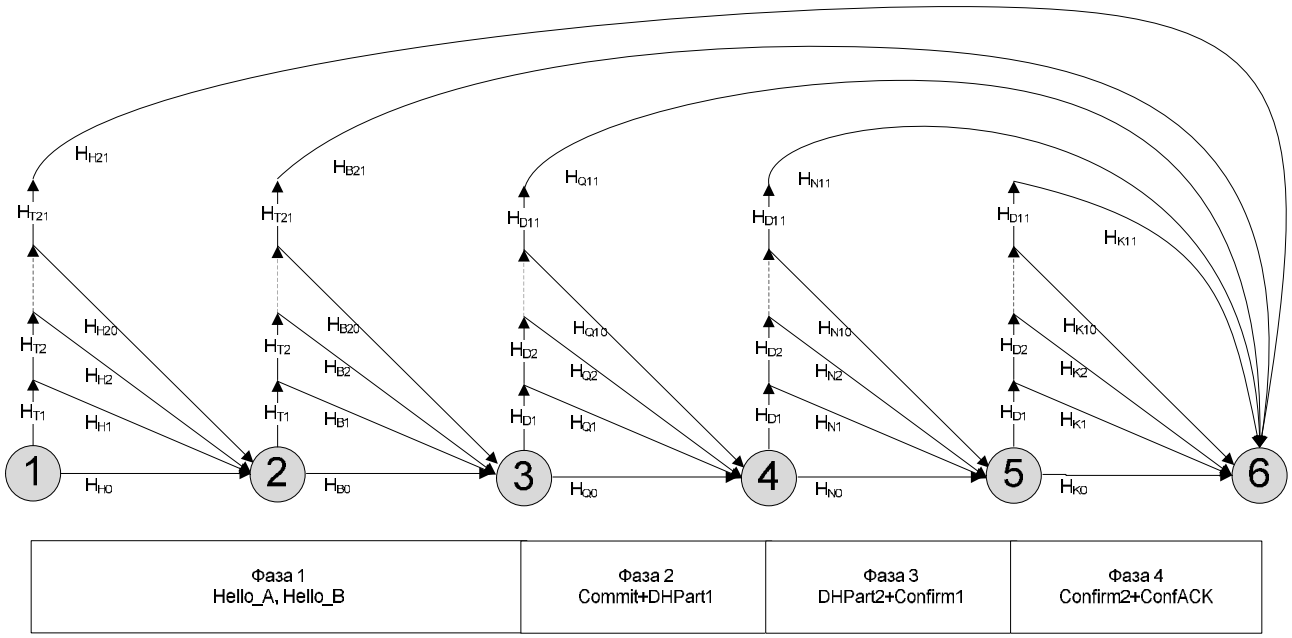


Рисунок 4.11 – Вероятностный граф протокола ZRTP

Для расчетов граф упрощается (рисунок 4.12, 4.13), а также разбивается на ветви, характеризующие успешное и неуспешное выполнение протокола в каждой фазе.

Для расчета среднего времени успешного завершения протокола необходимо определить производящую функцию успешной ветви выполнения протокола.

Для этого выполняется расщепление ветвей графа на успешное и неуспешное завершение протокола.

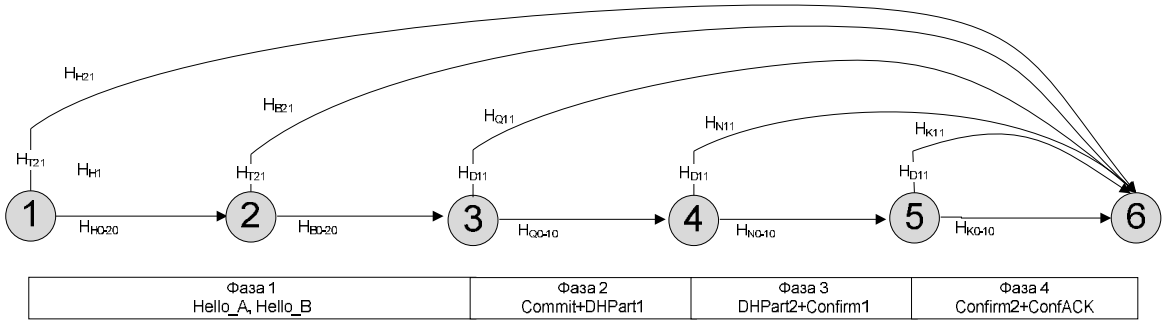


Рисунок 4.12 – Упрощенный вероятностный граф протокола ZRTP

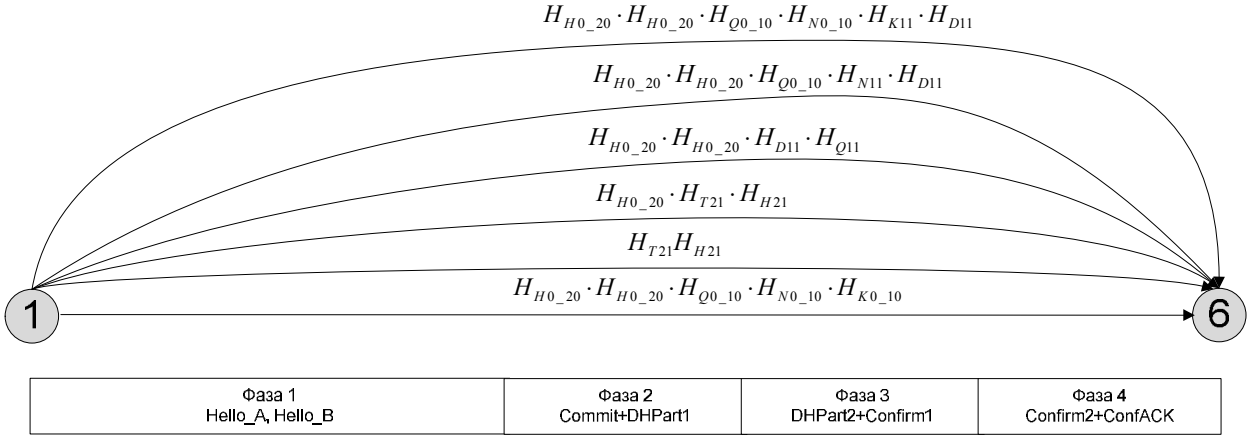


Рисунок 4.13 – Упрощенный вероятностный граф протокола ZRTP

Упрощенный граф с разделенными ветвями успешного и неуспешного завершения протокола приведен на рисунке 4.14.

Производящая функция всего графа имеет вид:

$$H_{full} = H_{H0\_20} \cdot H_{H0\_20} \cdot H_{Q0\_10} \cdot H_{N0\_10} \cdot H_{K0\_10} + H_{T21} H_{H21} + H_{H0\_20} \cdot (H_{T21} \cdot H_{H21} + + H_{H0\_20} \cdot H_{D11} [H_{Q11} + + H_{Q0\_10} \cdot (H_{N0\_10} \cdot H_{K11} + H_{N11})]) \quad (4.39)$$

Производящая функция ветви неуспешного завершения протокола:

$$H_{fail} = H_{T21} H_{H21} + H_{H0\_20} \cdot (H_{T21} \cdot H_{H21} + H_{H0\_20} \cdot H_{D11} [H_{Q11} + H_{Q0\_10} \cdot (H_{Q0\_10} \cdot H_{K11} + H_{Q11})]) \quad (4.41)$$

Производящая функция ветви успешного завершения протокола:

$$H_{success} = H_{H0\_20} \cdot H_{H0\_20} \cdot H_{N0\_10} \cdot H_{N0\_10} \cdot H_{K0\_10} \quad (4.42)$$

На первом и втором этапе первой фазы протокола ZRTP, при передаче Hello от корреспондента A к корреспонденту B, а также Hello от B к A, сообщения имеют одинаковую длину, поэтому передача сообщений для обоих итераций представлена в виде одинаковых производящих функций H_{H0_20}.

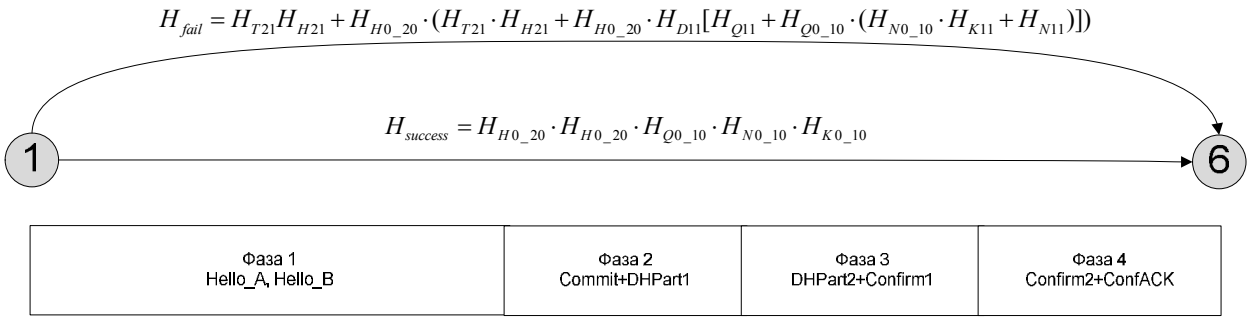


Рисунок 4.14 – Упрощенный вероятностный граф протокола ZRTP

Производящая функция H_{H0_20} определяется как

$$H_{H0\_20} = \left[\sum_{y=0}^{19}\left[H_A \cdot \left(\prod_{i=1}^{y} H_T\right)\right]\right] + H_{A\_ост} \cdot \prod_{i=0}^{20} H_T, \tag{4.43}$$

где производящая функция передачи i-го сообщения:

$$H_A = \left[(1-p_0)^{NH} \cdot x^{\frac{NH}{c}}\right] \cdot \left[\left[\left[1-(1-p_0)^{NH}\right] \cdot x^{T_{Hi}(y)}\right]^{y}\right] \tag{4.43}$$

$$H_{A\_ост} = 1 - \left[\sum_{y=0}^{19}\left[\left[(1-p_0)\right]^{NH} \cdot \left[\left[1-(1-p_0)^{NH}\right]^{y}\right]\right]\right] \cdot \tag{4.44}$$

производящая функция ветви ожидания перед повторной передачей сообщения, в случае недоставки на предыдущей попытке:

$$H_T(i,x) = x^{T_{Hi}(i)} \tag{4.45}$$

$T_{Hi}(i)$ - задержка перед повторной передачей сообщения Hello, с:

$$T_{Hi}(i) = \begin{cases} 0, \text{ при } i = 0 \\ 0.05, \text{ при } i = 1 \\ 0.1, \text{ при } i = 2 \\ 0.2, \text{ при } i \geq 3 \end{cases} \tag{4.46}$$

H_Q описывает передачу сообщений второй фазы протокола, а именно передачу Commit+DHPart1 сообщений.

$$H_{Q0\_10} = \left[\sum_{i=0}^{9} \left[H_Q \cdot \left(\prod_{i=0}^{y} H_D \right) \right] \right] + H_{Q\_ocm} \cdot \prod_{i=0}^{10} H_D \tag{4.47}$$

$$H_Q = \left[(1-p_0)^{NC+ND} x^{\frac{NC+ND}{c}} \right] \left(\left[1-(1-p_0)^{NC+ND} \right] x^{T_{Di}(y)} \right)^y \tag{4.48}$$

$$H_{Q\_ocm} = 1 - \left[\sum_{y=0}^{9} \left[\left[(1-p_0) \right]^{NC+ND} \cdot \left[\left[1-(1-p_0)^{NC+ND} \right]^y \right] \right] \right] \tag{4.49}$$

H_D – производящая функция ветви ожидания перед повторной передачей сообщения, в случае недоставки на предыдущей попытке.

$$H_D(i) = x^{T_{Hi}(i)} \tag{4.50}$$

$T_{Di}(i)$ - задержка перед повторной передачей сообщений Commit, DHPart2, Confirm2, с:

$$T_{Di}(i) = \begin{cases} 0, \text{ при } i = 0 \\ 0.05, \text{ при } i = 1 \\ 0.1, \text{ при } i = 2 \\ 0.2, \text{ при } i \geq 3 \end{cases} \tag{4.51}$$

H_N описывает передачу сообщений третьей фазы протокола, а именно передачу DHPart2+Confirm1 сообщений.

$$H_{N0\_10} = \left[\sum_{i=0}^{9} \left[H_N \cdot \left(\prod_{i=0}^{y} H_D \right) \right] \right] + H_{N\_ocm} \cdot \prod_{i=0}^{10} H_D \tag{4.52}$$

$$H_N = \left[(1-p_0)^{NP+NO} x^{\frac{NP+NO}{c}} \right] \left(\left[1-(1-p_0)^{NP+NO} \right] x^{T_{Di}(y)} \right)^y \tag{4.31}$$

$$H_{N\_ocm} = 1 - \left[\sum_{y=0}^{9} \left[\left[(1-p_0) \right]^{NP+NO} \cdot \left[\left[1-(1-p_0)^{NP+NO} \right]^y \right] \right] \right] \tag{4.53}$$

На четвертой фазе протокола передаются сообщения Confirm2 + ConfACK, общим размером *N_K* бит

N_K = NF+ NK, бит

Производящая функция определяется как:

$$H_{K0\_10} = \left[\sum_{i=0}^{9} \left[H_K \cdot \left(\prod_{i=0}^{y} H_D \right) \right] \right] + H_{K\_ost} \cdot \prod_{i=0}^{10} H_D \quad (4.54)$$

где $H_K = \left[(1-p_0)^{N\_K} \cdot x^{\frac{N\_K}{c}} \right] \cdot \left[\left[\left[1-(1-p_0)^{N\_K} \right] \cdot x^{T_{Di}(y)} \right]^y \right]$

$$H_{K\_ost} = 1 - \left[\sum_{y=0}^{10} \left[\left[(1-p_0) \right]^{N\_K} \cdot \left[\left[1-(1-p_0)^{N\_K} \right]^y \right] \right] \right] \cdot$$

Для расчета среднего времени успешного завершения протокола в соответствии с (4.6) определена производящая функцию ветви успешного выполнения протокола (4.27). Функция среднего времени и вероятности успешного завершения ПРК будет иметь вид:

$$T_{cp} = \frac{dH_{success}}{dx}(x=1) \quad (4.55)$$

$$P_{success} = H_{H0\_20}(x=1) \cdot H_{H0\_20}(x=1) \cdot H_{Q0\_10}(x=1) \cdot H_{N0\_10}(x=1) \cdot H_{K0\_10}(x=1) \quad (4.56)$$

4.3.3 Расчет ВВХ ZRTP

График среднего времени успешного выполнения протокола ZRTP для различных величин задержки пакетов в канале связи представлен на рисунке 4.15. Вероятность успешного завершения определяется в (4.36) и будет иметь вид, представленный на рисунке 4.16.

Очевидно, что в каналах хорошего качества ($p_o < 10^{-4}$) время успешного выполнения протокола существенно зависит от величины задержки сообщений в канале связи и практически не зависит от вероятности ошибки. При этом в каналах с задержкой более 150 мс время выполнения протокола ZRTP становится соизмеримым с величинами, определяющими полное время установления соединений в сетях телефонной связи общего пользования.

С ухудшением качества канала от $p_o = 10^{-4}$ до $p_o = 10^{-3}$ среднее время выполнения протокола резко возрастает, а зависимость от задержки пакетов в канале связи нивелируется.

Вероятность успешного выполнения протокола ZRTP в каналах хорошего качества не зависит от задержек в канале связи и близка к единице, и только в

каналах с вероятностью ошибки на символ более $5 \cdot 10^{-4}$ начинает снижаться до 0,8 при $p_o = 10^{-4}$.

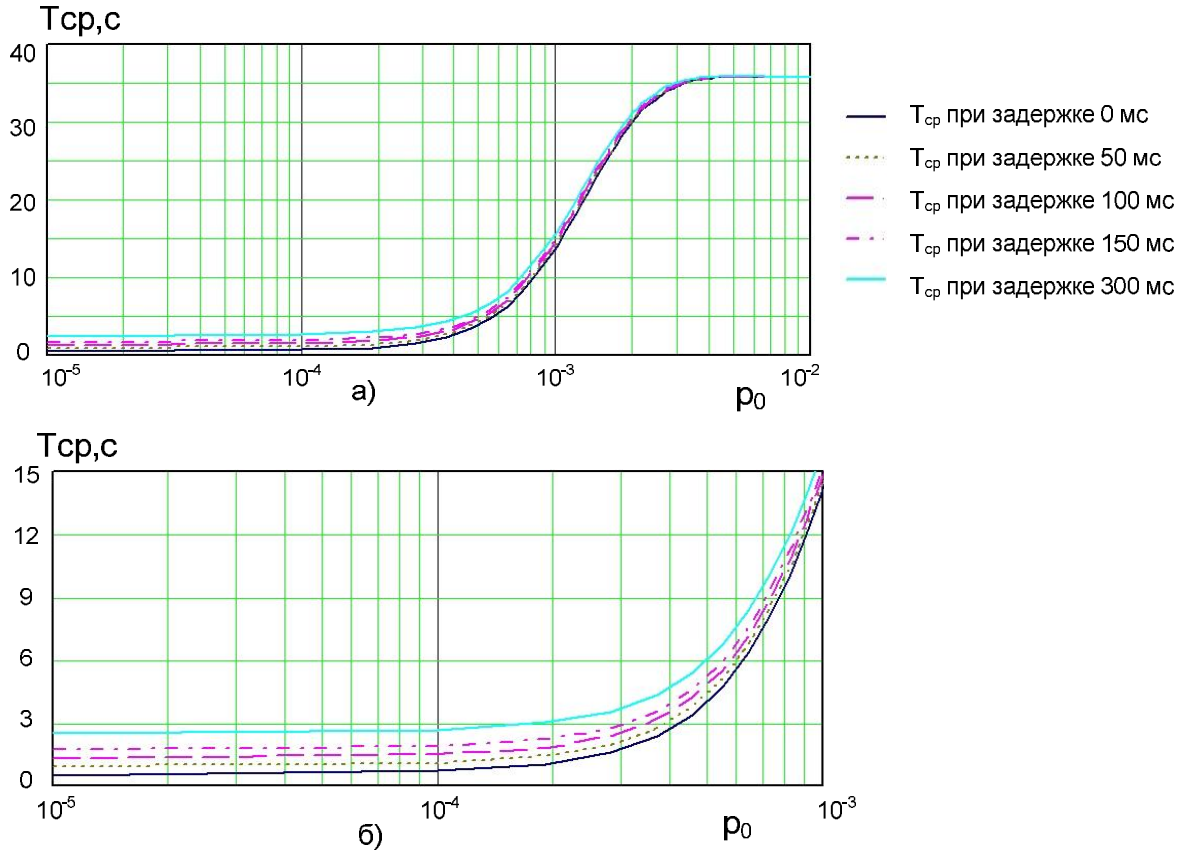


Рисунок 4.15 – Зависимость $T_{ср}$ ZRTP от вероятности ошибки в канале с задержками пакетов а)$10^{-5} \le p_0 \le 10^{-2}$ б) $10^{-5} \le p_0 \le 10^{-2}$

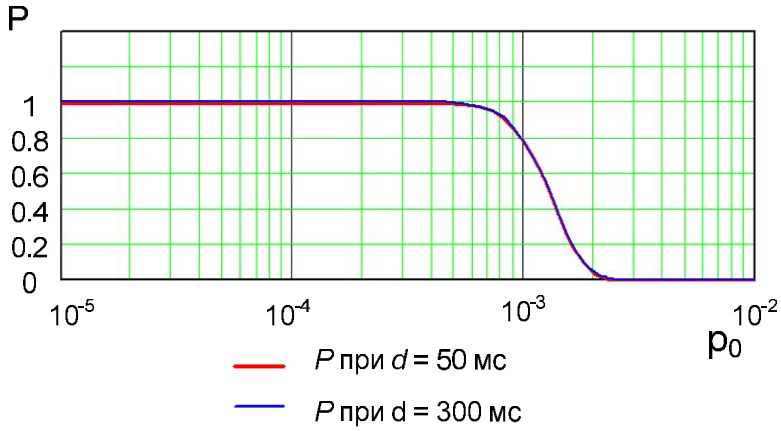


Рисунок 4.16 – Зависимость вероятности успешного завершения протокола от вероятности ошибки

На рисунке 4.17 представлено сравнение среднего времени успешного завершения ZRTP и DTLS. Очевидно, ZRTP обеспечивает меньшее значение $T_{ср}$ в каналах более плохого качества по сравнению с DTLS. Поэтому дальнейший анализ будет выполняться именно для протокола ZRTP.

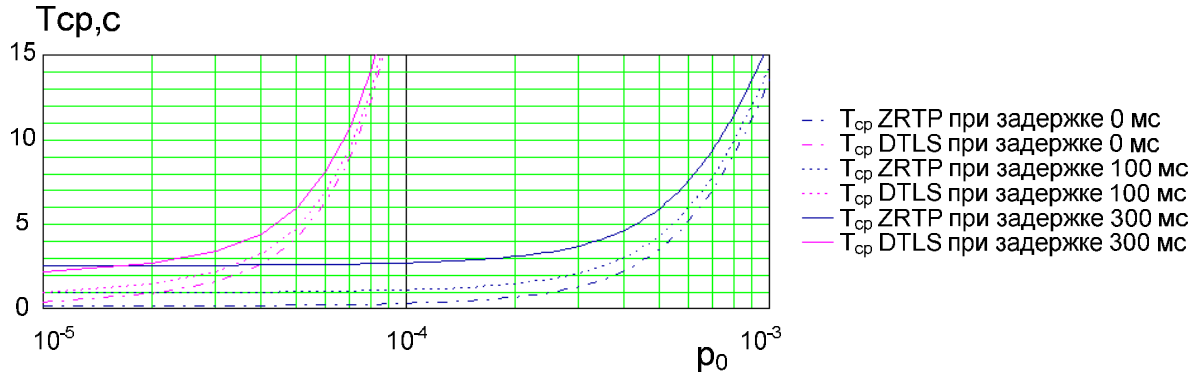


Рисунок 4.17 – Зависимость среднего времени выполнения протокола ZRTP и DTLS от вероятности ошибки в канале при разных значениях *d*

4.4 Практическая оценка временных характеристик протокола ZRTP

Цель проведенного эксперимента состоит в оценке влияния задержки и потери пакетов в канале передачи данных (ПД) на время установления защищенного соединения при использовании протоколов обеспечения безопасности IP-телефонии , а также в оценке среднего времени успешного завершения криптографического протокола ZRTP [121]. Схема экспериментальной установки приведена на рисунке 4.18.

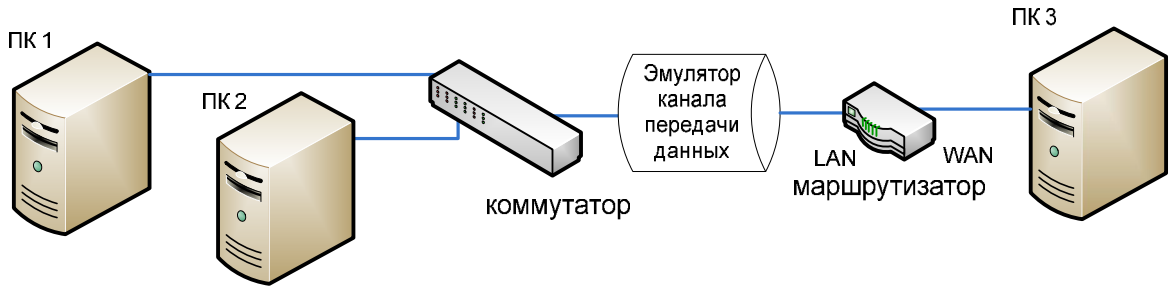


Рисунок 4.18 – Схема экспериментальной установки

Схема состоит из управляемого коммутатора, маршрутизатора на основе сетевой операционной системы FreeBSD, а также трех компьютеров (ПК 1, ПК 2,

ПК 3). Маршрутизатор имитирует канал ПД, обеспечивая различные состояния КС, и позволяет устанавливать величины следующих параметров: процент потерянных пакетов, а также задержку для пакетов, передаваемых через порт маршрутизатора.

На компьютере ПК1 установлено приложение Wireshark, обеспечивающее перехват и анализ пакетов, передаваемые между станциями 2 и 3. Для осуществления этой задачи на коммутаторе инициализируется функция зеркалирования портов.

На компьютерах ПК2 и ПК3 устанавливаются приложения Zfone и Phoner.

Программное обеспечение Phoner было выбрано в качестве клиента IP-телефонии, так как оно имеет настраиваемую встроенную поддержку ZRTP. Эта опция делает возможным включение и выключение встроенного модуля ZRTP при выполнении эксперимента. Программа распространяется бесплатно с сайта автора phoner.de.

Zfone – приложение, созданное Филлом Зимерманом, разработчиком протокола ZRTP. Оно предоставляется бесплатно для некоммерческого использования и получено с сайта проекта The Zfone™ Project http://zfoneproject.com. Приложение осуществляет роль шлюза для пакетов RTP, преобразуя их в SRTP. Программное обеспечение также делает возможным выполнение ZRTP протокола между корреспондентами для формирования общего ключа. При выключении опции поддержки ZRTP на Phoner и запуске программы Zfone – ZRTP протокол будет исполняться средствами приложения Zfone, что позволит сопоставить поведение ZRTP в реализациях разных разработчиков.

Для оценки ВВХ протокола ZRTP было произведено несколько измерений времени успешного завершения протокола при различных условиях. Перед каждым измерением на LAN интерфейсе маршрутизатора задавались параметры:

- процент потерянных пакетов, передаваемых через интерфейс маршрутизатора;

- задержка для передаваемых через интерфейс маршрутизатора пакетов.

На компьютере 3 в приложении Phoner был включен режим автоматического ответа с проигрыванием тестовой записи. При звонке с компьютера 2 на ПК 3, на ПК 2 автоматически инициировалась запись разговора и выполнялось сохранение тестовой записи в том виде и с тем качеством, с которым для пользователя она была доступна.

Оценка среднего времени успешного завершения ZRTP проводилась в следующей последовательности:

1) установка требуемых величин потери пакетов и задержки канала ПД на маршрутизаторе;

2) проверка точности установки задержки/потери пакетов утилитой ping;

3) включение сетевого анализатора трафика Wireshark на ПК1, выполнение звонка ПК2-ПК3, сохранение дампа данных и запись звонка;

4) определение времени работы ZRTP по дампу.

Работа ZRTP может быть организована одним из двух способов:

1) параллельно с RTP, т.е. до окончания работы ZRTP RTP трафик передается в открытом виде. После окончания работы ZRTP - голосовой трафик передается зашифрованным в SRTP.

2)до RTP – как только между абонентами включается голосовой канал, ZRTP начинает выполняться, при этом блокируется передача RTP. Разговор между абонентами начинается по окончании выполнения ZRTP, с использованием SRTP.

Программа Zfone обеспечивает второй способ, что делает возможным оценить работу ZRTP также по голосовым диаграммам.

В качестве источника эталонного речевого сигнала на компьютере 3 был включен автоответчик, который диктует фразу женским голосом "Нажмите 1, чтобы принять этот звонок, нажмите 2, чтобы отклонить его, нажмите 3, чтобы всегда принимать звонки с этого номера, нажмите 4, чтобы никогда не принимать звонки с этого номера, нажмите 5, чтобы сбрасывать звонки с этого номера и

сообщить звонящему, чтобы он внес вас в список абонентов 'кому не надо звонить'". Акустическая диаграмма этого сигнала изображена на рисунке 4.19.

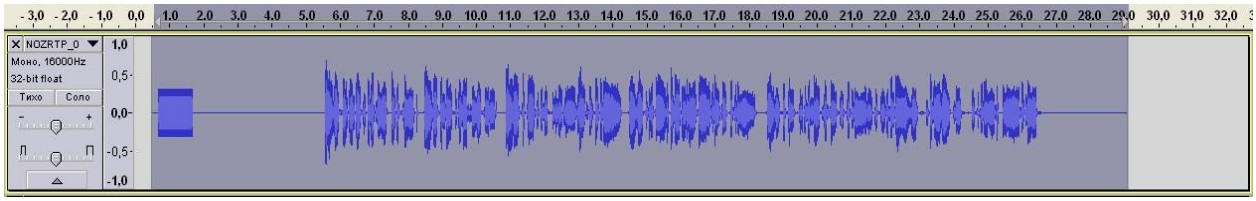


Рисунок 4.19 – Запись исходного речевого сообщения

На втором компьютере осуществлялась запись принятого речевого сигнала. На рисунке 4.20 представлены голосовые дорожки при передаче тестового звука по схеме – компьютер-компьютер с учетом работы ZRTP протокола. Из рисунка видно, что при работе по каналам связи с задержками время выполнения протокола может составлять до нескольких секунд. Например, для канала связи с задержкой 300 мс время выполнения протокола составило свыше двух секунд. При этом время начала передачи голоса по защищенному каналу между абонентами сдвигается на величину, равную времени работы протокола.

