А.М. Голиков

ЗАЩИТА ИНФОРМАЦИИ В РАДИОЭЛЕКТРОННЫХ СИСТЕМАХ ПЕРЕДАЧИ ИНФОРМАЦИИ

Сборник компьютерных лабораторных работ

Томск 2018

Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное
учреждение высшего образования
Томский государственный университет систем управления
и радиоэлектроники

А.М. ГОЛИКОВ

ЗАЩИТА ИНФОРМАЦИИ В РАДИОЭЛЕКТРОННЫХ СИСТЕМАХ ПЕРЕДАЧИ ИНФОРМАЦИИ

Сборник компьютерных лабораторных работ

Томск 2018

УДК 621.39(075.8)

ББК 32.973(я73)

Голиков, А. М. Защита информации в радиоэлектронных системах передачи информации: Сборник компьютерных лабораторных работ [Электронный ресурс] / А. М. Голиков. — Томск: ТУСУР, 2018. — 226 с. — Режим доступа: https://edu.tusur.ru/publications/8806

Сборник компьютерных лабораторных работ предназначен для направления подготовки магистров 11.04.02 "Инфокоммуникационные технологии и системы связи" по магистерским программам подготовки: "Радиоэлектронные системы передачи информации", "Оптические системы связи и обработки информации", "Инфокоммуникационные системы беспроводного широкополосного доспупа", "Защищенные системы связи", для направления подготовки магистров 11.04.01 "Радиотехника" по магистерской программе подготовки: "Радиотехнические системы и комплексы", "Радиоэлектронные устройства передачи информации", "Системы и устройства передачи, приема и обработки сигналов", "Видеоинформационные технологии и цифровое телевидение" и специалитета 11.05.01 "Радиоэлектронные системы и комплексы" специализации "Радиолокационные системы и комплексы", "Радиоэлектронные системы передачи информации", "Радиоэлектронные системы космических комплексов", а также бакалавриата направления 11.03.01 "Радиотехника" (Радиотехнические средства передачи, приема и обработки сигналов), бакалавриата 11.03.02 Инфокоммуникационные технологии и системы связи (Системы мобильной связи, Защищенные системы и сети связи, Системы радиосвязи и радиодоступа, Оптические системы и сети связи) и может быть полезна аспирантам. Представлены описания программных комплексов и методики выполнения лабораторных и практических работ.

СОДЕРЖАНИЕ

Лабораторная работа 1. Исследование системы анализа рисков и проверки политики информационной безопасности предприятия

Основные определения

Безопасность (защищенность) информации в компьютерных системах (КС) - это такое состояние всех компонент КС, при котором обеспечивается защита информации от возможных угроз на требуемом уровне. Компьютерные системы, в которых обеспечивается безопасность информации, называются защищенными [1].

Информационная безопасность достигается проведением руководством соответствующего уровня *политики информационной безопасности***.** Основным документом, на основе которого проводится политика информационной безопасности, является *программа информационной безопасности***.** Этот документ разрабатывается и принимается как официальный руководящий документ высшими органами управления организацией. В документе приводятся цели политики информационной безопасности и основные направления решения задач защиты информации в КС. В программах информационной безопасности содержатся также общие требования и принципы построения систем защиты информации в КС.

Под *системой защиты информации в КС* понимается единый комплекс правовых норм, организационных мер, технических, программных и криптографических средств, обеспечивающий защищенность информации в КС в соответствии с принятой политикой безопасности.

Угроза безопасности - потенциально возможное происшествие, которое может оказать воздействие на информацию в системе.

Уязвимость - некая неудачная характеристика системы, которая делает возможным возникновение угрозы.

Атака - действие по использованию уязвимости КС; атака - это реализация угрозы.

Угроза конфиденциальности - угроза раскрытия информации.

Угроза целостности - угроза изменения информации.

Угроза доступности - угроза нарушения работоспособности системы при доступе к информации.

Ущерб - стоимость потерь, которые понесет компания в случае реализации угроз конфиденциальности, целостности, доступности по каждому виду ценной информации. Ущерб зависит только от стоимости информации, которая обрабатывается в автоматизированной системе. Ущерб является характеристикой информационной системы и не зависит от ее защищенности.

Риск - вероятный ущерб, который зависит от защищенности системы. По определению риск всегда измеряется в деньгах.

В сущности, для коммерческой организации задача безопасного функционирования информационной системы сводится к выработке правил и выбору защитных средств. Комбинация двух этих составляющих позволит обеспечить необходимый уровень безопасности, как для ценных ресурсов организации, так и для всей информационной системы обработки этих ресурсов. Другими словами задача защиты – это разработка эффективной политики безопасности (или правил безопасности).

Чтобы меры политики безопасности по защите отвечали реальному состоянию дел необходимо знать - что, от кого и в какой степени нужно защищать. На сегодня существует только один процесс, способный в какой то мере дать ответы на поставленные вопросы, речь идет об анализе рисков.

Обзор программных продуктов в области анализа рисков и проверки организационных мер обеспечения информационной безопасности

В настоящее время имеется большое разнообразие как методов анализа и управления рисками, так и реализующих их программных средств. Приведем примеры некоторых отечественных продуктов.

Программный комплекс анализа и контроля рисков информационных систем компании – ГРИФ.

Для проведения полного анализа информационныхрисков прежде всего необходимо построить полную модель информационной системы с точки зрения ИБ. Для решения этой задачи ГРИФ, в отличие от представленных на рынке западных систем анализа рисков, которые громоздки, сложны в использовании и часто не предполагают самостоятельного применения ИТ-менеджерами и системными администраторами, ответственными за обеспечение безопасности информационных систем компаний, обладает простым и интуитивно понятным для пользователя интерфейсом. Однако за внешней простотой скрывается сложнейший алгоритм анализа рисков, учитывающий более ста параметров, который позволяет на выходе дать максимально точную оценку существующих

в информационной системе рисков, основанную на глубоком анализе особенностей практической реализации информационной системы. Основная задача системы ГРИФ – дать возможность ИТ- менеджеру самостоятельно (без привлечения сторонних экспертов) оценить уровень рисков в информационной системе, оценить эффективность существующей практики по обеспечению безопасности компании и иметь возможность доказательно (в цифрах) убедить топ-менеджмент компании в необходимости инвестиций в сферу информационной безопасности компании [2].

На первом этапе система ГРИФ проводит опрос ИТ-менеджера с целью определения полного списка информационных ресурсов, представляющих ценность для компании.

На втором этапе проводится опрос ИТ-менеджера с целью ввода в систему ГРИФ всех видов информации, представляющей ценность для компании. Введенные группы ценной информации должны быть размещены пользователем на ранее указанных на предыдущем этапе объектах хранения информации (серверах, рабочих станциях и так далее). Заключительная фаза – указание ущерба по каждой группе ценной информации, расположенной на соответствующих ресурсах, по всем видам угроз.

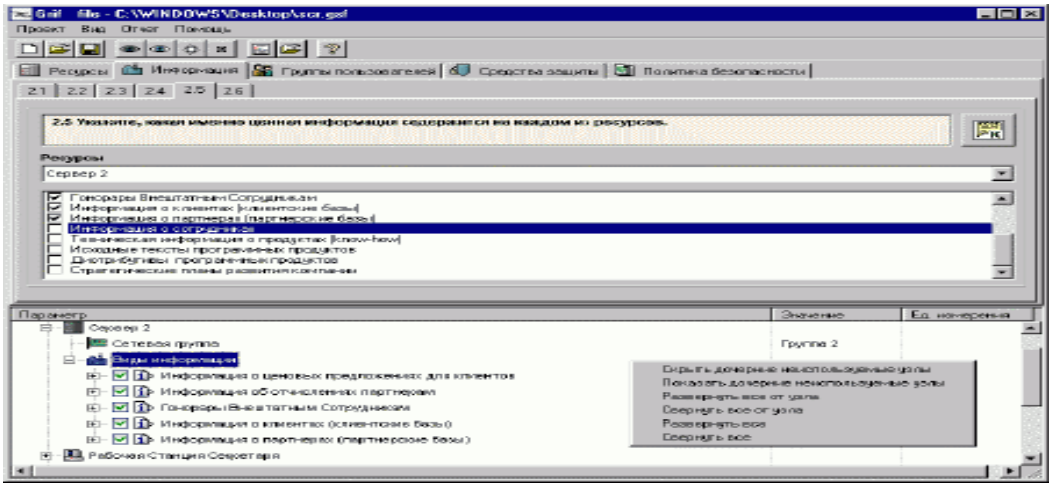


Рис.1. Интерфейс программного комплекса Гриф. Вкладка «Информация».

На третьем этапе вначале проходит определение всех видов пользовательских групп (и число пользователей в каждой группе). Затем определяется, к каким группам информации на ресурсах имеет доступ каждая из групп пользователей. В заключение определяются виды (локальный и/или удаленный) и права (чтение, запись, удаление) доступа пользователей ко всем ресурсам, содержащим ценную информацию.

На четвертом этапе проводится опрос ИТ-менеджера для определения средств защиты информации, которыми защищена ценная информация на ресурсах. Кроме того, в систему вводится информация о разовых затратах на приобретение всех применяющихся средств

защиты информации и ежегодные затраты на их техническую поддержку, а также ежегодные затраты на сопровождение системы информационной безопасности компании.

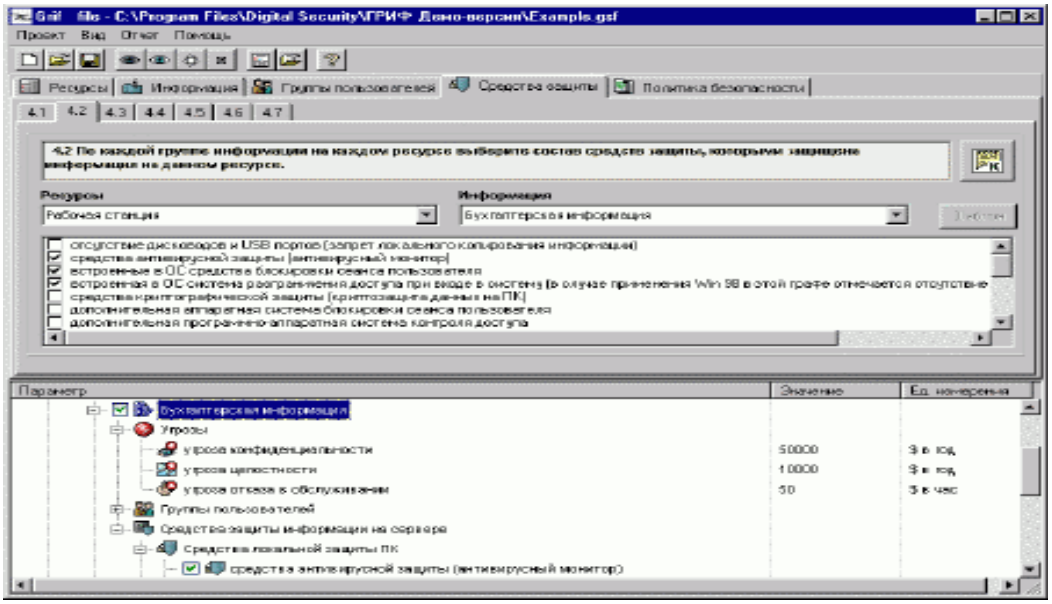


Рис. 2. Интерфейс программного комплекса Гриф. Вкладка «Средства защиты».

На завершающем этапе пользователь должен ответить на список вопросов по политике безопасности, реализованной в системе, что позволяет оценить реальный уровень защищенности системы и детализировать оценки рисков.

Наличие средств информационной защиты, отмеченных на первом этапе, само по себе еще не делает систему защищенной в случае их неадекватного использования и отсутствия комплексной политики безопасности, учитывающей все аспекты защиты информации, включая вопросы организации защиты, физической безопасности, безопасности персонала, непрерывности ведения бизнеса и так далее.

В результате выполнения всех действий по данным этапам на выходе сформирована полная модель информационной системы с точки зрения информационной безопасности с учетом реального выполнения требований комплексной политики безопасности, что позволяет перейти к программному анализу введенных данных для получения комплексной оценки рисков и формирования итогового отчета.

Отчет по системе представляет собой подробный, дающий полную картинувозможного ущерба от инцидентов документ, готовый для представления руководству компании.

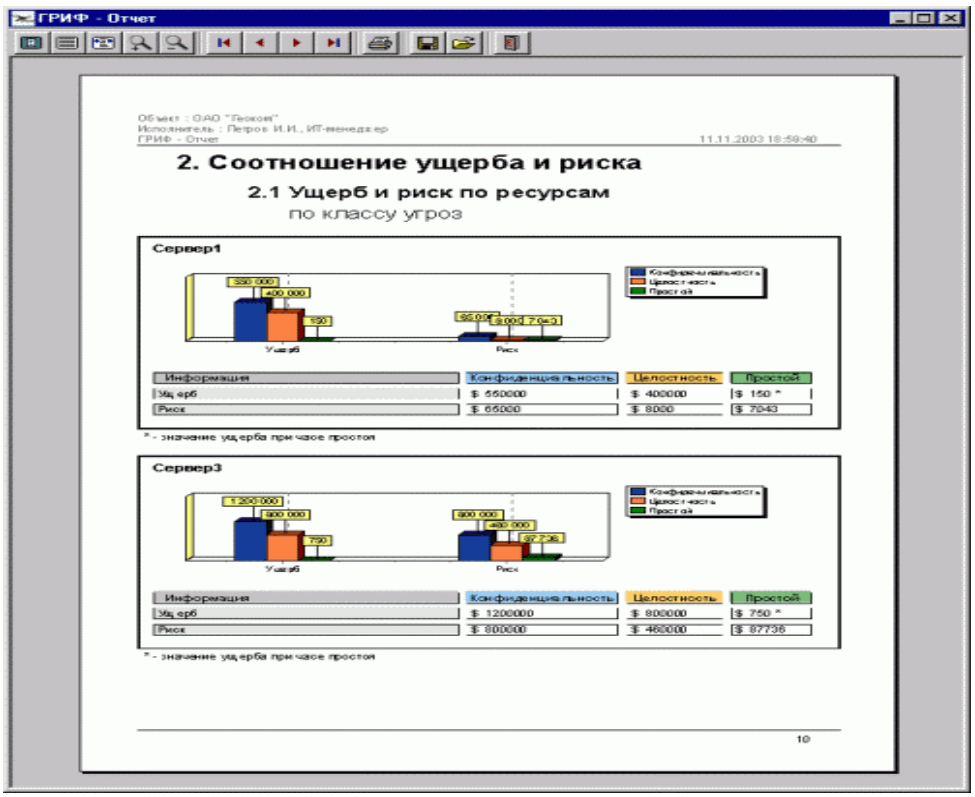


Рис.3. Интерфейс программного комплекса Гриф. Реализация отчета.

К недостаткам ГРИФ можно отнести следующее:

- отсутствует привязка к бизнес процессам (запланировано в следующей версии);
- нет возможности сравнения отчетов на разных этапах внедрения комплекса мер по обеспечению защищенности (запланировано в следующей версии);
- отсутствует возможность добавить специфичные для данной компании требования политики безопасности.

1.2. Программный комплекс управления политикой информационной безопасности компании - КОНДОР+

Российская компания Digital Security разработала программный продукт КОНДОР+, позволяющий специалистам (ИТ-менеджерам, офицерам безопасности) проверить политику информационной безопасности компании на соответствие требованиям международного стандарта безопасности ISO 17799.

Разработанный программный комплекс КОНДОР+ включает в себя более двухсот вопросов, ответив на которые, специалист получает подробный отчет о состоянии существующей политики безопасности, а так же модуль оценки уровня рисков соответствия требованиям ISO 17799 [3].

После регистрации пользователь получает возможность, выбрать соответствующий раздел стандарта ISO 17799 и ответить на вопросы.

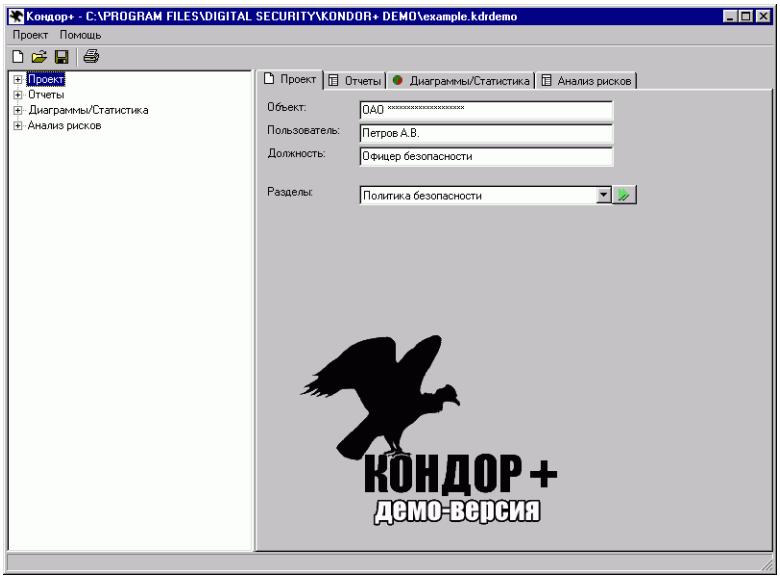


Рис.4. Интерфейс программного комплекса Кондор. Вкладка проект.

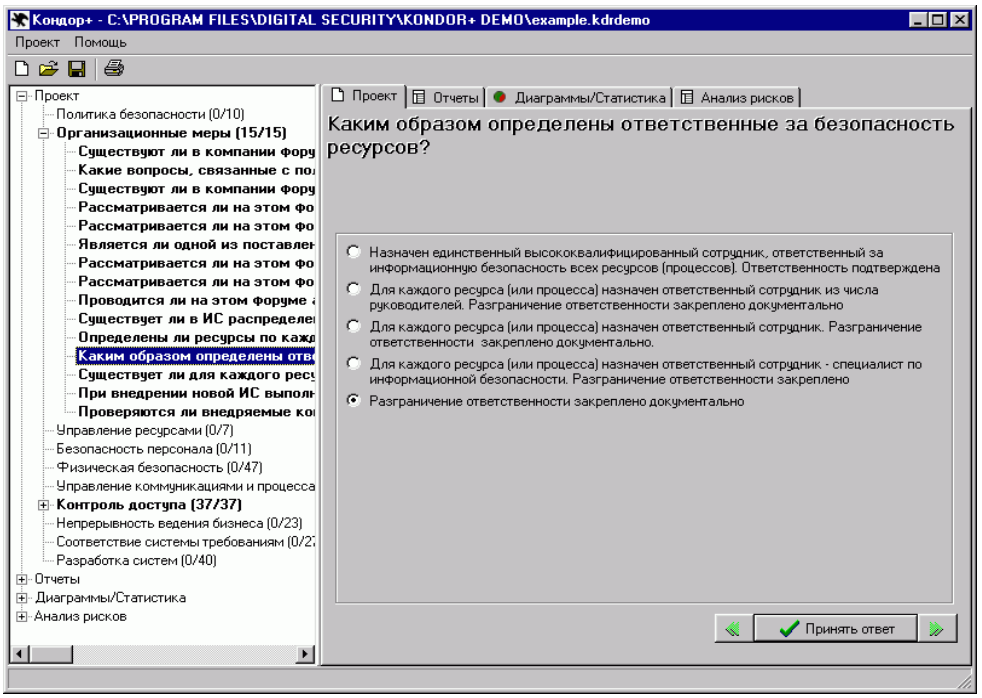


Рис.5. Интерфейс программного комплекса Кондор. Выбор раздела стандарта.

В отчете отражаются все положения политики безопасности, которые соответствуют стандарту и все, которые не соответствуют.

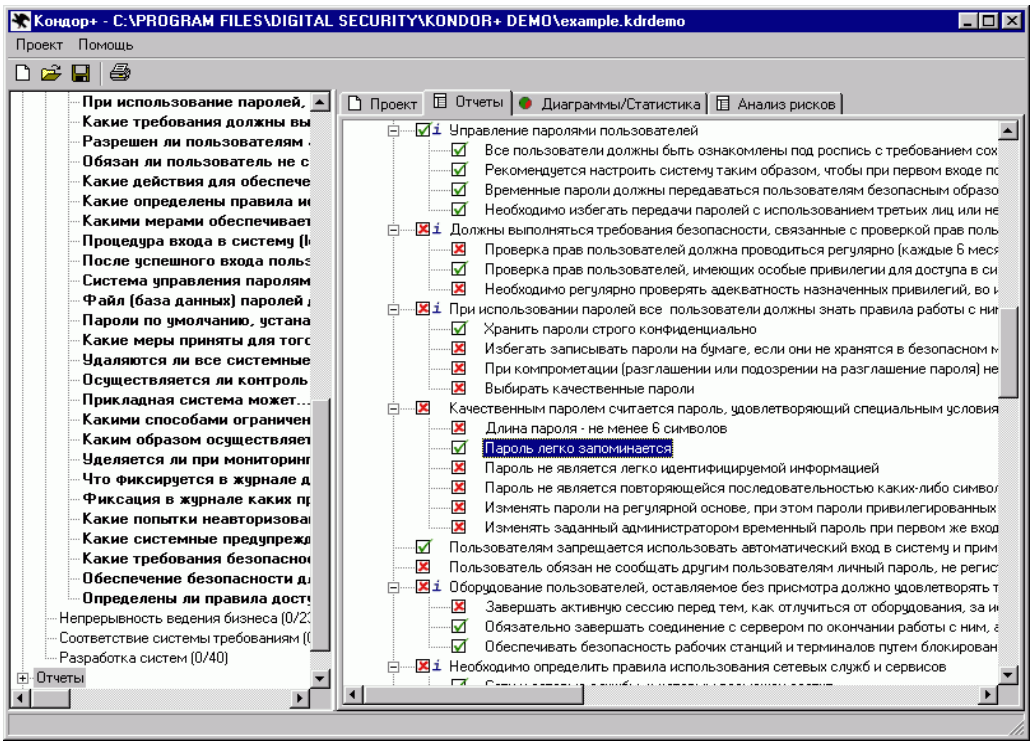


Рисунок.1.6. Интерфейс программного комплекса Кондор. Реализация отчета.