а)
б)
в)
г)

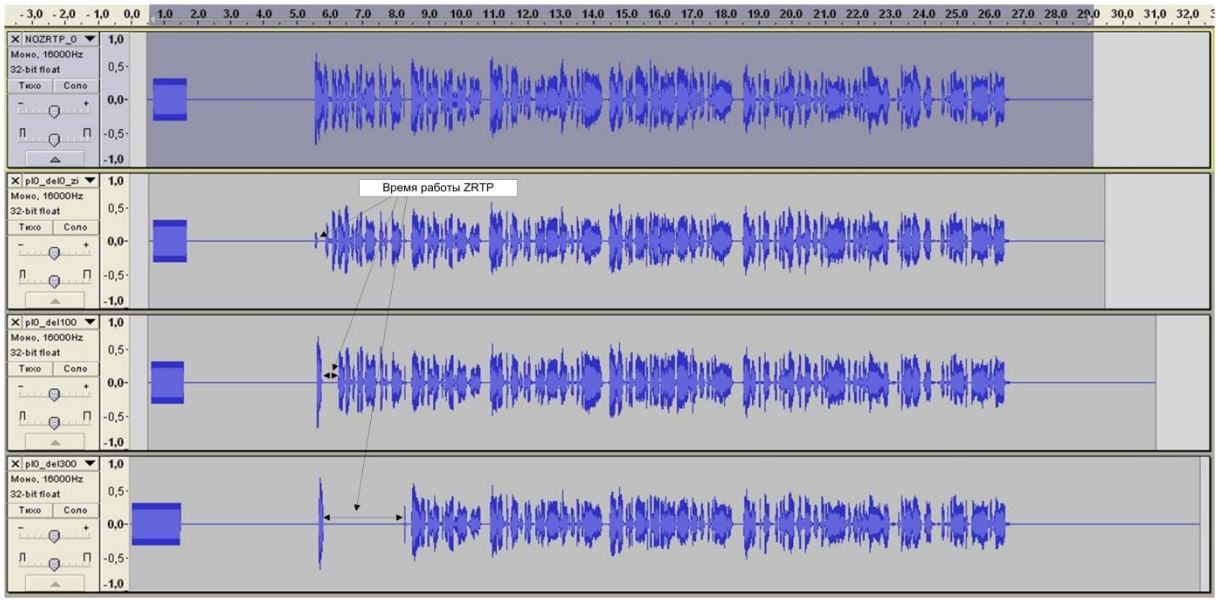


Рисунок 4.20 – Записи принятого речевого сообщения с учетом влияния протокола ZRTP в реализации Zfone

а) принятый звуковой сигнал при выключенном протоколе ZRTP;

б) принятый звуковой сигнал при передаче по каналу с односторонней задержкой 0 мс;

в) принятый звуковой сигнал стороне при передаче по каналу с односторонней задержкой 100 мс;

г) принятый звуковой сигнал стороне при передаче по каналу с односторонней задержкой 300 мс.

Для снижения случайной составляющей погрешности выполнялась серия из десяти измерений и рассчитывалось среднее значение измеряемого времени. Результаты обработки измерений для различных задержек и потери пакетов в канале связи приведены в таблице 4.2.

Таблица 4.2 – Усредненные результаты измерения времени выполнения протокола ZRTP

Потери %, p_0	Задержка, d, мс	Tср, с	σ	N	Доверительный интервал
~0% (10^{-10})	0	0,04	0,01	10	0,008
	100	0,85	0,04	10	0,031
	300	2,55	0,25	10	0,175
1% ($6{,}59*10^{-6}$)	0	0,26	0,12	10	0,087
	100	0,99	0,09	10	0,062
	300	2,89	0,35	10	0,249
5% ($3{,}36{,}*10^{-5}$)	0	0,42	0,19	10	0,139
	100	1,19	0,02	10	0,016
	300	3,08	0,42	10	0,300
10% ($6{,}90*10^{-5}$)	0	0,50	0,16	10	0,114
	100	1,38	0,36	10	0,256
	300	3,19	0,45	10	0,324
15% ($1{,}06*10^{-4}$)	0	0,71	0,32	10	0,23
	100	1,90	0,45	10	0,32
	300	3,40	0,46	10	0,33

На рисунке 4.21 представлены результаты оценки среднего времени выполнения протокола, полученные на основании проведенных измерений и экспериментов.

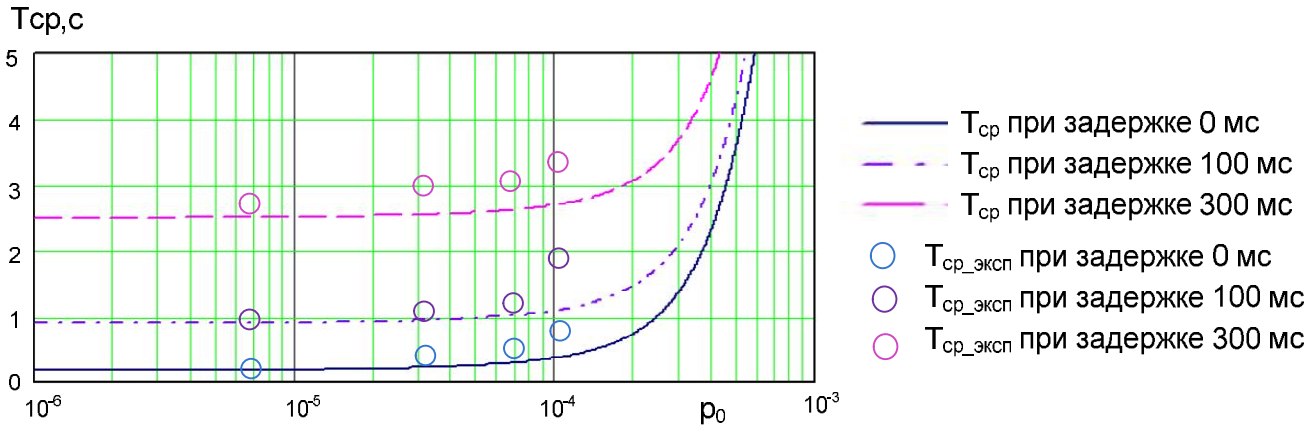


Рисунок 4.21 – Совмещенный график - зависимость времени выполнения протокола ZRTP от вероятности ошибки и от задержки в канале связи, а также экспериментально полученные значения

При анализе полученных данных, можно сделать следующие выводы:

1. Исследование показывает, что среднее время успешного выполнения протокола ZRTP определяется в основном величиной задержки сообщений в канале связи.

2. Зависимость среднего времени успешного выполнения ZRTP от вероятности битовых ошибок в каналах хорошего и удовлетворительного качества слабо выражена, но при увеличении вероятности ошибок свыше $1 \cdot 10^{-4}$ существенно возрастает.

3. Среднее время успешного выполнения протокола ZRTP в каналах с задержкой более 300 мс, превышает 2,5 с и в зависимости от используемого режима защищенной IP-телефонии приводит либо к передаче этого фрагмента речи в незащищенном режиме, либо к потере соответствующего фрагмента речевого сообщения.

Таким образом, имеются существенные предпосылки для совершенствования протокола ZRTP с целью снижения зависимости времени работы протокола от задержки в канале.

4.5 Разработка предложений по улучшению вероятностно-временных характеристик протокола ZRTP

Подробно принцип расчета ВВХ протокола ZRTP был изложен в разделе 4.1. В соответствии с Приказом Министерства информационных технологий и связи Российской Федерации от 27.09.2007 № 113 «Об утверждении Требований к организационно-техническому обеспечению устойчивого функционирования сети связи общего пользования» время с момента получения пользовательским (оконечным) оборудованием вызывающего абонента информации об ответе от пользовательского (оконечного) оборудования вызываемого абонента до момента установления соединения между пользовательским (оконечным) оборудованием вызывающего и вызываемого абонента (время выполнения соединения) не должно превышать 1 с в сети зоновой телефонной связи и в сети междугородной и международной телефонной связи, а также не должно превышать 1,5 с в сети местной телефонной связи [47].

В соответствии с теоретическим расчетом, а также практическим экспериментом при односторонней задержке в линии более 100 мс среднее время выполнения протокола ZRTP составляет около 0.9 с, а при 150 мс составляет 1.2 с, что превышает установленную норму. В случае наличия ошибок в канале связи время выполнения протокола также возрастает за счет необходимости повторной отправки сообщений.

Таким образом, при определенных условиях время выполнения протокола ZRTP не удовлетворяет существующим нормативам. Соответственно - имеет смысл выполнить модернизацию протокола для улучшения параметров ВВХ.

Протокол можно разделить на несколько этапов:

- согласование начальных параметров и условий;
- подготовка к обмену сообщениями;
- обмен и генерация общего ключа по протоколу Диффи-Хелмана;
- проверка общего ключа.

На этапе подготовки от одного корреспондента к другому передается параметр *hvi*, который располагается в сообщении Commit и определяется, как

hvi=hash(DHPart2||Hello респондента)

Экспериментальная оценка и теоретические расчеты показали, что в режиме Диффи-Хелмана протокола ZRTP общая длина сообщений Commit + Hello сравнима с длиной сообщений DHPart1 или DHPart2. Поэтому в качестве модернизации протокола предлагается объединить сообщения HelloB + Commit. При приеме сообщения Hello_A второй корреспондент уже обладает всеми необходимыми данными, чтобы выбрать криптографический набор для продолжения работы протокола.

Недостатком подхода может являться необходимость уже на первой фазе ZRTP выполнить вычисления для протокола Диффи-Хелмана, что требует задействовать вычислительные ресурсы на оборудовании обоих корреспондентов. Однако, дополнительно подход позволяет исключить из протокола последнее сообщения Conf2ACK. Необходимость сообщения в исходном протоколе вызвана наличием незавершенной четвертой фазы, где на сообщение инициатора Confirm2 респондент должен ответить сообщением. При объединении пакетов Hello + Commit сообщение DHPart2 будет ответным для DHPart1, сообщение Confirm2 будет ответным для сообщения Confirm1. При таком подходе сообщение Confirm2 будет ответным, и не потребует дополнительного сообщения Conf2ACK.

Так в обновленной версии протокола будет шесть сообщений: два сообщения Hello и Commit, сообщения DHPart1 и DHPart2, два сообщения проверки выработанного ключа.

Модернизированный протокол будет иметь сценарий обмена сообщениями, представленный на рисунке 4.22.

Необходимо выполнить оценку ВВХ обновленного протокола. Граф обновленного протокола представлен на рисунке 4.11. Выполнено упрощение графа по аналогии с полной версией протокола. Упрощенный граф представлен на рисунке 4.23.

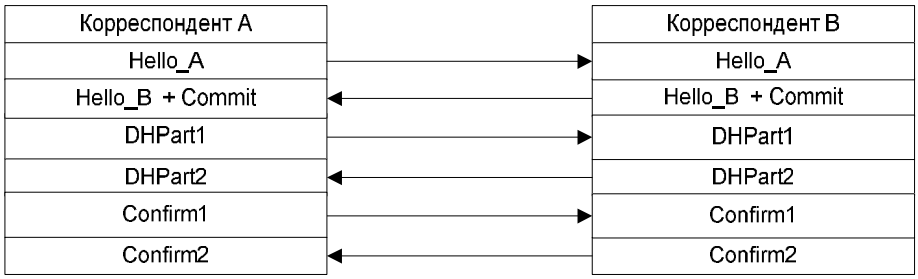


Рисунок 4.22 – Сценарий обмена сообщениями модернизированного протокола

Производящая функция ветви успешного завершения протокола будет определяться, как:

$$H_{success} = H_{HA0\_20} \cdot H_{HB0\_20} \cdot H_{N0\_10} \cdot H_{N0\_10} \tag{4.25}$$

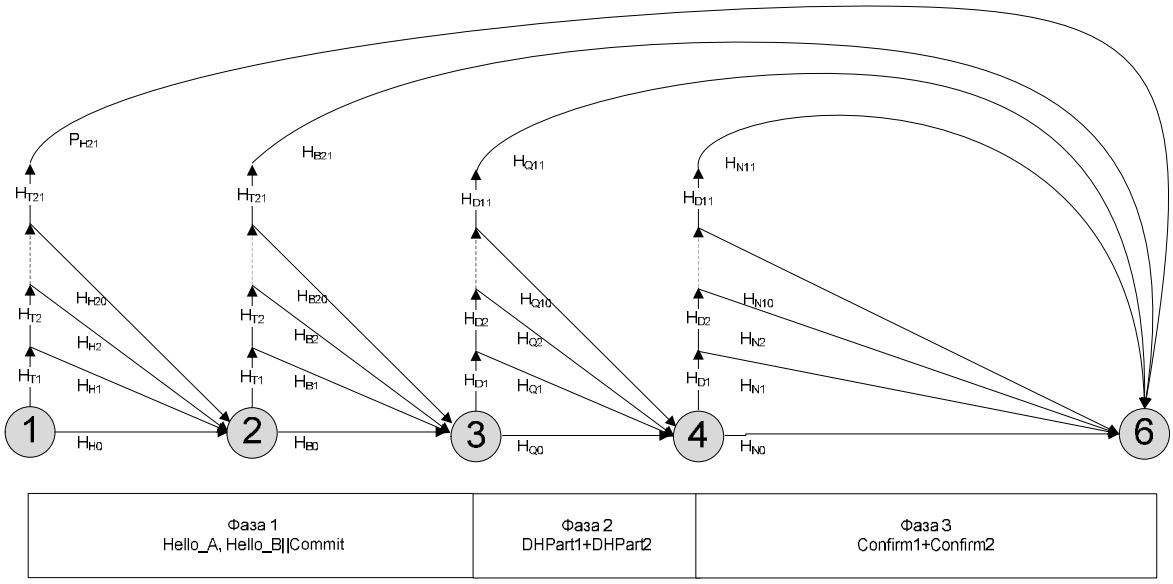


Рисунок 4.23 – Граф обновленного протокола ZRTP

$$H_{fail} = H_{T21}H_{H21} + H_{H0\_20} \cdot (H_{T21} \cdot H_{H21} + H_{H0\_20} \cdot H_{Q11}[H_{Q11} + H_{Q0\_10} \cdot H_{Q11}]$$

$$H_{success} = H_{H0\_20} \cdot H_{H0\_20} \cdot H_{N0\_10} \cdot H_{N0\_10}$$

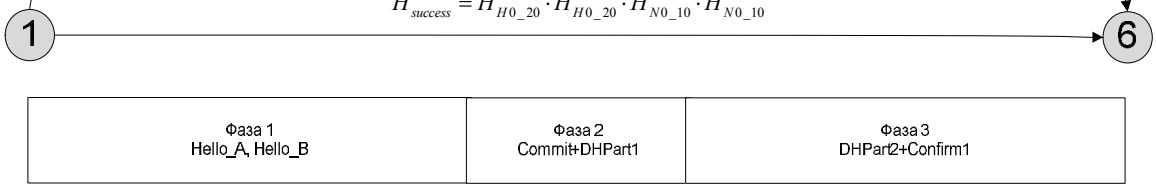


Рисунок 4.24 – Упрощенный граф обновленного протокола ZRTP

Зависимость среднего времени успешного выполнения обновленного протокола от p_0 представлена на рисунках 4.25. Проводится оценка выигрыша в модифицированном протоколе по сравнению с исходным. Для этого определяется время выполнения протокола при работе по каналам с задержками при следующих параметрах:

- задержка: 50мс, 150мс, 300мс
- p_0 : 10^{-5} , $5*10^{-5}$, 10^{-4}

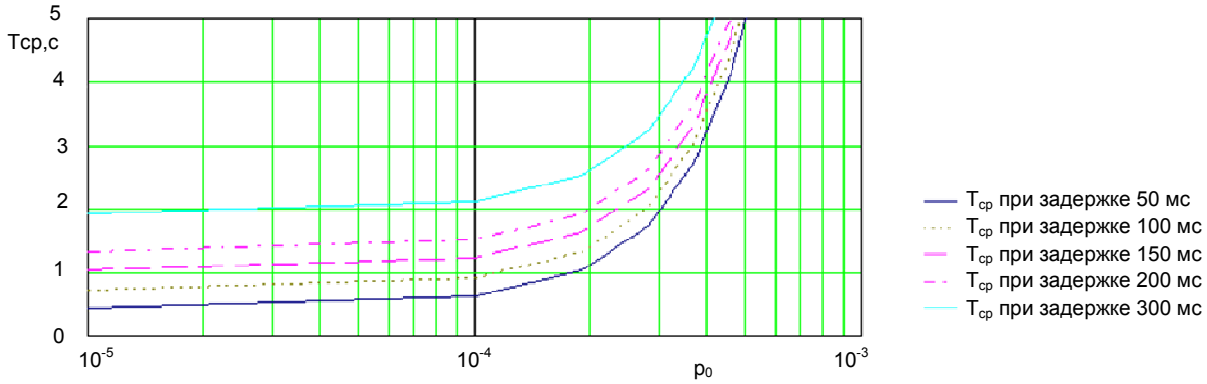


Рисунок 4.25 – Среднее время успешного завершения обновленного протокола ZRTP

Выигрыш оценивается, как

$$T_{B1}=T_{ZRTP} - T_{мод1} \quad (4.26)$$

$$B_{B1}=(T_{ZRTP} - T_{мод1})/ T_{ZRTP} \quad (4.27)$$

где T_{ZRTP} – среднее время выполнения исходного протокола, с;

$T_{мод1}$– среднее время выполнения модификации протокола, с;

Результаты вычислений представлены в таблице 4.5.

Выполняется дополнительное сокращение числа отдельных сообщений в протоколе ZRTP [122, 74]. Для этого объединяются сообщения Hello_B+Commit+DHPart1, а также сообщения DHPart2+Confirm1. Модернизированный протокол будет иметь сценарий обмена сообщениями, представленный на рисунке 4.26а.

Объединение сообщений приводит к потере предварительной передачи параметра *hvi*, однако позволяет сохранить концепцию протокола и выполнить

между корреспондентами проверку полученного ключа. Упрощение графа приведено на рисунке 4.27.

Таблица 4.5 – Оценка выигрыша среднего времени успешного завершения протокола ZRTP первой модификации

d	50мс			150мс			300мс			400мс		
p_0	10^{-5}	$5\cdot10^{-5}$	10^{-4}	10^{-5}	$5\cdot10^{-5}$	10^{-4}	10^{-5}	$5\cdot10^{-5}$	10^{-4}	10^{-5}	$5\cdot10^{-5}$	10^{-4}
T_{ZRTP}, 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
$T_{мод1}$, с	0,42	0,49	0,62	1,02	1,09	1,2	1,92	1,99	2,09	2,52	2,59	2,72
T_{B1}, с	0,1	0,09	0,08	0,28	0,29	0,3	0,58	0,6	0,61	0,8	0,79	0,79
B_{B1}, %	19,2	15,5	11,4	21,5	21	20	23,2	23,1	22,5	24,1	23,37	22,5

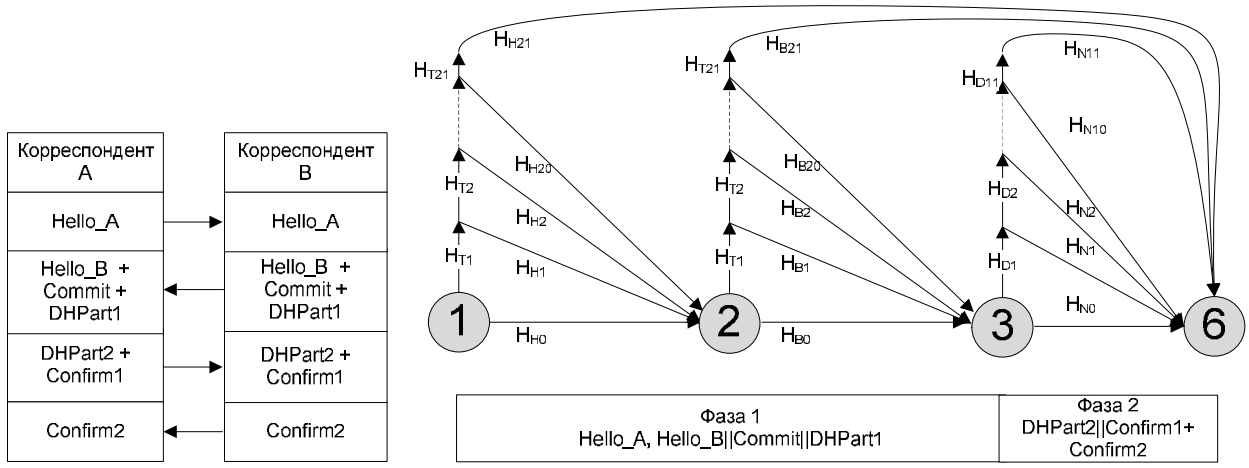


Рисунок 4.26 – Вторая модификация протокола; а) сценарий обмена сообщениями б) вероятностный граф

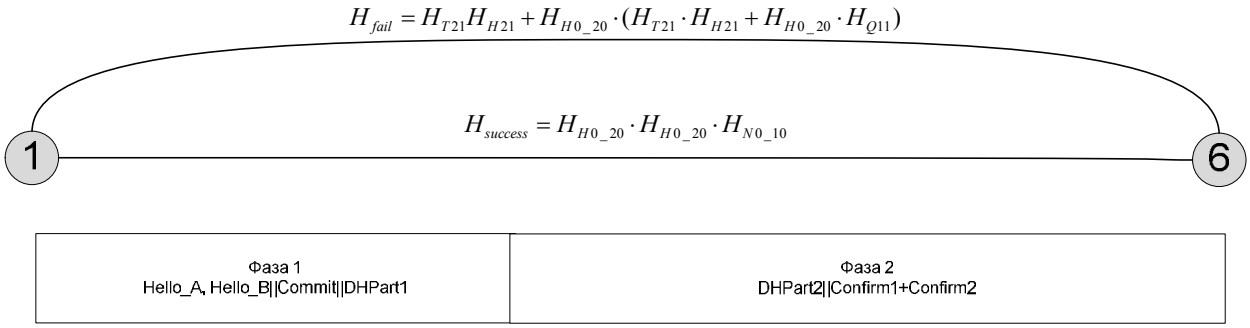


Рисунок 4.27 – Упрощенный граф модернизированного протокола ZRTP

По аналогии вычислено $T_{мод2}$ - среднее время выполнения второй модификации протокола в зависимости от задержки и потери пакетов в канале связи. График приведен на рисунке 4.28.

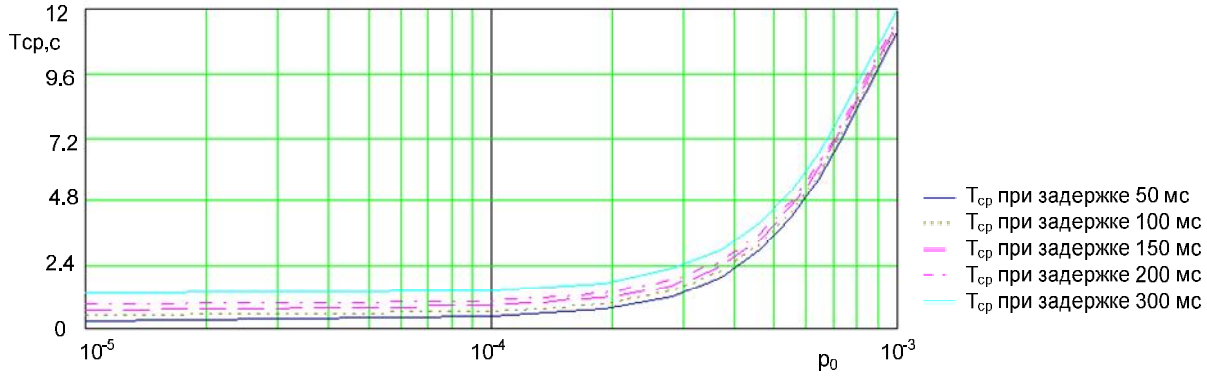


Рисунок 4.28 – Среднее время выполнения модернизированного протокола ZRTP второй модификации

Дополнительно выполнена оценка выигрыша в модифицированном протоколе по сравнению с исходным. Для этого определено время выполнения протокола при работе по каналам с задержками при следующих параметрах:

- задержка 50мс, 150мс, 300мс;
- $p_0 = 10^{-5}, 5*10^{-5}, 10^{-4}$.

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:

$$T_{B2} = T_{ZRTP} - T_{мод2} \quad (4.28)$$

$$B_{B2} = (T_{ZRTP} - T_{мод2}) / T_{ZRTP} \quad (4.29)$$

где $T_{мод2}$– среднее время выполнения второй модификации протокола, с;

Результаты вычислений представлены в таблице 4.6. Выигрыш модифицированного протокола из шести сообщений перед стандартным протоколом составляет от 11% до 24%.

Выигрыш перед стандартным протоколом модифицированного протокола, сокращенного до четырех сообщений, составил от 35% до 48% согласно таблице

4.6. Таким образом, модифицированный протокол ZRTP позволяет работать по каналам связи с большей задержкой по сравнению со стандартным протоколом ZRTP, при этом укладываясь в нормативы для параметров ТФОП.

Таблица 4.6 – Оценка выигрыша среднего времени успешного завершения протокола ZRTP второй модификации

d	50мс			150мс			300мс			400мс		
p_0	10^{-5}	$5\cdot10^{-5}$	10^{-4}	10^{-5}	$5\cdot10^{-5}$	10^{-4}	10^{-5}	$5\cdot10^{-5}$	10^{-4}	10^{-5}	$5\cdot10^{-5}$	10^{-4}
T_{ZRTP}, 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	0,31	0,36	0,45	0,71	0,76	0,85	1,31	1,36	1,45	1,71	1,76	1,85
T_{B2}, с	0,20	0,22	0,24	0,58	0,62	0,64	1,18	1,23	1,24	1,60	1,62	1,65
B_2, %	39,4	37,9	35,5	45,0	44,9	43,2	47,4	47,4	46,2	48,3	47,93	47,2

Для повышения безопасности модифицированного протокола предлагается использовать разработанный в третьей главе метод выявления нарушителя. В этом случае модифицированный протокол выполняется по нескольким каналам связи одновременно, а время успешного завершения протокола будет определяться КС, имеющим наибольшее значение d. Для выявления нарушителя используется либо двухканальный, либо трехканальный ражим с обнаружением или исключением нарушителя.

Выполнено имитационное моделирование для протокола ZRTP и второй модификации протокола, для чего было разработано приложение на языке программирования PHP. Исходный код приложения приведен в приложении. Результаты имитационного моделирования для исходного протокола ZRTP представлены на рисунке 4.29.

Результаты имитационного моделирования для второй модификации протокола ZRTP представлены на рисунке 4.30. Полученные результаты подтверждают теоретически полученную зависимость.

Сравнение зависимостей $T_{мод2,}$ $T_{мод2,}$ T_{ZRTP} приведено на рисунке 4.31. Насколько видно из таблицы 4.6, при $p_0 \leq 10^{-4}$ и $d \leq 300$ мс $T_{мод2} \leq$ 1,45 с. Таким

образом, задача о выполнении норм [47] при работе по каналам связи $d \leq 300$ мс решена.

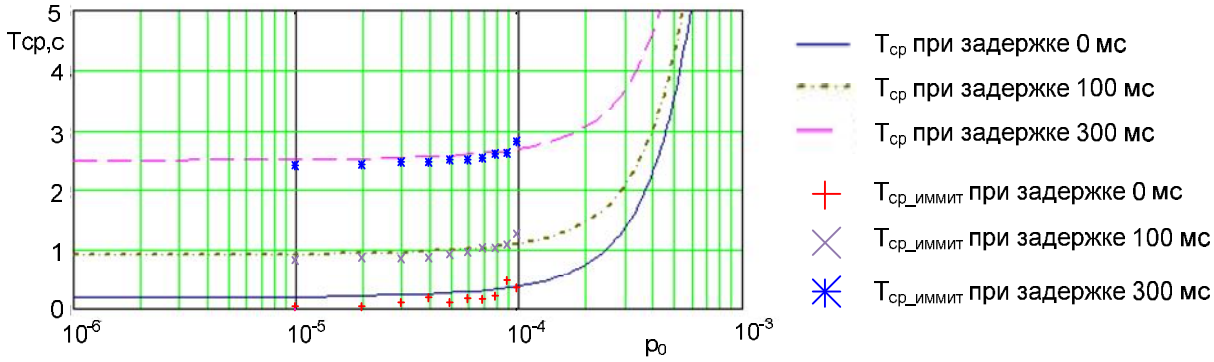


Рисунок 4.29 – Результаты имитационного моделирования Tcp для исходного протокола ZRTP

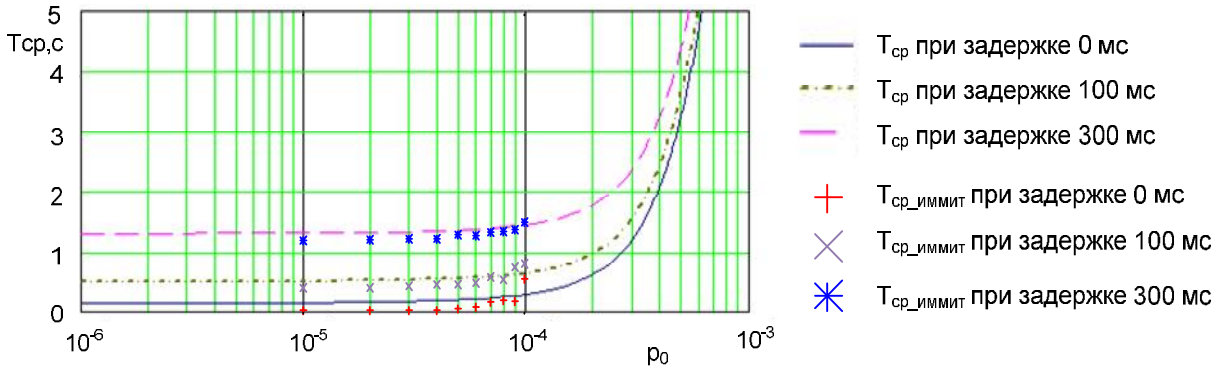


Рисунок 4.30 – Результаты имитационного моделирования Tcp для второй модификации протокола ZRTP

Выводы по главе 4

Представлена методика оценки вероятностно-временных характеристик протоколов распределения ключей защищенной IP-телефонии, позволяющая определить эффективность работы протоколов по каналам с задержками и ошибками, оценивая среднее время, а также вероятность успешного завершения протокола. Методика учитывает особенности ПРК, связанные с ограниченным числом повторов, а также с вариацией задержи в каждом из повторов, и опубликована в [109].

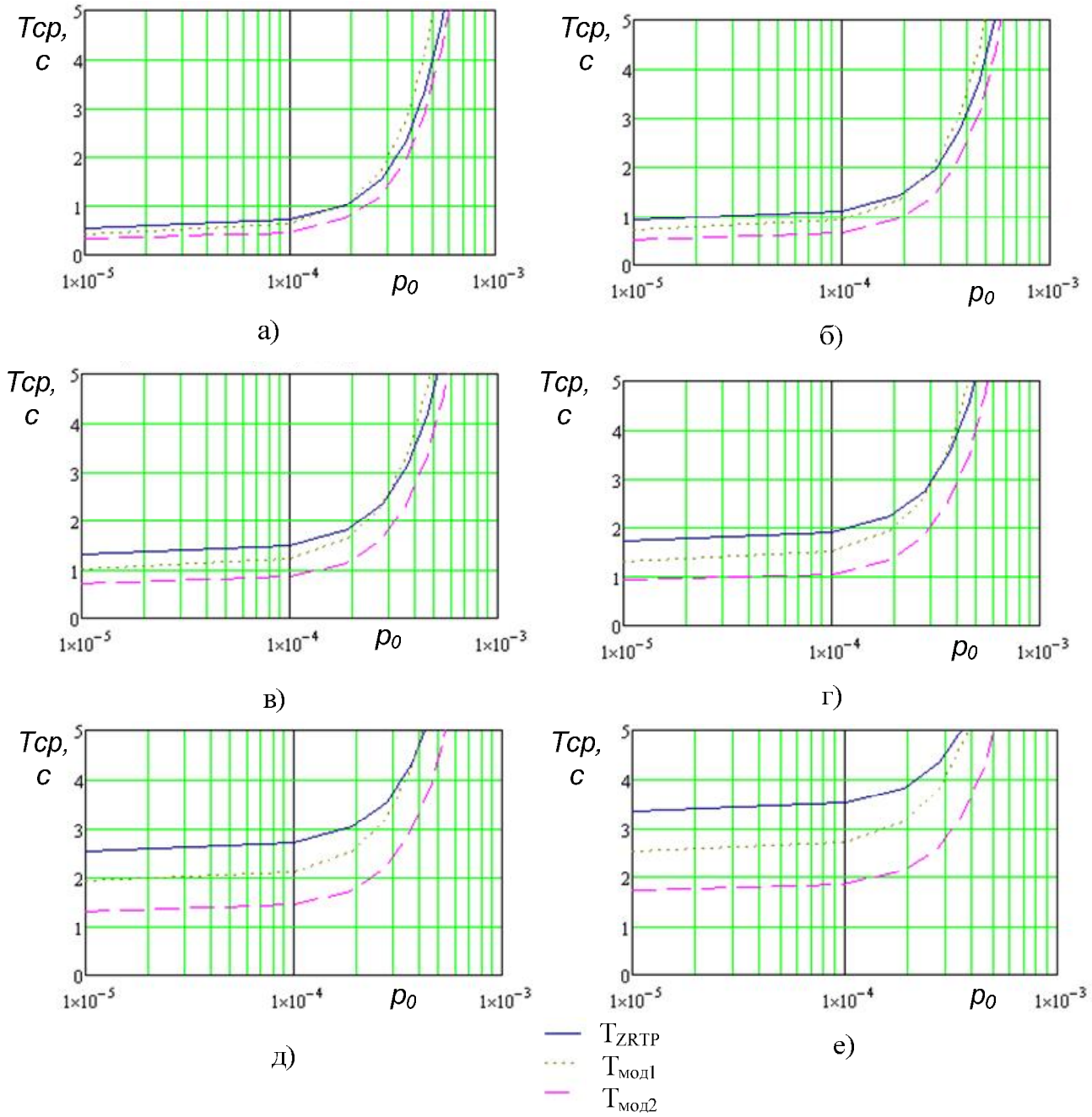


Рисунок 4.31 – Сравнение среднего времени успешного завершения оригинального ZRTP, первой и второй модификаций ZRTP а) *d*=50 мс; б) *d*=100 мс; в) *d*=150 мс; г) *d*=200 мс; д) *d*=300 мс; е) *d*=400 мс

Проведено исследование ВВХ протоколов DTLS и ZRTP, согласно предложенной методике вычислены среднее время успешного завершения и вероятность успешного завершения.

Для протокола ZRTP выполнена экспериментальная оценка среднего времени успешного завершения, а также выполнено сравнение полученной оценки с рассчитанным по методике значением. На основании сравнения сделан вывод о совпадении теоретических и практических результатов.

Показано, что в каналах с высокой задержкой протоколу ZRTP требуется достаточно большое время на установление защищенного соединения, что отрицательно сказывается на соблюдении норм на время установления голосового канала между корреспондентами.

Исходя из вышеописанного, модернизация протокола распределения ключей является актуальной задачей, позволяющей сохранить преимущества протокола ZRTP, при этом ускорив выполнение протокола при работе по каналам с большими задержками.

Разработан метод улучшения временных характеристик криптографического протокола ZRTP, состоящий в исключении механизма распределения ролей инициатора и респондента, а также в объединении информационного блока данных о поддерживаемых корреспондентами криптографических наборах с блоком данных протокола Диффи-Хелмана.

Выигрыш B_2 по сравнению с исходным ZRTP составил от 39,42% до 48,3%, позволив при задержке до 300 мс сократить время успешного выполнения протокола до 1,45, 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 снизить вероятность успешной атаки MITM на 3 порядка, 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 позволят 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 с 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 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" 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.

Апробация материалов диссертационной работы проводилась на конференциях: «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; II-й Международной научно-технической конференции «Актуальные проблемы инфотелекоммуникаций в науке и образовании”,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 г. Новосибирск, 13 ноября 2013 г; IX Санкт-Петербургской межрегиональной

конференции Информационная безопасность регионов России (ИБРР-2015) 28-30 октября 2015 г; 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 на предприятии ООО "Телкон", в Управлении Роскомнадзора по Северо-Западному федеральному округу, а также внедрены в преподавании курсов “Безопасность IP-телефонии” в СПб ГУТ им М.А. Бонч-Бруевича на кафедре Защищенных Систем Связи.

По теме диссертации опубликовано 16 работ, из которых 5 в журналах Информационно – управляющие системы, Фундаментальные исследования, Электросвязь, входящих в перечень рекомендованных ВАК, и 7 публикаций на конференциях, 4 из которых являются международными.

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

Список сокращений и условных обозначений

ВВХ – вероятностно-временные характеристики

ДКБП – дискретный канал без памяти

ДХ - Диффи-Хелман

МСЭ – Международный Союз Электросвязи

НСД - несанкционированный доступ

ПРК – протокол распределения ключей

ПФ – производящая функция

СПД – Сеть Передачи Данных

ТфОП – Телефонная сеть общего пользования

CoS – Class of Service

DSCP – Differentiated Services Code Point

DTLS – Datagram Transport Layer Security

H.323 – рекомендация ITU-T, определяющий набор стандартов для передачи мультимедиа-данных по сетям с пакетной передачей.

IP PBX – IP-АТС, учрежденческая телефонная станция на основе межсетевого протокола IP

IP АТС – учрежденческая телефонная станция на основе межсетевого протокола IP

MGCP – Media Gateway Control Protocol

MIKEY – Multimedia Internet KEYing

MiTM – Man in The Middle

MPLS – Multiprotocol Label Switching

MPLS-EXP – MPLS experimental bits

PKI – Public Key Infrastructure

QoS – Quality of Service

RTP – Real-time Transport Protocol

RTP/AVP Real-time Transport Protocol / Audio Video Profile

SAS – Short Authentication String

SDES –Session Description Protocol Security

SG – Signaling Gateway

SIP – Session Initiation Protocol

SRTCP –Secure Real-time Transport Control Protocol

SRTP – Secure Real-time Transport Protocol

SSIP – Secured SIP

TLS – Transport Layer Security

ToS – Type of Service

UDP – User Datagram Protocol

VoIP – Voice over IP, голос по IP-сетям

ZRTP – Zimmermann Real-time Transport Protocol

Список литературы

1. Росляков А.В. IP-телефония / А.В. Росляков., М.Ю. Самсонов, И.В.Шибаева. – М.:Эко-трендз,2003. – 256 с.
2. Нопин, С.В. Разработка защищенных от несанкционированного доступа систем IP-телефонии на основе операционной системы Windows / С.В. Нопин, В.Г. Шахов // Омский научный вестник. 2006. – №9(46). – С.137-142.
3. Нопин, С.В. Передача мультимедийных данных по цифровым каналам в режиме, защищенном от несанкционированого доступа: дис. канд. техн. наук. – Новосибирск: Омский государственный технический университет, 2008. - 233 с.
4. Нопин, С.В. Разработка защищенной от несанкционированного доступа системы IP-телефонии, функционирующей в операционной системе Windows / С.В. Нопин // Научная сессия ТУСУР-2007: Материалы докладов всероссийской научно-технической конференции студентов, аспирантов и молодых ученых, Томск, 3-7 мая, 2007 г. Томск: В-Спектр, 2007. Ч.2. с. 177-179.
5. Говор Т. А. Обеспечение безопасности современных VOIP-сетей / Т. А. Говор // Радиопромышленность. – 2011.– № 4.– с. 37–43.
6. Докучаев В.А. Защита информации на корпоративных сетях VoIP / В.А. Докучаев, А.В. Шведов // Электросвязь. –2012. –№ 4.– с. 5–8.
7. Макарова О. С. Методика формирования требований по обеспечению информационной безопасности сети IP-телефонии от угроз среднестатистического «хакера» / О. С. Макарова // Докл. Томского государственного университета систем управления и радиоэлектроники. –2012. –№ 1. с. 51–67.
8. Крюков, Ю. С. Безопасность VolP-контента. Текущая ситуация, анализ угроз и тенденции рынка / Ю. С. Крюков // Защита информации. INSIDE. – 2008. - №.3.– с. 83-99
9. Onica E. Securing the Media Stream Inside VoIP SIP Based Sessions Technical Report. /Onica E.// Technical report TR 09-01, October 2009. Режим доступа: http://thor.info.uaic.ro/~tr/tr09-01.pdf (дата обращения: 25.02.2014).
10. Bresciani R. ProVerif Analysis of the ZRTP Protocol/ Bresciani R. Butterfield A.// International Journal for Infonomics. – 2010. – V.3. – №3. – P.306–313
11. Атрощенко В.А. К вопросу оценки достоверности информации для предотвращения MITM-атаки при передаче закрытой информации по открытым каналам связи / Атрощенко В.А., Руденко М.В., Дьяченко Р.А., Багдасарян Р.Х. //Современные проблемы науки и образования. –2013– №. 3. – с. 82-88.
12. Canteaut A. Sieve-in-the-middle: improved mitm attacks /Canteaut A., Naya-Plasencia M., Vayssière B.// Lecture Notes in Computer Science. 2013. Т. 8042 LNCS. № PART 1. С. 222-240. Режим доступа: http://eprint.iacr.org/2013/324.pdf (Дата обращения: 22.04.2014)

13. Sun H. Survey of authentication in mobile IPv6 network /Sun H., Song J., Chen Z. // 2010 7th IEEE Consumer Communications and Networking Conference, CCNC 2010 Las Vegas, NV, 2010. С. 1-4.
14. Радивилова, Т.А., Анализ основных атак на dns-сервер и методы использования DNSSec при защите DNS-сервера / Т.А. Радивилова, В.С. Бушманов // Технологический аудит и резервы производства. –2013– Т. 2. № 1 (10).– С. 16-19.
15. Карпухин, Е.О., Метод формирования сетевых пакетов для защиты от информационных атак «человек посередине» в телекоммуникационных сетях / Е.О. Карпухин, В.Ю. Михайлов // Вопросы радиоэлектроники. – 2013– Т. 3. № 2. – С. 83-93.
16. Сухов, А. М. Научные основы анализа качества интернет трафика: диссертация на соискание ученой степени доктора технических наук по специальности 05.13.13/ Сухов Андрей Михайлович– Самара.:2007– 232 с.
17. Мошак, Н.Н. Модель сигнального трафика в защищенной мультисервисной сети / Н.Н. Мошак, С.Р. Рудинская// XVIII международная научно-техническая конфереция «Современные средства связи». Минск, 15-16 октября 2013 г.: Материалы конференции / Высший государственный колледж связи. – г. Минск, 2013. – С. 45-47
18. Федосеева, О.С. "Исследование особенностей обеспечения характеристик качества обслуживания различных типов трафика в NGN-мультисервисных сетях" [Электронный ресурс] / О. С. Федосеева – Режим доступа: http://masters.donntu.edu.ua/2007/kita/fedoseeva/diss/diss.htm (Дата обращения: 22.04.2014)
19. E. Gelenbe Cognitive Packet Networks: QoS and Performance / E. Gelenbe, R. Lent, A. Montuori , Z. Xu // School of Electrical Engineering and Computer Science, University of Central Florida, Orlando, FL 32816 [Электронный ресурс] – Режим доступа:
http://pdf.aminer.org/000/339/717/cognitive_routing_in_packet_networks.pdf (Дата обращения: 22.04.2014)
20. Lijing Ding Performance Study of Objective Voice Quality Measures in VoIP/ Lijing Ding, Radwan, A., El-Hennawey, M.S., Goubran, R.A.//ISCC 2007: P. 197-202 Режим доступа: http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=4381543&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxpls%2Fabs_all.jsp%3Farnumber%3D4381543 (Дата обращения: 22.09.2012)
21. Nikitin V., Yurkin D., Chilamkurti N. The influence of the cryptographic protocols on the quality of the radio transmission . // Proc. of International Conference on Ultra Modern Telecommunications. – ICUMT-2009, St.-Petersburg, Russia. P. 1–5.
22. Никитин, В. Н. Улучшение способов аутентификации для каналов связи с ошибками / В. Н. Никитин, Д. В. Юркин // Информационно-управляющие системы. – №6. – 2010. –С .42–46.

23. Никитин, В.Н. Анализ протоколов шифрования / В.Н. Никитин, Д.В. Юркин // Журнал радиоэлектроники. – 2009. – № 4. – С. 7.
24. Нсангу М. М. Разработка вероятностных моделей для анализа показателей эффективности установления сессий в мультисервисной сети : диссертация на соискание ученой степени кандидата физико-математических наук по специальности 05.13.17 / Нсангу Мушили Мама – М.:2012 – 105 с.
25. Д. В. Юркин, А. В. Винель, В. В. Таранин Анализ временных и сложностных характеристик парольной аутентификации в защищенных операционных системах семейства UNIX // Информационно-управляющие системы - № 3 (64) - 2013 - С. 62 - 66.
26. Галкин А.М. Галкин Анатолий Михайлович сследование вероятностно-временных характеристик и протоколов построения маршрутов в сетях Metro Ethernet 2008 , Санкт-Петербургском государственном университете телекоммуникаций им. проф. М.А. Бонч-Бруевича (рук Г.Г. Яновский)
27. Петров, М.Н. Об одном методе оценки вероятностно-временных характеристик сетей обработки информации / М.Н. Петров, Д.Ю. Пономарев // Вестник Сибирского государственного аэрокосмического университета им. академика М.Ф. Решетнева. – 2007. – № 4. – С. 28-31.
28. Ю.И. Лосев, К.М. Руккас Методика определения вероятности доставки пакетов за заданное время // Проблемы телекоммуникаций - № 2 (2). - 2010. - С. 69-76. (электронный журнал, Харьковский национальный университет радиоэлектроники, главный корпус, третий этаж, ауд. 305а, просп. Ленина, 14, Харьков, Украина, 61166.)
29. Миронова, В.Г. Модель нарушителя безопасности конфиденциальной информации / В.Г. Миронова, А.А. Шелупанов // Информационная безопасность систем. – 2012. – № 1. с. 28-35.
30. Мещеряков, Р.В. Комплексное обеспечение информационной безопасности автоматизированных систем: Монография. / Мещеряков Р.В., Шелупанов А. А. – Томск:В-Спектр, 2007. – 278 с.
31. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (Выписка) / [Электронный ресурс]: Выписка ФСТЭК России 15 февраля 2008г. Режим доступа справ.-правовая система «КонсультантПлюс».
32. Десницкий, В. А. Обобщенная модель нарушителя и верификация информационно-телекоммуникационных систем со встроенными устройствами/ Десницкий В. А., Чеулин А. А. // Технические науки — от теории к практике. Сб. ст. по материалам XXXIX междунар. науч.-практ. конф. – Новосибирск: Издательство СибАК – 2014. – №10(35) – С. 7-20
33. Бахметьев, Б. Безопасность VoIP-соединений / Бахметьев Б. // Первая миля. - 2014. - № 2 (41). - С. 88-93.
34. Балашов, Д. Безопасность VoIP / Балашов Д. // Технологии и средства связи. - 2013. - № 4 (97). - С. 38-40.

35. Синюк, А.Д. Математическая модель нарушителя открытого ключевого согласования сети с минимальным числом корреспондентов/А.Д. Синюк, О.А. Остроумов //Наукоемкие технологии в космических исследованиях Земли. - 2013. - Т. 5. № 1.- С. 20-24.
36. Шабуров, А.С. Моделирование оценки угроз безопасности информационных систем персональных данных/А.С. Шабуров, С.А. Юшкова, А.В. Бодерко // Вестник ПНИПУ. – 2013. – № 7. С. 149–159.
37. RFC 3550 (2003) – A Transport Protocol for Real-Time Applications – Режим доступа: http://www.ietf.org/rfc/rfc3550.txt (Дата обращения: 22.09.2012)
38. RFC 3261(2002) - SIP: Session Initiation Protocol. – Режим доступа:http://www.ietf.org/rfc/rfc3261.txt (Дата обращения: 22.04.2014)
39. Гольдштейн Б.С. IP-телефония. / Б.С.Гольдштейн, А.В.Пинчук, А.Л.Суховицкий. - М.: Радио и связь, 2003.–336 с.
40. Гольдштейн, Б. С. Протокол SIP. Справочник / Гольдштейн Б.С., Зарубин А.А., Саморезов В.В. – СПб.:БХВ-Петербург, 2005 – 456 с.
41 Глотов, В. Правовые вопросы рынка VoIP / Глотов В. // Первая миля. - 2014. - № 2 (41). - С. 118-120.
42. 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
43. Рекомендация Y.1291 (05/2004) – An architectural framework for support of Quality of Service in packet networks [Электронный ресурс] – Режим доступа: https://www.itu.int/rec/dologin_pub.asp?lang=e&id=43!!PDF-E&type=items (Дата обращения: 22.04.2014)
44. Гольдштейн, А.Б. Softswitch/ Гольдштейн А.Б., Гольдштейн Б.С. – Спб.:БХВ – Санкт-Петербург, 2006. – 368 с.
45. Рекомендация ITU-T Y.1541(12/2011) Требования к сетевым показателям качества для служб, основанных на протоколе IP [Электронный ресурс] – Режим доступа: http://www.itu.int/ITU-T/recommendations/rec.aspx?rec=11462&lang=ru (Дата обращения: 22.04.2014)
46. Рекомендация ITU-T G.114(12/2011) One-way transmission time [Электронный ресурс] – Режим доступа: https://www.itu.int/rec/T-REC-G.114/en (Дата обращения: 22.04.2014)
47. Об утверждении Требований к организационно-техническому обеспечению устойчивого функционирования сети связи общего пользования/ приказ Министерства информационных технологий и связи Российской Федерации от 27.09.2007 № 113. Минюст РФ 22 октября 2007 г. N 10380. [Электронный ресурс] – Режим доступа справ.- правовая система «КонсультантПлюс».
48. Яновский, Г.Г. Качество обслуживания в сетях IP / Г.Г. Яновский // Вестник связи. – 2008. – № 1. с 1-16

49. Comer, D. Internetworking With TCP/IP Vol I:Principles, Protocols, and Architecture/ D. Comer. – New Jersey: Pearson Education, Inc.,2014. – 698 p.
50. Григорьев, В. А. Анализ пропускной способности сети радиосвязи стандарта IEEE 1609 / Григорьев В.А., Никитин В.Н., Кузнецов В.И., Тараканов С.А., Ковцур М.М. //Электросвязь.–2014– №.1.–с. 10-12
51. RFC 2676 (08/1999) – QoS Routing Mechanisms and OSPF Extensions [Электронный ресурс]. – Режим доступа: http://tools.ietf.org/html/rfc2676.html (Дата обращения: 22.04.2014)
52. Рекомендация ITU-T G.107 (02/2014) The E-model: a computational model for use in transmission planning [Электронный ресурс]. – Режим доступа: http://www.itu.int/rec/T-REC-G.107 (Дата обращения: 22.04.2014)
53. Perlicki, K. Simple analysis of the impact of packet loss and delay on voice transmission quality. / Perlicki K. // Journal of telecommunications and information technology. – 2002. – No. 2. – C. 53-56
54. Математические модели и алгоритмы анализа и оптимизации функционирования локальной компьютерной сети: дис. канд. техн. наук : 05.13.13 /Аль-Шрайдех Халед Садек – М.:2007 – 173 с.
55. Каримжанова А.С. Исследование возможности улучшения качества предоставления услуг в мультисервисных сетях передачи: пояснительная записка к магистерской диссертации по специальности 6М071900, Некоммерческое акционерное общество «Алматинский университет энергетики и связи», Алматы 2013 [Электронный ресурс]. – Режим доступа: http://www.aipet.kz/student/mag_disser/2013/karimzhanova_ainur.pdf (Дата обращения: 30.04.2014)
56. Малаховский, А.А. Организация мультимедийной связи в сетях с низкоскоросными и нестабильными каналами связи / А.А. Малаховский, Н.И. Лычагин, А.С. Гузарев // Техника средств связи: Научно-технический сб. – №1 (140). – СПб: Политехнический университет, 2012. С 88-95
57. 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.
58. RFC 3711 (2004) – The Secure Real-time Transport Protocol (SRTP) [Электронный ресурс]. – Режим доступа: http://www.ietf.org/rfc/rfc3711.txt (дата обращения: 10.09.2013)
59. Никитин, В.Н. Обеспечение информационной безопасности ИТС /Никитин В.Н., Лагутенко О.И., Ковцур М.М. //Электросвязь.–2014– №.1.–с. 29-31
60. RFC 3830(08/2004) – MIKEY: Multimedia Internet KEYing [Электронный ресурс]. – Режим доступа: http://tools.ietf.org/html/rfc3830 (дата обращения: 25.10.2013).
61. RFC 6309(08/2011) – IANA Rules for MIKEY (Multimedia Internet KEYing) [Электронный ресурс]. – Режим доступа: http://tools.ietf.org/html/rfc6309 (дата обращения: 25.10.2013).