К наиболее важным элементам политики безопасности даются комментарии и рекомендации экспертов.

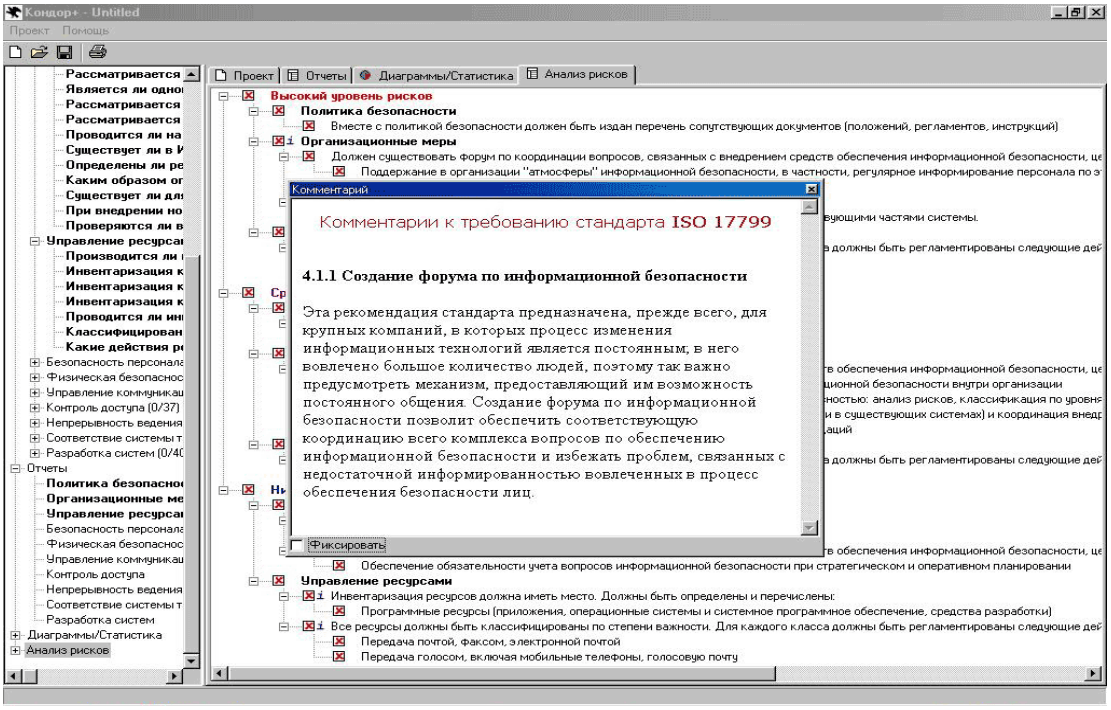


Рис.8. Интерфейс программного комплекса Кондор. Комментарии.

По желанию специалиста, работающего с программой, может быть выбрана генерация отчета, например, по какому-то одному или нескольким разделам стандарта ISO 17799,

общий подробный отчет с комментариями, общий отчет о состоянии политики безопасности без комментариев для представления руководству и другие. Все варианты отчетов для большей наглядности сопровождаются диаграммами.

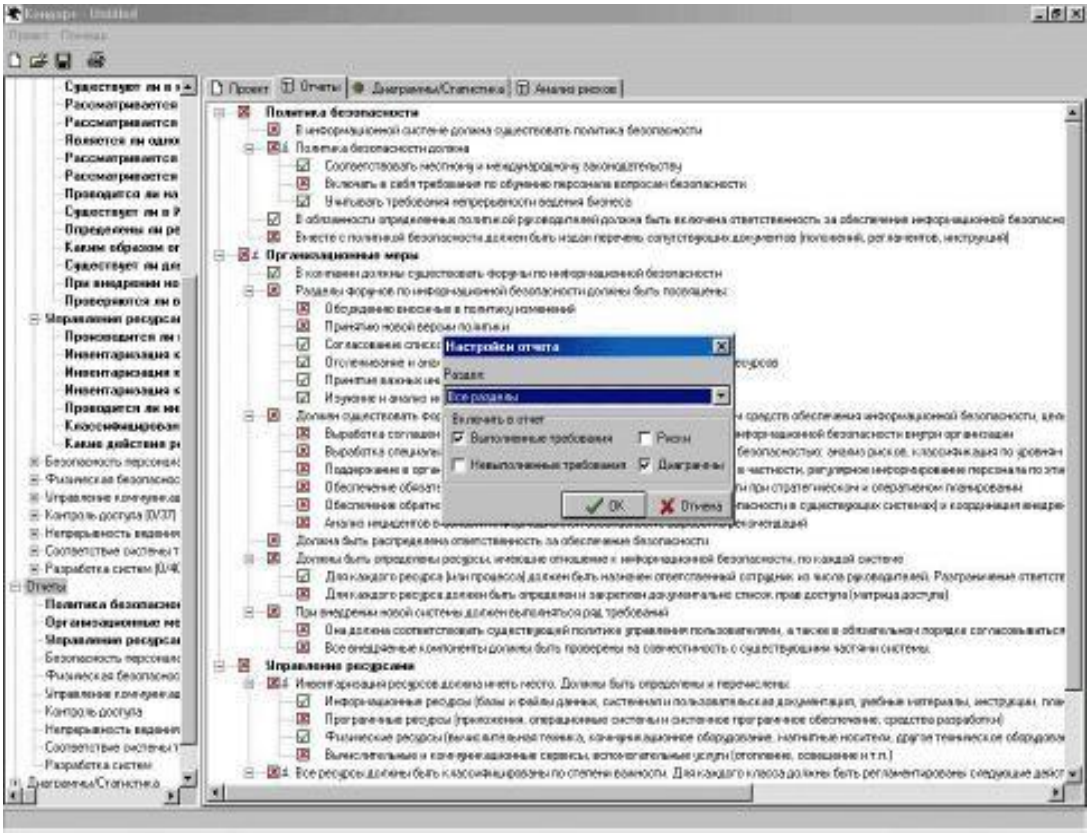


Рис.9. Интерфейс программного комплекса Кондор. Настройка отчета.

Кроме того, КОНДОР+ дает возможность специалисту отслеживать вносимые на основе выданных рекомендаций изменения в политику безопасности, постепенно приводя ее в полное соответствие с требованиями стандарта, а также иметь возможность представлять отчеты руководству, свидетельствующие о целесообразности и обоснованности инвестиций в обеспечение безопасности информационной системы компании.

Стоимость продукта составляет 225 долл. (КОНДОР) и 345 долл. (КОНДОР+ с модулем анализа рисков базового уровня).

К недостаткам КОНДОР+ можно отнести:

- отсутствие возможности установки пользователем веса на каждое требование (запланировано в следующих версиях);
- отсутствие возможности внесения пользователем комментариев (запланировано в следующих версиях).
-

1. Описание системы (лабораторного программного комплекса)

При разработке системы преследовались многие цели, одна из них заключалась в том, чтобы создать программный продукт, который будет способен ввести пользователя в «курс дела» не утаивая от него ни одного этапа анализа рисков.

Необходимо было разработать максимально простое в использовании программное решение, основная задача которого - дать возможность ИТ-менеджеру самостоятельно (без привлечения сторонних экспертов) оценить уровень рисков в информационной системе, оценить эффективность существующей практики по обеспечению безопасности компании и оптимизировать расходы и сформировать адекватный бюджет на информационную безопасность.

Система представляет интеграцию двух идей реализованных в системах Кондор и Гриф. В программном комплексе анализ рисков и политики безопасности информационной системы объединены в одном продукте. То есть данные, которые заносятся для анализа организационных мер, определяющих существующую политику безопасности компании, полностью используется при анализе рисков. Это означает что две составляющие управления информационной безопасностью - политика безопасности и анализ рисков - находятся в одном интегрированном решении. Кроме того, данный продукт может использоваться и в учебных целях как возможность изучить на практике методы и средства анализа рисков и проверки организационных мер обеспечивающих информационную безопасность. Благодаря значительно расширенной базе использованных положений стандарта ISO 17799 по сравнению с Кондором и Грифом в данной системе возможен более полный анализ организационных мер определяющих политику безопасности.

Известно, что существуют два подхода к анализу рисков - анализ рисков базового и полного уровня. В данной системе использованы сильные стороны разных методов, опирающихся на анализ рисков и на требования стандартов.

Но каким бы ни был подход, главная цель — формирование конкретных и применимых требований по безопасности к исследуемой информационной системе.

В системе использован наиболее распространенный в настоящее время основанный на учете различных факторов влияющих на уровни угроз и уязвимостей. Такой подход позволяет абстрагироваться от малосущественных технических деталей, учесть не только программно-технические, но и иные аспекты.

При работе система проводит анализ существующей политики безопасности на наличие так называемых дыр. Если их не устранять, то рано или поздно их обнаружат «плохие парни» и воспользуются для достижения своих, не всегда достойных целей.

В особенности отметим, что данная система позволяет также определить и

экономическую эффективность системы информационной защиты.

Данный продукт окажет не заменимую помощь организациям, которые планируют получить сертификат на соответствие международному стандарту безопасности ISO 17799, так как при не выполнении каких либо требований, даются пояснения - как и что предпринять.

Ни для кого не секрет, что анализ информационных рисков является на сегодняшний день актуальной задачей для современного бизнеса - последние годы на каждой конференции по информационной безопасности в России можно услышать серьезные доклады на данную тему.

Анализ информационных рисков - это процесс комплексной оценки защищенности информационной системы с переходом к количественным или качественным показателям рисков. При этом риск - это вероятный ущерб, который зависит от защищенности системы. Под управлением рисками понимается процесс идентификации и уменьшения рисков, которые могут воздействовать на информационную систему. Результаты анализа используются при выборе средств защиты, оценке эффективности существующих и проектируемых систем защиты информации [3].

Итак, из определения следует, что на выходе алгоритма анализа риска можно получить либо количественную оценку рисков (риск измеряется в деньгах), либо - качественную (уровни риска; обычно: высокий, средний, низкий).

Кроме того, анализ рисков также отличается по используемому подходу; обычно

условно выделяется анализ рисков базового и полного уровня. Для анализа рисков базового уровня достаточно проверить риск невыполнения требований общепринятого стандарта безопасности (обычно ISO 17799) с получением на выходе качественной оценки уровня рисков (высокий, средний, низкий).

Основное отличие полного анализа рисков от базового состоит в необходимости построения полной модели анализируемой информационной системы. Модель должна включать: виды ценной информации, объекты ее хранения; группы пользователей и виды доступа к информации; средства защиты (включая политику безопасности), виды угроз.

Далее после моделирования необходимо перейти к этапу анализа защищенности построенной полной модели информационной системы. И здесь мы попадаем в целый пласт теоретических и практических проблем, с которыми сталкиваются разработчики алгоритмов анализа риска полного уровня. Прежде всего, как алгоритмически (без эксперта) оценить защищенность информационной системы (заметим, что речь не идет о сканировании конкретных уязвимостей в конкретном применяемом программном обеспечении)? Следующая проблема - как алгоритмически определить все классы уязвимостей в системе

защиты анализируемой системы? Как оценить ущерб от всех существующих в системе угроз безопасности и как добиться адекватной оценки совокупного ущерба по всем классам угроз (необходимо избежать избыточного суммирования ущербов)? И самая сложная проблема: риск категория вероятностная - как оценить вероятность реализации множества угроз информационной системы?

Весь вышеуказанный комплекс проблем необходимо решить при создании алгоритма. Конечно, можно предложить пользователю самостоятельно ввести вероятность реализации угроз или оценить ее уровень, как в алгоритме RiskWatch. Но тогда мы сведем на нет весь процесс анализа.

При подсчете вероятности реализации тех или иных угроз можно опереться на некоторые статистические данные [5].

Таблица 1 Угрозы информационной безопасности

Угрозы	Вероятность проявления
Небрежность	0,188
Пиратство	0,166
Нарушение целостности	0,159
Утечка данных	0,159
"Шутки" над коллегами	0,150
Наблюдение за излучением	0,133
Умышленные повреждения данных и программ	0,129
Нарушение аутентификации	0,129
Перегрузка	0,119
Неправильная маршрутизация	0,106
Аппаратные сбои	0,090
Искажение	0,080
Сетевые анализаторы	0,074
Мошенничество	0,058
Пожары и другие стихийные бедствия	0,043

Подлог	0,033
"Логические бомбы"	0,032
Кража	0,032
Блокирование информации	0,016
"Потайные ходы и лазейки"	0,010

Но так как риск - это вероятный ущерб, который зависит от защищенности системы, то полученные данные будут не точными.

Из-за того что на оценку защищенности информационной системы существенным образом влияют организационные аспекты, то при анализе существующей защиты будем опираться на вопросник.

Так как на один и тот же вид информации может быть направлено сразу несколько угроз, то необходимо будет учесть так же и суммарный ущерб.

Необходимо смоделировать доступы всех групп пользователей ко всем видам информации и в зависимости от вида доступа и вида ресурса рассматривать конечное множество очевидных элементарных ситуаций, где начальную вероятность реализации угрозы можно определить достаточно просто и точно.

Далее анализируется множество опять же элементарных факторов (идет анализ комплексной защищенности объекта из вопросника) - которые так или иначе влияют на защищенность, а затем делается вывод об итоговых рисках.

1. Определение источника угроз.

В любой методике управления рисками необходимо идентифицировать риски, как вариант – их составляющие (угрозы и уязвимости).

Целью создания любой КС является удовлетворение потребностей пользователей в своевременном получении достоверной информации и сохранении ее конфиденциальности (при необходимости). Информация является конечным

«продуктом потребления» в КС и выступает в виде центральной компоненты системы. Безопасность информации на уровне КС обеспечивают такие компоненты системы как технические, программные средства, обслуживающий персонал и пользователи. Причем эта задача должна решаться путем защиты от внешних и внутренних неразрешенных (несанкционированных) воздействий. Особенности взаимодействия компонент заключаются в следующем. Внешние воздействия чаше всего оказывают несанкционированное влияние на информацию путем воздействия на другие компоненты системы. Следующей особенностью

является возможность несанкционированных действий, вызываемых внутренними причинами, в отношении информации со стороны технических, программных средств, обслуживающего, персонала и пользователей. В этом заключается основное противоречие взаимодействия этих компонент с информацией. Причем, обслуживающий персонал и пользователи могут сознательно осуществлять попытки несанкционированного воздействия на информацию. Таким образом, обеспечение безопасности информации в КС должно предусматривать защиту всех компонент от внешних и внутренних воздействий (угроз) [4].

Под **угрозой безопасности информации** понимается потенциально возможное событие, процесс или явление, которые могут привести к уничтожению, утрате целостности, конфиденциальности или доступности информации.

Все множество потенциальных угроз безопасности информации в КС может быть разделено на два класса (рис. 10).

Рис. 10. Угрозы безопасности информации в компьютерных системах

Случайные угрозы

Угрозы, которые не связаны с преднамеренными действиями злоумышленников и реализуются в случайные моменты времени, называют *случайными* или *непреднамеренными*.

Реализация угроз этого класса приводит к наибольшим потерям информации (по статистическим данным - до 80% от ущерба, наносимого информационным ресурсам КС любыми угрозами). При этом могут происходить уничтожение, нарушение целостности и доступности информации. Реже нарушается конфиденциальность информации, однако при этом создаются предпосылки для злоумышленного воздействия на информацию.

Стихийные бедствия и аварии чреваты наиболее разрушительными последствиями для КС, т.к. последние подвергаются физическому разрушению, информация утрачивается или доступ к ней становится невозможен.

Сбои и отказы сложных систем неизбежны. В результате сбоев и отказов нарушается работоспособность технических средств, уничтожаются и искажаются данные и программы, нарушается алгоритм работы устройств. Нарушения алгоритмов работы от дельных узлов и устройств могут также привести к нарушению конфиденциальности информации. Например, сбои и отказы средств выдачи информации могут привести к несанкционированному доступу к информации путем несанкционированной ее выдачи в канал связи, на печатающее устройство и т. п.

Ошибки при разработке КС, алгоритмические и программные ошибки приводят к последствиям, аналогичным последствиям сбоев и отказов технических средств. Кроме того, такие ошибки могут быть использованы злоумышленниками для воздействия на ресурсы КС. Особую опасность представляют ошибки в операционных системах (ОС) и в программных средствах защиты информации.

Согласно данным Национального Института Стандартов и Технологий США (NIST) 65% случаев нарушения безопасности информации происходит в результате *ошибок пользователей и обслуживающего персонала.* Некомпетентное, небрежное или невнимательное выполнение функциональных обязанностей сотрудниками приводят к уничтожению, нарушению целостности и конфиденциальности информации, а также компрометации механизмов защиты.

Характеризуя угрозы информации в КС, не связанные с преднамеренными действиями, в целом, следует отметить, что механизм их реализации изучен достаточно хорошо, накоплен значительный опыт противодействия этим угрозам. Современная технология разработки технических и программных средств, эффек- тивная система эксплуатации КС, включающая обязательное резервирование информации, позволяют значительно снизить потери от реализации угроз этого класса.

Преднамеренные угрозы

Второй класс угроз безопасности информации в КС составляют преднамеренно создаваемые угрозы. Данный класс угроз изучен недостаточно, очень динамичен и

постоянно пополняется новыми угрозами. Угрозы этого класса в соответствии с их физической сущностью и механизмами реализации могут быть распределены по пяти группам:

- традиционный или универсальный шпионаж и диверсии;
- несанкционированный доступ к информации;
- электромагнитные излучения и наводки;
- модификация структур КС;
- вредительские программы.

Традиционный шпионаж и диверсии

В качестве источников нежелательного воздействия на информационные ресурсы по-прежнему актуальны методы и средства шпионажа и диверсий**,** которые использовались и используются для добывания или уничтожения информации на объектах, не имеющих КС. Эти методы также действенны и эффективны в условиях применения компьютерных систем. Чаще всего они используются для получения сведений о системе защиты с целью проникновения в КС, а также для хищения и уничтожения информационных ресурсов.

К методам шпионажа и диверсий относятся:

- подслушивание;
- визуальное наблюдение;
- хищение документов и машинных носителей информации;
- хищение программ и атрибутов системы защиты;
- подкуп и шантаж сотрудников;
- сбор и анализ отходов машинных носителей информации;
- поджоги;
- взрывы.

Для *подслушивания* злоумышленнику не обязательно проникать на объект. Современные средства позволяют подслушивать разговоры с расстояния нескольких сотен метров. Так прошла испытания система подслушивания, позволяющая с расстояния 1 км фиксировать разговор в помещении с закрытыми окнами. В городских условиях дальность действия устройства сокращается до сотен и десятков метров в зависимости от уровня фонового шума. Принцип действия таких устройств основан на анализе отраженного луча лазера от стекла окна помещения, которое колеблется от звуковых волн. Колебания оконных стекол от акустических волн в помещении могут сниматься и передаваться на расстояния с помощью специальных устройств, укрепленных на оконном стекле. Такие устройства преобразуют механические колебания стекол в электрический сигнал с последующей

передачей его по радиоканалу. Вне помещений подслушивание ведется с помощью сверхчувствительных направленных микрофонов. Реальное расстояние подслушивания с помощью направленных микрофонов составляет 50-100 метров.

Разговоры в соседних помещениях, за стенами зданий могут контролироваться с помощью стетоскопных микрофонов. Стетоскопы преобразуют акустические колебания в электрические. Такие микрофоны позволяют прослушивать разговоры при толщине стен до 50-100 см. Съем информации может осуществляться также и со стекол, металлоконструкций зданий, труб водоснабжения и отопления.Аудиоинформация может быть получена также путем высокочастотного навязывания. Суть этого метода заключается в воздействии высокочастотным электромагнитным полем или электрическими сигналами на элементы, способные модулировать эти поля, или сигналы электрическими или акустическими сигналами с речевой информацией. В качестве таких элементов могут использоваться различные полости с электропроводной поверхностью, представляющей собой высокочастотный контур с распределенными параметрами, которые меняются под действием акустиче- ских волн. При совпадении частоты такого контура с частотой высокочастотного навязывания и при наличии воздействия акустических волн на поверхность полости контур переизлучает и модулирует внешнее поле (высокочастотный электрический сигнал). Чаще всего этот метод прослушивания реализуется с помощью телефонной линии. При этом в качестве модулирующего элемента используется телефонный аппарат, на который по телефонным проводам подается высокочастотный электрический сигнал. Нелинейные элементы телефонного аппарата под воздействием речевого сигнала модулируют высокочастотный сигнал. Модулированный высокочастотный сигнал может быть демодулирован в приемнике злоумышленника.

Одним из возможных каналов утечки звуковой информации может быть прослушивание переговоров, ведущихся с помощью средств связи. Контролироваться могут как проводные каналы связи, так и радиоканалы. Прослушивание переговоров по проводным и радиоканалам не требует дорогостоящего оборудования и высокой квалификации злоумышленника.

Дистанционная видеоразведка для получения информации в КС малопригодна и носит, как правило, вспомогательный характер.

Видеоразведка организуется в основном для выявления режимов работы и расположения механизмов защиты информации. Из КС информация реально может быть получена при использовании на объекте экранов, табло, плакатов, если имеются прозрачные окна и перечисленные выше средства размещены без учета необ- ходимости противодействовать такой угрозе.

Видеоразведка может вестись с использованием технических средств, таких какоптические приборы, фото-, кино- и телеаппаратура. Многие из этих средств допускают консервацию (запоминание) видеоинформации, а также передачу ее на определенные расстояния.

В прессе появились сообщения о создании в США мобильного микроробота для ведения дистанционной разведки. Пьезокерамический робот размером около 7 см и массой 60 г способен самостоятельно передвигаться со скоростью 30 см/с в течение 45 мин. За это время «микроразведчик» способен преодолеть расстояние в 810 метров, осуществляя транспортировку 28 г полезного груза (для сравнения - коммерческая микровидеокамера весит 15 г).

Для вербовки сотрудников и физического уничтожения объектов КС также не обязательно иметь непосредственный доступ на объект. Злоумышленник, имеющий доступ на объект КС, может использовать любой из методов традиционного шпионажа.

Злоумышленниками, имеющими доступ на объект, могут использоваться миниатюрные средства фотографирования, видео - и аудиозаписи. Для аудио- и видеоконтроля помещений и при отсутствии в них злоумышленника могут использоваться закладные устройства или «жучки». Для объектов КС наиболее вероятными являются закладные устройства, обеспечивающие прослушивание помещений. Закладные устройства делятся на проводные и излучающие. Проводные закладные устройства требуют значительного времени на установку и имеют существенный демаскирующий признак - провода. Излучающие «закладки» («радиозакладки») быстро устанавливаются, но также имеют демаскирующий при знак - излучение в радио или оптическом диапазоне. «Радиозакладки» могут использовать в качестве источника электрические сигналы или акустические сигналы. Примером использования электрических сигналов в качестве источника является применение сигналов внутренней телефонной, громкоговорящей связи. Наибольшее распространение получили акустические «радиозакладки». Они воспринимают акустический сигнал, преобразуют его в электрический и передают в виде радиосигнала на дальность до 8 км. Из применяемых на практике «радиозакладок» подавляющее большинство (около 90%) рассчитаны на работу в диапазоне расстояний 50 - 800 метров.

Для некоторых объектов КС существует *угроза вооруженного нападения террористических или диверсионных групп.* При этом могут быть применены средства огневого поражения.

Несанкционированный доступ к информации

Термин «несанкционированный доступ к информации» (НСДИ) определен как доступ к информации, нарушающий правила разграничения доступа с использованием штатных

средств вычислительной техники или автоматизированных систем.

Под правилами разграничения доступа понимается совокупность положений, регламентирующих права доступа лиц или процессов (субъектов доступа) к единицам информации (объектам доступа).

Право доступа к ресурсам КС определяется руководством для каждого сотрудника в соответствии с его функциональными обязанностями. Процессы инициируются в КС в интересах определенных лиц, поэтому и на них накладываются ограничения по доступу к ресурсам.

Выполнение установленных правил разграничения доступа в КС реализуется за счет создания системы разграничения доступа (СРД).

Несанкционированный доступ к информации возможен только с использованием штатных аппаратных и программных средств в следующих случаях:

- отсутствует система разграничения доступа;
- сбой или отказ в КС;

-ошибочные действия пользователей или обслуживающего персоналакомпьютерных систем;

- ошибки в СРД;
- фальсификация полномочий.

Если СРД отсутствует, то злоумышленник, имеющий навыки работы в КС, может получить без ограничений доступ к любой информации. В результате сбоев илиотказов средств КС, а также ошибочных действий обслуживающего персонала и пользователей возможны состояния системы, при которых упрощается НСДИ. Злоумышленник может выявить ошибки в СРД и использовать их для НСДИ. Фальсификация полномочий является одним из наиболее вероятных путей (каналов) НСДИ.

Электромагнитные излучения и наводки

Процесс обработки и передачи информации техническими средствами КС сопровождается электромагнитными излучениями в окружающее пространство и наведением электрических сигналов в линиях связи, сигнализации, заземлении и других проводниках. Они получили названия *побочных электромагнитных излучений и наводок (ПЭМИН)***.** С помощью специального оборудования сигналы принимаются, выделяются, усиливаются и могут либо просматриваться, либо записываться в запоминающих устройствах. Наибольший уровень электромагнитного излучения в КС присущ работающим устройствам отображения информации на электронно-лучевых трубках. Содержание экрана такого устройства может просматриваться с помощью обычного телевизионного приемника, дополненного несложной схемой, основной функцией которой является синхронизация сигналов. Дальность

удовлетворительного приема таких сигналов при использовании дипольной антенны составляет 50 метров. Использование направленной антенны приемника позволяет увеличить зону уверенного приема сигналов до 1 км. Восстановление данных возможно также путем анализа сигналов излучения неэкранированного электрического кабеля на расстоянии до 300 метров.

Наведенные в проводниках электрические сигналы могут выделяться и фиксироваться с помощью оборудования, подключаемого к этим проводникам на расстоянии в сотни метров от источника сигналов. Для добывания информации злоумышленник может использовать также «просачивание» информационных сигна- лов в цепи электропитания технических средств КС. «Просачивание» информационных сигналов в цепи электропитания возможно при наличии магнитной связи между выходным трансформатором усилителя и трансформатором выпрямительного устройства. «Просачивание» также возможно за счет падения напряжения на внутреннем сопротивлении источника питания при прохождении токов усиливаемых информационных сигналов. Если затухание в фильтре выпрямительного устройства недостаточно, то информационные сигналы могут быть обнаружены в цепи питания. Информационный сигнал может быть вы- делен в цепи питания за счет зависимости значений потребляемого тока в оконечных каскадах усилителей (информационные сигналы) и значений токов в выпрямителях, а значит и в выходных цепях.

Электромагнитные излучения используются злоумышленниками не только для получения информации, но и для ее уничтожения. Электромагнитные импульсы способны уничтожить информацию на магнитных носителях. Мощные электромагнитные и сверхвысокочастотные излучения могут вывести из строя электронные блоки КС. Причем для уничтожения информации на магнитных носителях с расстояния нескольких десятков метров может быть использовано устройство, помещающееся в портфель.

Несанкционированная модификация структур

Большую угрозу безопасности информации в КС представляет *несанкционированная модификация алгоритмической, программной и технической структур системы***.** Несанкционированная модификация структур может осуществляться на любом жизненном цикле КС. Несанкционированное изменение структуры КС на этапах разработки и модернизации получило название «закладка». В процессе разработки КС «закладки» внедряются, как правило, в специализированные системы, предназначенные для эксплуатации в какой-либо фирме или государственных учреждениях. В универсальные КС «закладки» внедряются реже, в основном для дискредитации таких систем конкурентом или на государственном уровне, если предполагаются поставки КС во враждебное государство. «Закладки», внедренные на этапе разработки, сложно выявить ввиду высокой

квалификации их авторов и сложности современных КС.

Алгоритмические, программные и аппаратные «закладки» используются либо для непосредственного вредительского воздействия на КС, либо для обеспечения неконтролируемого входа в систему. Вредительские воздействия «закладок» на КС осуществляются при получении соответствующей команды извне (в основном характерно для аппаратных «закладок») и при наступлении определенных событий в системе. Такими событиями могут быть: переход на определенный режим работы (например, боевой режим системы управления оружием или режим устранения ава- рийной ситуации на атомной электростанции т. п.), наступление установленной даты, достижение определенной наработки и т. д.

Программные и аппаратные «закладки» для осуществления неконтролируемого входа в программы, использование привилегированных режимов работы (например, режимов операционной системы), обхода средств защиты информации получили название «люки».

Вредительские программы

Одним из основных источников угроз безопасности информации в КС является использование специальных программ, получивших общее название «вредительские программы».

В зависимости от механизма действия вредительские программы делятся на четыре класса:

- «логические бомбы»;
- «черви»;
- «троянские кони»;
- «компьютерные вирусы».

«Логические бомбы» - это программы или их части, постоянно находящиеся в ЭВМ или вычислительных системах (ВС) и выполняемые только при соблюдении определенных условий. Примерами таких условий могут быть: наступление заданной

даты, переход КС в определенный режим работы, наступление некоторых событий установленное число раз и т.п.

«Червями» называются программы, которые выполняются каждый раз при загрузке системы, обладают способностью перемещаться в ВС или сети и самовоспроизводить копии. Лавинообразное размножение программ приводит к перегрузке каналов связи, памяти и, в конечном итоге, к блокировке системы.

«Троянские кони» - это программы, полученные путем явного изменения или добавления команд в пользовательские программы. При последующем выполнении пользовательских программ наряду с заданными функциями выполняются

несанкционированные, измененные или какие-то новые функции.

«Компьютерные вирусы» - это небольшие программы, которые после внедрения в ЭВМ самостоятельно распространяются путем создания своих копий, а при выполнении определенных условий оказывают негативное воздействие на КС.

Поскольку вирусам присущи свойства всех классов вредительских программ, то в последнее время любые вредительские программы часто называют вирусами.

Классификация злоумышленников

Возможности осуществления вредительских воздействий в большой степени зависят от статуса злоумышленника по отношению к КС. Злоумышленником может быть:

- разработчик КС;
- сотрудник из числа обслуживающего персонала;
- пользователь;
- постороннее лицо.

Разработчик владеет наиболее полной информацией о программных и аппаратных средствах КС и имеет возможность внедрения "закладок" на этапах создания и модернизации систем. Но он, как правило, не получает непосредственного доступа на эксплуатируемые объекты КС. Пользователь имеет общее представление о структурах КС, о работе механизмов защиты информации. Он может осуществлять сбор данных о системе защиты информации методами традиционного шпионажа, а также предприимать попытки несанкционированного доступа к информации. Возможности внедрения закладок пользователями очень ограничены. Постороннее лицо, не имеющее отношения к КС, находится в наименее выгодном положении по отношению к другим злоумышленникам. Если предположить, что он не имеет доступ на объект КС, то в его распоряжении имеются дистанционные методы традиционного шпионажа и возможность диверсионной деятельности. Он может осуществлять вредительские воздействия с использованием электромагнитных излучений и наводок, а также каналов связи, если КС является распределенной.

Большие возможности оказания вредительских воздействий на информацию КС имеют специалисты, обслуживающие эти системы. Причем, специалисты разных подразделений обладают различными потенциальными возможностями злоумышленных действий. Наибольший вред могут нанести работники службы безопасности информации. Далее идут системные программисты, прикладные программисты и инженерно-технический персонал.

На практике опасность злоумышленника зависит также от финансовых, материально-технических возможностей и квалификации злоумышленника.

2.2.Примеры методик анализа рисков

Концепции анализа рисков, управления рисками на всех стадиях жизненного цикла информационной технологии были предложены многими крупными организациями, занимающимися проблемами информационной безопасности. Отечественные аналитики начали использовать различные методики на практике. Несколькими российскими организациями были разработаны собственные методики анализа и управления рисками, разработано собственное программное обеспечение, которое, наряду с зарубежным, имеется на отечественном рынке [3].

Оценка рисков

Для измерения какого-либо свойства необходимо выбрать шкалу. Шкалы могут быть разной «силы», выбор той или иной шкалы зависит как от свойств измеряемой величины, так и от имеющихся в наличии измерительных инструментов.

В качестве примера рассмотрим варианты выбора шкалы для измерения характеристического свойства «ценность информационного ресурса». Она может измеряться опосредованно в шкалах отношений, таких как стоимость восстановления ресурса, время восстановления ресурса и других. Другой вариант — определить ранговую шкалу для получения экспертной оценки, имеющую, например, три возможных значения лингвистической переменной:

1) Малоценный информационный ресурс - от него не зависят критически важные задачи, и он может быть восстановлен с небольшими затратами времени и денег;

2) Ресурс средней ценности - от него зависит ряд важных задач, но в случае его утраты он может быть восстановлен за время менее, чем критически допустимое, стоимость восстановления высокая;

3) Ценный ресурс: от него зависят критически важные задачи, в случае утраты время восстановления превышает критически допустимое, либо стоимость чрезвычайно высока.

Для измерения рисков не существует абсолютной шкалы. Риски можно оценивать по объективным либо субъективным критериям. Примером объективного критерия является вероятность выхода из строя какого-либо оборудования, например ПК за определенный промежуток времени. Примером субъективного критерия является оценка администратора информационного ресурса риска выхода из строя ПК. Для этого обычно разрабатывается ранговая шкала с несколькими градациями, например: низкий, средний, высокий уровни.

Существует ряд подходов к измерению рисков. Рассмотрим наиболее распространенные: оценка по двум факторам и оценка по трем факторам.

Оценка рисков по двум факторам

В простейшем случае используется оценка двух факторов: вероятность происшествия и тяжесть возможных последствий. Обычно считается, что риск тем больше, чем больше вероятность происшествия и тяжесть последствий. Общая идеяможет быть выражена формулой:

РИСК=Рпроисшествия х **ЦЕНА ПОТЕРИ** (1)

Если переменные являются количественными величинами, риск — это оценка математического ожидания потерь.

Если переменные являются качественными величинами - то операция умножения не определена. Таким образом, в явном виде эта формула использоваться не должна.

Рассмотрим вариант использования качественных величин (наиболее часто встречающаяся ситуация).

Сначала должны быть определены значения лингвистической переменной вероятности событий, например такой шкалы:

A - событие практически никогда не происходит; B - событие случается редко;

C - вероятность события за рассматриваемый промежуток времени — около 0,5; B - скорее всего, событие произойдет;

E - событие почти обязательно произойдет.

Кроме того, определяется лингвистическая переменная; серьезности происшествий, например:

N (Negligible) — воздействием можно пренебречь.

Mi (Minor) — незначительное происшествие - последствия легко устранимы, затраты на ликвидацию последствий невелики, воздействие на информационную технологию незначительно;

Mo (Moderate) — происшествие с умеренными результатами - ликвидация последствий не связана с крупными затратами, воздействие на информационную технологию невелико и не затрагивает критически важные задачи;

S (Serious) — происшествие с серьезными последствиями: ликвидация последствий связана со значительными затратами, воздействие на информационные технологии ощутимо, воздействует на выполнение критически важных задач;

C (Critical) — происшествие приводит к невозможности решения критически важных задач. Для оценки рисков определяется переменная из трех значений: низкий риск, средний риск, высокий риск.

Риск, связанный с определенным событием, зависит от двух факторов и может быть определен как показано в таблице 2.

Шкалы факторов риска и сама таблица могут быть определены иначе, иметь другое

число градаций.

Таблица.2. Определение риска в зависимости от двух факторов

Negligible	Minor	Moderate	Serious	Critical
Низкий риск	Низкий риск	Низкий риск	Средний риск	Средний риск
Низкий риск	Низкий риск	Средний риск	Средний риск	Высокий риск
Низкий риск	Средний риск	Средний риск	Средний риск	Высокий риск
Средний риск	Средний риск	Средний риск	Средний риск	Высокий риск
Средний риск	Высокий риск	Высокий риск	Высокий риск	Высокий риск

Подобный подход к оценке рисков достаточно распространен. При разработке (использовании) методик оценки рисков необходимо учитывать следующие особенности:

- значения шкал должны быть четко определены (словесное описание) и пониматься одинаково всеми участниками процедуры экспертной оценки;
- требуются обоснования выбранной таблицы. Необходимо убедиться, что разные инциденты, характеризующиеся одинаковыми сочетаниями факторов риска, имеют с точки зрения экспертов одинаковый уровень рисков.

Подобные методики широко применяются при проведении анализа рисков базового уровня.

Оценка рисков по трем факторам.

В большинстве методик, рассчитанных на более высокие требования, чем базовый уровень, используется модель оценки риска с тремя факторами: угроза, уязвимость, цена потери. Угроза и уязвимость определяются следующим образом.

Угроза — совокупность условий и факторов, которые могут стать причиной нарушения целостности, доступности, конфиденциальности информации.

Уязвимость — слабость в системе защиты, которая делает возможным реализацию угрозы.

Цена потери — это качественная или количественная оценка степени серьезности происшествия.

Вероятность происшествия, которая в данном подходе может быть объективной либо субъективной величиной, зависит от уровней (вероятностей) угроз и уязвимостей:

Рпроисшествия = Ругрозы Х Руязвимости (2)

РИСК = Ругрозы Х Руязвимости Х ЦЕНА ПОТЕРИ (3)

Данное выражение можно рассматривать как математическую формулу, если используются количественные шкалы, либо как формулировку общей идеи, если хотя бы одна из шкал - качественная. В последнем случае используются различного рода табличные методы для определения риска в зависимости от трех факторов.

Например, показатель риска измеряется в шкале от 0 до 8 со следующими определениями уровней риска:

Риск практически отсутствует. Теоретически возможны ситуации, при которых событие наступает, но на практике это случается редко, а потенциальный ущерб сравнительно невелик:

Риск очень мал. События подобного рода случались достаточно редко, кроме того, негативные последствия сравнительно невелики;

8) Риск очень велик. Событие, скорее всего, наступит, и последствия будут чрезвычайно тяжелыми.

Матрица может быть определена

следующим образом (табл.2.3). В данной таблице уровни уязвимости Н, С, В означают соответственно низкий, средний и высокий уровни.

Подобные таблицы используются как в «бумажных» вариантах методик оценки рисков, так и в различного рода инструментальных средствах анализа рисков.

Степень серьезности происшествия (цена потери)	Уровень угрозы								
	Низкий			Средний			Высокий		
	Уровни уязвимостей			Уровни уязвимостей			Уровни уязвимостей		
	Н	С	В	Н	С	В	Н	С	В
Незначительная	0	1	2	1	2	3	2	3	4
Несущественная	1	2	3	2	3	4	3	4	5

Умеренная	2	3	4	3	4	5	4	5	6
Серьезная	3	4	5	4	5	6	5	6	7
Критическая	4	5	6	5	6	7	6	7	8

Практические сложности в реализации этого подхода следующие.

Во-первых, должен быть собран весьма обширный материал о происшествиях в этой области.

Во-вторых, применение этого подхода оправдано далеко не всегда. Если информационная система достаточно крупная (содержит много элементов, расположена на обширной территории), имеет давнюю историю, то подобный подход, скорее всего, применим. Если система сравнительно невелика, использует новейшие элементы технологии (для которых пока нет достоверной статистики), оценки угроз и уязвимостей могут оказаться недостоверными.

Выбор методика анализа рисков

Как уже упоминалась выше для оценки угроз и уязвимостей используются различные методы, в основе которых могут лежать [6]:

- Экспертные оценки.
- Статистические данные.
- Учет факторов, влияющих на уровни угроз и уязвимостей.

Мы же, выбрали наиболее распространенный в настоящее время подход, основанный на учете различных факторов, влияющих на уровни угроз и уязвимостей. Такой подход позволяет абстрагироваться от малосущественных технических деталей, учесть не только программно-технические, но и иные аспекты.

Нам необходимо оценит следующие вероятности:

- вероятность уровня(степени) угрозы и вероятность уровня уязвимости . Для оценки угроз выберем следующие косвенные факторы:
- Статистика по зарегистрированным инцидентам.
- Тенденции в статистке по подобным нарушениям.
- Наличие в системе информации, представляющей интерес для потенциальных внутренних или внешних нарушителей.
- Моральные качества персонала.
- Возможность извлечь выгоду из изменения обрабатываемой в системе информации.

- Наличие альтернативных способов доступа к информации.

Для оценки уязвимостей выберем следующие косвенные факторы:

- Количество рабочих мест (пользователей) в системе.
- Размер рабочих групп.
- Осведомленность руководства о действиях сотрудников (разные аспекты).
- Характер используемого на рабочих местах оборудования и ПО.
- Полномочия пользователей.

Далее мы берем подготовленный список вопросов, составленный при изучении разделов стандарта ISO 17799, и делим его на две части, влияющих на уровень угроз и влияющих на уровень уязвимости. Напротив фиксированных вариантов ответов поставим определенное количество баллов, определяющих уровень критичности.

Для определения факторов влияющих на уровень угроз, приведем следующий вопрос с вариантами ответов:

Может ли сокрытие информации принести прямую финансовую или иную выгоду сотрудникам?

Варианты ответов:

а) Да 15

б) Нет 0

Для определения факторов влияющих на уровень уязвимости, приведем следующий вопрос с вариантами ответов:

Есть ли у сотрудников возможность осуществить несанкционированный доступ к информации (например, когда их непосредственно не контролируют, по вечерам и т.п.)?

а) Да 20

б) Нет 0

Итоговая оценка угрозы и уязвимости данного класса будет определяться суммированием баллов. Программный код сам оценит степень угрозы и уязвимости по количеству накопленных балов.

Таблица 4.Степень угрозы при количестве баллов.