62. RFC4568 (07/2006) – Session Description Protocol (SDP) Security Descriptions for Media Streams [Электронный ресурс]. – Режим доступа: http://tools.ietf.org/html/rfc4568 (дата обращения: 25.02.2014).
63.RFC 5764. Datagram Transport Layer Security (DTLS) Extension to Establish Keys for the Secure Real-time Transport Protocol (SRTP). [Электронный ресурс]. — Режим доступа: http://tools.ietf.org/html/rfc5764 (дата обращения: 29.10.2013).
64. RFC6189 (04/2011) – ZRTP: Media Path Key Agreement for Unicast Secure RTP – Режим доступа: http://tools.ietf.org/html/rfc6189 (дата обращения: 25.02.2014).
65. Ковцур, М.М. Протоколы обеспечения безопасности IP-телефонии. / М.М. Ковцур // Первая миля. – 2012. – №5. – С.18-26.
66. Bresciani, R. Formal security proof for the ZRTP Protocol/ Bresciani, R. , Butterfield, A. // International Conference for Internet Technology and Secured Transactions. London, 9-12 Nov. 2009 ICITST.–2009. – P. 1-6
67. Shmatikov V. Security Analysis of Voice-over-IP Protocols / V. Shmatikov, P. Gupta // The University of Texas at Austin, Computer Security Foundations Symposium, 2007. CSF '07. 20th IEEE. [Электронный ресурс]. — Режим доступа: https://www.cs.utexas.edu/~shmat/shmat_csf07.pdf (дата обращения: 25.02.2014).
68. Charles V. W Spot me if you can:Uncovering spoken phrases in encrypted VoIP conversations /Charles V. W., Ballard L.. Coull S. E. , Monrose F., Masson G. M. // Johns Hopkins University Baltimore, MD USA 21218, 2008 [Электронный ресурс]. — Режим доступа: http://www.cs.jhu.edu/~cwright/oakland08.pdf (дата обращения: 25.02.2014).
69. ГОСТ Р ИСО/МЭК 15408-1—2012, Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель. М.: Изд. Стандартинформ, 2014
70. Привалов, А.А. Модель процесса вскрытия параметров сети передачи данных оператора IP-телефонной сети компьютерной разведкой организованного нарушителя /Привалов А.А., Евглевская Н.В., Зубков К.Н. // Известия петербургского университета путей сообщения. -2014 -№2 (39).- С. 106-111
71. ГОСТ Р ИСО/МЭК 15408-2-2013 - Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные компоненты безопасности– 2013 – М.: Изд. Стандартинформ России, 2014.
72. Лопатников Л. И. Экономико-математический словарь: Словарь современной экономической науки./ Л. И. Лопатников — 5-е изд., перераб. и доп. — М.: Дело, 2003. — 520 с.
73. Красов, А.В. Методика построения системы обнаружения вторжений для voip-трафика/А.В. Красов, Д.И. Кириллов //63-я научно-техническая

конференция профессорско-преподавательского состава, научных сотрудников и аспирантов СПбГУТ. – СПб.: СПбГУТ, 2011, т1. – С.248-249.
74. Ковцур М.М. Исследование путей совершенствования протоколов распределения ключей в защищенной IP-телефонии / М.М. Ковцур //Фундаментальные исследования. – 2014 – № 8(часть 6). – С. 1300-1308.
75. Статистика уязвимостей корпоративных информационных систем (2013 год) [Электронный ресурс]. — Режим доступа: http://www.ptsecurity.ru/download/PT_Corporate_vulnerability_2014_rus.pdf (дата обращения: 20.08.14).
76. PGPfone Pretty Good Privacy Phone Owner's Manual ,Version 1.0 beta 7 -8 July 1996 Philip R. Zimmermann [Электронный ресурс]. — Режим доступа: ftp://ftp.pgpi.org/pub/pgp/pgpfone/manual/pgpfone10b7.pdf (дата обращения: 29.10.2013).
77. АНБ занимается экономическим шпионажем [Электронный ресурс]. — Режим доступа: http://www.securitylab.ru/news/444645.php/ (дата обращения: 01.05.13).
78. Facebook не может защитить пользователей от MITM-атак [Электронный ресурс]. — Режим доступа: http://www.securitylab.ru/news/450391.php / (дата обращения: 01.05.13).
79. Wi-Fi spies - 34% use no protection at Wi-Fi hot spots [Электронный ресурс]. — Режим доступа: http://www.kaspersky.com/about/news/press/2013/Wi-Fi_spies_-_34_percent_use_no_protection_at_Wi-Fi_hot_spots / (дата обращения: 01.05.13).
80. Таргетированные MiTM-атаки с перенаправлением интернет-трафика по BGP [Электронный ресурс]. — Режим доступа: http://www.xakep.ru/post/61620/default.asp (дата обращения: 01.05.2014).
81. 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: 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
82. Шварцман, В.О. Теория передачи дискретной информации: учебник для вузов связи/ В.О. Шварцман, Г.А. Емельянов. – М.: Связь, 1979. – 424 с.
83. Радько, Н.М Сравнительная оценка вероятностно-временных характеристик преодоления парольной защиты/ Н.М.Радько, В.М. Аксютин, Д.Н. Курдяев, А.С. Суховерхов // Информация и безопасность. – 2007. –Т. 10. № 3.– С. 439-444.
84. Advanced Encryption Standard [Электронный ресурс]. – Режим доступа: http://ru.wikipedia.org/wiki/Advanced_Encryption_Standard#cite_note-19 (Дата обращения 02.03.2013)

85. Никитин, В.Н. Пути совершенствования протоколов распределения ключей для IP-телефонии / В.Н. Никитин, М.М. Ковцур // 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. С 852 - 855
86. Коржик, В.И. Основы криптографии/В.И. Коржик, В.П. Просихин, В.А.Яковлев - СПб.: СПбГУТ, 2014. - 276 с.
87. Яковлев, В. А. Протоколы формирования ключа на основе каналов связи с шумом в условиях активного перехвата с использованием экстракторов / В. А. Яковлев, В. И. Коржик, М. В. Бакаев // Проблемы информационной безопасности. Компьютерные системы. – 2006. – № 1. – С. 51–67.
88. Лобашев, А.И. Защита сигнально-управляющего трафика стохастическими методами /А.И. Лобашев А.И., С.В. Баранов С.В., И.В. Симоненко И.В., Е.В. Шалашов //Вопросы оборонной техники. Серия 16: Технические средства противодействия терроризму. - 2015. - № 3-4.- С. 32-34.
89. Яковлев, В.А.Распределения ключей в беспроводных локальных сетях на основе использования антенн с изменяемой диаграммой направленности в условиях многолучевого распространения радиоволн. часть 2. система распределения ключей и ее оптимизация / В.А. Яковлев, В.И. Коржик, Ю.В. Ковайкин //Проблемы информационной безопасности. Компьютерные системы. – 2011. – № 1. – С. 87-99.
90. Коржик, В.И. Протокол выработки ключа в канале с помехами. / В.И. Коржик, В.А. Яковлев, А.Д. Синюк. // Проблемы информационной безопасности. Компьютерные системы. – 2000. – № 1. – С. 52.
91. Синюк А.Д. Информационно-теоретическая модель формирования ключа по открытым каналам без ошибок / А.Д. Синюк , А.В. Козленко, К.А. Чирушкин //Труды СПИИРАН. - 2010. № 2(13). С. 156-170
92. Демьянчук А.А. Способ повышения уровня безопасности протоколов аутентификации с нулевым разглашением секрета/ А.А. Демьянчук , Е.С. Новикова, Д.Н. Молдовян// Материалы VIII СПб межрегион. конф.«Информационная безопасность регионов России (ИБРР-2013)».- Спб.:ООО «К-8» - 2013 - С. 51-52.
93. C++ Implementation of ZRTP protocol - GNU ZRTP C++ [Электронный ресурс]. – Режим доступа: https://github.com/wernerd/ZRTPCPP (Дата обращения 12.06.2014)
94. ZRTP Protocol Library [Электронный ресурс]. – Режим доступа: http://freecode.com/projects/libzrtpcpp (Дата обращения 10.06.2014)
95. Перфильев, Ю.Ю. Российское интернет-пространство: развитие и структура / Ю.Ю. Перфильев. – М.:Гардарики, 2003. – 272 с.
96. Кипчатов А. Введение в индустрию интернета: структура провайдинга [электронный ресурс] // Сайт ООО "Наг". — 2007.— Режим доступа:

http://nag.ru/articles/reviews/15477/vvedenie-v-industriyu-interneta-struktura-provaydinga.html (дата обращения 02.11.2013)
97. Рынок телекоммуникаций в России — что, где, как [Электронный ресурс]. – Режим доступа: http://habrahabr.ru/post/113086/ (Дата обращения 07.05.2014)
98. Tier 1 network Definition from PC Magazine Encyclopedia [Электронный ресурс]. – Режим доступа: http://www.pcmag.com/encyclopedia/term/60763/tier-1-network (Дата обращения 02.05.2014)
99. Tier-1-операторы [Электронный ресурс]. – Режим доступа: http://ru.wikipedia.org/wiki/Tier-1-операторы (Дата обращения 02.03.2013)
100. The Cooperative Association for Internet Data Analysis [Электронный ресурс]. – Режим доступа: http://as-rank.caida.org/ (Дата обращения 02.03.2013)
101. S Rank: AS 12389 OJSC Rostelecom -- AS Relationship Graph - CAIDA : http://as-rank.caida.org [Электронный ресурс]. – Режим доступа: http://as-rank.caida.org/?mode0=as-info&mode1=as-graph&as=12389 (Дата обращения 05.06.2014)
102. Ковцур, М.М. Исследование непересекающихся маршрутов глобальной сети / Ковцур М.М. // VI международная научно-практическая конференция "Наука вчера, сегодня, завтра." №6. материалы конф. – Новосибирск:Издательство СибАК – 2013. – С. 19-24.
103. Geo IP Tool [Электронный ресурс]. – Режим доступа: http://www.geoiptool.com/ (Дата обращения 20.06.2014)
104. Коржик, В. И. Основы криптографии/ В. И. Коржик, В. П. Просихин – СПб.: Линк, 2008. – 256 с.
105. Пат. 2183348 Российская Федерация, G06F12/14, H04L9/32. Способ аутентификации объектов/ Молдовян А. А., Молдовян Н. А., Никитин В. Н., Фокин А. О. – № 2000119274/09; заявл. 19.07.2000; опубл. 10.06.2002, Бюл. № 6. – 9 с.: ил.
106. Кирюшкин, С.А. Трансграничный юридически-значимый документооборот: нюансы решений актуального вопроса / С.А. Кирюшкин // Connect! Мир связи – 2011. – № 4. – С. 120-123.
107. Липатников, В.А. Метод многоуровневой проактивной информационной безопасности компьютерной сети / Липатников В.А., Костарев С.В., Корольков А.П. // Проблемы управления рисками в техносфере.– 2014.– № 1 (29) – С. 81-89.
108. 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.
109. 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.
110. Красов, А.В., О вероятностно-временных характеристиках синхронизации систем передачи с широкополосными сигналами / А.В. Красов,

М.М. Ковцур, В.Н. Никитин //Труды конференции Телекоммуникационные и вычислительные системы, 28 ноября 2012 г.–М.: Московский технический университет связи и информатики, 2012. – с. 142
111. Юркин, Д.В. Сравнение стойкости реализаций протокола при выборе различных криптографических систем / Юркин Д.В., Никитин В.Н.// Защита информации. Инсайд. – 2008. №6.–С. 17–21.
112. Ковцур, М.М. Исследование ВВХ протоколов обеспечения безопасности VoIP телефонии при работе по каналам связи с ошибками. / М.М. Ковцур // Международная научно-техническая и научно-методическая конференции "Актуальные проблемы инфотелекоммуникаций в науке и образовании" №64.: материалы конф. – СПб.: Издательство СПбГУТ, 2012. – С. 235 - 236.
113. Eppinger, S. D. Generalized Models of Design Iteration Using Signal Flow Graphs / S. D. Eppinger, M. V. Nukala, D. E. Whitney // Research in Engineering Design. – 1997.– V. 9, – No. 2 – C. 112-123.
114. Ковцур, М. М. Оценка вероятностно-временных характеристик защищенной IP-телефонии / М. М. Ковцур, В. Н. Никитин // Защита информации. Инсайд. – 2012. №4. – С. 38-44.
115. Никитин, В. Н. Улучшение способов аутентификации для каналов связи с ошибками / В. Н. Никитин, Д. В. Юркин // Информационно-управляющие системы. – 2010 – №6.– С. 42–46.
116. Коржик В.И. Error detecting codes. General theory and their application in feedback communication systems / В.И. Коржик, T. Klove. – Kluwer Acdemic Publishers, 1995. – 247 с.
117. С.Мэзон Электронные цепи, сигналы и системы / С.Мэзон, Г.Циммерман. – М.: издательство иностранной литературы, 1963. – 622 с.
118. RFC6347 (01/2012) Datagram Transport Layer Security Version 1.2 [Электронный ресурс]. – Режим доступа: http://tools.ietf.org/html/rfc6347 (дата обращения 02.09.2013)
119. RFC 6298 - Computing TCP\x27s Retransmission Timer RFC6298 [Электронный ресурс]. – Режим доступа: https://tools.ietf.org/html/rfc6298 (дата обращения 02.09.2014)
120. Menezes, A. J. Handbook of Applied Cryptography / A. J. Menezes, P. C. van Oorschot, S. A. Vanstone. – CRC Press LLC, 1996. – 780 p.
121. 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» / Межрегиональный открытый социальный институт (МОСИ). – Йошкар-Ола. – 2012. –С. 30–35.
122. Ковцур, М.М. Оптимизация вероятностно-временных характеристик криптографического протокола распределения ключей IP-телефонии / М.М. Ковцур // Universum: технические науки. – 2014. – № 2 (3). – С. 1-9.

Приложение А. Акты о внедрении

РОСКОМНАДЗОР

УПРАВЛЕНИЕ ФЕДЕРАЛЬНОЙ СЛУЖБЫ ПО НАДЗОРУ В СФЕРЕ СВЯЗИ, ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И МАССОВЫХ КОММУНИКАЦИЙ ПО СЕВЕРО-ЗАПАДНОМУ ФЕДЕРАЛЬНОМУ ОКРУГУ
(Управление Роскомнадзора по Северо-Западному федеральному округу)

ул. Галерная, д.27, Санкт-Петербург, 190000
тел.: (812) 5719566; факс (812) 5712731
E-mail: rsockanc78@rkn.gov.ru

17.04.2014 № 6545-03/78
на № _____ от _____

УТВЕРЖДАЮ
Руководитель Управления
Роскомнадзора по Северо-Западному
федеральному округу, к.т.н.

_____ Д. В. Сахаров

АКТ
о внедрении научных результатов,
полученных Ковцуром Максимом Михайловичем

Комиссия в составе: председателя - Сёмина Владимира Юрьевича, заместителя руководителя - начальника отдела надзора в сфере электросвязи, членов комиссии: Потехина Игоря Юрьевича, к.ф.-м.н., начальника отдела административного обеспечения; Иванова Игоря Борисовича, к.в.н., доцента, главного специалиста-эксперта отдела надзора в сфере использования и регистрации РЭС и ВЧУ, составила настоящий акт о том, что при разработке методики контроля защищенных сетей электросвязи использованы следующие материалы диссертационной работы, полученные Ковцуром Максимом Михайловичем, а именно:

1. Математическая модель активного нарушителя для защищенной IP-телефонии;
2. Методы повышения информационной безопасности для протоколов распределения ключей, основанных на алгоритме Диффи-Хелмана.

Комиссия отмечает практическую значимость и новизну полученных в работе результатов.

Председатель комиссии: В.Ю. Сёмин

Члены комиссии: И.Ю. Потехин

И.Б. Иванов

04046

МИНИСТЕРСТВО
СВЯЗИ И МАССОВЫХ КОММУНИКАЦИЙ
РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ АГЕНТСТВО СВЯЗИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ
ОБРАЗОВАТЕЛЬНОЕ БЮДЖЕТНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ
«САНКТ-ПЕТЕРБУРГСКИЙ
ГОСУДАРСТВЕННЫЙ
УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ
ИМ. ПРОФ.М.А. БОНЧ-БРУЕВИЧА»
(СПбГУТ)

Юридический адрес: набережная реки Мойки,
д. 61, Санкт-Петербург, 191186

Почтовый адрес: пр. Большевиков, д. 22, корп. 1,
Санкт-Петербург, 193232
Тел.(812) 3263156, Факс: (812) 3263159
E-mail: rector@sut.ru
ИНН 7808004760 КПП 784001001
ОГРН 1027809197635 ОКТМО 40909000

31.03.2015 № 754/79
на №_____ от_____

УТВЕРЖДАЮ

Первый проректор -
проректор по учебной работе,
д-р техн. наук, профессор

Г.М.Машков

АКТ
о внедрении научных результатов, полученных Ковцуром Максимом Михайловичем

Комиссия в составе:

- Просихина Владимира Павловича, д-ра техн. наук, профессора, заведующего кафедрой "Защищенные системы связи";

- Яковлева Виктора Алексеевича, д-ра техн. наук, профессора, профессора кафедры "Защищенные системы связи";

- Красова Андрея Владимировича, канд. техн. наук, доцента, профессора кафедры "Защищенные системы связи"

составила настоящий акт о том, что научные результаты, полученные Ковцуром Максимом Михайловичем, а именно:

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

использованы в учебном процессе при чтении лекций и проведении лабораторных работ бакалавров по специальностям 210700.62 «Инфокоммуникационные технологии и системы связи» и 090900.62 «Информационная безопасность», при чтении лекций и проведении лабораторных работ магистров по специальностям 210700.68 «Инфокоммуникационные технологии и системы связи» и 090900.68 «Информационная безопасность» по дисциплине “Безопасность IP-телефонии” в Санкт-Петербургском государственном университете телекоммуникаций им. проф. М.А. Бонч-Бруевича.

д-р. техн. наук, профессор, заведующий
кафедрой "Защищенные системы связи"; Просихин В. П.

д-р. техн. наук, профессор, профессор
кафедры "Защищенные системы связи" Яковлев В. А.

канд. техн. наук, доцент, профессор
кафедры "Защищенные системы связи" Красов А. В.

ООО “Телкон”

ул. Черняховского, д.10,

г. Санкт-Петербург, 191119

2.07.2014 № 237

На №_____ от _____

УТВЕРЖДАЮ
Генеральный директор
ООО “Телкон”

М. А. Чечельницкий

АКТ
о внедрении научных результатов,
полученных Ковцуром Максимом Михайловичем

Комиссия в составе:

- Алексеев Владимира Николаевича, ведущего инженера по направлению телекоммуникации;
- Тихомирова Дмитрия Евгеньевича, инженера по информационной безопасности;
- Гукина Виктора Александровича, инженера I-й категории;

составила настоящий акт о том, что научные результаты, полученные Ковцуром Максимом Михайловичем, а именно:

1. Методика оценки вероятностно-временных характеристик протоколов распределения ключей защищенной IP-телефонии;
2. Метод улучшения временных характеристик криптографического протокола ZRTP;
3. Метод повышения безопасности протоколов распределения ключей, основанных на алгоритме Диффи-Хелмана;
4. Метод автоматического обнаружения вторжений нарушителя в середину канала связи для протокола ZRTP.

использованы в отчете о научно-исследовательской работе "Исследование путей совершенствования характеристик протоколов IP-телефонии для внедрения в абонентских голосовых терминалах, предназначенных для работы по беспроводным каналам связи ": отчет о НИР (заключ.): 1-3/ ООО "Телкон"; рук. В.Н. Алексеев; исполн.: Тихомиров Д.В. [и др.]. – СПб., 2014. – 214 с. – Библиогр.: с. 201–213. –Инв. № 432521.

Ведущий инженер по направлению телекоммуникации В.Н. Алексеев

Инженер по информационной безопасности Д.Е.Тихомиров

Инженер I-й категории В.А. Гукин

Приложение Б. Листинг программы – поиск пар и троек маршрутов

Листинг программы – поиск троек маршрутов

```
<?
include 'conf.php';
?>
<html>
<head>
<title>TraceAnalyzer4</title>
<link rel="stylesheet" type="text/css" href="styles/style.css">
<meta http-equiv="content-type" content="text/html; charset=windows-1251">
<link rel='icon' href='favicon.ico' type='image/x-icon' />
<link rel='shortcut icon' href='favicon.ico' type='image/xicon' />
</head>
<body bgcolor="#ffffff" leftmargin=0 topmargin=0 marginwidth=0 marginheight=0>
<p><a href="#top">К итогам</a></p>
<p><a href="#tbl_itog">К таблицам итоговым анализа</a></p>
<p><a href="#tbl">К таблицам - исходные данные</a></p>
<?
$module["show_detail"]=0;
$anyrequestcondition=" AND tracerezult.dsc_city  ";
$rules ="SELECT  *  FROM tracerezult WHERE 1 ".$anyrequestcondition." ";
$rs = $db->Execute($rules);
$dataip=$rs->GetRows();
  //STARTS ALL PATH ANALYZ
  foreach ($dataip as $k => $Row) {
  $module["current"]=$Row;
  preg_match_all("/((25[0-5]|2[0-4]\d|[01]?\d\d?)\.){3}(25[0-5]|2[0-4]\d|[01]?\d\d?)|(([a-zA-Z0-9]([a-zA-Z0-9\-]{0,61}[a-
zA-Z0-9])?\.)+[a-zA-Z]{2,6})/",
              $Row["tracerezult"],  $matches4);
  if ($module["show_detail"])  echo "IP+Domains<pre>";
  if ($module["show_detail"])  print_r ($matches4[0]);
  if ($module["show_detail"])  echo "</pre>";
  $module["ipontheway"]="";
  $tr_id++; // Trace ID counter
  $module["path"]=$Row["src_provider"]."->".$Row["dsc_provider"]."".$Row["dsc_city"]."";
 foreach ($matches4[0] as $id => $value) $module["ipontheway"]= $module["ipontheway"].", ".$value;
  $tablerow[$tr_id]["path"]=$module["path"];
```

```
 $tablerow[$tr_id]["ipontheway"]=$module["ipontheway"];
 Echo 'module["current"]["src_city"]=',$module["current"]["src_city"];
    $dublicatesearchsql="SELECT tracerezult.id, tracerezult.src_ip, tracerezult.src_provider, tracerezult.src_country, tracerezult.src_city, tracerezult.dsc_ip, tracerezult.dsc_provider, tracerezult.dsc_country, tracerezult.dsc_city, tracerezult.tracerezult FROM tracerezult WHERE
tracerezult.dsc_city LIKE '".$module["current"]["dsc_city"]."' AND tracerezult.src_provider NOT LIKE '".$module["current"]["src_provider"]."' AND
tracerezult.dsc_provider NOT LIKE '".$module["current"]["dsc_provider"]."' AND tracerezult.id >= '".$module["current"]["id"]."' ";
    $module["dublicatemsg"]="";
    $ds = $db->Execute($dublicatesearchsql);
    $dublicatesearc=$ds->GetRows();
    foreach ($dublicatesearc as $k => $Rowd) { $module["dublicatemsg_per_cicle"]="";
     $module["dublicatemsg_ip_per_cicle"]="";
     $module["compare_id"]++; // shows numbe of compared, made by script
     //Exemining alternative way 2
     preg_match_all("/((25[0-5]|2[0-4]\d|[01]?\d\d?)\.){3}(25[0-5]|2[0-4]\d|[01]?\d\d?)|(([a-zA-Z0-9]([a-zA-Z0-9\-]{0,61}[a-zA-Z0-9])?\.)+[a-zA-Z]{2,6})/",$Rowd["tracerezult"], $matches21);
     $module["common_points"] = array_unique( array_intersect( $matches4[0],$matches21[0] ));
     $dublicatesearchsql3w="SELECT
tracerezult.id, tracerezult.src_ip, tracerezult.src_provider, tracerezult.src_country, tracerezult.src_city, tracerezult.dsc_ip,
tracerezult.dsc_provider, tracerezult.dsc_country, tracerezult.dsc_city, tracerezult.tracerezult FROM tracerezult WHERE
tracerezult.dsc_city LIKE '".$module["current"]["dsc_city"]."' AND tracerezult.src_provider NOT LIKE '".$module["current"]["src_provider"]."' AND
tracerezult.dsc_provider NOT LIKE '".$Rowd["dsc_provider"]."' AND tracerezult.src_provider NOT LIKE '".$Rowd["src_provider"]."' AND
tracerezult.dsc_provider NOT LIKE '".$Rowd["dsc_provider"]."' AND tracerezult.id >= '".$module["current"]["id"]."' AND tracerezult.id >= '". $Rowd["id"]."'
     ";
     $ds = $db->Execute($dublicatesearchsql3w);
     $dublicatesearc3w=$ds->GetRows();
     foreach ($dublicatesearc3w as $k3 => $Rowd3)
          {
          $module["dublicatemsg_per_cicle"]="";
          $module["dublicatemsg_ip_per_cicle"]="";
          $path=$Rowd["src_provider"]."->".$Rowd["dsc_provider"]."&".$module["current"]["src_provider"]."->".$module["current"]["dsc_provider"]."&".$Rowd3["src_provider"]."->".$Rowd3["dsc_provider"] ;
          preg_match_all("/((25[0-5]|2[0-4]\d|[01]?\d\d?)\.){3}(25[0-5]|2[0-4]\d|[01]?\d\d?)|(([a-zA-Z0-9]([a-zA-Z0-9\-]{0,61}[a-zA-Z0-9])?\.)+[a-zA-Z]{2,6})/",$Rowd3["tracerezult"], $matches31);
```

```
$module["common_points_1-2"] = array_unique( array_intersect( $matches4[0],$matches21[0] ));
$module["common_points_1-3"] = array_unique( array_intersect( $matches4[0],$matches31[0] ));
$module["common_points_3-2"] = array_unique( array_intersect( $matches31[0],$matches21[0] ));
 $idts=$module["current"]["dsc_city"];
$tablesovpadid[$idts]["country"]=$module["current"]["dsc_country"];
$tablesovpadid[$idts]["ciyt"]=$idts;
$tablesovpadid[$idts]["no_1_point"]=$tablesovpadid[$idts]["no_1_point"];
$tablesovpadid[$idts]["have_1_point"]=$tablesovpadid[$idts]["have_1_point"];
if (count($module["common_points_1-2"]))
    {$module["dublicatemsg_per_cicle"]=implode(",", $module["common_points_1-
2"]).",".$module["dublicatemsg_per_cicle"];
     $tablesovpadid[$idts]["3w_common_points"]++;
    }
if (count($module["common_points_1-3"]))
    {$module["dublicatemsg_per_cicle"]=implode(",", $module["common_points_1-
3"]).",".$module["dublicatemsg_per_cicle"];
    $tablesovpadid[$idts]["3w_common_points"]++;
    }
if (count($module["common_points_3-2"]))
    {$module["dublicatemsg_per_cicle"]=implode(",", $module["common_points_3-
2"]).",".$module["dublicatemsg_per_cicle"];
    $tablesovpadid[$idts]["3w_common_points"]++;
    }
echo "3W[",$module["compare_id"],"]:",$path,"<br>";
  //Analyze block
 if (strlen($module["dublicatemsg_per_cicle"])>3)
 {$module["dublicate"][$module["current"]["dsc_city"]][$path]="".$Rowd["src_provider"]."-
>".$Rowd["dsc_provider"]."";
 $module["itog"][$module["current"]["dsc_city"]]["have_1_point"][]=$path;
 $module["itog_count"][$module["current"]["dsc_city"]]["have_1_point"]++;
 $module["itog_count"][$module["current"]["dsc_city"]]["Prov"][$Rowd["dsc_provider"]]["have_1_point"]++;
 $tablesovpadid[$idts]["have_1_point"]++;
 $module["itog"][$module["current"]["dsc_city"]]["1_point_is"]=$module["dublicatemsg_ip_per_cicle"];
 }
 else {
 $module["itog"][$module["current"]["dsc_city"]]["no_1_point"][]=$path;
 $module["itog_count"][$module["current"]["dsc_city"]]["no_1_point"]++;
 $module["itog_count"][$module["current"]["dsc_city"]]["Prov"][$Rowd["dsc_provider"]]["no_1_point"]++;
 $tablesovpadid[$idts]["no_1_point"]++;
 }
```

```
            $tablesovpadid[$idts]["vsego"]=
$tablesovpadid[$idts]["no_1_point"]+$tablesovpadid[$idts]["have_1_point"];
            $tablesovpadid[$idts]["vsego2"]=
$tablesovpadid[$idts]["no_1_point"]+$tablesovpadid[$idts]["have_1_point"];
            $module["itog"][$module["current"]["dsc_city"]]["sql"]=$dublicatesearchsql;
            //End Analyze block
           if ($module["dublicatemsg_per_cicle"]) echo "Dublicates found:",$module["dublicatemsg_per_cicle"],"<br>";
            }
$module["tablesovpadid_comment"]="3w_common_points - счетчик совпадений 1-2, 2-3, 1-3;vsego2 -
вспомогательное; no_1_point/have_1_point  - число независимых / зависимых маршрутов ";
$module["show_detail"]=0;
if (count($module["common_points"]))
{echo "<br><h3>Compare - found dublicates</h3>matches4<pre>";
print_r ($matches4[0]);
echo "<br>matches21";
print_r ($matches21[0]);
echo "<br>common_points";
print_r ($module["common_points"]);
echo "</pre>";}
   $module["pathnumberanalyzed"]++;
   }
 }
 //END ALL PATH ANALYZ
echo " <p><a name='top'></a></p><br>", $module["pathnumberanalyzed"]/2," two-way paths were analyzed, <br> Ways
with 1pointdetected: (",$module["pathnumberwithMITMGlobal"],")",$module["pathnumberwithMITM"],"
:<br>",$module["pathnumberwithMITMGlobalT"],"<br>";
echo "<br><br> Ways with NO 1point detected:
(",$module["pathnumberNOMITMGlobal"],")",$module["pathnumberwithNOMITM"],"
:<br>",$module["pathnumberwithNOMITMGlobalT"],"<br>";
print "Ways with NO 1point detected:<pre>";  print_r($module["itog"]); print "</pre>";
print "COUNT with NO 1point detected:<pre>";  print_r( $module["itog_count"]); print "</pre>";
print "Dublicates via analyz<pre>";  print_r($module["dublicate"]); print "</pre>";
print "Bad ways for protocol<pre>";  print_r($module["badways"]); print "</pre>";
echo "<table border=1 >";
foreach ($tablerow as $row) {
        echo "<tr>";
        foreach ($row as $column) {
        echo "<td>$column</td>";
        }
        echo "</tr>";
}
```

```
echo "</table>";
echo " <p><a name='tbl_itog'></a> ",$module["tablesovpadid_comment"],"</p>";
echo "Таблица совпадений Город/Страна/Независимых маршрутов/Совпадающих троек маршрутов<table border=1 >";
  //t_HEADER
  foreach ($tablesovpadid as $row) {}
  echo "<tr>";
  foreach ($row as $rname => $column) {
    echo "<td>$rname</td>";
  }
  echo "</tr>";
  //t_CONTENT
  foreach ($tablesovpadid as $row) {
  echo "<tr>";
  foreach ($row as $rname => $column) {
    echo "<td>$column</td>";
  }
  echo "</tr>";
}
echo "</table>";
echo " <p><a name='tbl'></a> </p>";
```