До 60	Очень низкая
От 60 до 150	Низкая
От 150 до 250	Средняя
От 250 до 400	Высокая

400 и более	Очень высокая

Таблица 5. Степень уязвимости при количестве баллов.

До 100	Низкая
От 100 до 300	Средняя
300 и более	Высокая

Эта методика проста и дает владельцу информационных ресурсов ясное представление, каким образом получается итоговая оценка и что надо изменить, чтобы улучшить показатели.

Далее используя метод оценка рисков по трем факторам произведем расчет по формуле 3.

В результате проделанной работы по оценки рисков мы получим качественные показатели. А при использовании оценки ущерба в случае реализации угроз конфиденциальности, целостности и доступности– мы сможем получить и некоторые количественные результаты.

Методика проверки организационных мер на соответствие положениям международного стандарта безопасности ISO 17799.

Политика информационной безопасности компании является важнейшим нормативным документом, определяющим комплекс мер и требований по обеспечению информационной безопасности бизнеса. Политика безопасности должна описывать реальное положение дел в информационной системе компании и являться обязательным руководством к действию для всего персонала компании. На сегодняшний день общепризнанным стандартом при создании комплексной политики безопасности компании является международный стандарт управления информационной безопасностью ISO 17799, созданный в 2000 году Международной организацией по стандартизации и Международной электротехнической комиссией на основе разработок Британского института стандартов [7].

Ниже приведены основные разделы стандарта ISO 17799:

Политика безопасности

Организационные меры по обеспечению безопасности

Управление форумами по информационной безопасности Координация вопросов, связанных с информационной безопасностью Распределение ответственности за обеспечение безопасности *Классификация и управление ресурсами*

Инвентаризация ресурсов Классификация ресурсов *Безопасность персонала*

Безопасность при выборе и работе с персоналом Тренинги персонала по вопросам безопасности Реагирование на секьюрити инциденты и неисправности *Физическая безопасность*

Управление коммуникациями и процессами Рабочие процедуры и ответственность Системное планирование

Защита от злонамеренного программного обеспечения (вирусов, троянских коней) Управление внутренними ресурсами

Управление сетями Безопасность носителей данных

Передача информации и программного обеспечения

Контроль доступа

Бизнес требования для контроля доступа Управление доступом пользователя Ответственность пользователей

Контроль и управление удаленного (сетевого) доступа Контроль доступа в операционную систему

Контроль и управление доступом к приложениям Мониторинг доступа и использования систем

Разработка и техническая поддержка вычислительных систем

Требования по безопасности систем Безопасность приложений Криптография

Безопасность системных файлов

Безопасность процессов разработки и поддержки

Управление непрерывностью бизнеса

Процесс управления непрерывного ведения бизнеса Непрерывность бизнеса и анализ воздействий

Создание и внедрение плана непрерывного ведения бизнеса

Тестирование, обеспечение и переоценка плана непрерывного ведения бизнеса

Соответствие системы основным требованиям Соответствие требованиям законодательства Анализ соответствия политики безопасности Анализ соответствия техническим требованиям

Анализ соответствия требованиям системного аудита

После изучения русской редакции ISO 17799 был разработан вопросник, ответив на вопросы которого получаем подробный отчет о состоянии дел в существующей политики безопасности организации.

Алгоритм работы данного раздела поясним на следующем примере.

При выборе раздела стандарта ‒Политика безопасности. Организационные меры‖

пользователю предлагается ответить на следующий вопрос с вариантами ответов:

Существует ли в компании разработанная политика информационной безопасности, все положения которой на практике внедрены в информационную систему?

а) Да

б) Нет

в) Положения политики внедрены частично.

После обработки ответа в таблицу базы данных записывается следующее:

При ответе ‒Нет‖ - ‒Необходимо разработать и внедрить комплексную политику информационной безопасности‖.

При ответе ― Положения политики внедрены частично‖- Необходимо добиться полного внедрения всех положений политики безопасности в информационную систему компании.

При ответе на остальные вопросы происходят те же действия.

Разработка функциональных схем элементов автоматизированной системы.

С позиции обеспечения безопасности информации в КС такие системы целесообразно рассматривать в виде единства трех компонент, оказывающих взаимное влияние друг на друга:

информация;

технические и программные средства; обслуживающий персонал и пользователи.

Поэтому на первом этапе идет определения вида ресурсов, представляющих ценность для компании

Осуществляем выполнение следующего алгоритма:

Вводим блок опроса, предназначенный для получения нашей системой данных, которые в последствии понадобятся для оценки рисков. Блок опроса при взаимодействии с пользователем определяет информацию, функционирующую в данной информационной системе, пользователей системы и аппаратные средства, предназначенные для обработки и хранения информации. Далее все это заноситься в файл базы данных Access. Это самый первый, и наверно даже ключевой этап работы, после проведения которого мы имеем в базе данных определенное количество таблиц , каждая из которых соответствует тому или иному ресурсу.

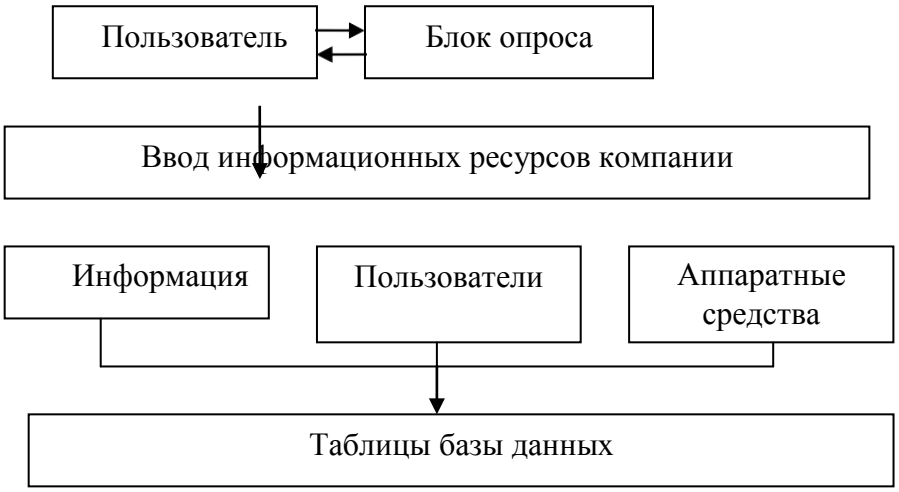


Рис. 11. Схема функционирования блока опроса по выявлению ресурсов компании.

Следующий этап работы позволяет определить места хранения информации (Осуществить привязку данных) и оценить ущерб, который понесет компания в случае реализации одной из трех классических угроз, направленных на информацию. Речь идет об угрозах: конфиденциальности (право на чтение), целостности (право на запись) и отказа в обслуживании (нарушение работоспособности ресурса, на котором хранится ценная информация).

Из сформированных таблиц базы данных выводиться информация, циркулирующая в данной системе и аппаратные средства, предназначенные для ее хранения. Блок опроса определяет место хранения и одновременно оценивает ущерб. Полученные данные формируют очередную таблицу.

На следующем этапе работы происходит определение уровня угроз и уровня уязвимости.

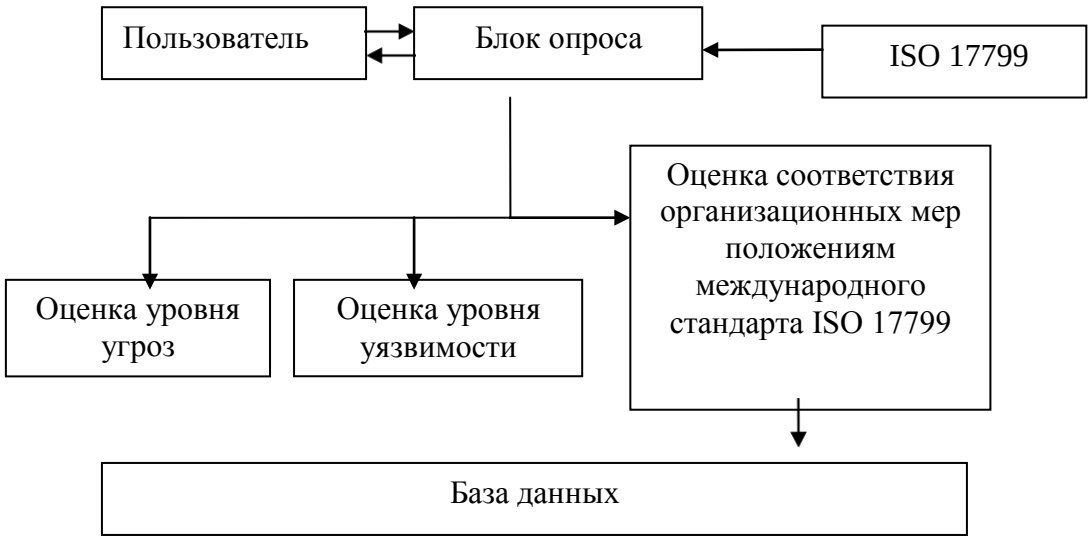


Рис. 12. Схема функционирования блока опроса по оценкам уровня уязвимости, угроз

и существующей политики безопасности.

Блок опроса, учитывая ответы на вопросы, оценивает уровни уязвимости и угрозы. Кроме этого происходит формирование в базе данных очередной таблицы с комментариями о не выполненных положениях стандарта.

Теперь осталось заполнить таблицы доступом субъектов системы к объектам системы. Это необходимо для того - чтобы программа, при расчете рисков знала какая категория пользователей (или кто из пользователей) к какому ресурсу имеет доступ, а к какому – нет. Кроме самого доступа, блок опроса определяет и права (чтение, запись, удаление). Блок опроса при взаимодействии с пользователем определяет доступ к ресурсам. Данные о ресурсах и пользователях выводятся на суд пользователю из уже сформированных таблиц базы данных. Полученные данные позволяют пересмотреть оценку уровня угрозы.

Далее с целью определение эффективности системы защиты информации требуется определить и внести в систему полную стоимость затрат на обеспечение информационной безопасности в год.

Блок опроса при взаимодействии с пользователем определяет полную стоимость затрат на обеспечение информационной безопасности. Полученные данные сохраняются в память.

Следующий этап работы системы происходит анализ рисков.

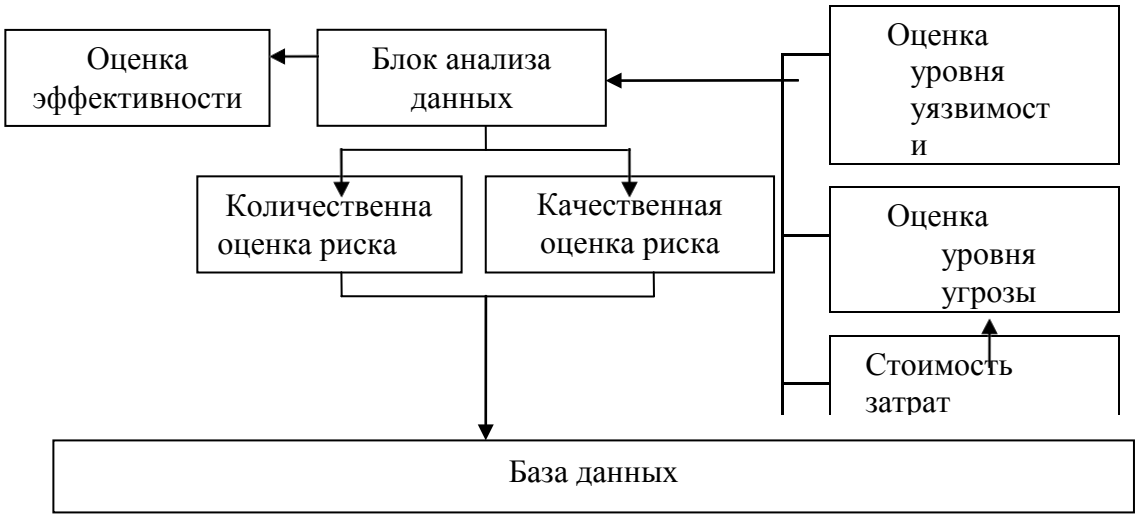


Рис. 13. Схема функционирования блока анализа рисков

В блок анализа данных поступает информация об оценках уровни уязвимости и угроз и информации о затратах на поддержании системы безопасности. В нем по выбранной методики происходит анализ рисков , и выдаются качественная и количественная оценки рисков. Полученные данные отображаются в отчете.

Разработка алгоритма и интерфейса программы анализа информационных рисков.

Из существующих функциональных схем анализа и контроля рисков и проверки политики информационной безопасности компании можно построить алгоритм работы всей системы анализа.

На этом этапе необходимо определить взаимосвязь отдельных функциональных схемв самой системе анализа. Необходимо создать такой алгоритм который позволит с минимальными вложением сил реализовать нашу систему в программном коде. Это позволить проверить правильность построения, верность функционирования и определить эффективность проведенной работы.

На анализе выше стающих функциональных схем и структурной схемы был построен следующий алгоритм.

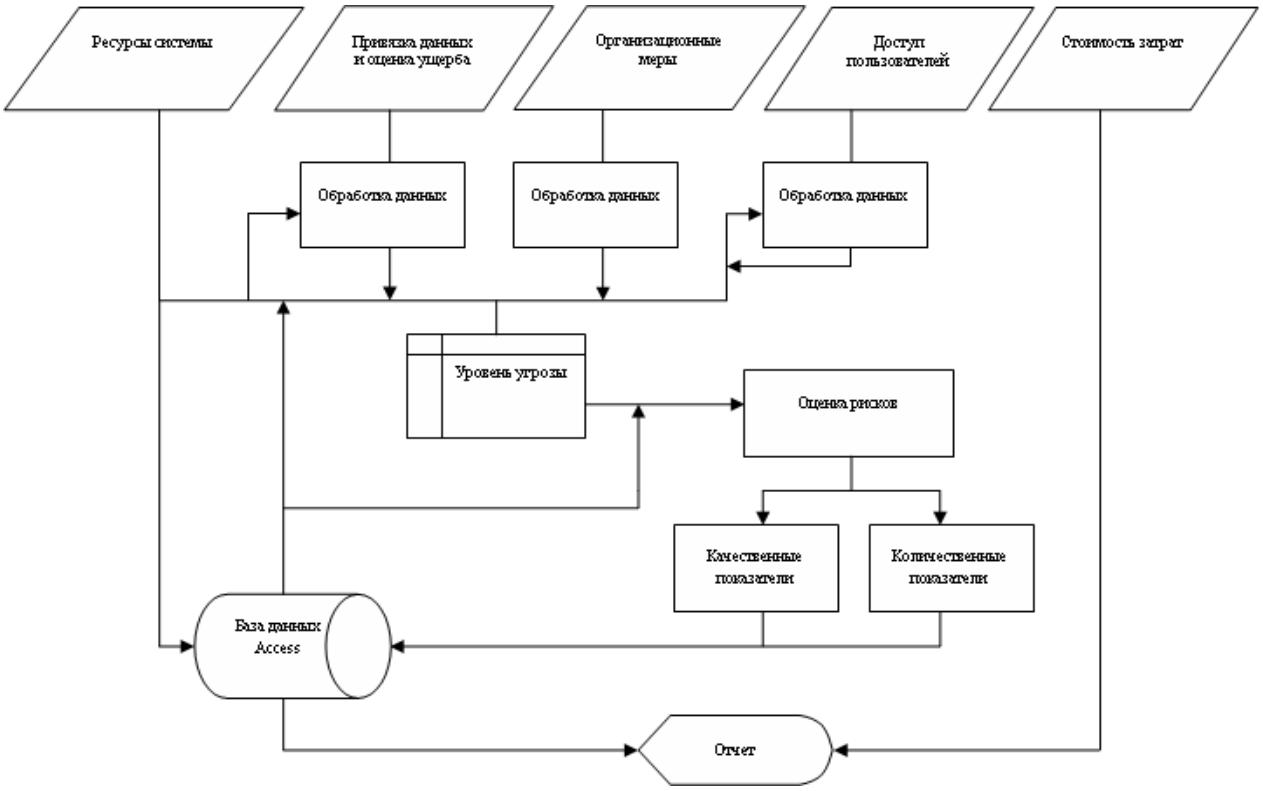


Рис. 14. Алгоритм интерфейса программы анализа информационных рисков.

Этапы функционирования

Первым этапом работы всей системы – является получение необходимой информации для анализа. С помощью блока опроса и дальнейшей обработки , информация заноситься в базу данных. В результате – на начальном этапе заполняются данными три таблицы. В этих таблицах храниться:

Таблица‖Inform‖. Информация об основных категориях информационных ресурсоворганизации.

Таблица‖Polzovateli‖. Информация о пользователях. Таблица‖Server‖. Информация о серверах.

Таблица‖Stanzii‖. Информация о рабочих станциях.

На втором этапе данные, после привязке и оценки ущерба заносятся в таблицу ‖Stoimost‖.

На третьем этапе происходит проверка организационных мер на соответствие положениям международного стандарта безопасности ISO 17799. Полученные данные записываются в таблицу –ISO17799‖.

На третьем и четвертом этапах формируются данные о доступе, правах доступа и оценки ежегодные затраты на обеспечения информационной безопасности организации, которые поступают в –Блок анализа данных‖ где после запроса необходимой информации из базы данных Access происходит процесс анализа информационных рисков.

Пятый заключительный этап работы программы, полученные данные используются для формирования отчета.

2. Интерфейс системы

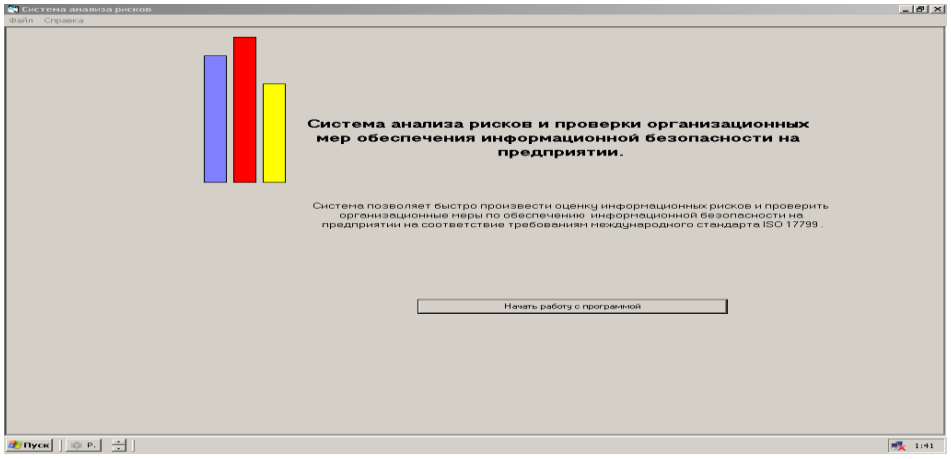


Рис.15. Главное окно программы

Первым этап. Определения полного списка информационных ресурсов, представляющих ценность для компании.

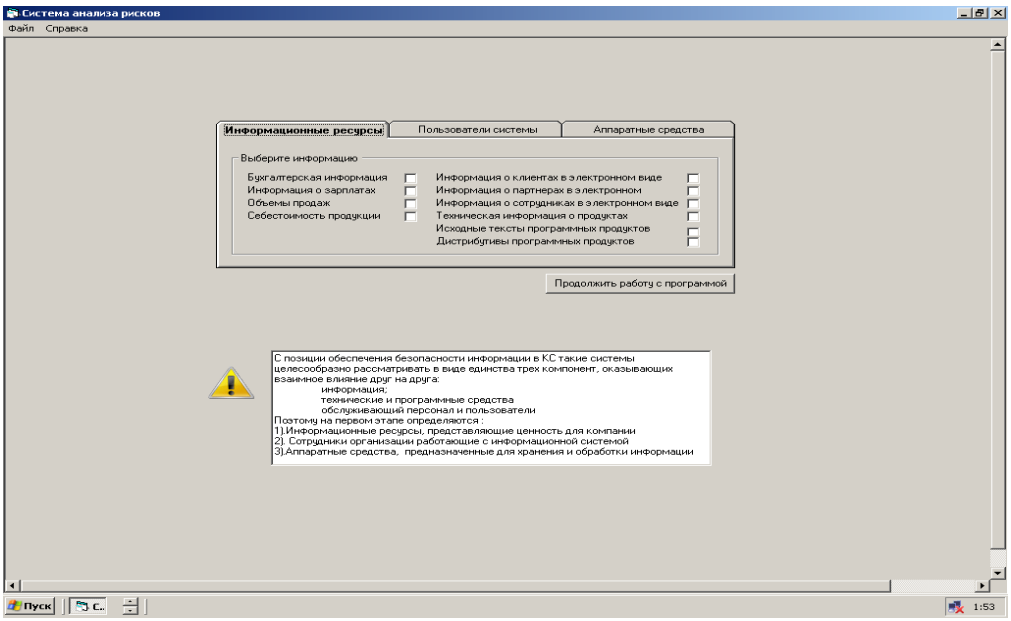


Рис. 16. Интерфейс программы. Вкладка «Информационные ресурсы».

Данная вкладка позволяет отметить виды информации, циркулирующие в системе: Это может быть:

- Финансовая информация
- Бухгалтерская информация
- Информация о зарплатах
- Объемы продаж
- Себестоимость продукции
- Ценная информация
- Информация о клиентах в электронном виде
- Информация о партнерах в электронном виде
- Информация о сотрудниках в электронном виде
- Техническая информация о продуктах
- Исходные тексты программных продуктов

Дистрибутивы программных продуктов (в том числе и собственные)

Стратегические планы развития компании в электронном виде:

Вкладка «Пользователи системы» дает возможность выбрать из приведенного списка тех пользователей, которые имеют отношение к данной информационной системе.

Это могут быть: Системные администраторы Офицеры безопасности Менеджеры Операторы или обычные пользователи

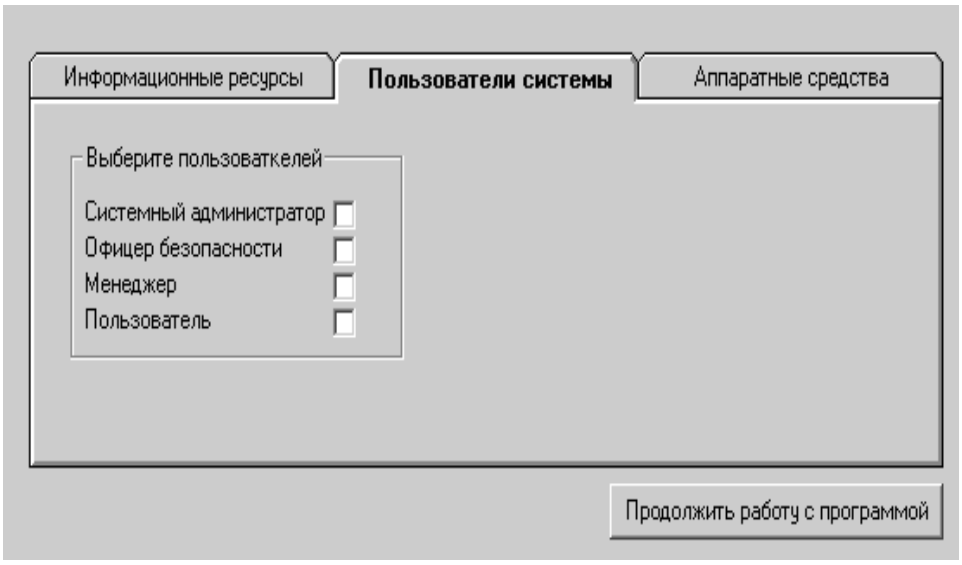


Рис. 17. Интерфейс программы. Вкладка «Пользователи системы»

Вкладка «Аппаратные средства» позволяет определить, место хранение и обработки информации.

Это могут быть: Сервера Рабочие станции Твердые копии

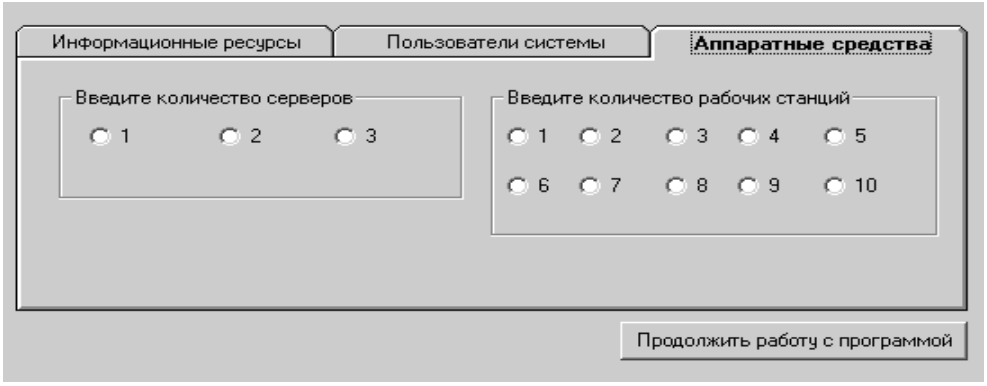


Рис. 18. Интерфейс программы. Вкладка «Аппаратные средства».

На вкладке приведенной ниже происходит привязка данных. Требуется расположить на каждом из ранее введенных ресурсов все указанные ранее виды ценной информации.

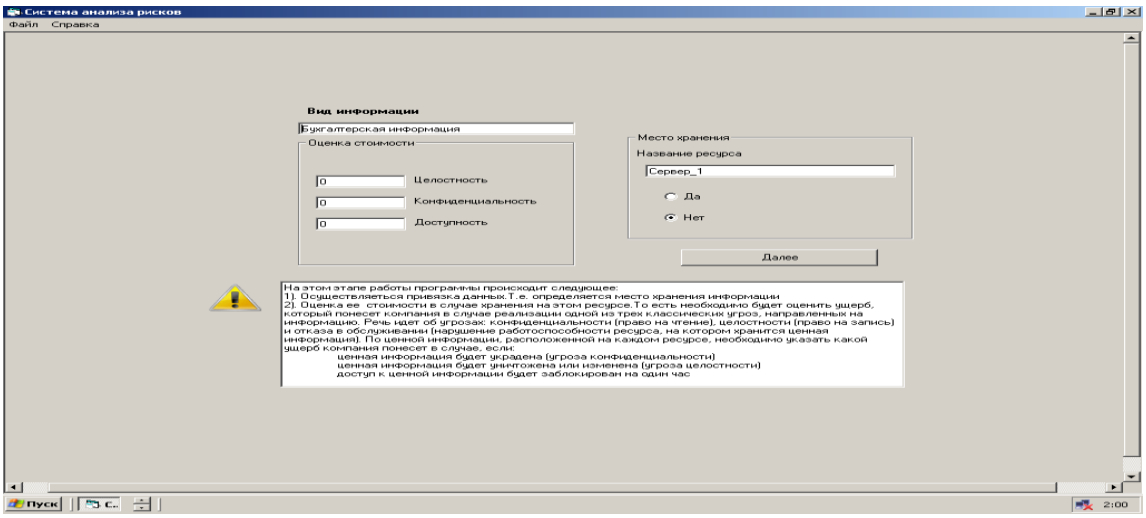


Рис. 19. Интерфейс программы. Вкладка «Привязка данных».

Кроме этого на этом этапе работы необходимо ещеопределить стоимость информации. То есть необходимо оценить ущерб, который понесет компания в случае реализации одной из трех классических угроз, направленных на информацию. Речь идет об угрозах: конфиденциальности (право на чтение), целостности (право на запись) и отказа в обслуживании (нарушение работоспособности ресурса, на котором хранится ценная информация). По ценной информации, расположенной на каждом ресурсе, необходимо указать какой ущерб компания понесет в случае, если:

ценная информация будет украдена (угроза конфиденциальности)

ценная информация будет уничтожена или изменена (угроза целостности) доступ к ценной информации будет заблокирован на один час

Оценивая ущерб от реализации угроз, необходимо учитывать: цену ресурса - затраты на производство;

стоимость восстановления или создания (покупку) нового ресурса;

стоимость восстановления работоспособности организации (при работе с искаженным ресурсом, без него, при дезинформации);

стоимость вынужденного простоя;

стоимость упущенной выгоды (потерянный контракт);

стоимость выплаты неустоек, штрафов (за невыполнение обязательств контракта); стоимость затрат на реабилитацию подмоченной репутации, престижа, имени фирмы; стоимость затрат на поиск новых клиентов, взамен более не доверяющих фирме; стоимость затрат на поиск (или восстановление) новых каналов связи, информационных источников.

Часто люди реально даже не представляют , чем владеют. Однако за владельцев оценить информацию не возможно. Предполагаемый злоумышленник может, конечно, оценить туже информацию иначе. Значить кто-то тут ошибается: владелец или злоумышленник. Здесь речь идет о приблизительной оценки. Точно оценить информацию

очень сложно.

После проделанной работы мы переходим к следующему этапу, этапу «Проверки организационных мер обеспечения информационной безопасности на соответствие положением МСБ ISO 17799».

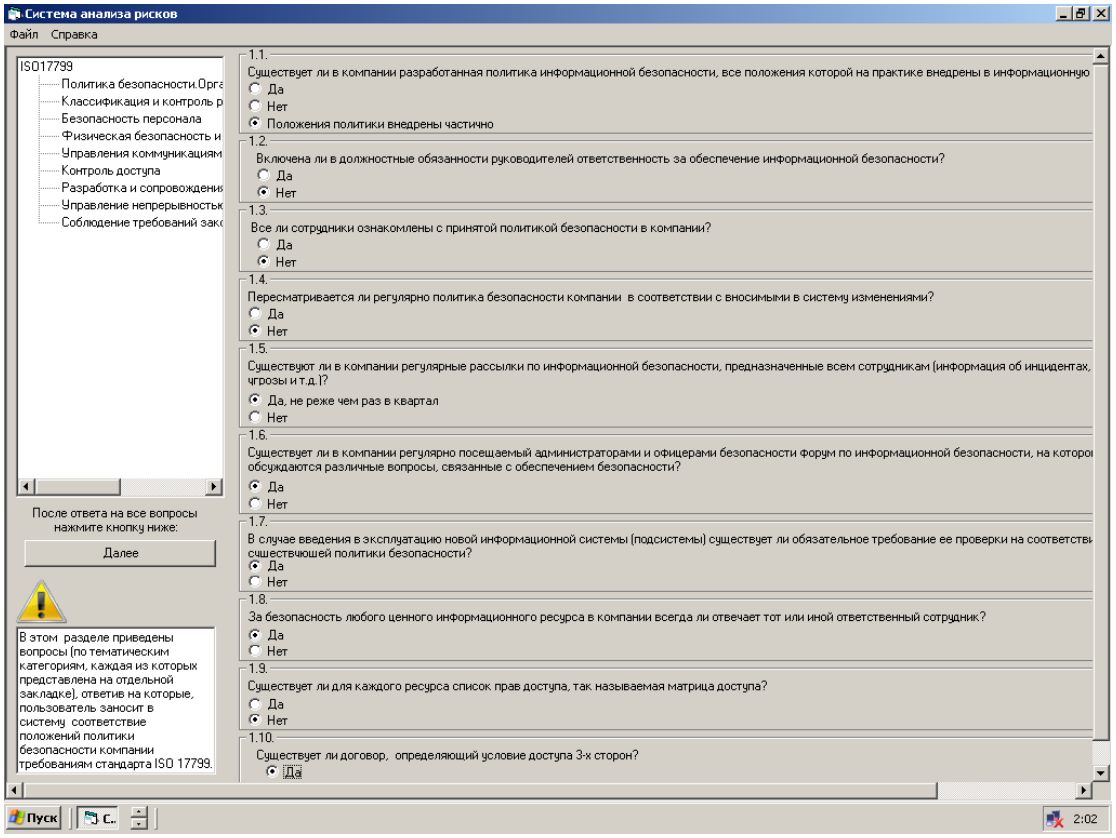


Рис. 20. Интерфейс программы. Вкладка «Организационные меры».

Пользователю предлогается ответить на вопросы, разработанные после изучение положений МБО. Вопросы структурированы по разделам стандарта. Выбор раздела осуществляется в левой части экрана щелчком правой кнопки мыши. Вопросы отображаются в правой части. Это форма, как и все остальные, снабжена подсказками.

После ответа на все вопросы, пользователь нажимает кнопку далее и программа переходит к следующему окну.

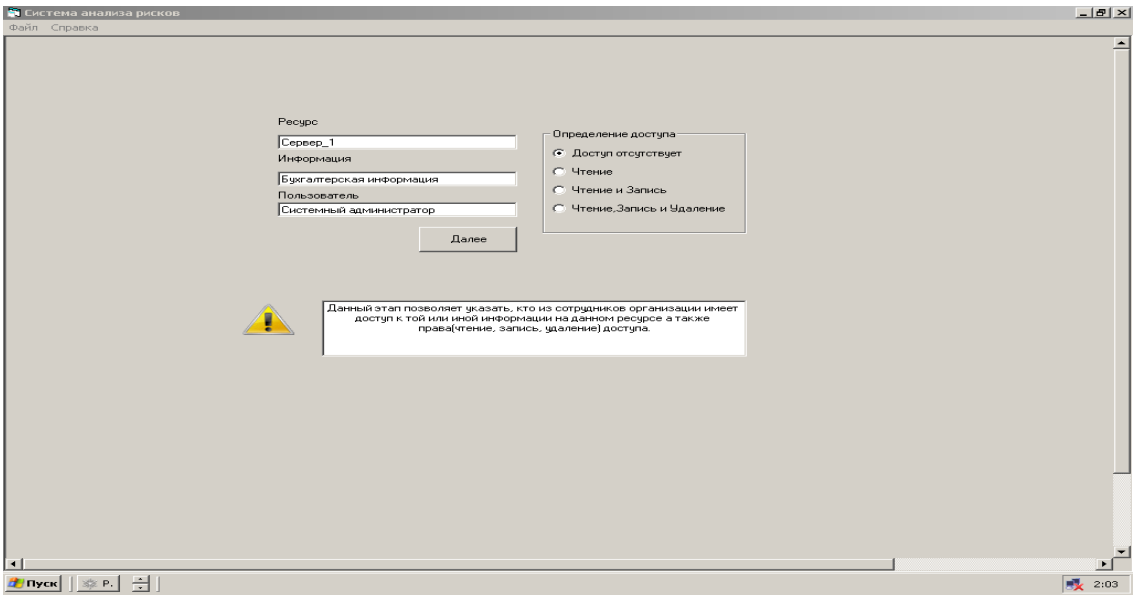


Рис. 21. Интерфейс программы. Вкладка «Доступ».

Здесь необходимо определить доступ пользователей и его права (чтение, запись, удаление) ко всем ресурсам, содержащим ценную информацию. Переходим к следующему окну.

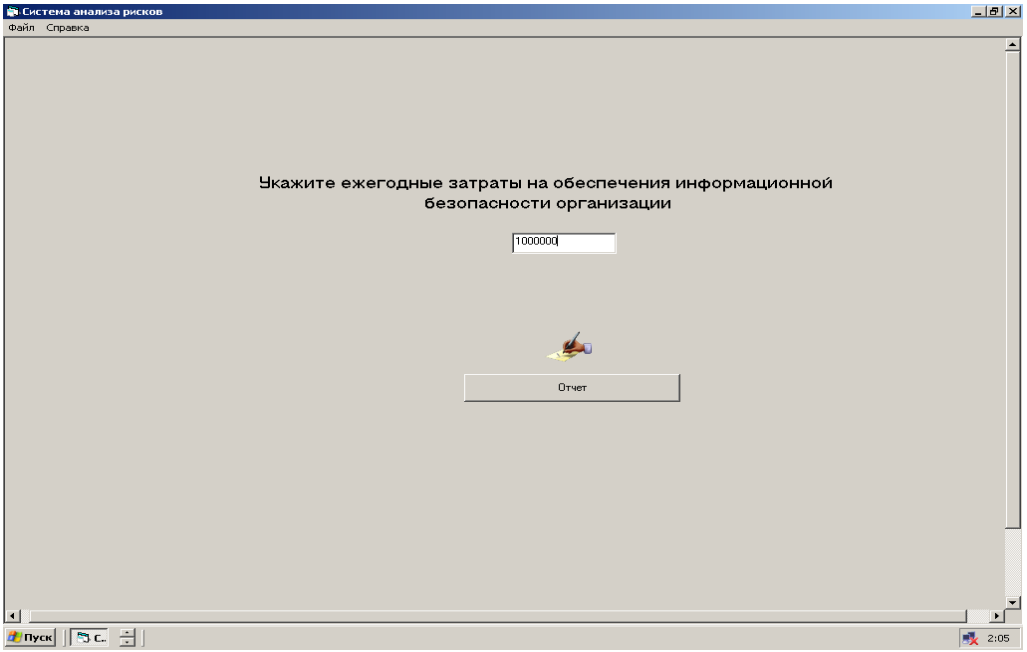
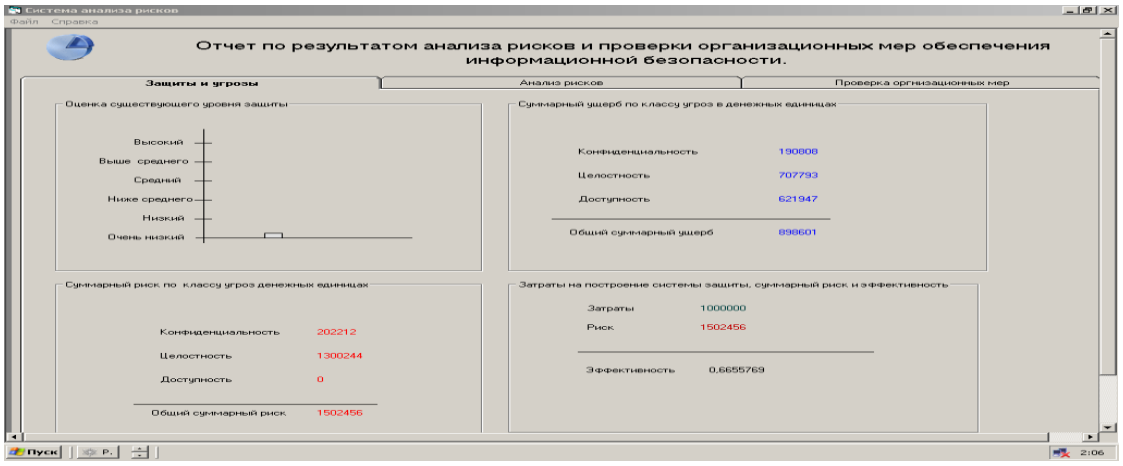


Рис. 25. Интерфейс программы. Оценка затрат на поддержаниесистемы безопасности

На данном этапе работы с целью определение эффективности системы защиты информации требуется определить и внести в систему полную стоимость затрат на обеспечение информационной безопасности.

В этом случае эффективность можно определить как отношение затрат к потерям которые понесет компания в случае реализации угроз безопасности.

Это могут быть:



Затраты на покупку систем защиты информации. Другими словами, это стоимость лицензии программного обеспечения. Кроме того, необходимо также учесть в данном пункте затраты на аппаратное обеспечение - стоимость одного или нескольких компьютеров, на которых развернуты компоненты системы защиты. Также необходимо учесть затраты на покупку или создание средств технической защиты. Помимо этого, часто система защиты использует дополнительное программное и аппаратное обеспечение, стоимость которого также необходимо учитывать. К такому обеспечению можно отнести базы данных, системы настройки оборудования, системы резервирования, сетевые кабели, тройники, системы бесперебойного питания и т.д. В крупных компаниях, имеющих распределенную корпоративную сеть, не стоит забывать о затратах на внедрение (включая этап предварительного аудита).

Затраты на поддержку и обучение (если она не включена в стоимость системы защиты). Сюда же можно отнести и командировочные расходы IT-специалистов на поездки в удаленные офисы и настройку удаленных компонентов системы обеспечения информационной безопасности.

Затраты на управление (администрирование) системой защиты, которые включают зарплату администраторов безопасности и другого персонала, связанного с системой обнаружения атак и модернизацию ее программно-аппаратного обеспечения. К этой статье расходов относится оплата за услуги аутсорсинговых компаний и реагирование на инциденты безопасности. Теперь система генерирует отчет и выводит полученные данные на обозрение.

Данная вкладка позволяет пользователю визуально оценить существующий уровень информационной защиты, суммарный риск и ущерб по трем классам угроз и эффективность существующей системы защиты.

При щелчке мыши по вкладке «Анализ рисков»№ появляются еще две вкладки , демонстрирующие качественные и количественные показатели рисков

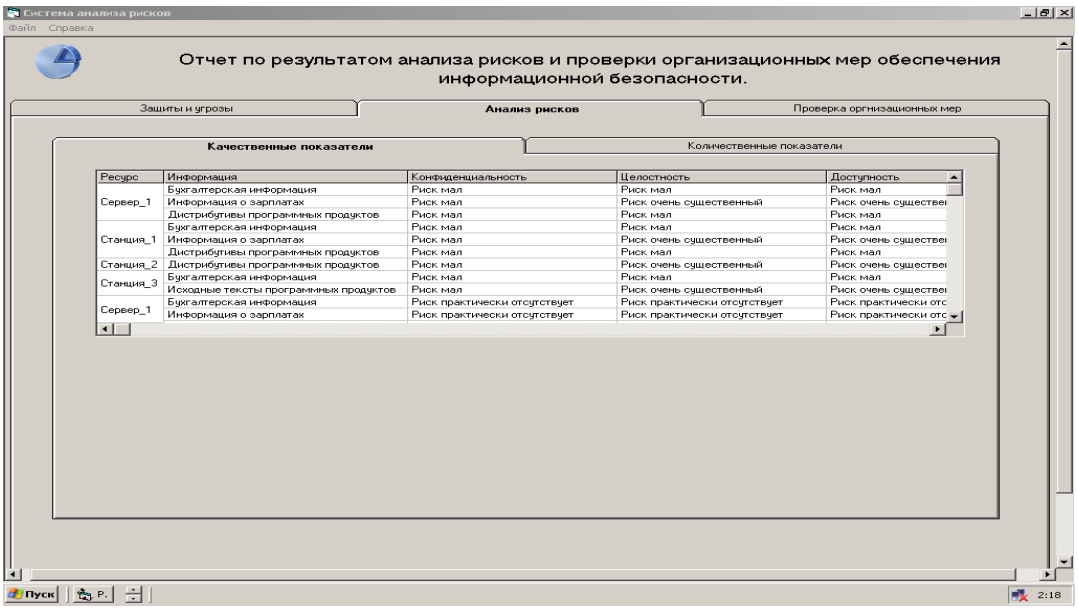


Рис. 27. Интерфейс программы. Вкладка «Анализ рисков.