Листинг программы – поиск совпадения пар маршрутов

```
<?
include 'conf.php';
?>
<html>
<head>
<title>TraceAnalyzer4</title>
<link rel="stylesheet" type="text/css" href="styles/style.css">
<meta http-equiv="content-type" content="text/html; charset=windows-1251">
<link rel='icon' href='favicon.ico' type='image/x-icon' />
<link rel='shortcut icon' href='favicon.ico' type='image/xicon' />
</head>
<body bgcolor="#ffffff" leftmargin=0 topmargin=0 marginwidth=0 marginheight=0>
```

```
<p><a href="#top">К итогам</a></p>

<p><a href="#tbl">К таблицам</a></p>

<?  $module["show_detail"]=0;

$rules ="SELECT  *  FROM  tracerezult WHERE 1 ".$anyrequestcondition." ";

$rs = $db->Execute($rules);

$dataip=$rs->GetRows();

    foreach ($dataip as $k => $Row) {

    $module["current"]=$Row;

    //ip only

    preg_match_all("/((25[0-5]|2[0-4]\d|[01]?\d\d?)\.){3}(25[0-5]|2[0-4]\d|[01]?\d\d?)/",

    $Row["tracerezult"],  $matches1);

    //ip+domain

    preg_match_all("/((25[0-5]|2[0-4]\d|[01]?\d\d?)\.){3}(25[0-5]|2[0-4]\d|[01]?\d\d?)|(([a-zA-Z0-9]([a-zA-Z0-9\-
]{0,61}[a-zA-Z0-9])?\.)+[a-zA-Z]{2,6})/",

    $Row["tracerezult"],  $matches4);

    if ($module["show_detail"])  echo "IP+Domains<pre>";

    if ($module["show_detail"])  print_r ($matches4[0]);

    if ($module["show_detail"])  echo "</pre>";

    $module["ipontheway"]="";

    $tr_id++;

    $module["path"]=$Row["src_provider"]."->".$Row["dsc_provider"]."".$Row["dsc_city"]."";

    foreach ($matches4[0] as $id => $value) $module["ipontheway"]= $module["ipontheway"].", ".$value;

    $tablerow[$tr_id]["path"]=$module["path"];

    $tablerow[$tr_id]["ipontheway"]=$module["ipontheway"];

    Echo 'module["current"]["src_city"]=',$module["current"]["src_city"];

    //Dublicate_search_start

    $dublicatesearchsql="SELECT

    tracerezult.id, tracerezult.src_ip, tracerezult.src_provider, tracerezult.src_country, tracerezult.src_city,
tracerezult.dsc_ip,

    tracerezult.dsc_provider,tracerezult.dsc_country, tracerezult.dsc_city,tracerezult.tracerezult

    FROM   tracerezult WHERE tracerezult.dsc_city LIKE  '".$module["current"]["dsc_city"]."' AND
```

```
tracerezult.src_provider NOT LIKE  '".$module["current"]["src_provider"]."' AND

tracerezult.dsc_provider NOT LIKE  '".$module["current"]["dsc_provider"]."'  ";

$module["dublicatemsg"]="";

$ds = $db->Execute($dublicatesearchsql);

$dublicatesearc=$ds->GetRows();

if ($module["show_detail"])

{print "<pre>";  print_r($dublicatesearc); print "</pre>";}

 foreach ($dublicatesearc as $k => $Rowd) { $module["dublicatemsg_per_cicle"]="";

        $module["dublicatemsg_ip_per_cicle"]="";

        //Exemining alternative way

        //$tablesovpadid - table with sovpad

        $idts=$module["current"]["dsc_city"];

        $tablesovpadid[$idts]["country"]=$module["current"]["dsc_country"];

        $tablesovpadid[$idts]["ciyt"]=$idts;

        $tablesovpadid[$idts]["no_1_point"]=$tablesovpadid[$idts]["no_1_point"];

        $tablesovpadid[$idts]["have_1_point"]=$tablesovpadid[$idts]["have_1_point"];

        foreach ($matches4[0] as $id => $value)

        {

        if ($module["show_detail"]) echo " Search ", $value,"in trace №",$Rowd["id"],"<br>";

        $path=$Rowd["src_provider"]."->".$Rowd["dsc_provider"]."&".$module["current"]["src_provider"]."-
>".$module["current"]["dsc_provider"] ;

        if (preg_match("/".$value."/",$Rowd["tracerezult"]))

        {$module["dublicatemsg"]="Found ".$value." in trace ".$Rowd["id"]."(".$Rowd["src_provider"]."-
>".$Rowd["dsc_provider"].",".$Rowd["dsc_city"].") while analize
".$module["current"]["id"]."(".$module["current"]["src_provider"]."-
>".$module["current"]["dsc_provider"].",".$module["current"]["dsc_city"].")<br><br>";

        $module["dublicatemsg_per_cicle"]=$module["dublicatemsg"];

        $module["dublicatemsg_ip_per_cicle"]=$value.", ".$module["dublicatemsg_ip_per_cicle"];

        echo $module["dublicatemsg"];

        }

        }

        if (strlen($module["dublicatemsg"])>3)
```

```
{  $module["pathnumberwithMITM"]++;

$module["badways"][$module["current"]["dsc_city"]]++;

}

if ($Rowd["id"]>$module["current"]["id"] )

{       if (strlen($module["dublicatemsg_per_cicle"])>3)

{

$module["dublicate"][$module["current"]["dsc_city"]][$path]="".$Rowd["src_provider"]."-
>".$Rowd["dsc_provider"]."";

$module["itog"][$module["current"]["dsc_city"]]["have_1_point"][]=$path;

$module["itog_count"][$module["current"]["dsc_city"]]["have_1_point"]++;

$module["itog_count"][$module["current"]["dsc_city"]]["Prov"][$Rowd["dsc_provider"]]["have_1_point"]++;

$tablesovpadid[$idts]["have_1_point"]++;

$module["itog"][$module["current"]["dsc_city"]]["1_point_is"]=$module["dublicatemsg_ip_per_cicle"];

}

else {

//$module["nodublicate"][$module["current"]["dsc_city"]][$path]="".$Rowd["src_provider"]."-
>".$Rowd["dsc_provider"]."";

$module["itog"][$module["current"]["dsc_city"]]["no_1_point"][]=$path;

$module["itog_count"][$module["current"]["dsc_city"]]["no_1_point"]++;

$module["itog_count"][$module["current"]["dsc_city"]]["Prov"][$Rowd["dsc_provider"]]["no_1_point"]++;

$tablesovpadid[$idts]["no_1_point"]++;

}

$tablesovpadid[$idts]["vsego"]=
$tablesovpadid[$idts]["no_1_point"]+$tablesovpadid[$idts]["have_1_point"];

$module["itog"][$module["current"]["dsc_city"]]["sql"]=$dublicatesearchsql;

}

$module["pathnumberanalyzed"]++;

}

if (strlen($module["dublicatemsg"])>3)

{  $module["pathnumberwithMITMGlobal"]++;

$module["pathnumberwithMITMGlobalT"]=  $module["current"]["src_provider"]." ->".
$module["current"]["dsc_city"]."(".$module["current"]["dsc_provider"].")<br>".$module["pathnumberwithMITMGlobalT
"]."";
```

```
$module["badwaysGlobal"][$module["current"]["dsc_city"]]++;

}

else {  $module["pathnumberNOMITMGlobal"]++;

$module["pathnumberwithNOMITMGlobalT"][$module["current"]["dsc_city"]]=  $module["current"]["src_provider"]." ->".
$module["current"]["dsc_city"]."(".$module["current"]["dsc_provider"].")<br>".$module["pathnumberwithNOMITMGlobalT"]."";

}

  }

  echo "<table border=1 >";

  foreach ($tablerow as $row) {

  echo "<tr>";

  foreach ($row as $column) {

  echo "<td>$column</td>";

  }

  echo "</tr>";

  }

  echo "</table>";

  echo "Таблица совпадений  пар      Город/Страна/Независимых маршрутов/Совпадающих маршрутов<table border=1 >";

  foreach ($tablesovpadid as $row) {

  echo "<tr>";

  foreach ($row as $column) {

  echo "<td>$column</td>";

  }

  echo "</tr>";

  }

  echo "</table>";

 echo " <p><a name='tbl'></a> </p>";

$sql='

SELECT   tracerezult.id,  racerezult.src_ip,   tracerezult.src_provider,

tracerezult.dsc_country, tracerezult.dsc_city,
```

```
COUNT(*),  tracerezult.`date` FROM  tracerezult  WHERE 1  '.$anyrequestcondition.'
GROUP BY tracerezult.dsc_provider
';
include_once('adodb5/adodb-pager.inc.php');
$pager = new ADODB_Pager($db,$sql);
$pager->Render($rows_per_page=200);
$sql='
SELECT tracerezult.id, tracerezult.src_ip,
tracerezult.src_provider, tracerezult.dsc_provider  ,  tracerezult.dsc_country,
tracerezult.dsc_city, COUNT(*),  tracerezult.`date`
FROM  tracerezult   WHERE 1  '.$anyrequestcondition.'    GROUP BY
tracerezult.src_provider   ';
include_once('adodb5/adodb-pager.inc.php');
$pager = new ADODB_Pager($db,$sql);
$pager->Render($rows_per_page=200);
$sql="
SELECT tracerezult.id, tracerezult.src_ip, tracerezult.src_provider,
tracerezult.dsc_provider  , tracerezult.dsc_country,tracerezult.dsc_city,
COUNT(*),   tracerezult.`date`   FROM  tracerezult
WHERE 1  ".$anyrequestcondition."    GROUP BY
tracerezult.dsc_city   ORDER BY   tracerezult.dsc_country ASC,   tracerezult.dsc_city ASC
";
include_once('adodb5/adodb-pager.inc.php');
$pager = new ADODB_Pager($db,$sql);
$pager->Render($rows_per_page=200);
echo "Operator 2 Operator";
$sql="
SELECT
tracerezult.id, tracerezult.src_ip, tracerezult.src_provider,
tracerezult.dsc_provider  , tracerezult.dsc_country, tracerezult.dsc_city,
```

```
COUNT(*),tracerezult.`date`

FROM tracerezult  WHERE 1    ".$anyrequestcondition."

GROUP BY tracerezult.dsc_provider,   tracerezult.dsc_city

ORDER BY tracerezult.dsc_country ASC, tracerezult.dsc_city ASC  ";

include_once('adodb5/adodb-pager.inc.php');

$pager = new ADODB_Pager($db,$sql);

$pager->Render($rows_per_page=200);
```

Приложение В. Общая характеристика протоколов распределения ключей IP-телефонии

Протокол DTLS

Протокол DTLS для SRTP представлен в RFC 5764. Протокол описывает формирование медиа-сессий точка-точка с двумя участниками с жесткой привязкой портов UDP корреспондента и респондента. Сообщения протокола передаются совместно с RTP пакетами (Рисунок В.1). Каждая сессия содержит одну DTLS ассоциацию и два SRTP контекста, применяемых для SRTP и SRTCP. Для организации сессии, называемой также DTLS-ассоциация, корреспонденты выполняют обмен сообщениями - DTLS handshake.

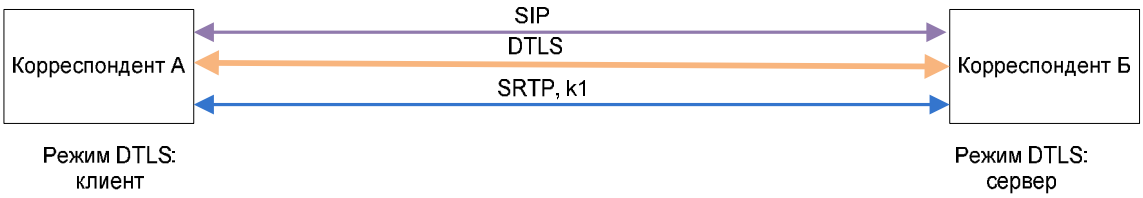


Рисунок В.1 – Применение DTLS при работе по сценарию клиент-клиент

Протокол DTLS поддерживает режимы аутентификации и обмена ключами, приведенные на рисунке В.2. Протокол поддерживает работу в двух сценариях:

А. Клиент – сервер, когда оба участника имеют предварительно распределенный секрет.

Б. Клиент – клиент, при условии, что нет заранее распределенного ключевого материала.

В сценарии А протокол может работать в любом из доступных режимов. Далее рассмотрена работа протокола в режиме Диффи-Хелмана. Обмен сообщениями представлен на рисунке В.3. При наличии общего секрета корреспондент А отправляет корреспонденту Б сообщение, подписанное цифровой подписью корреспондента А. Корреспондент Б, получив сообщение, проверяет его подлинность, используя цифровую подпись. Далее Б отправляет А

сообщение, подписанное цифровой подписью Б. А аналогично выполняет проверку, что сообщение принадлежит Б.

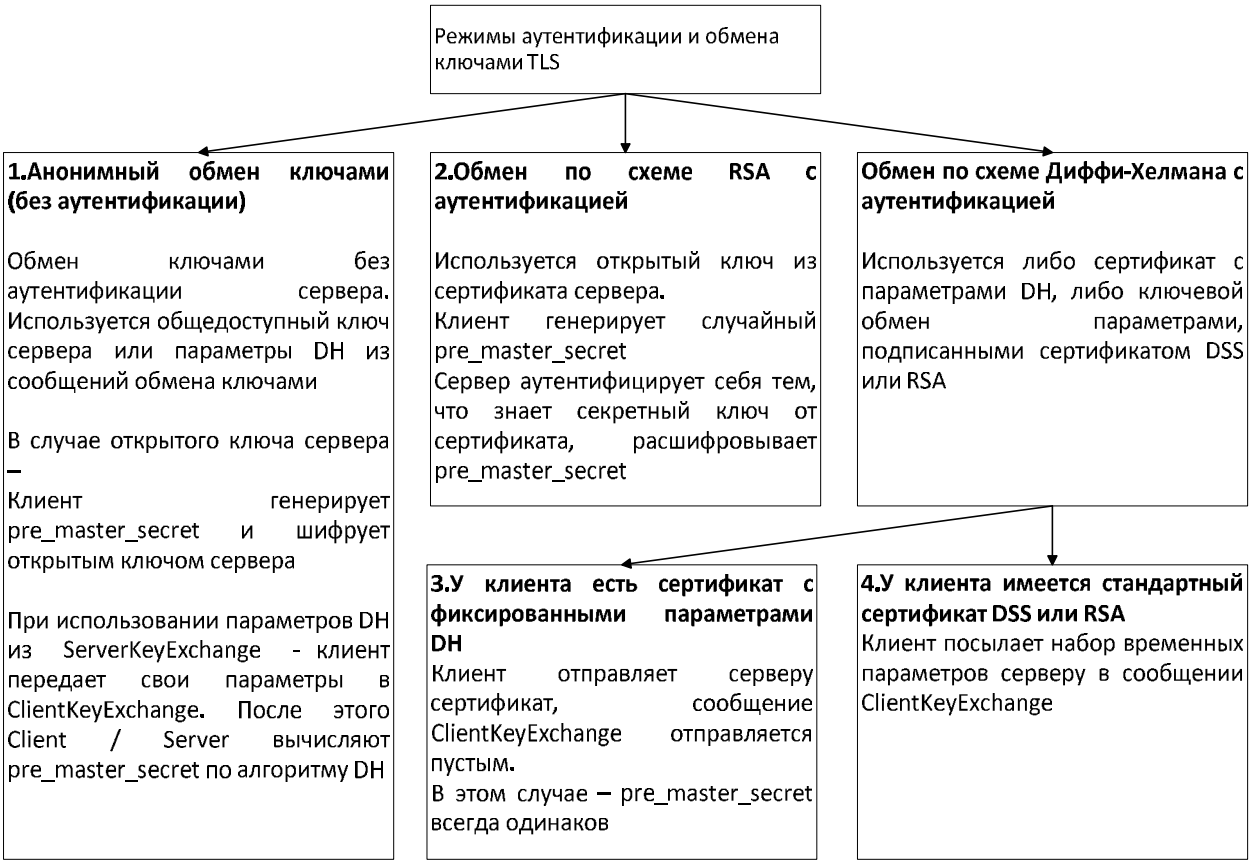


Рисунок В.2 – Режимы аутентификации и обмена ключами протокола DTLS

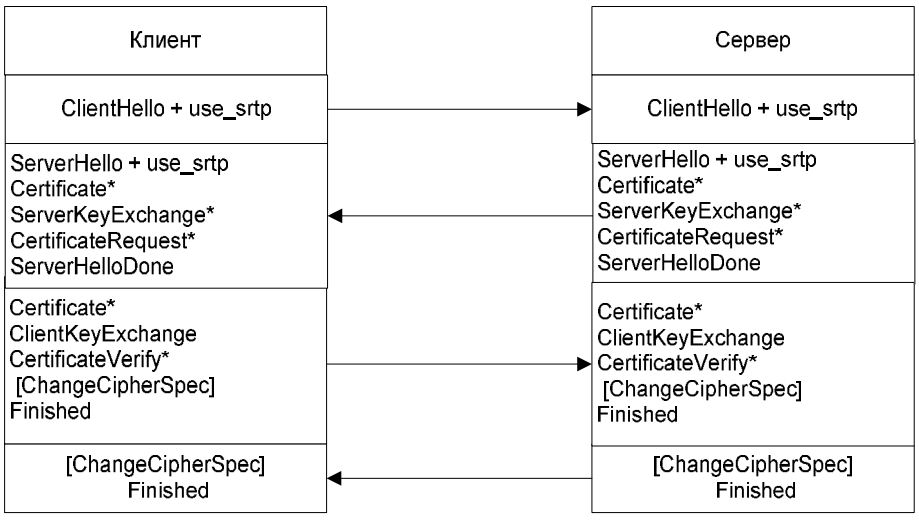


Рисунок В.3 – Обмена сообщениями в протоколе DTLS в режиме Диффи-Хелмана

В этом случае, нарушитель, пытающийся подменить сообщения, будет сразу обнаружен, так как не сможет пройти проверку цифровой подписью.

Рассмотрена работа протокола DTLS в сценарии Б при следующих условиях:

- сценарий работы: клиент-клиент без централизованного сервера;
- корреспонденты не имеют заранее обработанных ключей и общего секрета;
- корреспонденты не имеют общего доверенного центра сертификации;
- корреспонденты могут иметь предустановленные сертификаты, но при этом не имеют общего центра сертификации. Корреспонденты также могут иметь самоподписанные сертификаты.

Исходя из условий, протокол может работать в режимах 3 и 4, представленных на рисунке В.2. Между корреспондентами будет выполнен обмен сообщениями в соответствии с рисунком В.3.

Рассмотрена устойчивость протокола к атакам описанных ранее нарушителей. Введено допущение, что имеет место наличие внешнего нарушителя в канале связи, выполняющего атаку на захват оборудования оператора. Такой нарушитель может выполнить вторжение в канал связи, при этом схема взаимодействия показана на рисунке В.4.

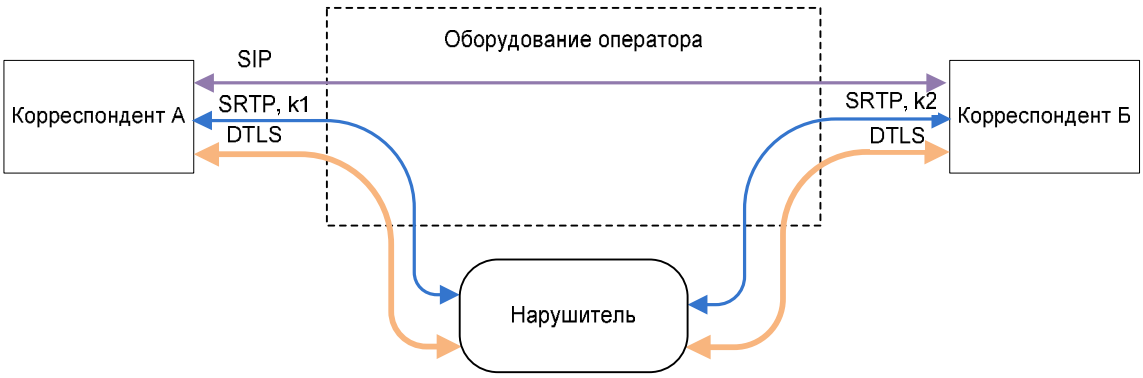


Рисунок В.4 – Схема атаки MITM на DTLS

Так нарушитель может поменять ключевой материал на другой. Протокол DTLS имеет способ двусторонней проверки выработанного ключа, который выражается в шифровании данных с помощью выработанного ключевого материала и передаче результата между корреспондентами. Однако, в случае

описанной атаки нарушитель успешно может выполнить проверку выработанного ключа с каждым из корреспондентов.

При атаках на оборудование клиента возможны такие атаки, как изменение параметров работы протокола DTLS, изменение параметров DTLS, влияющих на SRTP.

Протокол MIKEY

Протокол обмена ключами MIKEY описан в рекомендациях RFC3830 и RFC6043. MIKEY имеет несколько режимов работы, определяющих способ формирования секретного ключа сессии SRTP – режим предустановленного ключа (PSK), режим открытого ключа (PKE) и режим Диффи–Хелмана (DH). Транспортом для переноса сообщений протокола может выступать как SIP/SDP-сообщения, так и протокол RTSP (Real Time Streaming Protocol).

Далее рассмотрена работа протокола MIKEY при условиях – сценарий клиент-клиент без сервера, корреспонденты не имеют заранее выработанных ключей, а так же общих центров сертификации. В качестве транспортного выбирается протокол RTSP, чтобы MIKEY мог функционировать независимо от сигнализации (Рисунок В.5).

В случае отсутствия общего секрета режим предустановленного ключа нельзя использовать. В случае отсутствия общего центра сертификации режим открытого ключа также нельзя использовать, так как будет невозможно выполнить аутентификацию корреспондентов и сообщений. Соответственно необходимо использовать режим Диффи-Хелмана. При применении этого режима также нужна цифровая подпись, а в случае отсутствия цифровой подписи проверить подлинность корреспондента при использовании MIKEY не представляется возможным. Обмен сообщениями протокола MIKEY приведен на рисунке В.6.

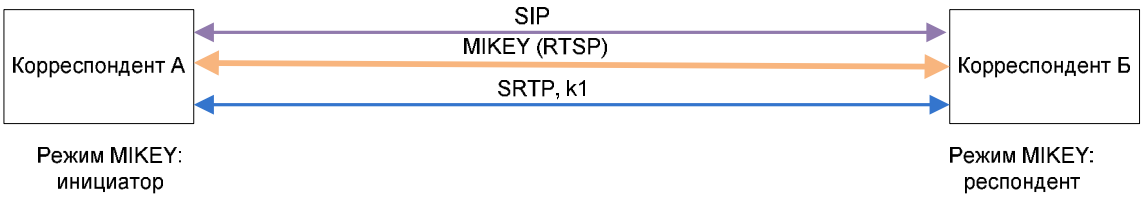


Рисунок В.5 – MIKEY в сценарии клиент-клиент

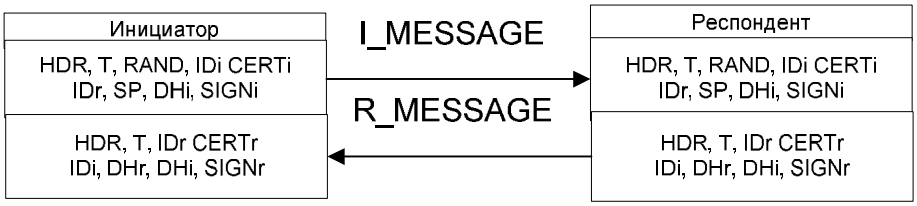


Рисунок В.6 – Обмен сообщениями протокола MIKEY в режиме Диффи-Хелмана

Далее выполнена оценка устойчивости потока MIKEY к атакам нарушителя. С помощью способов, описанных ранее в главе 2, нарушитель может выполнить вторжение в канал связи. При этом схема взаимодействия корреспондентов и нарушителя показана на рисунке В.7:

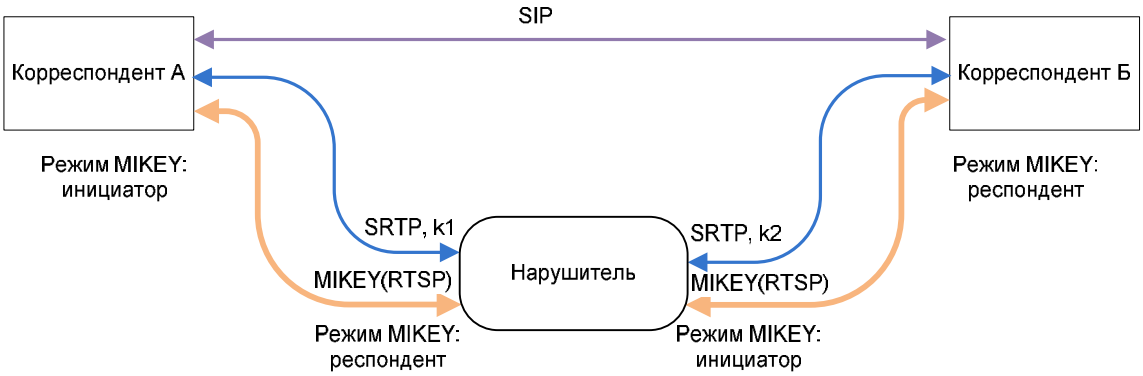


Рисунок В.7 – Схема атаки MITM на MIKEY

Так нарушитель может выработать независимые ключи с каждым из корреспондентов. Протокол не имеет способов двухсторонней проверки выработанного ключа с помощью дополнительных алгоритмов. Возможные следующие действия нарушителя при атаке на протокол:

- понижение безопасности MIKEY, т.е. установка в обмене более слабых протоколов шифрования, чем могут поддерживать корреспонденты;
- Подмена любой опции протокола, а также выполнение проксирования SRTP;
- понижение безопасности SRTP, т.е. установка в обмене более слабых протоколов шифрования, чем могут поддерживать корреспонденты.

Протокол ZRTP

Протокол ZRTP для SRTP описывается в RFC 6189. Особенностью протокола является передача параметров внутри RTP пакетов, оставляя пакеты совместимыми с RTP\AVP профилем. В этом случае, ZRTP-несовместимым устройством ZRTP-пакеты не обрабатываются и не влияют на установленное соединение.

Протокол предусматривает работу корреспондентов по топологии точка-точка, при этом отдельно выделяется возможность применении протокола при многопоточном режиме, когда необходимо организовать несколько защищенных медиа-потоков. Также предусмотрен вариант работы с легитимным посредником, которым может выступать, например, корпоративная телефонная станция.

В основе протокола ZRTP – обмен ключами по алгоритму Диффи-Хелмана во время установления соединения в области медиапотока (рисунок В.8).

Протокол ZRTP поддерживает следующие режимы обмена ключами:

- Режим предустановленного ключа (общего секрета);
- Режим распределения ключей по протоколу Диффи-Хелмана;
- Многопоточный режим.

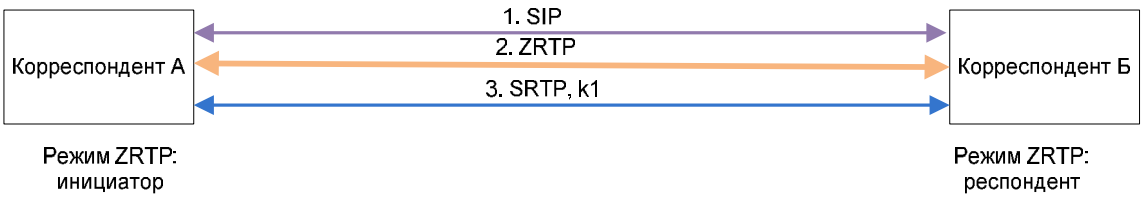


Рисунок В.8 – Применение ZRTP при работе по сценарию клиент-клиент

Рассмотрена работа протокола ZRTP в двух вариантах:

А. Клиент – сервер, когда оба участника имеют предварительно распределенный секрет.

Б. Клиент – клиент, при условии, что нет заранее распределенного ключевого материала.

В Варианте А протокол может работать в любом из доступных режимов. Рассмотрена работа протокола в режиме Диффи-Хелмана. Обмен сообщениями представлен на рисунке В.9.

При наличии общего секрета корреспондент А отправляет корреспонденту Б сообщение, подписанное цифровой подписью корреспондента А. Корреспондент Б, получив сообщение, проверяет его подлинность, используя цифровую подпись. Далее Б отправляет А сообщение, подписанное цифровой подписью Б. А аналогично выполняет проверку, что сообщение принадлежит Б. В этом случае, нарушитель, пытающийся подменить сообщения, будет сразу обнаружен, так как не сможет пройти проверку цифровой подписью.

Рассмотрена работа протокола ZRTP в варианте Б при следующих условиях:

- сценарий работы: клиент-клиент без централизованного сервера
- корреспонденты не имеют заранее обработанных ключей и общего секрета
- корреспонденты не имеют общего доверенного центра сертификации
- корреспонденты могут иметь предустановленные сертификаты, но при этом не имеют общего центра, выдавшего сертификат. Корреспонденты также могут иметь самоподписанные сертификаты.