Последняя вкладка Проверка организационных мер демонстрирует пользователю, количество не соответствующих организационных мер положениям МБО и выводит пояснение.

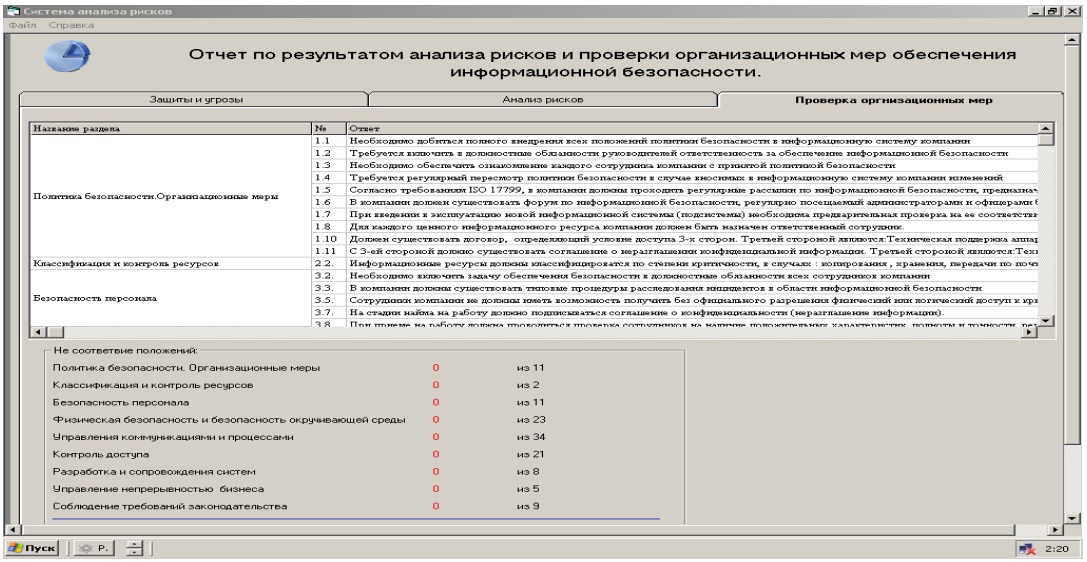


Рис. 29. Интерфейс программы. Вкладка « Проверка организационных мер» Ⅱ.

Тестирование системы

Данный пункт необходим для проведения проверки верного функционирования расчетного блока программного кода (его части). Тестирование направленно на изучение зависимости потерь организации от некоторых факторов (от классификация злоумышленника, права доступа пользователей системы и организационных мер обеспечения информационной безопасности**).**

Используемая при тестировании программного продукта информация не основывается

на конкретных значениях, для конкретного предприятия – это абстрактные данные об абстрактном предприятии, необходимые для процесса тестирования.

Таблица 5. Исходные данные для исследования.

Виды информации	Бухгалтерская информация Информация о зарплатах Информация о клиентах в электронном виде

	Исходные тексты программных продуктов Дистрибутивы программных продуктов (в том числе и собственные) Информация о партнерах в электронном виде
Пользователи системы	Системный администратор Офицеры безопасности Пользователь
Аппаратные средства	Сетевая группа: Один сервер Три рабочих станции

Теперь осуществим привязку данных. Расположим на каждом из ранее введенных ресурсов указанные виды ценной информации.

Сервер	Исходные тексты программных продуктов Дистрибутивы программных продуктов (в том числе и собственные)
Рабочая станция один	Бухгалтерская информация Информация о зарплатах
Рабочая станция два	Бухгалтерская информация Информация о зарплатах
Рабочая станция три	Информация о клиентах в электронном виде
	Информация о партнерах в электронном виде

Для определения стоимости информации, необходимо оценить ущерб, который

понесет компания в случае реализации трех классических угроз.

В предыдущем шаге мы разместили один и тот же тип информации на двух рабочих станциях. В этом шаге мы еще и оценим их одинаково. В конце тестов мы посмотрим результат и оценим, на сколько правильно работает алгоритм системы.

Таблица 7. Оценка информации

Ресурс	Информация	Ущерб, в случае угрозы конфиденциальности, руб.	Ущерб, в случае угрозы целостности, руб.	Ущерб, в случае угрозы доступности руб.
Сервер	Исходные тексты программных продуктов	80 000	50 000	120 000
	Дистрибутивы программных продуктов	110 000	80 000	170 000
Рабочая станция один	Бухгалтерская информация	5 000	140 000	120 000
	Информация о зарплатах	130 000	260 000	100 000
Рабочая станция	Бухгалтерская информация	5 000	140 000	120 000

два	Информация о зарплатах	130 000	260 000	100 000
Рабочая станция три	Информация о клиентах в электронном виде	150 000	170 000	250 000
	Информация о партнерах в электронном виде	160 000	145 000	300 000

Пользователи	Информация	Права доступа
Системный администратор	Бухгалтерская информация	Чтение , запись, удаление
	Информация о зарплатах	Чтение и запись
Офицер безопасности	Бухгалтерская информация	Чтение , запись, удаление
	Информация о зарплатах	Чтение и запись
Пользователь	Бухгалтерская информация	Чтение и запись

Определение доступа мы произведем по следующей схеме:

1) Ограничим доступ всех пользователей к информации, хранящейся на первой рабочей станции.

2) К тем же видам информации на второй рабочей станции права доступа оценим по разному.Укажем доступ к информации, хранящейся на сервере и на третей рабочей станции в хаотичном порядке.

Таблица 9. Определение прав доступа пользователей на рабочей станции три

Пользователи	Информация	Права доступа
Системный администратор	Информация о клиентах в электронном виде	Чтение , запись, удаление
	Информация о партнерах в электронном виде	Чтение
Офицер безопасности	Информация о клиентах в электронном виде	Доступ отсутствует
	Информация о партнерах в электронном виде	Чтение, запись
Пользователь	Информация о клиентах в электронном виде	Доступ отсутствует
	Информация о партнерах в электронном виде	Чтение

Таблица 10. Определение прав доступа пользователей на сервере

Пользователи	Информация	Права доступа
Системный администратор	Исходные тексты программных продуктов	чтение

	Дистрибутивы программных продуктов (в том числе и собственные)	Чтение и запись
Офицер безопасности	Исходные тексты программных продуктов	Чтение, запись, удаление
	Дистрибутивы программных продуктов (в том числе и собственные)	Чтение и запись
Пользователь	Исходные тексты программных продуктов	Доступ отсутствует
	Дистрибутивы программных продуктов (в том числе и собственные)	Доступ отсутствует

Далее, для проверки организационных мер, осуществим невыполнение большинства требования международного стандарта ISO 17799. Это позволит увеличить уровень уязвимости системы. С помощью ответов на вопросы связанных с тем, на сколько сотрудники заинтересованы в неправомерных действиях, мы увеличим уровень угроз.

Оценим ежегодные затраты на обеспечения информационной безопасности в 500 тысяч рублей. Процесс тестирования дал следующие результаты.

Таблица 11.Результат расчета количественной характеристики рисков

Ресурс	Информация	Риск связанный с угрозой	Риск связанный с	Риск связанный с

		конфиденциальности, руб.	угрозой целостности, руб.	угрозой доступности, руб.
Сервер	Исходные тексты программных продуктов	480 000	400 000	960 000
	Дистрибутивы программных продуктов	660 000	640 000	1 020 000
Рабочая станция один	Бухгалтерская информация	30000	840000	720000
	Информация о зарплатах	780000	1560000	600000
Рабочая станция два	Бухгалтерская информация	40000	1120000	960000
	Информация о зарплатах	1040000	2080000	600000
Рабочая станция три	Информация о клиентах в электронном виде	900000	1020000	1500000
	Информация о партнерах в электронном виде	960000	870000	1800000

Таблица 12. Результат расчета качественной характеристики рисковРесурс	Информация	Риск связанный с угрозой конфиденциальности	Риск связанный с угрозой целостности	Риск связанный с угрозой доступности
Сервер	Исходные тексты программных продуктов	Риск велик	Риск очень велик	Риск очень велик
	Дистрибутивы программных продуктов	Риск велик	Риск очень велик	Риск очень велик
Рабочая станция один	Бухгалтерская информация	Риск велик	Риск велик	Риск велик
	Информация о зарплатах	Риск велик	Риск велик	Риск велик
Рабочая станция два	Бухгалтерская информация	Риск очень велик	Риск очень велик	Риск очень велик
	Информация о зарплатах	Риск очень велик	Риск очень велик	Риск очень велик
Рабочая станция три	Информация о клиентах в электронном виде	Риск велик	Риск велик	Риск велик

	Информация о партнерах в электронном виде	Риск велик	Риск велик	Риск велик

При этом система показала уровень системы защиты как низкий.

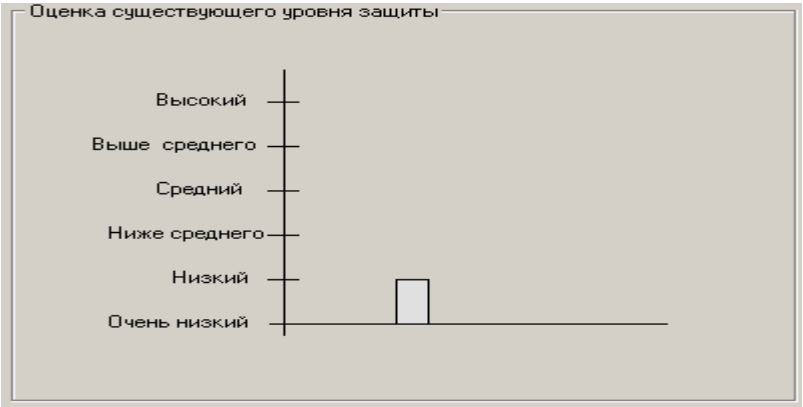


Рис. 30. Оценка уровня защиты. Тест номер один.

Далее проведем следующее испытание программного комплекса. Теперь наоборот, попробуем выполнить как можно больше требований стандарта ISO17799.Это позволит увеличить уровень уязвимости системы и в некоторых случаях уровень угроз. Ответы ответов на вопросы связанные с тем, на сколько сотрудники заинтересованы в неправомерных действиях оставим такими же как и в первом тесте.

Процесс тестирования дал следующие результаты.

Ресурс	Информация	Риск связанный с угрозой конфиденциальности, руб.	Риск связанный с угрозой целостности, руб.	Риск связанный с угрозой доступности, руб.

Сервер	Исходные тексты программных продуктов	160000	100000	240000
	Дистрибутивы программных продуктов	220000	240000	340000
Рабочая станция один	Бухгалтерская информация	10000	280000	240000
	Информация зарплатах	260000	520000	200000
Рабочая станция два	Бухгалтерская информация	10000	420000	240000
	Информация зарплатах	260000	780000	200000
Рабочая станция три	Информация клиентах в электронном виде	300000	340000	500000
	Информация партнерах в электронном виде	320000	290000	600000

Организационные меры не соответствовали 23 положениям международного стандарта ISO 17799.

Рис. 31. Оценка уровня защиты. Тест номер два

Из представленного материала мы видим , что произошло уменьшение риска до определенного уровня. Однако уровень угрозы со стороны сотрудников остался на определенном уровне, и это дало о себе знать. В целом система оценила уровень защиты как выше среднего.

Полученные данные говорят о том, что не соблюдение положений стандарта ISO 17799 приводит к увеличению риска связанного с угрозой конфиденциальности, целостности и доступности. Это в полнее справедливо так как, стандарт определяет базовый набор требований безопасности для широкого класса ИС, который формируется в результате обобщения мировой практики.

Мы заметили, что уровень рисков на рабочей станции два выше чем на номер один. Это говорит о том что, предоставление привилегированный прав доступа к информации, увеличивает уровень угрозы. Для борьбы с этим можно предпринять следующие меры.

Для того, чтобы понизить риск вредоносного воздействия со стороны сотрудников, необходимо уже при составлении должности максимально минимизировать количество информационных объектов, к которым пользователь будет иметь доступ впоследствии. В литературных источниках подобный принцип носит название принципа минимизации привилегий (либо прав доступа).

Потери предприятия тем меньше, чем меньше в этих потерях заинтересованы сотрудники данного предприятия. Очевидна необходимость ввода личной ответственности за собственную деятельность в отношении информационных активов компании. Личная ответственность предполагает разделение обязанностей по отношению к объектам, к

которым пользователь имеет доступ. Отсюда суть второго результата тестирования: чтобы понизить риск вредоносного воздействия со стороны сотрудников, нужно следовать правилу разделения обязанностей.

При приеме на работу проводить проверку сотрудников на наличие положительных характеристик, полноты и точности резюме, подтверждение заявленного образования и профессиональной квалификации и независимую проверку документов – паспорта.

Методика проведения лабораторной работы

1. Цель работы.

Целью данной лабораторной работы является ознакомление с методикой анализа рисков, ролью анализа рисков в построении системы защиты, а также ознакомление с международным стандартом информационной безопасности ISO 17799.

2.Теоретическая часть.

Информацию по этому пункту вы в полном объеме найдете в меню ‒Справка‖.

3. Порядок выполнения работы

1. После ознакомление с теорией получите у вашего преподавателя номер варианта на лабораторную работу. Каждый номер варианта представляет определенную модель информационной системы. Номера вариантов приведены ниже.

Название	Компания ‖РеалСофт‖
Сотрудники	Директор (сотрудник) Системный администратор Офицер безопасности Бухгалтер (сотрудник) Менеджер Программисты (сотрудники)
Информация	Бухгалтерская информация Информация о зарплатах Исходные тексты программных продуктов Дистрибутивы программных продуктов

Аппаратные средства для обработки информации	Два сервера Шесть рабочих станций
Описание	Организация занимается разработкой программного обеспечения. Расположена в отдельном здании. На входе расположена будка с охраной.
Затраты на информационную безопасность в год	100 000

Название организации	Нотариальная контора ‖Парус‖
Сотрудники	Директор Бухгалтер (сотрудник) Менеджер
Информация	Бухгалтерская информация Информация о зарплатах Дистрибутивы программных продуктов Информация о клиентах в электронном виде
Аппаратные средства для обработки информации	Один сервер Три рабочих станции

Описание	Занимается оформление договоров купли-продажи, обмена, дарения жилья, автомашин, земельных участков, копий документов. Проводит квалифицированные консультации по нотариальным вопросам Арендуемое помещение на втором этаже. Кроме этой организации в здании расположено еще несколько фирм. На входе существует охрана , которую интересует целью прихода
Затраты на информационную безопасность в год	10 000

Название организации	Страховая компания –Под крылом
Сотрудники	Директор (пользователь) Бухгалтер (пользователь) Системный администратор Менеджеры
Информация	Бухгалтерская информация Информация о зарплатах Информация о клиентах в электронном виде Информация о сотрудниках в электронном виде Дистрибутивы программных продуктов

Аппаратные средства для обработки информации	Один сервер Четыре рабочих станции
Название организации	Филиал нефтяной компании в Томске
Описание	Компания занимается страхованием всех видов деятельности. Расположена в отдельном здании. На входе сидит охранник.
Затраты на информационную безопасность в год	200 000 РусНефть‖
Сотрудники	Директор (сотрудник) Системный администратор Офицер безопасности Бухгалтер (сотрудник) Менеджер Программисты (сотрудники)
Информация	Бухгалтерская информация Информация о зарплатах Информация о клиентах в электронном виде Дистрибутивы программных продуктов Объемы продаж Себестоимость продукции
Описание	Занимается транспортировкой и переработкой нефти. Расположена в отдельном здании. Существует служба безопасности. На входе охрана регистрирует цель прихода.

Название организации	Компьютерная фирма ‖Ваш компьютер‖
Сотрудники	Директор (сотрудник) Системный администратор
	Бухгалтер (сотрудник) Менеджеры
Информация	Бухгалтерская информация Информация о зарплатах Дистрибутивы программных продуктов Объемы продаж Информация о партнерах в электронном виде Техническая информация о продуктах
Аппаратные средства для обработки информации	Два сервера Три рабочих станции
Описание	Занимается продажей компьютеров, офисной техники, сетевого оборудования, программного обеспечения. Расположена в отдельном здании. Существует служба охраны.
Затраты на информационную безопасность в год	1 000 000

Для того чтобы приступить к работе с ― Системой анализа рисков и проверки организационных мер обеспечения информационной безопасности на предприятия‖, необходимо запустить файл Project.exe. Далее система покажет окно с предложением начать работу с программой

Выберите те виды информационных ресурсов которые представлены в вашем варианте. Теперь перейдите к вкладке –Пользователи системы‖, где надо будетотметить пользователей информационной системы. На вкладке –Аппаратные средства‖ определите количество серверов и рабочих станций из вашего варианта. Нажмите кнопку ‖Продолжить работу с программой‖.

Укажите на сервере хранение двух любых видов информации из списка, а на рабочих станциях по четыре вида информационных ресурса, желательно разных и оцените предполагаемый ущерб, в случае угроз конфиденциальности, целостности и доступности. Так как данные хранятся на разных ресурсах, то предполагается, что они имеют разную ценность. В случае если информация не храниться на выбранном ресурсе, то ее оценка не имеет смысла - эти данные все равно не будут использованы. В случае затруднения обратитесь к подсказке.

Далее система отобразит окно, с вопросами по разделу стандарта в правой части и выбором раздела стандарта в левой части экрана. Отвечать на вопросы лучше всего, начиная с первого раздела –Политика безопасности. Организационные меры‖. Оцените систему безопасности выбранной организации, учтите как можно больше недостатков, так как полное описание организационных мер обеспечения информационной безопасности для представленных вариантов не представляется возможным. Нажмите кнопку –Далее‖.

Перед вами окно с определением доступа пользователей к информационным ресурсам.

Ограничьте доступ к информации на первой выбранной станции. К тем же видам информации на второй рабочей станции, определите разные виды доступа пользователей.

На остальных серверах и рабочих станциях виды доступа определите сами.

Теперь на экране должно появиться окно для ввода затрат на информационнуюбезопасность. Затраты можно определить из вашего варианта. Это заключительный этап сбора информации о вашей организации. Далее программа генерирует отчет по результатам анализа.

Ознакомьтесь с представленным отчетом. Сравните риск и ущерб по трем классам угроз. Оцените на ваш взгляд эффективность системы защиты. Перейдите к вкладке

–Анализ рисков‖. Сравните данные о риске по трем классом угроз на рабочих станциях , к информации на которых был представлен доступ и к которым нет. Сделайте выводы.

Перейдите к вкладке –Проверка организационных мер‖. Посмотрите, какое количество организационных мер соответствуют положениям стандарта, и какое нет. Далее вам предстоит ознакомиться с основными положениями международного стандарта

безопасности ISO 17999.

Сделайте скриншоты трех вкладок отчета и сохраните их в своей отчет по лабораторной работе. Закройте окно программы. Снова откройте файл Project.exe. Повторите 3 и 4 пункт. Попытайтесь в 5 пункте соблюсти как можно больше положений МСБ ISO 17999. Далее повторите 7, 8, 9 пункт. Сделайте выводы.

Контрольные вопросы

1. Дайте определение понятия - Политика информационной безопасности.

2.Что такое процесс анализа рисков? Какова роль анализа рисков в процессе формирования политики безопасности компании.

3. В чем отличие полного анализа рисков от базового? 4.Что понимается под угрозой безопасности информации?

5.На какие два класса делиться все множество потенциальных угроз безопасности информации?

6.В чем заключается оценка рисков по двум факторам? 7.В чем заключается оценка рисков по трем факторам?

8. Дайте определение понятию –Уязвимость|.

9.Дайте определение понятиям –угроза конфиденциальности|, |угроза целостности| и –угроза доступности|.

10. Назовите основные разделы стандарта ISO 17799.

Рекомендуемая литература

1. Егоров Н.А. Комплексная защита информации в компьютерных системах**.** Учебное пособие. - М.: Логос, 2001. - 264 с.

2. Программный комплекс анализа и контроля рисков информационных систем компаний –Гриф‖[Электронный ресурс].Компании Digital Security //http://www.dsec.ru.

3. Программный комплекс проверки политики информационной безопасности компании –Кондор+| [Электронный ресурс]. Компании Digital Security // http://www.dsec.ru.

4. Интрасети: Доступ в Интернет , защита /Милославская Н.Г., Толстой А.И. Учебное пособие для вузов . - М.: ЮНИТИ-ДАНА, 2000. – 527 с.

5. Домарев В.В. Защита информации и безопасность компьютерных систем**.** - Киев: Изда-во "ДиаСофт", 1999. - 480 с.

6. Информационные технологии. Практическое правило управления информационной безопасность. Русский перевод стандарта ISO 17799 [Электронный ресурс].

7. Cobra и КОНДОР [Электронный ресурс].

8. Методики и технологии управления информационными рисками. [Электронный ресурс] // Журнал «IT Manager». 2003, №3

9.Аудит безопасности фирмы: теория и практика: Учебное пособие.

- М.: Академический Проект «Парадигма», 2005. - 352 с.

10. Основы безопасности информационных технологий, 2001.

//http://www.crime-research.ru.

Лабораторная работа 2. Исследование защищенности беспроводных сетей передачи данных

1. Цель работы

Объектом исследования является беспроводная высокозащищенная сеть передачи данных. Беспроводная высокозащищенная сеть передачи данных, работающая по стандарту 802.11g в диапазоне частот 2.4-2.483 ГГц. Скорость передачи данных составляет не менее 24 Мбит/сек, в расчете на одного пользователя. В системе, обеспечивается бесшовный роуминг, применяется надежная двухсторонняя аутентификация, для шифрования передаваемой по радиоканалу информации применяется алгоритм шифрования AES. В сети применяется оборудование компании D-Link.

Основными задачами сети являются:

- обеспечение роуминга на территории охваченной беспроводной сетью;
- определение зон покрытия каждой из точек доступа и частотное планирование;
- обеспечение заданной скорости передачи;
- выбор надежных метод аутентификации и шифрования трафика;
- выбор программно – аппаратного комплекса.

2. Краткие теоретические сведения

Беспроводные сети стандарта 802.11 или Wi-Fi, приобретают все большую популярность. В качестве среды передачи используется радиоканал. По мере развития стандарта увеличивалась скорость передачи, совершенствовались методы защиты передаваемой информации. На сегодняшний день уровень защищенности трафика сравним с таковым в проводных сетях Ethernet, однако скорости передачи информации все еще значительно меньше чем в проводных сетях. Стандарты

802.11a/g предоставляют в распоряжение пользователей полудуплексный канал с пропускной способностью 54 Мбит/с. Однако беспроводные сети дарят пользователям мобильность, быстрее развертываются и в некоторых случаях дешевле. Беспроводные сети развертываются, как правило, там, где не нужны высокие скорости передачи (кафе, вокзалы, аэропорты).

Назначение и область применения системы

Сеть стандарта 802.11g относится к классу беспроводных сетей, т.е. в качестве среды передачи используется радиоканал. Передача ведется в диапазоне частот 2.4 ГГц. Беспроводные сети обеспечивают мобильность пользователю имеющему портативный ПК, технологии роуминга в сетях 802.11 позволяют абоненту перемещаться в пределах зоны обслуживания и при этом сохранять текущие соединения. Во многих компаниях используются телефоны стандарта 802.11, их применение дает возможность владельцам без потери связи перемещаться по зоне покрытой сетью. Такая связь значительно дешевле сотовой, так как затраты связаны только с приобретением и настройкой оборудования. Развертывать беспроводные сети значительно быстрее и в некоторых случаях дешевле, к тому же конфигурацию (зону покрытия, количество точек) можно менять без значительных затрат и в короткое время.

Основным назначением беспроводных сетей, как и любых сетей передачи данных, является предоставление пользователям возможности обмениваться данными друг с другом и предоставление доступа в Интернет. Важными характеристиками сети являются скорость передачи и задержки при передаче пакетов. Сети стандарта 802.11g предлагают потребителю полудуплексный канал с максимальной скоростью передачи 54 Мбит/с. Если предположить что одна точка доступа обслуживает 16 клиентов, то каждому из них достанется по 3.4 Мбит/с. Задержки в беспроводных сетях несколько больше чем в проводных, и сильно зависят от зашумленности эфира, однако это не мешает успешно передавать голосовой трафик.

Функции сети

Основные функции:

- предоставление доступа к ресурсам корпоративной сети;
- защита передаваемой по сети информации;
- надежная аутентификация пользователей.

Состав сети

Исходя из перечисленных функций можно указать минимальный состав системы:

Клиентские устройства. Будем понимать любое оборудование пользователя соответствующее стандарту 802.11g. (например ПК или ноутбук с беспроводными сетевым

адаптером).

Устройство беспроводного доступа в ЛВС. Программно-аппаратный комплекс, позволяющий передавать данные по беспроводному каналу (точка доступа).

Беспроводной коммутатор, в задачи которого входит обеспечение роуминга между точками доступа.

Система аутентификации. Система централизованного доступа на базе сервера RADIUS (Remote Access Dial-In User Service – сервис дистанционного пользовательского доступа).

Методы построения современных беспроводных сетей

Можно выделить три основных варианта построения (топологий) беспроводных сетей стандарта 802.11:

- независимые базовые зоны обслуживания (independent basic service sets,

IBSSs);

- базовые зоны обслуживания (basic service sets, BSSs);
- расширенные зоны обслуживания (extended service sets, ESSs).

Зона обслуживания (service set) в данном случае — это логически сгруппированные устройства. Технология WLAN обеспечивает доступ к сети путем передачи широковещательных сигналов через эфир на несущей в диапазоне радиочастот. Принимающая станция может получать сигналы в диапазоне работы нескольких передающих станций. Передающая станция вначале передает идентификатор зоны обслуживания (service set identifier, SSID). Станция-приемник использует SSID для фильтрации получаемых сигналов и выделения того, который ей нужен.

Независимые базовые зоны обслуживания IBSS

IBSS представляет собой группу работающих в соответствии со стандартом

802.11 станций, связывающихся непосредственно одна с другой. IBSS также называют специальной, или неплановой (ad-hoc) сетью, потому что она, по сути, представляет собой простую одноранговую WLAN. Специальная сеть, или независимая базовая зона обслуживания (IBSS), возникает, когда отдельные устройства-клиенты формируют самоподдерживающуюся сеть без использования отдельной точки доступа (рис. 1).

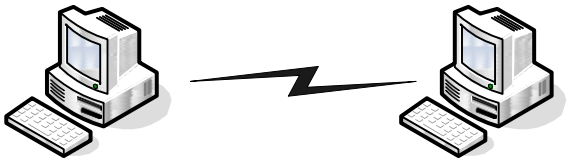


Рис. 1. Структура IBSS

При создании таких сетей не разрабатывают какие-либо карты места их развертывания и предварительные планы, поэтому они обычно невелики и имеют ограниченную протяженность, достаточную для передачи совместно используемых данных при возникновении такой необходимости. В отличие от варианта использования расширенной зоны обслуживания (ESS), клиенты непосредственно устанавливают соединения друг с другом, в результате чего создается только одна базовая зона обслуживания (BSS), не имеющая интерфейса для подключения к проводной локальной сети (т.е. отсутствует какая-либо распределительная система, которая необходима для объединения BSS и организации таким образом ESS). На данный момент не существует каких-либо оговоренных стандартом ограничений на количество устройств, которые могут входить в одну независимую базовую зону обслуживания. Но, поскольку каждое устройство является клиентом, зачастую определенное число членов IBSS не может связываться один с другим вследствие проблемы скрытого узла (hidden node issue). Несмотря на это, в IBSS не существует какого-либо механизма для реализации функции ретрансляции.

Поскольку в IBSS отсутствует точка доступа, распределение времени (timing) осуществляется нецентрализованно. Клиент, начинающий передачу в IBSS, задает сигнальный (его еще называют маячковый) интервал (beacon interval) для создания набора моментов времени передачи маячкового сигнала (set of target beacon transmission time, TBTT). Когда завершается TBTT, каждый клиент IBSS выполняет следующее. Приостанавливает все несработавшие таймеры задержки (backoff timer) из предыдущего TBTT. Определяет новую случайную задержку.

Если маячковый сигнал поступает до окончания случайной задержки, возобновляет работу приостановленных таймеров задержки. Если никакой маячковый сигнал не поступает до окончания случайной задержки, посылает маячковый сигнал и возобновляет работу приостановленных таймеров задержки.

Отсюда видно, что распределение времени для передачи маячковых сигналов осуществляется в специальных сетях не точкой доступа и не каким-то одним из клиентов. Поскольку такой схеме связи присуща проблема скрытого узла, вполне возможно, что в течение сигнального интервала будет передано множество маячковых сигналов от разных

клиентов и другие клиенты получат множество маячковых сигналов. Однако, стандарт вполне допускает такую ситуацию и никаких проблем не возникает, поскольку клиенты ожидают приема только первого маячкового сигнала, относящегося к их собственному таймеру случайной задержки. В маячковые сигналы встроена функция синхронизации таймера (timer synchronization function, TSF). Каждый клиент сравнивает TSF в маячковом сигнале со своим собственным таймером и, если полученное значение больше, считает, что часы передающей станции идут быстрее и подстраивает свой собственный таймер в соответствии с полученным значением. Это имеет долговременный эффект синхронизации работы всей неплановой сети по клиенту с самым быстрым таймером. В больших распределенных неплановых сетях, когда многие клиенты не могут связываться напрямую, может понадобиться некоторое время для достижения синхронизации всех клиентов.

Базовые зоны обслуживания BSS

BSS — это группа работающих по стандарту 802.11 станций, связывающихся одна с другой. Технология BSS предполагает наличие особой станции, которая называется точка доступа (access point) (рис. 2).

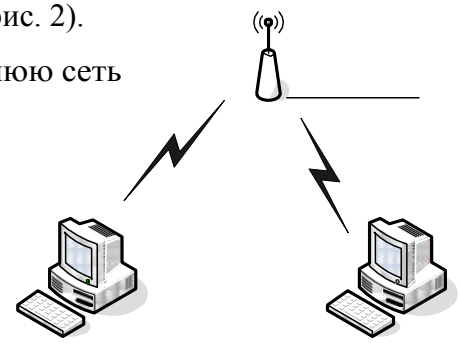


Рис. 2. Структура BSS

Точка доступа — это центральный пункт связи для всех станций BSS. Клиентские станции не связываются непосредственно одна с другой. Вместо этого они связываются с точкой доступа, а уже она направляет фреймы станции-адресату. Точка доступа может иметь порт восходящего канала (uplink port), через который BSS подключается к проводной сети (например, восходящий канал Ethernet). Поэтому BSS иногда называют инфраструктурой BSS.

Расширенные зоны обслуживания ESS

Несколько инфраструктур BSS могут быть соединены через их интерфейсы восходящего канала. Там, где действует стандарт 802.11, интерфейс восходящего канала соединяет BSS с распределительной системой (distribution system, DS). Несколько BSS, соединенных между собой через распределительную систему, образуют расширенную зону

обслуживания (ESS). Восходящий канал к распределительной системе не обязательно должен использовать проводное соединение. На рисунке 4.3 представлен пример структуры ESS. Спецификация стандарта 802.11 оставляет возможность реализации этого канала в виде беспроводного. Но чаще восходящие каналы к распределительной системе представляют собой каналы проводной Ethernet.

Обзор механизмов доступа к среде

Предотвращение коллизий является ключевым моментом для беспроводных сетей, поскольку последние не имеют явного механизма для их обнаружения. При использовании технологии CSMA/CA, коллизия обнаруживается только при неполучении передающей станцией ожидаемого подтверждения. Реализация технологии CSMA/CA стандартом 802.11 осуществляется при использовании распределенной функции координации (distributed coordination function, DCF). Для предотвращения коллизий в сетях с точкой доступа предусмотрен опциональный механизм централизованной функции координации PCF (Point Coordination Function).

Функция распределенной координации DCF

На первый взгляд организовать совместный доступ к среде передачи данных достаточно просто. Для этого необходимо лишь обеспечить, чтобы все узлы передавали данные только тогда, когда среда является свободной, то есть когда ни один из узлов не производит передачу данных. Однако такой механизм неизбежно приведет к коллизиям, поскольку велика вероятность того, что два или более узлов одновременно, пытаясь получить доступ к среде передачи данных, решат, что среда свободна и начнут одновременную передачу. Именно поэтому необходимо разработать алгоритм, способный снизить вероятность возникновения коллизий и в то же время гарантировать всем узлам сети равноправный доступ к среде передачи данных.

Одним из вариантов организации такого равноправного доступа к среде передачи данных является функция распределенной координации (DCF). Эта функция основана на методе коллективного доступа с обнаружением несущей и механизмом избежания коллизий (Carrier Sense Multiple Access/Collision Avoidance, CSMA/CA). При такой организации каждый узел, прежде чем начать передачу,

«прослушивает» среду, пытаясь обнаружить несущий сигнал, и только при условии, что среда свободна, может начать передачу данных.

Однако, в этом случае велика вероятность возникновения коллизий: когда два или более узлов сети одновременно (или почти одновременно) решат, что среда свободна, и начнут предавать данные. Для того чтобы снизить вероятность возникновения подобных ситуаций, используется механизм избежания коллизий (Collision Avoidance, CA). Суть

данного механизма заключается в следующем.

Каждый узел сети, убедившись, что среда свободна, прежде чем начать передачу, выжидает в течение определенного промежутка времени. Этот промежуток является случайным и складывается из двух составляющих: обязательного промежутка DIFS (DCF Interframe Space) и выбираемого случайным образом промежутка обратного отсчета (backoff time). В результате каждый узел сети перед началом передачи выжидает в течение случайного промежутка времени, что, естественно, значительно снижает вероятность возникновения коллизий, поскольку вероятность того, что два узла сети будут выжидать в течение одного и того же промежутка времени, чрезвычайно мала.

Для того чтобы гарантировать всем узлам сети равноправный доступ к среде передачи данных, необходимо соответствующим образом определить алгоритм выбора длительности промежутка обратного отсчета (backoff time). Промежуток обратного отсчета хотя и является случайным, но в то же время определяется на основании множества некоторых дискретных промежутков времени, то есть, равен целому числу элементарных временных промежутков, называемых тайм-слотами (SlotTime). Для выбора промежутка обратного отсчета каждый узел сети формирует так называемое окно конкурентного доступа (Contention Window, CW), использующееся для определения количества тайм-слотов, в течение которых станция выжидала перед передачей. Фактически окно CW – это диапазон для выбора количества тайм-слотов, причем минимальной размер окна определяется в 31 тайм-слот, а максимальный размер — в 1023 тайм-слота. Промежуток обратного отсчета определяется как количество тайм-слотов, определяемое исходя из размера окна CW:

$$Backoff\ time = Random[CW_{min}, CW_{max}] \times SlotTime$$

Когда узел сети пытается получить доступ к среде передачи данных, то после обязательного промежутка ожидания DIFS запускается процедура обратного отсчета, то есть включается обратный отсчет счетчика тайм-слотов начиная от выбранного значения окна CW. Если в течение всего промежутка ожидания среда оставалась свободной (счетчик обратного отсчета равен нулю), то узел начинает передачу.

После успешной передачи окно CW формируется вновь. Если же за время ожидания передачу начал другой узел сети, то значение счетчика обратного отсчет останавливается и передача данных откладывается. После того как среда станет свободной, данный узел снова начинает процедуру обратного отсчета, но уже с меньшим размером окна CW, определяемого предыдущим значением счетчика обратного отсчета и соответственно с меньшим значением времени ожидания. При этом очевидно, что чем большее число раз узел откладывает передачу по причине занятости среды, тем выше вероятность того, что в

следующий раз он получит доступ к среде передачи данных (рис. 4).

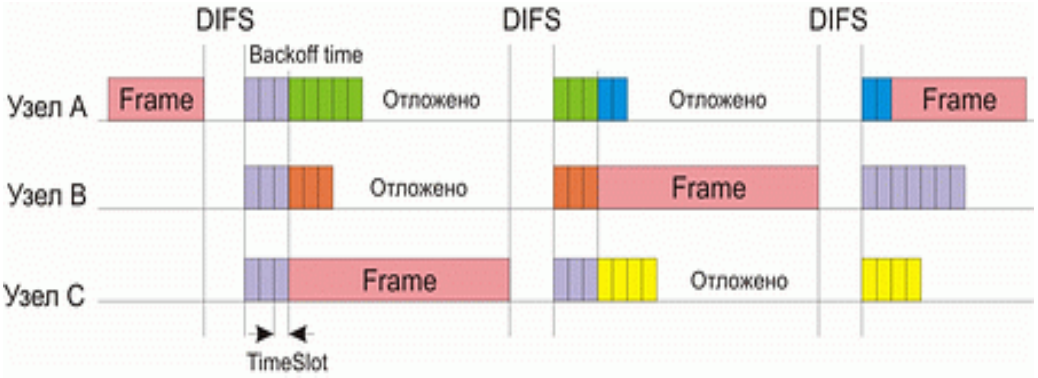


Рис. 4. Реализация равноправного доступа к среде передачи данных в методе DCF

Рассмотренный алгоритм реализации коллективного доступа к среде передачи данных гарантирует равноправный доступ всех узлов сети к среде. Однако при таком подходе вероятность возникновения коллизий хотя и мала, но все-таки существует. Понятно, что снизить вероятность возникновения коллизий можно путем увеличения максимального размера формируемого окна CW. В то же время это увеличит времена задержек при передачи и тем самым снизит производительность сети. Поэтому в методе DCF для минимизации коллизий используется следующий алгоритм. После каждого успешного приема кадра принимающая сторона через короткий промежуток SIFS (Short Interframe Space)подтверждает успешный прием, посылая ответную квитанцию – кадр ACK (ACKnowledgement) (рис. 5). Если в процессе передачи данных возникла коллизия, то передающая сторона не получает кадр ACK об успешном приеме. В этом случае размер CW-окна для передающего узла увеличивается почти вдвое. Так, если для первой передачи размер окна равен 31 слоту, то для второй попытки передачи он уже составляет 63 слота, для третьей – 127 слотов, для четвертой – 255, для пятой – 511, а для всех последующих – 1023 слота. То есть для каждой i-й передачи (если все предыдущие оказались безуспешными) размер CW-окна увеличивается по следующему правилу:

$$CW_i = 2CW_{i-1} + 1$$

Таким образом, увеличение размера окна происходит динамически по мере роста числа коллизий, что позволяет, с одной стороны, уменьшить временные задержки и, с другой стороны, снизить вероятность возникновения коллизий.

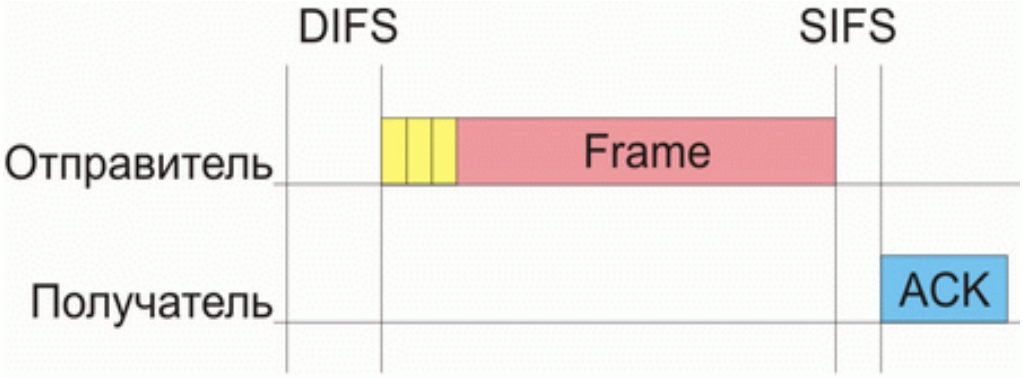


Рис. 5. Кадры квитанции, отсылаемые в случае успешной передачи данных

Говоря об алгоритме реализации равноправного доступа к среде передачи данных, необходимо также учитывать и размер кадра данных. Действительно, если кадры данных будут слишком большими, то при возникновении коллизий придется повторно передавать большой объем информации, что приведет к снижению производительности сети. Кроме того, при большом размере кадров данных узлы сети вынуждены простаивать в течение довольно продолжительного времени, прежде чем начать передачу.

В то же время использование кадров данных небольшого размера, хотя и позволяет гарантировать равноправный доступ всех узлов к среде передачи данных и минимизирует издержки при возникновении коллизий, не может не отразиться негативно на полезном сетевом трафике. Дело в том, что каждый кадр наряду с полезной информацией содержит информацию служебную (заголовок кадра). При уменьшении размера кадра сокращается величина именно полезной информации (пользовательских данных), что обусловливает передачу по сети избыточного количества служебной информации. Поэтому размер кадра — это своего рода золотая середина, от правильного выбора которой зависит эффективность использования среды передачи данных.

Рассмотренный механизм регламентирования коллективного доступа к среде передачи данных имеет одно узкое место — так называемую проблему скрытых узлов. Из-за наличия естественных препятствий возможна ситуация, когда два узла сети не могут «слышать» друг друга напрямую. Такие узлы называют скрытыми.

Для того чтобы разрешить проблему скрытых узлов, функция DCF опционально предусматривает возможность использования алгоритма RTS/CTS.

Алгоритм RTS/CTS

В соответствии с алгоритмом RTS/CTS каждый узел сети, перед тем как послать данные в «эфир», сначала отправляет специальное короткое сообщение, которое называется RTS (Ready To Send) и означает готовность данного узла к отправке данных. Такое RTS-сообщение содержит информацию о продолжительности предстоящей передачи и об

адресате и доступно всем узлам в сети (если только они не скрыты от отправителя). Это позволяет другим узлам задержать передачу на время, равное объявленной длительности сообщения. Приемная станция, получив сигнал RTS, отвечает посылкой сигнала CTS (Clear To Send), свидетельствующего о готовности станции к приему информации. После этого передающая станция посылает пакет данных, а приемная станция должна

передать кадр ACK, подтверждающий безошибочный прием. Последовательность отправки кадров между двумя узлами сети показана на рис.6.