Исходя из условий, протокол может работать в режиме Диффи-Хелмана. Между корреспондентами будет выполняться обмен сообщений в соответствии с рисунком В.9.

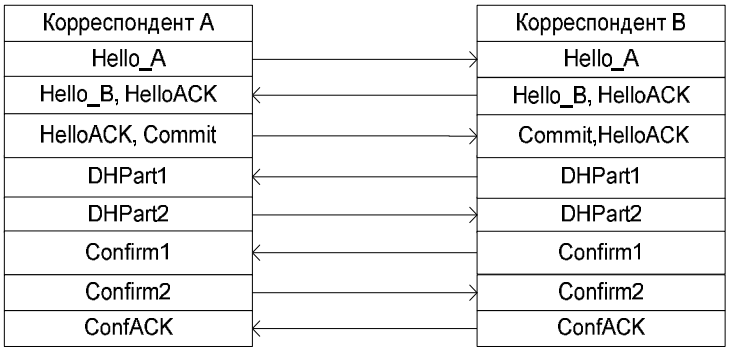


Рисунок В.9 – Взаимодействие корреспондентов по протоколу ZRTP

Произведена оценка устойчивости протоколов к атакам нарушителей, описанных в главе 2. Введено допущение, что имеет место наличие внешнего нарушителя в канале связи, выполняющего атаку на захват оборудования оператора. С помощью способов, описанных ранее, нарушитель может выполнить вторжение в канал связи.

При этом схема взаимодействия показана на рисунке В.10:

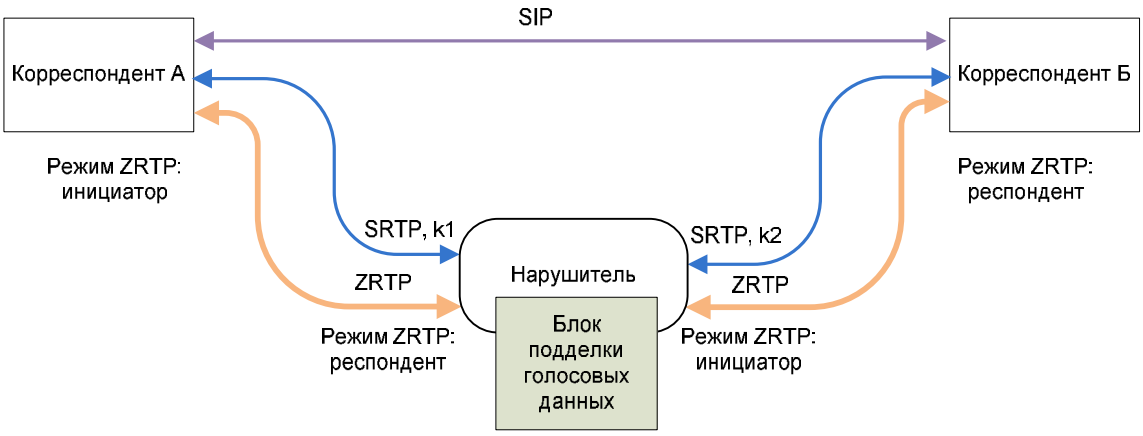


Рисунок В.10 – Схема атаки MITM на ZRTP.

Так нарушитель может поменять ключевой материал на другой. Протокол имеет способ двусторонней проверки выработанного ключа, который выражается в шифровании данных с помощью полученного общего секрета и передаче их между корреспондентами. Однако, в случае описанной атаки нарушитель может успешно выполнить проверку выработанного ключа с каждым из корреспондентов в отдельности.

Протокол имеет дополнительный алгоритм проверки наличия MITM, проявляющийся в проверке короткой строки аутентификации *SAS (Short Authentication String)*

*SAS= f(hash(*Hello респондента||Commit||DHPart1||DHPart2*))*

Внутренний нарушитель может выполнять эквивалентные действия, как и внешний нарушитель. При атаках на оборудование клиента возможны такие действия, как изменение параметров работы протокола ZRTP, влияющих также на SRTP.

Протокол SDES

Протокол SDES (Security Description), определяемый в рекомендации RFC4568, фактически является механизмом согласования криптографических ключей и параметров протокола SRTP между корреспондентами и не является протоколом управления ключами. SDES не поддерживает распределение ключей в топологии точка-многоточка. Один из корреспондентов передает ключ в SIP-сообщении по сигнальному каналу. Респондент получает его и использует для шифрования. Данные протокола передаются в составе SDP-сообщений (рисунок В.11), которые обычно инкапсулируются в сообщения протокола SIP или MGCP. При использовании SDES необходимо, чтобы нижестоящий транспортный протокол (как правило, TLS) обеспечивал аутентификацию и конфиденциальность для защиты ключевого материала от атак прослушивания, повторных сообщений и атак, связанных с изменением передаваемых сообщений.

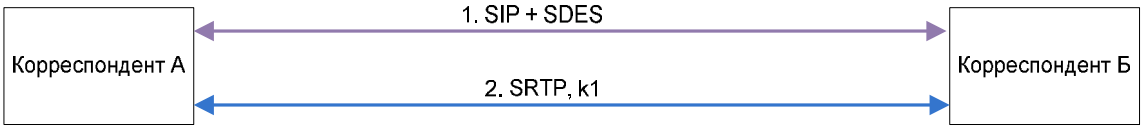


Рисунок В.11 Применение SDES при работе по сценарию клиент-клиент

Рассмотрена работа протокола SDES в двух вариантах:

А. Клиент – сервер, когда оба участника имеют предварительно распределенный секрет.

B. Клиент – клиент, при условии, что нет заранее распределенного ключевого материала.

Во всех режимах протокол требует, чтобы нижестоящий транспортный протокол (TLS) выполнял дополнительную защиту сообщений. Таким образом безопасность SDES определяется безопасностью протокола TLS.

Обмен сообщениями представлен на рисунке В.12. Протокол SDES не имеет нескольких режимов работы по аналогии ZRTP, DTLS и MIKEY. Также протокол не поддерживает механизмов защиты сообщений цифровой подписью или дополнительными методами.

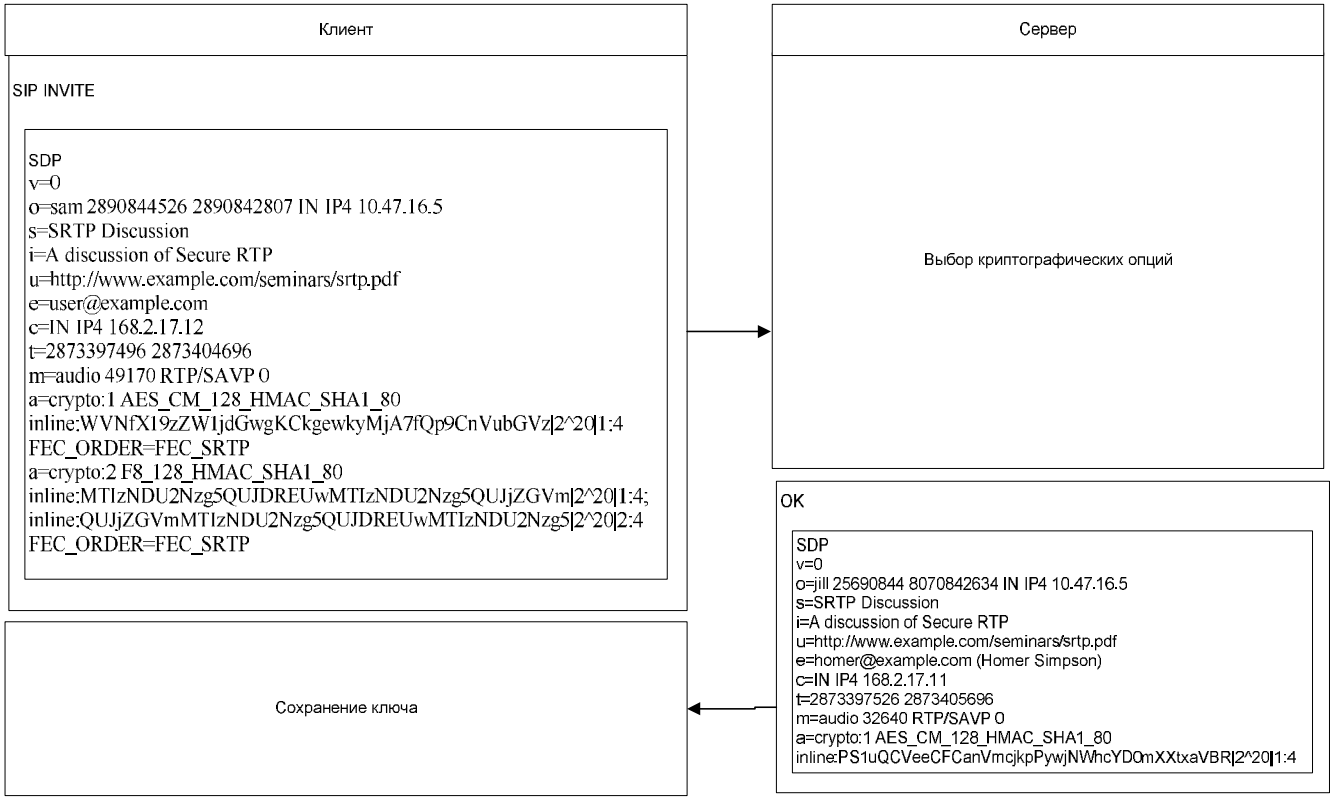


Рисунок В.12 – Обмена сообщениями в протоколе SDES

Введено допущение, что имеет место наличие внешнего нарушителя в канале связи, выполняющего атаку на захват оборудования оператора. Такой нарушитель может выполнить вторжение в канал связи. При этом схема взаимодействия показана на рисунке В.13:

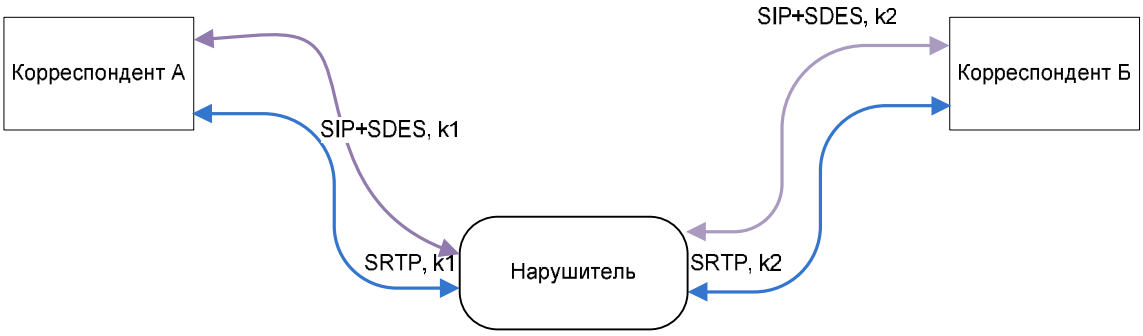


Рисунок В.13 – Схема атаки MITM на SDES

Протокол не имеет способа двусторонней проверки согласованного ключа, который выражается в шифровании данных с помощью полученного общего секрета и передаче их между корреспондентами. Таким образом – нарушитель может успешно выполнить атаку на протокол MIKEY для реализации НСД.

Приложение Г. Протокол ZRTP

Протокол ZRTP предназначен для решения следующих задач:

- Генерация ключевых параметров SRTP сессии;
- Обеспечение конфиденциальности сообщений протокола;
- Обеспечение аутентификации корреспондентов;
- Защита от атаки вторжения посередине (MITM, Man In The Middle), как с использованием, так и без использования инфраструктуры открытых ключей.

Каждый из корреспондентов-участников протокола должен иметь предустановленный идентификатор ZID, который должен быть уникален для каждого из корреспондентов. Для выполнения протокола ZRTP корреспонденты должны поддерживать одинаковые криптографические алгоритмы, наборы которых представленные в таблице Г.1

Таблица Г.1. Криптографические наборы протокола ZRTP

Криптографические функции	Обязательная поддержка		Опциональная поддержка	
	Алгоритм	Длина ключа	Алгоритм	Длина ключа
Шифрование данных	AES	128 бит	AES TwoFish TwoFish TwoFish	256 бит 128 бит 192 бит 256 бит
Аутентификация	HMAC-SHA1 HMAC-SHA1	32 бит 80 бит	Skein-512-MAC Skein-512-MAC	32 бит 64 бит
Хеш-функция	SHA-256 SHA-384	256 бит 384 бит	NIST SHA-3 NIST SHA-3	256 бит 384 бит
Обмен ключами	DH 3k		EC 25, EC 38 DH 2k	
Аутентификация корреспондентов	PGP X.509v3			

В основу протокола ZRTP положен алгоритм Диффи-Хелмана. Особенностью протокола ZRTP является передача параметров внутри RTP пакетов, оставляя пакеты совместимыми с RTP\AVP профилем. В этом случае,

ZRTP-несовместимым устройством ZRTP-пакеты просто отклоняются и не влияют на установленное соединение.

Протокол выполняется последовательно в четыре фазы (Рисунок Г.1)

1. Обнаружение
2. Подтверждение
3. Вычисление ключей
4. Завершение

Протокол требует определения сторон – инициатора и отвечающего (респондента). Эта операция выполняется в течении фазы обнаружения и подтверждения.

Корреспонденты обмениваются сообщениями Hello на первой фазе протокола. Эти сообщения содержат данные о поддерживаемых криптографических наборах для определения возможности использования SRTP: поддерживаемые алгоритмы хеширования, алгоритмы шифрования, типы аутентификационных тегов, протоколы согласования ключей, типы SAS (Short Authentication String). Также передается информация об идентификаторе производителя ZRTP программного обеспечения, о версии ZRTP, набор флагов для различных операций. Повторная передача сообщения Hello предусмотрена протоколом до 20 раз, после чего формируется решение о невозможности выполнения криптографического протокола ZRTP до конца и установления сессии в защищенном режиме. Повторная передача этого сообщения выполняется с задержкой, величина которой имеет переменное значение: 50, 100, 200 мс. Начиная с четвертого повтора задержка не меняется и имеет постоянную величину 200 мс. Полученное респондентом сообщение Hello подтверждается ответным сообщением HelloACK, после приема которого повторная передача Hello не производится.

Каждый из корреспондентов должен получить сообщение Hello, и хотя бы один из них должен получить сообщение HelloACK для перехода протокола в

следующую фазу. Корреспондент, который первым получает сообщение HelloACK, принимает на себя роль инициатора сессии.

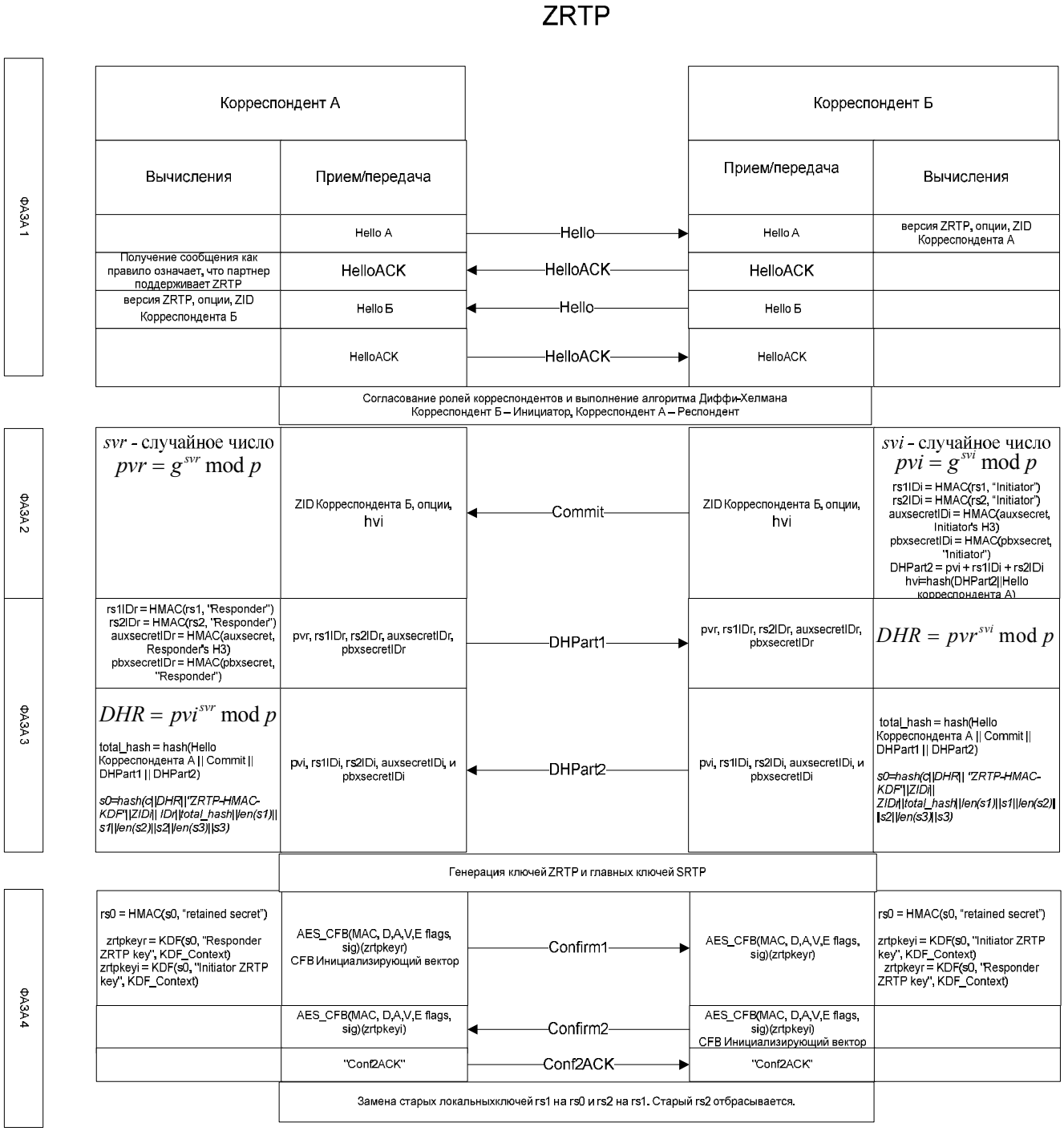


Рисунок Г.1 – Взаимодействие корреспондентов при выполнении протокола ZRTP

На второй фазе протокола корреспонденты согласуют между собой, кто будет инициатором для выполнения алгоритма Диффи-Хелмана. Для этого перед

началом второй фазы каждый из корреспондентов генерирует свое случайное число и производит вычисления:

Первый корреспондент– $pvi = g^{svi} \bmod p$,

Второй корреспондент– $pvr = g^{svr} \bmod p$,

где *svi* и *svr* – случайные числа.

Корреспонденты подготавливают сообщение Confirm, и формируют параметр *hvi.* Он вычисляется, как хеш-функция от конкатенации сообщений DHPart2, и сообщения Hello респондента, укороченная до 256 бит:

*hvi=hash(*DHPart2||Hello_B*).*

Параметр *hvi* предназначен для выбора одного из корреспондентов в качестве инициатора. Он передается в составе сообщения Commit. Инициатор первым посылает сообщение *"*Commit*"*. В случае, если оба устройства выбирают роль инициатора и одновременно посылают сообщение *"*Commit*"*, сравнивается значение хеша *hvi*. Тот, у кого значение *hvi* будет больше – сохраняет роль инициатора.

Протокол предусматривает повторную передачу сообщения *"Commit"*до 10 раз, после чего протокол завершается неуспешно и сессия не устанавливается в защищенном режиме. Повторная передача *Commit* сообщения выполняется с переменной задержкой, величина которой имеет значения: 150, 300, 600, 1200 мс. Начиная с четвертого повтора, задержка имеет постоянное значение 1200 мс. Каждое полученное по каналу связи сообщение *Commit* подтверждается ответным сообщением *DHPart1* третьей фазы, после приема которого повторная передача *Commit* прекращается.

На третьей фазе в результате обмена открытыми сообщениями DHPart1 и DHPart2 производится формирование секретных ключей для SRTP сессии. Для защиты от атаки MITM протокол позволяет использовать данные, накопленные от предыдущих соединений. Для этого используется специальная таблица в памяти устройств, поддерживающих ZRTP протокол. В качестве индексов записей таблицы выступает ZID респондента.

Каждый из корреспондентов сгенерировал закрытый и открытый ключ алгоритма Диффи-Хелмана на предыдущих этапах алгоритма. Для инициатора эти ключи обозначаются соответственно: pvi – открытый и svi – секретный ключ. Для респондента – *pvr* и *svr* соответственно.

В сообщениях DHPart1 и DHPart2 передается рассчитанный ранее *pvi/pvr* открытый ключ, хеш функции, значения регистров данных, распределенных в предыдущей сессии.

Корреспонденты сверяют полученные в сообщениях значения регистров данных, распределенных в предыдущей сессии, со значениями, рассчитанными локально, и используют совпавшие данные в дальнейшем для вычисления параметров *s1, s2, s3* и параметра *s0*.

Оба корреспондента используют полученные открытые ключи *pvi* и *pvr* для расчета результирующего ключа обмена Диффи-Хелмана.

Протокол предусматривает повторную передачу *DHPart2* сообщения до 10 раз, после чего протокол завершается неуспешно и сессия не устанавливается в защищенном режиме.. Повторная отправка *DHPart2* сообщения выполняется с переменной задержкой, величина которой имеет значения: 150, 300, 600, 1200 мс. Начиная с четвертого повтора задержка имеет постоянное значение 1200 мс. Каждое полученное сообщение *DHPart2* подтверждается ответным сообщением *Confirm1*четвертой фазы, после приема которого повторная передача *DHPart2* прекращается.

На четвертой фазе для подтверждения успешного формирования секретных ключей происходит обмен сообщениями Confirm2 и Confirm2, которые передают зашифрованное с помощью AES в режиме обратной связи по шифротексту сообщение, содержащее несколько флагов и параметров, включая время действия нового сгенерированного ключа, а также некоторые служебные флаги и опциональные цифровые подписи. Для шифрования используются ключи, рассчитанные на предыдущей фазе протокола.

Для аутентификации корреспондентов, а также исключения атаки вторжения в середину, протокол ZRTP предусматривает использование короткой аутентификационной строки (SAS, Short Authentication String).

*SAS= f(hash(*Hello респондента||Commit||DHPart1||DHPart2*))*

Для контроля целостности передаваемых сообщений каждое сообщение ZRTP включает в себя проверочный код CRC, а также код аутентификации сообщения MAC (Message Authentication Code). MAC вычисляется, как ключевая хеш-функция, которая согласовывается на первой фазе протокола. Возможные типы хеширования представлены в таблице 1. В качестве ключа при вычислении хеш функции используется содержание специального поля Hx(x=0..3), передаваемое в ZRTP сообщении. Особенностью протокола является то, что ключ проверки текущего сообщения для большинства сообщений, передается в следующем ZRTP сообщении.

Обнаружение ошибки в хеш-сообщении, как правило, означает обнаружение атаки MiTM, так как искажения за счет канальных ошибок проявляются при проверке CRC ZRTP пакета.

Последовательность обмена сообщениями между взаимодействующими корреспондентами в процессе выполнения протокола ZRTP показана на рисунке Г.1. Протокол считается завершенным, когда респондент отправляет сообщение Conf2ACT или первый SRTP пакет с верным тегом аутентификации. Инициатор воспринимает верный SRTP пакет, как эквивалент получения Conf2ACK сообщения.

В процессе выполнения протокола ZRTP передаются несколько сообщений различной длительности, представленных в таблице Г.2.

Таблица Г.2. Параметры сообщений протокола ZRTP

Назначение сообщения	Обозначение	Полная длина UDP пакета (бит)	Подтверждение	Число повторных передач (max)
Согласование параметров и возможностей корреспондентов	Hello	1392	нужно	20
Подтверждение получения Hello-сообщения	HelloACK	650	нет	
Согласования хеш-функций hvi	Commit	1392	нужно	10
1ое сообщение обмена ключами Диффи-Хелмана	DHPart1	4208	нет	
2ое сообщение обмена ключами Диффи-Хелмана	DHPart2	4208	нужно	10
Подтверждение обмена с применением сгенерированного общего ключа	Confirm1	1072	нет	
Подтверждение обмена с применением сгенерированного общего ключа	Confirm2	1072	нужно	10
Подтверждение Confirm2	Conf2ACK	560	нет	

Приложение Д. Протокол DTLS

DTLS – один из протоколов обмена ключевым материалом между корреспондентами в IP-телефонии, описанный в рекомендации RFC6347. DTLS является адаптацией другого протокола обеспечения безопасности – TLS. В отличии от предшественника, DTLS адоптирован для работы по сети с негарантированной доставкой сообщений, с использованием протокола UDP. Главной задачей DTLS протокола является согласование между корреспондентами главного секретного ключа, применяемого впоследствии для SRTP протокола.

Таблица Д.1 – Криптографические наборы DTLS

Шифрование	RC4_40/ RC4_128/ RC2_CBC_40/ DES40_CBC, AES и т.д.
Цифровая подпись	X.509
Протокол обмена ключами	DHE_DSS/ DHE_RSA, ECDHE и т.д.
Хеш-функция	MD5 / SHA256 / SHA384

Для работы по UDP протоколу в DTLS по сравнению с TLS было произведено несколько изменений. Для работы протокола по каналу с негарантированной доставкой, вводиться дополнительный механизм повторной передачи недоставленных сообщений по истечению таймера повторной передачи. Для того, чтобы сделать возможным независимую расшифровку отдельных сообщений, в протоколе введен запрет на использование потокового шифрования. Если N сообщение не будет доставлено, это позволит избежать ошибки при проверке целостности N+1 сообщения. Процедура обмена сообщениями TLS предполагает, что все сообщения должны быть доставлены в исходном порядке и заканчивается неуспешно, если хотя бы одно сообщение потеряно, или при условии нарушения порядка пакетов. Для решения этой проблемы, характерной для TLS, в DTLS вводиться явный порядковый номер сообщений внутри обмена. Когда один из корреспондентов получает сообщение – он определяет, то ли это

сообщение, которое он ожидает. Если полученное сообщение соответствует ожидаемому – то оно обрабатывается. Если нет – то сообщение согласно RFC6347 становиться в очередь для дальнейшей обработки до тех пор, пока не получены предшествующие ему сообщения.

Сообщения обмена TLS и DTLS могут быть очень большими (теоретически 2^24-1, практически – много килобайт). Однако, UDP датаграммы очень часто ограничены размером до 1500 байт при условии, что не применяется фрагментация пакетов. Для преодоления ограничения – одно DTLS сообщение разбивается на несколько DTLS записей, каждая из которых помещается в отдельную датаграмму. Каждое DTLS сообщение содержит смещение фрагмента и длину фрагмента. Таким образом, респондент, получив все байты сообщения, воспроизводит нефрагментированное сообщение.

В общем виде – схема обмена сообщениями протокола DTLS для генерации ключей для SRTP представлена на рисунке Д.1.

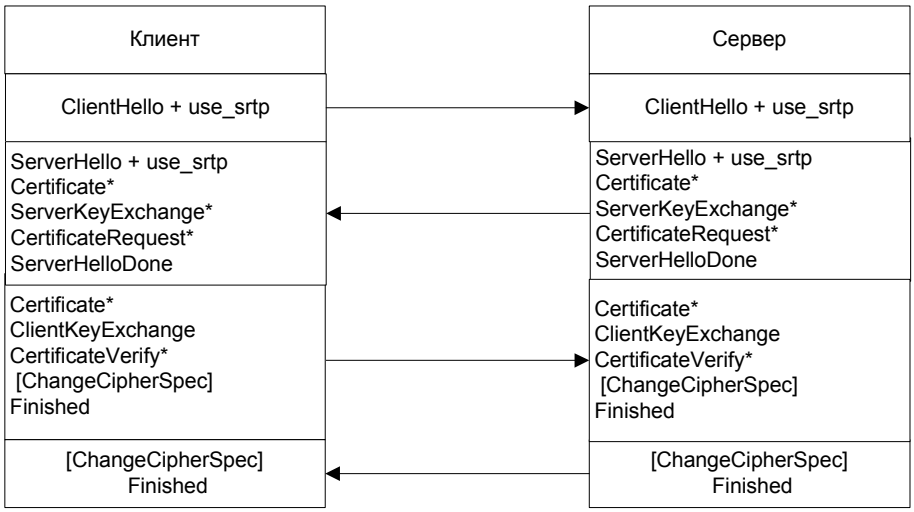


Рисунок Д.1 – Обмен сообщениями по протоколу DTLS

Каждое сообщение в алгоритме протокола имеет явный порядковый номер, который передается в поле seq. В случае повторной передачи одного и того сообщения – номер сообщения остается прежним, и изменяется только при передаче следующего сообщения по алгоритму (рисунок Д.2).

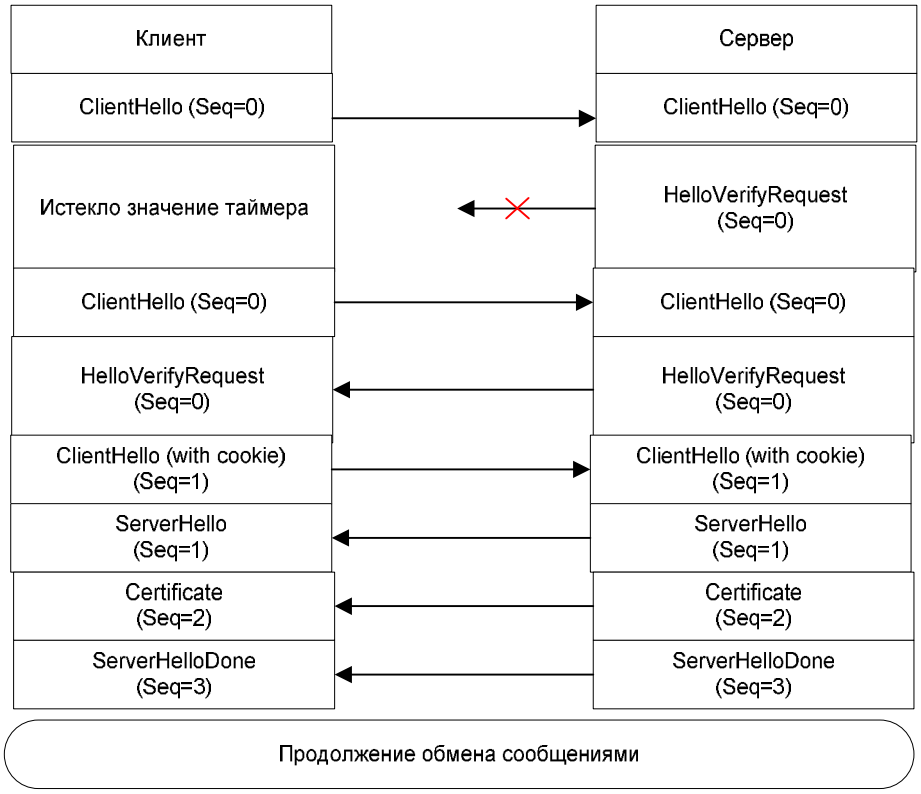


Рисунок Д.2 – Применение sequence_number в протоколе DTLS

Обмен ключами и генерация ключей в DTLS происходят по тому же принципу, что в протоколе TLS 1.2. Протокол DTLS имеет две составляющих – уровень записей и уровень диалога. Уровень записей используется для инкапсуляции протоколов и сообщений более высокого уровня. К ним, например, относятся сообщения уровня диалога DTLS, который позволяет корреспондентам согласовать применяемые криптографические алгоритмы и их параметры.

Протокол DTLS поддерживает несколько режимов обмена ключами и аутентификации, представленные на рисунке Д.3.

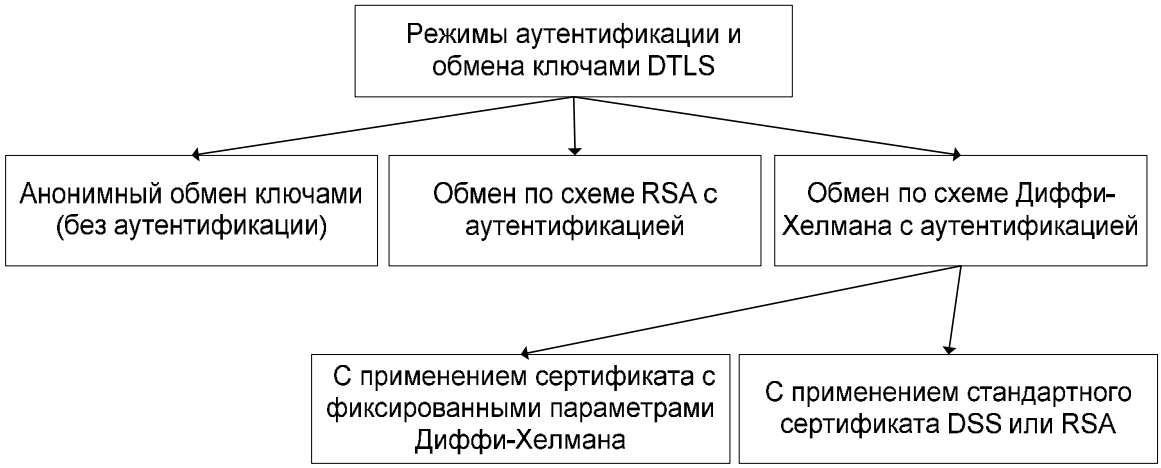


Рисунок Д.3 – Режимы работы протокола DTLS

DTLS протокол поддерживает несколько алгоритмов обмена ключами, а также работу с сертификатами. Передача сертификатов выполняется в сообщениях протокола диалога DTLS. Тип сертификата должен соответствовать выбранным параметрам криптографических протоколов. Обычно это сертификат типа X.509v3.

В зависимости от выбранного режима работы и алгоитма обмена ключами, используют ключи и типы сертификатов, приведенные в таблице Д.2.

В результате выбора алгоритма обмена ключами и выполнения процедуры диалога корреспонденты получают предварительный ключ - *pre_master_secret*. Для всех методов ключевого обмена используется один и тот же алгоритм преобразования *pre_master_secret* в главный секретный ключ *master_secret*. Значение *pre_master_secret* удаляется из памяти, как только завершится вычисление *master_secret*:

master_secret = PRF(pre_master_secret, "master secret", ClientHello.random + ServerHello.random)

Таблица .Д.2 – Поддерживаемые алгоритмы обмена ключами в DTLS

Алгоритм обмена ключами	Тип сертификата ключа
RSA	Общедоступный ключ RSA; сертификат должен допускать использование ключа для шифрования.
RSA_EXPORT	Общедоступный ключ RSA с длиной больше чем 512 бит, который может быть использован для подписи, или ключ длиной 512 бит или короче, который может быть использован для шифрования или подписи.
DHE_DSS	Общедоступный ключ DSS.
DHE_DSS_EXPORT	Общедоступный ключ DSS.
DHE_RSA	Общедоступный ключ RSA, который может использоваться для подписи.
DHE_RSA_EXPORT	Общедоступный ключ RSA, который может использоваться для подписи.
DH_DSS	Ключ Diffie-Hellman. Алгоритмом, используемым для подписи сертификата, должен быть DSS.
DH_RSA	Ключ Diffie-Hellman. Алгоритмом, используемым для подписи сертификата, должен быть RSA.

Главный секретный ключ всегда имеет длину 48 байт. Длина предварительного секретного кода варьируется в зависимости от метода ключевого обмена. Этот ключ впоследствии хэшируется и применяется для получения секретных кодов MAC, ключей и инициализирующего вектора IV.

Параметры протокола DTLS, определяющие вероятностно- временные характеристики

При расчете вероятностно-временных характеристик протокола DTLS, следует учесть особенность повторной передачи сообщений. Согласно рекомендации RFC6347, значения таймеров повторной передачи сообщения выбираются реализацией протокола, несогласованность таймеров может привести к возникновению очередей сообщений. Начальное значение таймера повторной передачи согласно RFC 6298 рекомендуется установить в 1 секунду и удваивать значение таймера каждый раз, до достижения значения в 60 секунд. Значение таймера обнуляется каждый раз, как имеет место успешная передача сообщения.

После долгого периода бездействия значение таймера может быть сброшено на начальное значение. Это происходит в случае, когда повторное рукопожатие выполняется после завершения передачи данных.

Протокол не регламентирует ограничение по числу повторных передач сообщения. При передаче – несколько сообщений протокола, как правило, группируются в комплексные сообщения.

Повторные сообщения отправляет только клиент, не получивший следующего по сценарию сообщения в течении времени, равного текущему значению таймера повторной передачи. Стандарт не описывает количество повторов сообщений, однако в соответствии с рекомендацией RFC 6298 значение таймера повторной передачи сообщения должно изменяться в диапазоне от 1 до 60 секунд, а таймер будет принимать значения: 1 с., 2 с., 4 с., 8 с., 16 с., 32 с., 60с. Таким образом –таймер может принимать семь разных значений. В соответствии с этим, при расчете введено допущение, что при передаче одного сообщения максимальное число повторов составляет семь, после чего протокол завершает работу.

Протокол может работать в разных режимах работы. В зависимости от режима – может меняться длина передаваемых сообщений. Список сообщений, а также их длины, приведены в таблице Д.3.

Таблица Д.3 – Длины сообщений протокола DTLS

Название Сообщения	Размер пакета, байт
Client Hello	161
Hello Verify Request	70
Client Hello with COOKIE	161
Server Hello, Certificate, Server Hello Done	1019
Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message	288
Change Cipher Spec, Encrypted Handshake Message	135

Приложение Е. Структура глобальной сети

Структура глобальной сети в России детально описана в интернете и в печатных изданиях. В рамках глобальной сети России выделяют четыре класса (tier) операторов связи. Каждый оператор и участник глобальной сети имеет свою автономную систему (AS). Под автономной системой понимают систему IP – сетей и маршрутизаторов, управляемых одним оператором и имеющую единую политику маршрутизации с другими автономными системами.

К операторам первого класса (tier-1) относят меж-континентальных операторов связи, формирующих основу глобальной сети. Как правило, эти операторы соединяются друг с другом по принципу каждый с каждым на безвозмездной основе. Кроме этого, они присоединяют к себе операторов второго уровня, но уже на платной основе. Число операторов первого класса 10-15 штук и постоянно меняются. С соответствии с разными источниками в список операторов первого класса входят следующие компании:

1. Verizon (бывший UUNET)
2. AboveNet (AS 6461)
3. AT&T (AS 7018, AS 2686, AS 5623, и др.)
4. Global Crossing (AS 3549)
5. Level 3 (AS 3356)
6. MCI EMEA (AS 702)
7. Verizon (бывший MCI UUNET) (AS 701/703)
8. NTT Communications (AS 2914)
9. SAVVIS (AS 3561)
10. Sprint (AS 1239)
11. Teleglobe (AS 6453), стал частью VSNL
12. Qwest(AS 209)
13. Telia Sonera(AS 1299)
14. Tata Communications (бывший Teleglobe) (AS 6453)

15. STARTTELECOM

В соответствии с исследованиями компании The Cooperative Association for Internet Data Analysis также можно выделить список основных провайдеров, формирующих структуру глобальной сети. В таблице Е.2 приведен список самых крупных операторов связи. На рисунке Е.2 также приведен пример взаимодействия оператора Level 3 с другими операторами как первого, так и более низких классов.

Ко второму классу относятся национальные операторы связи, которые присоединяются к операторам первого класса на платной основе. Как правило, такие операторы имеют несколько точек подключения к операторам первого уровня. Также операторы соединяются с другими операторами второго класса для взаимного обмена трафиком.

Операторы второго класса могут охватывать несколько стран одного континента, а также крупные территории внутри стран. К операторам этого класса в России относят Ростелеком, Трансстелеком. На рисунке Е.1 по данным [101] приведена схема взаимодействия Ростелеком (AS 12389) с другими операторами связи на 2013.03.02. В таблице 1 перечислены первые 20 из 639 возможных автономных систем, с которыми установлены отношения у оператора Ростелеком.

К операторам третьего класса относятся региональные операторы, присоединяющиеся к операторам второго уровня несколькими подключениями. Как правило – это 3 – 5 точек подключения. Также операторы могут обмениваться трафиком между собой через организованные точки пирринга. К операторам третьего уровня относят: УралСвязьИнформ, ДальСвязь, МТС, Мегафон, Билайн и прочих операторов.

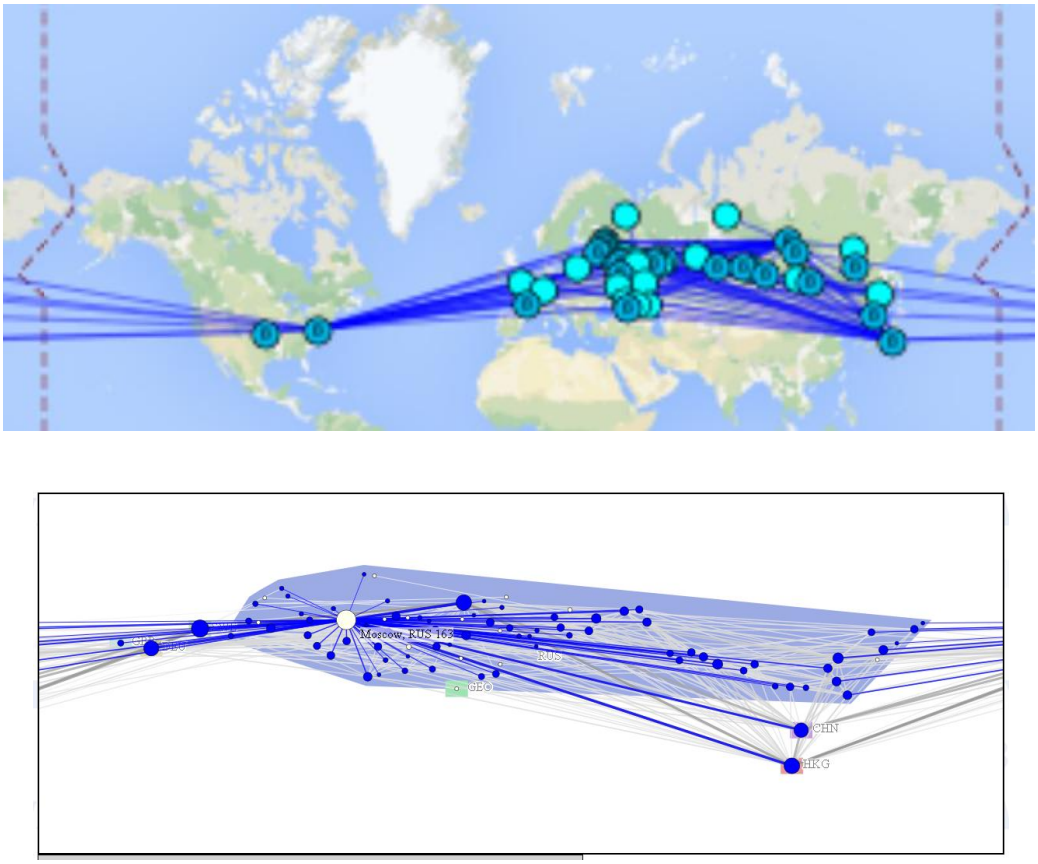


Рисунок Е.1 – Схема взаимодействия оператора Ростелеком (AS 12389) с другими операторами связи

Таблица Е.1 Отношения оператора Ростелеком (AS 12389)с другими компаниями на 2013.03.02. Первые 20 из 639 возможных

Neighbor				type
AS rank	AS	AS name	Org name	
1	3356	LEVEL3	Level 3 Communications	↑ provider
2	3549	LVLT-3549	Level 3 Communications	↑ provider
3	3257	TINET-BACK...	Tinet SpA	↑ provider
5	1299	TELIANET	TeliaNet Global Network	↑ provider
6	2914	NTT-COMMUN...	NTT America, Inc.	↑ provider
4	174	COGENT-174	Cogent/PSI	↔ peer
7	6453	AS6453	TATA Communications	↔ peer
9	6762	SEABONE-NET	TELECOM ITALIA SPARKLE S.p.A.	↔ peer
13	6939	HURRICANE	Hurricane Electric, Inc.	↔ peer
15	3491	BTN-ASN	Beyond The Network America, Inc.	↔ peer
18	1273	CW	Init7 Global Backbone	↔ peer
19	20485	TRANSTELECOM	JSC Company TransTeleCom	↔ peer
26	8928	INTEROUTE	Interoute Communications Limited	↔ peer
27	31133	MF-MGSM-AS	OJSC MegaFon	↔ peer
28	8359	MTS	MTS OJSC	↔ peer
31	10026	PACNET	Pacnet Global Ltd	↔ peer
33	50952	PEERING-AS	Prometey Ltd. Autonomous System	↔ peer
38	2516	KDDI	KDDI CORPORATION	↔ peer
39	4766	KIXS-AS-KR	Korea Telecom	↔ peer
40	9498	BBIL-AP	BHARTI Airtel Ltd.	↔ peer

К операторам четвертого класса относят операторов услуг, присоединяющихся к операторам второго и третьего класса. К этому классу относится множество компаний. Из известных компаний в Петербурге к операторам четвертого класса относятся ИнтерЗет/Z-Телеком, ТКТ, Эртелеком , МТУ-Интел, Комстар (Стрим), Комкор (Акадо) и другие. Взаимодействие

оператора четвертого уровня с операторами других уровней на примере провайдера ИнтерЗет приведен на рисунке Е.3 и в таблице Е.3.

Следует отметить, что в случае построения полносвязной сети из существующих автономных систем нельзя определить точный маршрут, по которому пакеты будут передаваться между корреспондентами, подключенными к разным автономным системам. Маршрутизация пакетов в сети любого оператора связи зависит от загрузки каналов связи, возникающих аварий на оборудовании, а также от действующих дополнительных соглашений между операторами, определяющих ценовую политику и параметры SLA.

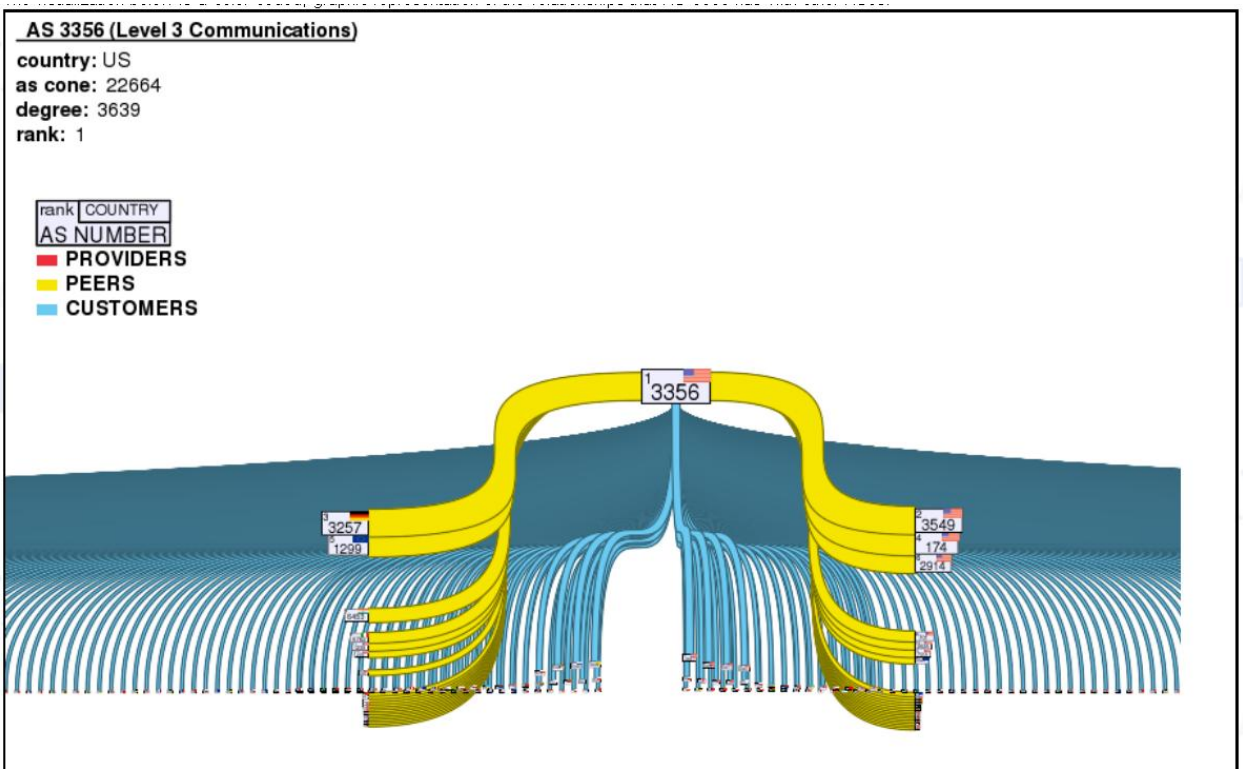
Таким образом, структура глобальной сети является случайной и выполнить теоретическую оценку числа непересекающихся маршрутов между разными точками не представляется возможным. Для оценки наличия непересекающихся маршрутов необходимо проводить практическую проверку.

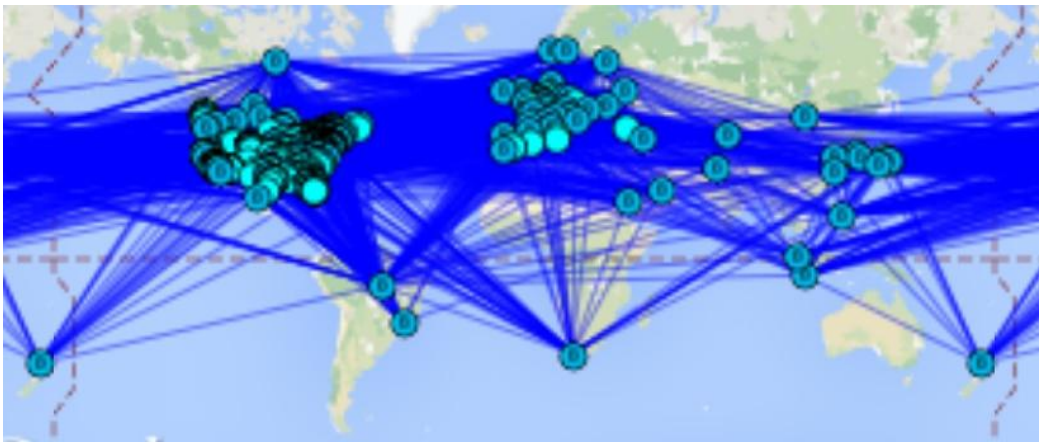
Таблица Е.2 Список самых крупных операторов связи по данным The Cooperative Association for Internet Data Analysis (CAIDA) на 2013.03.02

rank	AS number	AS name	Org name	customer cone						AS transit degree
				Number of			Percentages of all			
				ASes	IPv4 Prefixes	IPv4 Addresses	ASes	IPv4 Prefixes	IPv4 Addresses	
1	3356	LEVEL3	Level 3 Communications	22,685	261,219	1,401,759,501	51%	57%	65%	3621
2	3549	LVLT-3549	Level 3 Communications	15,103	200,586	698,222,855	34%	44%	32%	3264
3	3257	TINET-BACK...	Tinet SpA	14,873	188,737	709,433,321	33%	41%	33%	942
4	174	COGENT-174	Cogent/PSI	13,594	147,701	589,730,708	30%	32%	27%	3855
5	1299	TELIANET	TeliaNet Global Network	12,722	160,514	616,234,216	28%	35%	28%	764
6	2914	NTT-COMMUN...	NTT America, Inc.	11,159	169,846	711,971,065	25%	37%	33%	888
7	6453	AS6453	TATA Communications	7,062	120,037	459,993,873	16%	26%	21%	580
8	701	UUNET	MCI Communications Services, Inc. d/b/a Verizon Business	5,402	96,864	738,082,126	12%	21%	34%	1693
9	6762	SEABONE-NET	TELECOM ITALIA SPARKLE S.p.A.	4,808	61,319	190,002,775	10%	13%	8.8%	284
10	2828	XO-AS15	XO Communications	4,118	80,165	353,394,094	9.3%	17%	16%	1047
11	1239	SPRINTLINK	Sprint	4,043	92,421	603,330,796	9.2%	20%	28%	819
12	7018	ATT-INTERNET4	AT&T Services, Inc.	3,812	67,159	428,234,464	8.6%	14%	19%	2323
13	6939	HURRICANE	Hurricane Electric, Inc.	3,639	44,839	235,940,410	8.3%	9.9%	10%	2810
14	209	ASN-QWEST	Qwest Communications Company	3,11	44,674	330,781,168	7.1%	9.9%	15%	1458

Продолжение таблицы Е.2

rank	AS number	AS name	Org name	customer cone						AS transit degree
				Number of			Percentages of all			
				ASes	IPv4 Prefixes	IPv4 Addresses	ASes	IPv4 Prefixes	IPv4 Addresses	
15	3491	BTN-ASN	Beyond The Network America, Inc.	3,054	71,176	256,071,011	6.9 %	15%	11%	560
16	3320	DTAG	Deutsche Telekom AG	2,923	51,26	351,461,594	6.6 %	11%	16%	542
17	9002	RETN-AS	ReTN.net Autonomous System	2,469	13,327	20,477,488	5.6 %	3.0 %	0.95 %	1562
18	1273	CW	Init7 Global Backbone	2,435	37,976	142,589,068	5.5 %	8.4 %	6.6 %	302
19	20485	TRANSTELECOM	JSC Company TransTeleCom	2,351	13,652	18,679,552	5.3 %	3.0 %	0.87 %	629
20	12389	ROSTELECOM-AS	OJSC Rostelecom	2,269	16,07	36,834,608	5.1 %	3.6 %	1.7 %	634
21	6461	ABOVENET	Metromedia Fiber Network	2,22	24,747	126,246,412	5.0 %	5.5 %	5.9 %	1111
22	4323	TWTC	tw telecom holdings, inc.	2,109	24,274	60,692,144	4.8 %	5.4 %	2.8 %	1649
23	3216	SOVAM-AS	OJSC MegaFon	1,77	11,399	20,636,592	4.0 %	2.5 %	0.96 %	604
24	3561	SAVVIS	Qwest Communications, LLC	1,733	42,335	242,545,973	3.9 %	9.4 %	11%	344
25	7473	SINGTEL-AS-AP	Singapore Telecommunications Ltd	1,722	36,408	114,006,144	3.9 %	8.1 %	5.3 %	287
26	8928	INTEROUTE	Interoute Communications Limited	1,615	11,679	49,869,664	3.7 %	2.6 %	2.3 %	708
27	31133	MF-MGSM-AS	OJSC MegaFon	1,31	10,346	19,776,464	3.0 %	2.3 %	0.92 %	919
28	8359	MTS	MTS OJSC	1,186	5,023	9,786,624	2.7 %	1.1 %	0.46 %	398
29	15412	FLAG-AS	Flag Telecom Global Internet AS	1,028	31,043	63,077,928	2.3 %	6.9 %	2.9 %	351
30	286	KPN	KPN Internet Backbone	972	10,224	58,111,466	2.2 %	2.3 %	2.7 %	318





data sources				
geo	database	2013.03.02	netacquity	
organization	whois	0000.00.00	JPNIC, KRNIC, LACNIC	
		2012.06.29	AFRINIC, APNIC, ARIN, LACNIC, RIPE	
topology	BGP	2013.04.01, 2013.04.02, 2013.04.03, 2013.04.04, 2013.04.05	ripe	rrc00, rrc03, rrc04, rrc05, rrc06, rrc07, rrc10, rrc12, rrc13, rrc14, rrc15
			routeviews	eqix, isc, jinx, kixp, linx, routeviews2, saoppaulo, sydney, telxatl, wide
	ITDK	2012.07.23	MIDAR IFF	

Рисунок Е.2 – Пример взаимодействия оператора Level 3 с другими автономными системами, по данным http://as-rank.caida.org/?mode0=as-info&mode1=as-graph&as=3356

AS number: 41733
AS name: ZTELECOM-AS
Org name: ZTELECOM-AS
AS rank: 4934
Country: RU
Customer cone size: 2
AS transit degree: 2 (6 Provider, 0 Sibling, 36 Peer, 1 Customer)

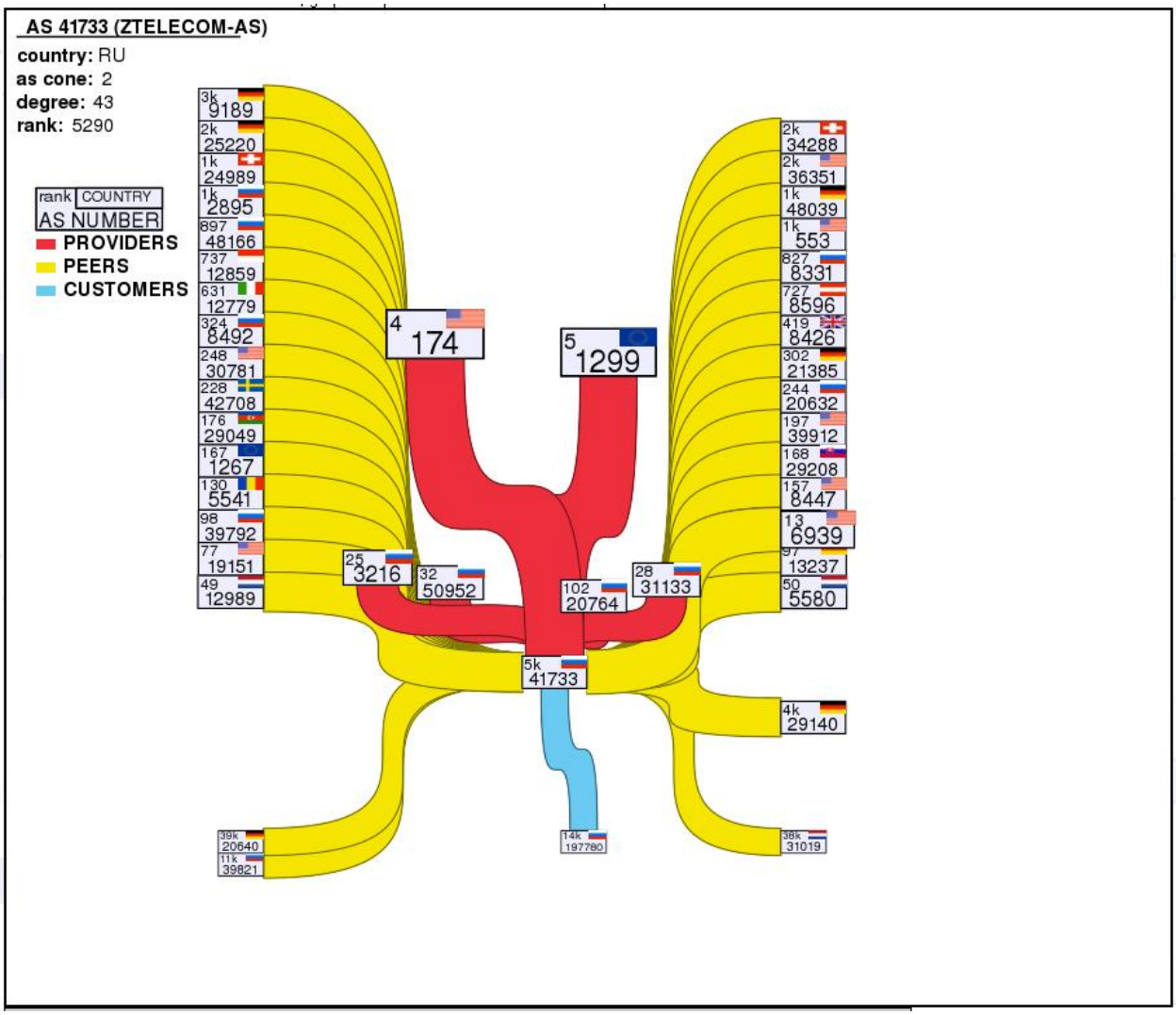


Рисунок Е.3 – Взаимодействие оператора Interzet с другими автономными системами

Таблица Е.3 Взаимодействие оператора Interzet с другими автономными системами

neighbor				type
AS rank	AS	AS name	Org name	
4	174	COGENT-174	Cogent/PSI	↑ provider
5	1299	TELIANET	TeliaNet Global Network	↑ provider
23	3216	SOVAM-AS	OJSC MegaFon	↑ provider
27	31133	MF-MGSM-AS	OJSC MegaFon	↑ provider
33	50952	PEERING-AS	Prometey Ltd. Autonomous System	↑ provider
104	20764	RASCOM-AS	CJSC Rascom, St.Petersburg, Russia	↑ provider
13	6939	HURRICANE	Hurricane Electric, Inc.	↔ peer
51	12989	HWNG	Eweka Internet Services B.V.	↔ peer
52	5580	ATRATO	Atrato IP Networks	↔ peer
81	19151	WVFIBER-1	WV FIBER	↔ peer
84	13237	LAMBDANET-AS	Lambdanet Communications Deutschland GmbH	↔ peer
100	39792	ANDERS-AS	Anders Telecom Ltd.	↔ peer
112	13030	INIT7	Init7 Global Backbone	↔ peer
132	5541	AdNet-Telecom	AdNet-Telecom	↔ peer
155	8447	TELEKOM-AT	Init7 Global Backbone	↔ peer
174	1267	ASN-INFOST...	WIND Telecomunicazioni S.p.A.	↔ peer
178	29208	DIALTELECO...	Dial Telecom, a.s.	↔ peer
185	39912	i3B-AS	Init7 Global Backbone	↔ peer
188	29049	Delta-Tele...	Delta Telecom LTD.	↔ peer
207	30781	JAGUAR-AS	Init7 Global Backbone	↔ peer
214	20632	PETERSTAR-AS	OJSC MegaFon	↔ peer
244	42708	PORTLANE	Portlane Networks AB	↔ peer
310	8492	OBIT-AS	Obit Telecommunications, St.Petersburg, Russia	↔ peer
326	21385	TNIB	TNIB	↔ peer
433	8426	CLARANET-AS	ClaraNET LTD	↔ peer
595	12779	ITGATE	ITGate.NET	↔ peer
698	8331	RINET-AS	Cronyx Plus Ltd	↔ peer
767	8596	HOTZE-AS	hotze.com GmbH	↔ peer
806	12859	NL-BIT	BIT BV	↔ peer

Продолжение таблицы Е.3

984	48166	FORTEX-AS	FORTEX-AS	↔ peer
1045	2895	FREE-NET-AS	FREEnet	↔ peer
1313	553	BELWUE	Init7 Global Backbone	↔ peer
1339	48039	KGT-AS	KGT new media	↔ peer
1739	24989	IXEUROPE-D...	NETCOLOGNE AS	↔ peer
2166	36351	SOFTLAYER	SoftLayer Technologies Inc.	↔ peer
2634	25220	GLOBALNOC-AS	Averbo GmbH	↔ peer
2913	34288	AS34288	Public Schools in the Canton of Zug	↔ peer
2948	9189	ACCOM	NetAachen GmbH	↔ peer
3671	29140	HOSTSERVER-AS	IAG-AS	↔ peer
6935	20640	TITAN-NETW...	Titan Networks Internet & Telecommunications	↔ peer
8521	39821	CANMOS-AS	CANMOS-AS	↔ peer
8554	31019	MEANIE	Prolocation AS	↔ peer
8557	197780	CMIRIT-AS	CMIRIT-AS	↓ customer

Приложение Ж. Листинг программы – имитационное моделирование протокола ZRTP

```
<?    session_start();   ?>
<!DOCTYPE html>
<head>
<title>ZRTP immitation model software v5</title>
</head>
<?
$p=1;   $t=1;     $tm=15000;//time of experiment
$msg_size_lib["HB"]=1456+560;   $msg_size_lib["HA"]=1456+560;
$msg_size_lib["Commit"]=1392;   $msg_size_lib["DH1"]=3184;
$msg_size_lib["DH2"]=3184;      $msg_size_lib["Confirm1"]=1072;
$msg_size_lib["Confirm2"]=1072; $msg_size_lib["Conf2ACK"]=560;
$msg_resend_lib["HA"][0]=50;    $msg_resend_lib["HA"][1]=100;
$msg_resend_lib["HA"][2]=200;   $msg_resend_lib["Commit"][0]=150;
$msg_resend_lib["Commit"][1]=300; $msg_resend_lib["Commit"][2]=600;
$msg_resend_lib["Commit"][2]=1200;
$msg_size_lib["RND_MIN"]=1;   $msg_size_lib["RND_MAX"]=1500;
$msg_size_lib["RND"]=rand($msg_size_lib["RND_MIN"],$msg_size_lib["RND_MAX"]);
$msg_size_lib["HB_Commit_DH1"]=$msg_size_lib["HB"]+$msg_size_lib["Commit"]+$msg_size_li
b["Confirm1"];
$msg_size_lib["DH2_Confirm1"]=$msg_size_lib["DH2"]+$msg_size_lib["Confirm1"];
$ch[0]["refreshcounter"]=0;
$_SESSION['p0']= 0.0001; $ch[0]["p0"]=$_SESSION['p0'];
$_SESSION['d']=100; $ch[0]["d"]=$_SESSION['d'];
$samplesize=2*(round(1/$ch[0]["p0"])-1);
$model["samplesize"]=$samplesize;
$model["icmp_count"]=100;
$icmp_pkt_size=1744;   //$samplesize/100;//1304
$ev_err_ratio=$ch[0]["p0"];

function ProcessOverChannel($msg_size,$p=0)
{
global $ev, $evc,$ch;
$strt_ev=$evc;
$if_error=0;
if ($strt_ev+$msg_size>=count($ev))
          { $strt_ev=0;
          $evc=0;
          shuffle($ev);
          $ch[0]["refreshcounter"]++;
          }
$errors=array_slice($ev, $strt_ev, $msg_size);
$if_error=array_sum($errors);
$evc=$evc+$msg_size;
$ch[0]["total_rx_bits"]=$ch[0]["total_rx_bits"]+$msg_size;
$ch[0]["total_discard_bits"]=$ch[0]["total_discard_bits"]+$if_error;
```

```
        if ($if_error) {  return 0;}
        else {  return 1;  }
}

function AggentCreate ($AgentId, $AgentType)
{
global $ev, $evc, $agent, $t;
        if (!isset($agent[$AgentId]["type"]))
        {
          $agent[$AgentId]["type"]=$AgentType;
          $agent[$AgentId]["state"]="Start";
          $agent[$AgentId]["time2act"]=0;
          $agent[$AgentId]["repeat_counter"]=0;
          $agent[$AgentId]["timestarted"]=$t;
        }
else echo "Agent ",$AgentId , " exists<br>";
}

function AggentProcess ($AgentId, $RAgentId=0)
{
global $ev, $evc, $agent,$t,$msg_resend_lib,$packet,$tm,$msg_size_lib;
if (!isset($agent[$AgentId]["type"]))
        {
          die("Agent  NOT exists<br>");
        }
if ($agent[$AgentId]["rx"][$t])
      { //Incomming packet exist
  if ($agent[$AgentId]["type"]=="ZRTPResp" &&
$packet[$agent[$AgentId]["rx"][$t]]["content"]=="HA")
                {
 $RAgentId=$packet[$agent[$AgentId]["rx"][$t]]["src"];
 CreatePacket($RAgentId, "HB", $AgentId);
            }
 if ($agent[$AgentId]["type"]=="ZRTPInit"  && $agent[$AgentId]["state"]=="WaitHB" &&
$packet[$agent[$AgentId]["rx"][$t]]["content"]=="HB")
                {
 $RAgentId=$packet[$agent[$AgentId]["rx"][$t]]["src"];
 CreatePacket($RAgentId, "Commit", $AgentId);
 $agent[$AgentId]["repeat_counter"]=0;
 $agent[$AgentId]["time2act"]=$t+$msg_resend_lib["Commit"][0];
 $agent[$AgentId]["state"]="WaitDH1";
          }
 if ($agent[$AgentId]["type"]=="ZRTPResp" &&
$packet[$agent[$AgentId]["rx"][$t]]["content"]=="Commit")
                {
 $RAgentId=$packet[$agent[$AgentId]["rx"][$t]]["src"];
 CreatePacket($RAgentId, "DH1", $AgentId);
            }
 if ($agent[$AgentId]["type"]=="ZRTPInit"  && $agent[$AgentId]["state"]=="WaitDH1" &&
$packet[$agent[$AgentId]["rx"][$t]]["content"]=="DH1")
                {
```

```
$RAgentId=$packet[$agent[$AgentId]["rx"][$t]]["src"];
CreatePacket($RAgentId, "DH2", $AgentId);
$agent[$AgentId]["repeat_counter"]=0;
            $agent[$AgentId]["time2act"]=$t+$msg_resend_lib["Commit"][0];
$agent[$AgentId]["state"]="WaitConfirm1";
        }
if ($agent[$AgentId]["type"]=="ZRTPResp" &&
$packet[$agent[$AgentId]["rx"][$t]]["content"]=="DH2")
                {
$RAgentId=$packet[$agent[$AgentId]["rx"][$t]]["src"];
CreatePacket($RAgentId, "Confirm1", $AgentId);
            }
if ($agent[$AgentId]["type"]=="ZRTPInit" && $agent[$AgentId]["state"]=="WaitConfirm1" &&
$packet[$agent[$AgentId]["rx"][$t]]["content"]=="Confirm1")
                {
$RAgentId=$packet[$agent[$AgentId]["rx"][$t]]["src"];
CreatePacket($RAgentId, "Confirm2", $AgentId);
$agent[$AgentId]["repeat_counter"]=0;
$agent[$AgentId]["time2act"]=$t+$msg_resend_lib["Commit"][0];
$agent[$AgentId]["state"]="WaitConf2ACK";
        }
if ($agent[$AgentId]["type"]=="ZRTPResp" &&
$packet[$agent[$AgentId]["rx"][$t]]["content"]=="Confirm2")
                {
$RAgentId=$packet[$agent[$AgentId]["rx"][$t]]["src"];
CreatePacket($RAgentId, "Conf2ACK", $AgentId);
$agent[$AgentId]["state"]="Finished";
            }
if ($agent[$AgentId]["type"]=="ZRTPInit" && $agent[$AgentId]["state"]=="WaitConf2ACK" &&
$packet[$agent[$AgentId]["rx"][$t]]["content"]=="Conf2ACK")
                {
$RAgentId=$packet[$agent[$AgentId]["rx"][$t]]["src"];
$agent[$AgentId]["repeat_counter"]=0;
$agent[$AgentId]["state"]="Finished";
$agent[$AgentId]["timefinished"]=$t;
        }
if ($agent[$AgentId]["type"]=="ZRTPRespM2" &&
$packet[$agent[$AgentId]["rx"][$t]]["content"]=="HA")
                {
$RAgentId=$packet[$agent[$AgentId]["rx"][$t]]["src"];
CreatePacket($RAgentId, "HB_Commit_DH1", $AgentId);
            }
if ($agent[$AgentId]["type"]=="ZRTPInitM2"  && $agent[$AgentId]["state"]=="WaitHB" &&
$packet[$agent[$AgentId]["rx"][$t]]["content"]=="HB_Commit_DH1")
                {
$RAgentId=$packet[$agent[$AgentId]["rx"][$t]]["src"];
CreatePacket($RAgentId, "DH2_Confirm1", $AgentId);
$agent[$AgentId]["repeat_counter"]=0;
$agent[$AgentId]["time2act"]=$t+$msg_resend_lib["Commit"][0];
$agent[$AgentId]["state"]="WaitConfirm2";
        }
```

```
          if ($agent[$AgentId]["type"]=="ZRTPRespM2" &&
$packet[$agent[$AgentId]["rx"][$t]]["content"]=="DH2_Confirm1")
                {
$RAgentId=$packet[$agent[$AgentId]["rx"][$t]]["src"];
 CreatePacket($RAgentId, "Confirm2", $AgentId);
 $agent[$AgentId]["state"]="Finished";
           }
 if ($agent[$AgentId]["type"]=="ZRTPInitM2" && $agent[$AgentId]["state"]=="WaitConfirm2" &&
$packet[$agent[$AgentId]["rx"][$t]]["content"]=="Confirm2")
                {
 $RAgentId=$packet[$agent[$AgentId]["rx"][$t]]["src"];
 $agent[$AgentId]["repeat_counter"]=0;
 $agent[$AgentId]["state"]="Finished";
 $agent[$AgentId]["timefinished"]=$t;
          }
}
else if ($agent[$AgentId]["time2act"]<=$t)
           {
  if ($agent[$AgentId]["type"]=="RNDDATA")
         {
         $msg_size_lib["RND"]=rand($msg_size_lib["RND_MIN"],$msg_size_lib["RND_MAX"]);
                CreatePacket($RAgentId, "RND", $AgentId);
                $agent[$AgentId]["time2act"]=$t+rand(1,300);
           }
  if ($agent[$AgentId]["type"]=="ZRTPInit" && $agent[$AgentId]["state"]=="Start")
         {
                CreatePacket($RAgentId, "HA", $AgentId);
                $agent[$AgentId]["state"]="WaitHB";

         $agent[$AgentId]["time2act"]=$t+$msg_resend_lib["HA"][$agent[$AgentId]["repeat_counter"
]];
                 }
            else
  if ($agent[$AgentId]["type"]=="ZRTPInit" && $agent[$AgentId]["state"]=="WaitHB" &&
$agent[$AgentId]["time2act"]<=$t)
         {      $agent[$AgentId]["repeat_counter"]++;
                CreatePacket($RAgentId, "HA", $AgentId);
                if (!$msg_resend_lib["HA"][$agent[$AgentId]["repeat_counter"]])
$msg_resend_lib["HA"][$agent[$AgentId]["repeat_counter"]]=200;

         $agent[$AgentId]["time2act"]=$t+$msg_resend_lib["HA"][$agent[$AgentId]["repeat_counter"
]];
                if ($agent[$AgentId]["repeat_counter"]>20) {
             $agent[$AgentId]["state"]="ProtocolFailed";
$agent[$AgentId]["time2act"]=$tm;
              echo "Set agent ",$AgentId," ProtocolFailed -  agent[$AgentId][time2act] to
",$agent[$AgentId]["time2act"],"<br>";
         }
                }
            else
```

```
 if ($agent[$AgentId]["type"]=="ZRTPInit" && $agent[$AgentId]["state"]=="WaitDH1" &&
$agent[$AgentId]["time2act"]<=$t)
        {       $agent[$AgentId]["repeat_counter"]++;
                CreatePacket($RAgentId, "Commit", $AgentId);
                if (!$msg_resend_lib["Commit"][$agent[$AgentId]["repeat_counter"]])
$msg_resend_lib["Commit"][$agent[$AgentId]["repeat_counter"]]=1200;

        $agent[$AgentId]["time2act"]=$t+$msg_resend_lib["Commit"][$agent[$AgentId]["repeat_cou
nter"]];
                if ($agent[$AgentId]["repeat_counter"]>10) {
            $agent[$AgentId]["state"]="ProtocolFailed";
$agent[$AgentId]["time2act"]=$tm;
             echo "Set agent ",$AgentId," ProtocolFailed -  agent[$AgentId][time2act] to
",$agent[$AgentId]["time2act"],"<br>";
        }
                }
           else
 if ($agent[$AgentId]["type"]=="ZRTPInit" && $agent[$AgentId]["state"]=="WaitConfirm1" &&
$agent[$AgentId]["time2act"]<=$t)
        {       $agent[$AgentId]["repeat_counter"]++;
                CreatePacket($RAgentId, "DH2", $AgentId);
                if (!$msg_resend_lib["Commit"][$agent[$AgentId]["repeat_counter"]])
$msg_resend_lib["Commit"][$agent[$AgentId]["repeat_counter"]]=1200;

        $agent[$AgentId]["time2act"]=$t+$msg_resend_lib["Commit"][$agent[$AgentId]["repeat_cou
nter"]];
                if ($agent[$AgentId]["repeat_counter"]>10) {
            $agent[$AgentId]["state"]="ProtocolFailed";
$agent[$AgentId]["time2act"]=$tm;
             echo "Set agent ",$AgentId," ProtocolFailed -  agent[$AgentId][time2act] to
",$agent[$AgentId]["time2act"],"<br>";
        }
                }
           else
 if ($agent[$AgentId]["type"]=="ZRTPInit" && $agent[$AgentId]["state"]=="WaitConf2ACK" &&
$agent[$AgentId]["time2act"]<=$t)
        {       $agent[$AgentId]["repeat_counter"]++;
                CreatePacket($RAgentId, "Confirm2", $AgentId, $agent[$AgentId]["repeat_counter"]);
                if (!$msg_resend_lib["Commit"][$agent[$AgentId]["repeat_counter"]])
$msg_resend_lib["Commit"][$agent[$AgentId]["repeat_counter"]]=1200;

        $agent[$AgentId]["time2act"]=$t+$msg_resend_lib["Commit"][$agent[$AgentId]["repeat_cou
nter"]];
                if ($agent[$AgentId]["repeat_counter"]>10) {
            $agent[$AgentId]["state"]="ProtocolFailed";
$agent[$AgentId]["time2act"]=$tm;
             echo "Set agent ",$AgentId," ProtocolFailed -  agent[$AgentId][time2act] to
",$agent[$AgentId]["time2act"],"<br>";
        }
                }
        if ($agent[$AgentId]["type"]=="ZRTPInitM2" && $agent[$AgentId]["state"]=="Start")
```

```
        {
                CreatePacket($RAgentId, "HA", $AgentId);
                $agent[$AgentId]["state"]="WaitHB";

        $agent[$AgentId]["time2act"]=$t+$msg_resend_lib["HA"][$agent[$AgentId]["repeat_counter"
]];
                 }
            else
  if ($agent[$AgentId]["type"]=="ZRTPInitM2" && $agent[$AgentId]["state"]=="WaitHB" &&
$agent[$AgentId]["time2act"]<=$t)
        {       $agent[$AgentId]["repeat_counter"]++;
                CreatePacket($RAgentId, "HA", $AgentId);
                if (!$msg_resend_lib["HA"][$agent[$AgentId]["repeat_counter"]])
$msg_resend_lib["HA"][$agent[$AgentId]["repeat_counter"]]=200;

        $agent[$AgentId]["time2act"]=$t+$msg_resend_lib["HA"][$agent[$AgentId]["repeat_counter"
]];
                if ($agent[$AgentId]["repeat_counter"]>20) {
             $agent[$AgentId]["state"]="ProtocolFailed";
$agent[$AgentId]["time2act"]=$tm;
              echo "Set agent ",$AgentId," ProtocolFailed -  agent[$AgentId][time2act] to
",$agent[$AgentId]["time2act"],"<br>";
             }
                }
            else
  if ($agent[$AgentId]["type"]=="ZRTPInitM2" && $agent[$AgentId]["state"]=="WaitConfirm2" &&
$agent[$AgentId]["time2act"]<=$t)
        {       $agent[$AgentId]["repeat_counter"]++;
                CreatePacket($RAgentId, "DH2_Confirm1", $AgentId);
                if (!$msg_resend_lib["Commit"][$agent[$AgentId]["repeat_counter"]])
$msg_resend_lib["Commit"][$agent[$AgentId]["repeat_counter"]]=1200;

        $agent[$AgentId]["time2act"]=$t+$msg_resend_lib["Commit"][$agent[$AgentId]["repeat_cou
nter"]];
                if ($agent[$AgentId]["repeat_counter"]>10) {
             $agent[$AgentId]["state"]="ProtocolFailed";
$agent[$AgentId]["time2act"]=$tm;
              echo "Set agent ",$AgentId," ProtocolFailed -  agent[$AgentId][time2act] to
",$agent[$AgentId]["time2act"],"<br>";
        }
                }
}
}
function CreatePacket($RAgentId, $content, $AgentId, $r="")
{
global $ev, $evc, $p, $t, $agent,$packet,$msg_size_lib;
$packet[$p]["content"]=$content;
$packet[$p]["length"]=$msg_size_lib[$content];
$packet[$p]["src"]=$AgentId;
$packet[$p]["dsc"]=$RAgentId;
$packet[$p]["tsend"]=$t;
```

```
$packet[$p]["trecv"]="";
$packet[$p]["r"]=$r;
$packet[$p]["notdropped"]=1;
SendPacket($p);
$p++;
}

function SendPacket($pkt_id)
{
global $ev, $evc, $p, $t, $agent,$packet,$ch, $msg_size_lib,$tm;
if (ProcessOverChannel($packet[$pkt_id]["length"],$packet))
          {
           $packet_rx_time=$t+$ch[0]["d"];
           $agent[$packet[$pkt_id]["dsc"]]["rx"][$packet_rx_time]=$pkt_id;
           $packet[$pkt_id]["trecv"]=$packet_rx_time;
          }
else  {  $packet[$pkt_id]["notdropped"]=0;    }
}

$i=0;
for ($l=0; $l<$ev_err_ratio*$samplesize; $l++) $ev[$i+$l]=1;
for ($i=0; $i<(1-$ev_err_ratio)*$samplesize; $i++) $ev[$i+$l]=0;
$model["p0_cacl"]=$l/($l+$i);
$model["ppl_cacl_icmp"]=1-pow((1-$model["p0_cacl"]),$icmp_pkt_size);  //1-(1-p0)^pkt_size
shuffle($ev);
$evc=0;
 AggentCreate (1, "ZRTPInit");
 AggentCreate (2, "ZRTPResp");
 AggentCreate (3, "ZRTPInitM2");
 AggentCreate (4, "ZRTPRespM2");
 AggentCreate (5, "RNDDATA");
 AggentCreate (6, "RNDDATA");
 $agent[2]["time2act"]=$tm;
  for ($i=0; $i<=$tm; $i++)
   {
    AggentProcess (1, 2);
          AggentProcess (2, 1);
          AggentProcess (5, 6);
    AggentProcess (3, 4);
          AggentProcess (4, 3);
          AggentProcess (6, 5);
           $t++;
          }

 echo "ZRTP<br><pre>t       src       msg               dsc       t_rcv<br>";
  foreach($packet as $k => $v) {
   if ($packet[$k]["notdropped"])
      { if ($packet[$k]['src']==1)  echo $packet[$k]['tsend'],"", $packet[$k]['src'], "---
",$packet[$k]['content'],"--",$packet[$k]['r'],"->       ", $packet[$k]['dsc']," ",$packet[$k]['trecv'],"<br>";
             else  if ($packet[$k]['src']==2)  echo $packet[$k]['tsend']," ", $packet[$k]['dsc'], "
          <---",$packet[$k]['content'],"---         ", $packet[$k]['src']," ",$packet[$k]['trecv'],"<br>";
```

```
    }
        else
    { if ($packet[$k]['src']==1)  echo $packet[$k]['tsend'],"", $packet[$k]['src'], "---
",$packet[$k]['content'],"--->X<br>";
            else  if ($packet[$k]['src']==2)  echo $packet[$k]['tsend']," X---
",$packet[$k]['content'],"---   ", $packet[$k]['src'],"<br>";
    }
}
 echo "ZRTP MOD2<br>
 t       src      msg              dsc      t_rcv<br> ";
  foreach($packet as $k => $v) {
   if ($packet[$k]["notdropped"])
    {  if ($packet[$k]['src']==3)  echo $packet[$k]['tsend']," ", $packet[$k]['src'], "---
",$packet[$k]['content'],"--",$packet[$k]['r'],"->      ", $packet[$k]['dsc']," ",$packet[$k]['trecv'],"<br>";
            else  if ($packet[$k]['src']==4)  echo $packet[$k]['tsend']," ", $packet[$k]['dsc'], "
        <---",$packet[$k]['content'],"---       ", $packet[$k]['src']," ",$packet[$k]['trecv'],"<br>";
    }
        else
    {  if ($packet[$k]['src']==3)  echo $packet[$k]['tsend']," ", $packet[$k]['src'], "---
",$packet[$k]['content'],"--->X<br>";
            else  if ($packet[$k]['src']==4)  echo $packet[$k]['tsend']," X---
",$packet[$k]['content'],"---   ", $packet[$k]['src'],"<br>";
    }
}
$zrtp_T_avg=($agent[1]["timefinished"]-$agent[1]["timestarted"])/1000;
$zrtpM2_T_avg=($agent[3]["timefinished"]-$agent[3]["timestarted"])/1000;
$rez=date("Y-m-d H:i:s").'    '.$ch[0]["d"].'  '.$ch[0]["p0"].'          '.$zrtp_T_avg.'          ms
        '.$agent[1]["state"].'   '.$model["p0_cacl"].' '.$model["ppl_cacl_icmp"].'
        '.$model["samplesize"].'       '.$ch[0]["total_discard_bits"]/$ch[0]["total_rx_bits"].'
';
$rez2=date("Y-m-d H:i:s").'  '.$ch[0]["d"].'  '.$ch[0]["p0"].'          '.$zrtpM2_T_avg.'     ms
        '.$agent[3]["state"].'   '.$model["p0_cacl"].' '.$model["ppl_cacl_icmp"].'
        '.$model["samplesize"].'       '.$ch[0]["total_discard_bits"]/$ch[0]["total_rx_bits"].'
';
echo "dated(ms)        p0       T_avg_ZRTP(ms) <br><br>",$rez,"<br>",$rez2;
?>
```