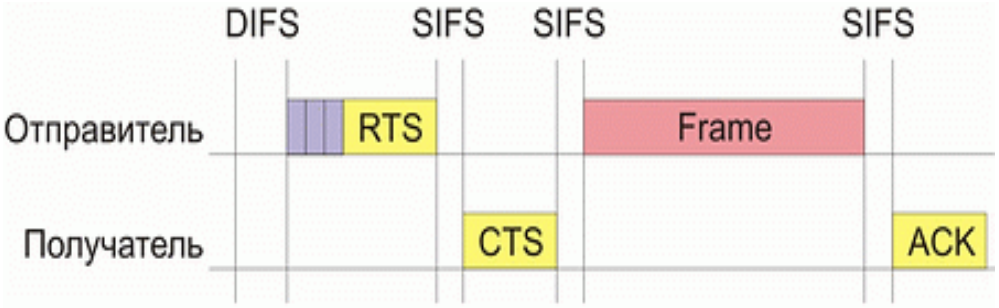


Рис. 6. Взаимодействие между двумя узлами сети в соответствии с алгоритмом RTS/CTS

Теперь рассмотрим ситуацию, когда сеть состоит из четырех узлов: A, B, C и D (рис. 4.4). Предположим, что узел C находится в зоне досягаемости только узла A, узел A находится в зоне досягаемости узлов C и B, узел B находится в зоне досягаемости узлов A и D, а узел D находится в зоне досягаемости только узла B. То есть в такой сети имеются скрытые узлы: узел C скрыт от узлов B и D, узел A скрыт от узла D.

В подобной сети алгоритм RTS/CTS позволяет справиться с проблемой возникновения коллизий, которая не решается посредством рассмотренного базового способа организации коллективного доступа в DCF. Действительно, пусть узел A пытается передать данные узлу B. Для этого он посылает сигнал RTS, который, помимо узла B, получает также узел C, но не получает узел D. Узел C, получив данный сигнал, блокируется, то есть приостанавливает попытки передавать сигнал до момента окончания передачи между узлами A и B. Узел B, в ответ на полученный сигнал RTS, посылает кадр CTS, который получают узлы A и

D. Узел D, получив данный сигнал, также блокируется на время передачи между узлами A и B.

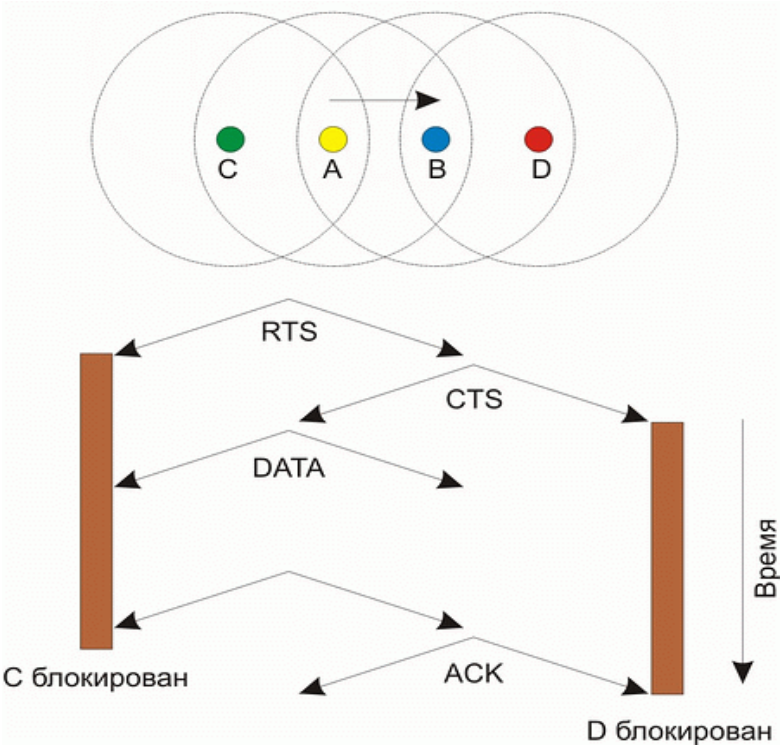


Рис.7. Решение проблемы скрытых узлов в алгоритме RTS/CTS

У алгоритма RTS/CTS имеются свои подводные камни, которые в определенных ситуациях могут приводить к снижению эффективности использования среды передачи данных. К примеру, в некоторых ситуациях возможно такое явление, как распространение эффекта ложных блокировок узлов, что в конечном счете может привести к ступору в сети.

Рассмотрим, к примеру, сеть, показанную на рис. 4.5. Пусть узел B пытается передать данные узлу A, посылая ему кадр RTS. Поскольку этот кадр получает также и узел C, то он блокируется на время передачи между узлами A и B. Узел D, пытаясь передать данные узлу C, посылает кадр RTS, но поскольку узел C заблокирован, то он не получает ответа и начинает процедуру обратного отсчета с увеличенным размером окна. В то же время кадр RTS, посланный узлом D, получает и узел E, который, ложно предполагая, что за этим последует сеанс передачи данных от узла D к узлу C, блокируется. Однако это ложная блокировка, поскольку реально между узлами D и C передачи нет. Более того, если узел F попытается передать данные ложно заблокированному узлу E и пошлет свой кадрRTS, то он ложно заблокирует узел G.

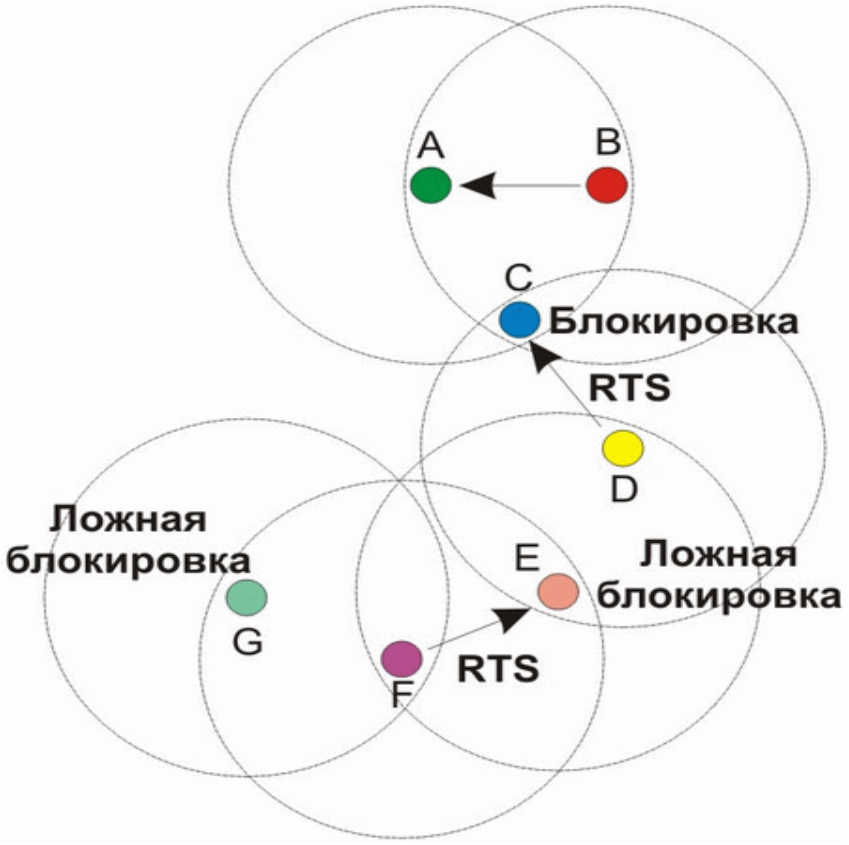


Рис. 7. Возникновение ложных блокировок узлов сети

Описанное явление ложной блокировки узлов может приводить к кратковременному ступору всей сети.

Фрагментация фрейма по стандарту 802.11

Фрагментация фрейма – это выполняемая на уровне MAC функция, назначение которой – повысить надежность передачи фреймов через беспроводную среду. Под фрагментацией понимается дробление фрейма на меньшие фрагменты и передача каждого из них отдельно. Предполагается, что вероятность успешной передачи меньшего фрагмента через зашумленную беспроводную среду выше. Получение каждого фрагмента фрейма подтверждается отдельно; следовательно, если какой-нибудь фрагмент фрейма будет передан с ошибкой или вступит в коллизию, только его придется передавать повторно, а не весь фрейм. Это увеличивает пропускную способность среды.

Размер фрагмента может задавать администратор сети. Фрагментации подвергаются только одноадресные фреймы. Широковещательные, или многоадресные, фреймы передаются целиком. Кроме того, фрагменты фрейма передаются пакетом, с использованием только одной итерации механизма доступа к среде DSF.

Хотя за счет фрагментации можно повысить надежность передачи фреймов в беспроводных локальных сетях. Она приводит к увеличению «накладных расходов» MAC-

протокола стандарта 802.11. Каждый фрагмент фрейма включает информацию, содержащуюся в заголовке 802.11 MAC, а также требует передачи соответствующего фрейма подтверждения. Это увеличивает число служебных сигналов MAC-протокола и снижает реальную производительность беспроводной станции. Фрагментация – это баланс между надежностью и непроизводительной загрузкой среды.

Функция централизованной координации PCF

Рассмотренный выше механизм распределенной координации DCF является базовым для протоколов 802.11 и может использоваться как в беспроводных сетях, функционирующих в режиме Ad-Hoc, так и в сетях, функционирующих в режиме Infrastructure, то есть в сетях, инфраструктура которых включает точку доступа.

Однако для сетей в режиме Infrastructure более естественным является несколько иной механизм регламентирования коллективного доступа, известный как функция централизованной координации (Point Coordination Function, PCF). Отметим, что механизм PCF является опциональным и применяется только в сетях с точкой доступа.

В случае задействования механизма PCF один из узлов сети (точка доступа) является центральным и называется центром координации (Point Coordinator, PC). На центр координации возлагается задача управления коллективным доступом всех остальных узлов сети к среде передачи данных на основе определенного алгоритма опроса или исходя из приоритетов узлов сети. То есть центр координации опрашивает все узлы сети, внесенные в его список, и на основании этого опроса организует передачу данных между всеми узлами сети. Важно, что такой подход полностью исключает конкурирующий доступ к среде, как в случае механизма DCF, и делает невозможным возникновение коллизий, а для времезависимых приложений гарантирует приоритетный доступ к среде. Таким образом, PCF может использоваться для организации приоритетного доступа к среде передачи данных.

Функция централизованной координации не отрицает функцию распределенной координации, а скорее, дополняет ее, накладываясь поверх. Фактически в сетях с механизмом PCF реализуется как механизм PCF, так и традиционный механизм DCF. В течение определенного промежутка времени реализуется механизм PCF, затем – DCF, а потом все повторяется заново.

Для того чтобы иметь возможность чередовать режимы PCF и DCF, необходимо, чтобы точка доступа, выполняющая функции центра координации и реализующая режим PCF, имела бы приоритетный доступ к среде передачи данных. Это можно сделать, если использовать конкурентный доступ к среде передачи данных (как и в методе DCF), но для центра координации разрешить использовать промежуток ожидания, меньший DIFS. В этом

случае если центр координации пытается получить доступ к среде, то он ожидает (как и все остальные узлы сети) окончания текущей передачи и, поскольку для него определяется минимальный режим ожидания после обнаружения «тишины» в эфире, первым получает доступ к среде. Промежуток ожидания, определяемый для центра координации, называется PIFS (PCF Interframe Space), причем SIFS<PIFS<DIFS.

Режимы DCF и PCF объединяются в так называемом суперфрейме, который образуется из промежутка бесконкурентного доступа к среде, называемого CFP (Contention-Free Period), и следующего за ним промежутка конкурентного доступа к среде CP (Contention Period) (рис. 8).

Рис. 8. Объединение режимов PCF и DCF в одном суперфрейме

Суперфрейм начинается с кадра-маячка (beacon), получив который все узлы сети приостанавливают попытки передавать данные на время, определяемое периодом CFP. Кадры маячки несут служебную информацию о продолжительности CFP-промежутка и позволяют синхронизировать работу всех узлов сети. Во время режима PCF точка доступа опрашивает все узлы сети о кадрах, которые стоят в очереди на передачу, посылая им служебные кадры CF_POLL. Опрашиваемые узлы в ответ на получение кадров CF_POLL посылают подтверждение CF_ACK. Если подтверждения не получено, то точка доступа переходит к опросу следующего узла.

Кроме того, чтобы иметь возможность организовать передачу данных между всеми узлами сети, точка доступа может передавать кадр данных (DATA) и совмещать кадр опроса с передачей данных (кадр DATA+CF_POLL). Аналогично узлы сети могут совмещать кадры подтверждения с передачей данных DATA+CF_ACK (рис. 4.7).

Допускаются следующие типы кадров во время режима PCF:

- DATA – кадр данных
- CF_ACK – кадр подтверждения
- CF_POLL – кадр опроса
- DATA+CF_ACK – комбинированный кадр данных и подтверждения
- DATA+CF_POLL – комбинированный кадр данных и опроса

- DATA+CF_ACK+CF_POLL — комбинированный кадр данных, подтверждения и опроса
- CF_ACK+CF_POLL – комбинированный кадр подтверждения и опроса

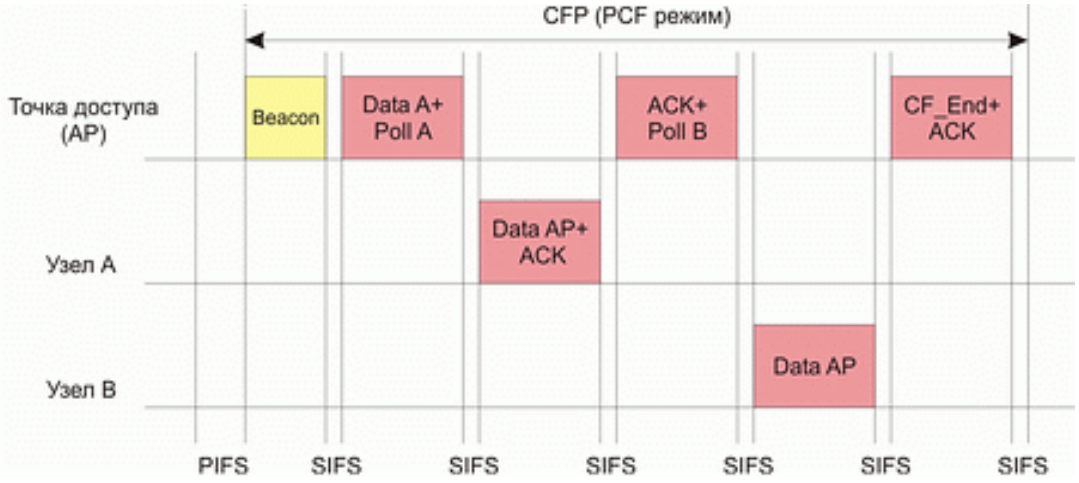


Рис. 9. Организация передачи данных между узлами сети в режиме PCF

Физические уровни стандартов

Основное назначение физических уровней стандарта 802.11 – обеспечение механизма беспроводной передачи для подуровня MAC, а также поддержание вторичных функций (оценка состояние беспроводной среды и сообщение об этом MAC). MAC и PHY не зависимы это дает возможность использовать более скоростные физические уровни, описанные в стандартах 802.11a/b/g.

Каждый физический уровень стандарта имеет два подуровня:

- PLCP (Physical Layer Convergence Procedure) – процедура определения состояния физического уровня;
- PMD (Physical Medium Dependent) – подуровень физического уровня, зависящий от среды передачи.

На рис. 10 показана как эти уровни соотносятся между собой и вышестоящими уровнями.

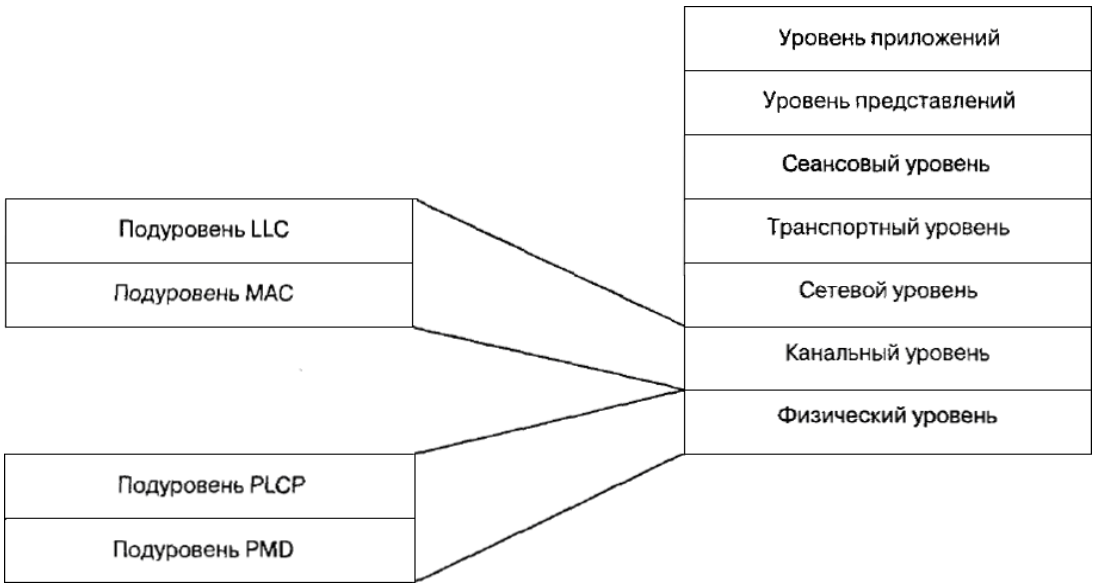


Рис. 10. Подуровни уровня PHY модели взаимодействия открытых систем (OSI)

Подуровень PLCP является уровнем обеспечения взаимодействия, на котором осуществляется перемещение элементов данных протокола MAC (MAC protocol data units, MPDU) между MAC – станциями с использованием подуровня PMD, на котором реализуется тот или иной метод передачи и приема данных через беспроводную сеть. Подуровни PLCP и PMD отличаются в разных вариантах стандарта 802.11.

Физический уровень беспроводных сетей стандарта 802.11

Исходный стандарт 802.11 определяет два метода передачи на физическом уровне.

- Технология расширения спектра путем скачкообразной перестройки частоты (FHSS)
- Технология широкополосной модуляции с расширением спектра методом пря- мой последовательности (DSSS)

Обе технологии работают в диапазоне 2,4 ГГц, в котором выделена полоса шириной 82 МГц для промышленного, научного и медицинского применения (ISM).

Беспроводные локальные сети со скачкообразной перестройкой частоты (FHSS)

Беспроводные локальные сети FHSS (Frequency Hopping Spread Spectrum) поддерживают скорости передачи 1 и 2 Мбит/с. Как следует из названия, устройства FHSS осуществляют скачкообразную перестройку частоты по предопределенной схеме, как показано на рис. 11. Устройства FHSS делят предназначенную для их работы полосу частот от 2,402 до 2,480 ГГц на 79 неперекрывающихся каналов (это справедливо для Северной

Америки и большей части Европы). Ширина каждого из 79 каналов составляет 1 МГц.

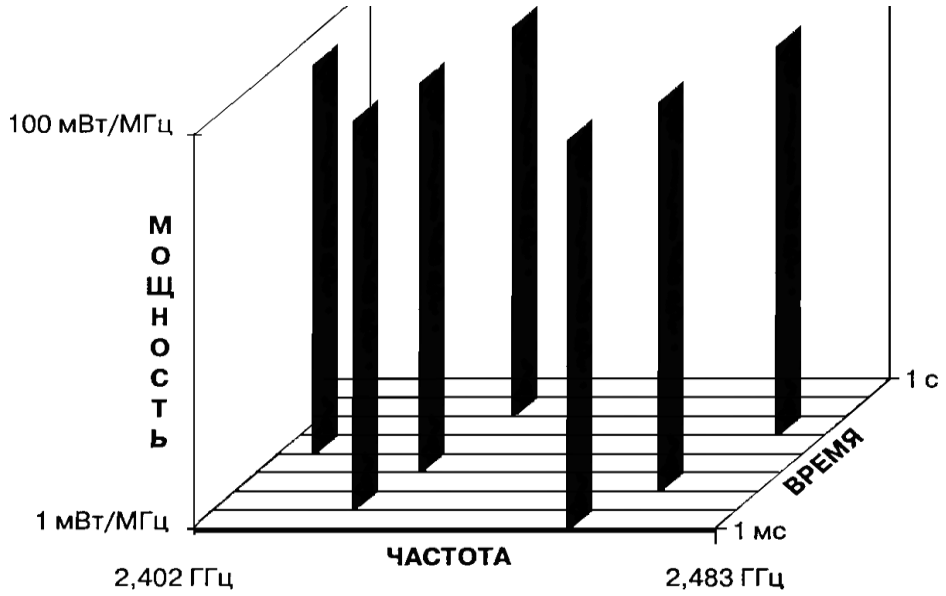


Рис. 11. Пример скачкообразной перестройки частоты

Последовательность перестройки частоты имеет следующие параметры: частота перескоков не менее 2,5 раз в секунду, как минимум между 6-ю каналами. Чтобы избежать коллизий между перекрывающимися зонами покрытия, возможные последовательности перескоков разбиты на три набора последовательностей, длина которых для северной Америки и большей части Европы равна 26. В таблице 4.1 представлены схемы скачкообразной перестройки частоты, обеспечивающие минимальные перекрытия.

Таблица 1. Схемы скачкообразной перестройки частоты

Набор частот	Схема скачкообразной перестройки частоты
1	0,3,6,9,12,15,18,21,24,27,30,33, 6,39,42,45,48,51,54,57,60,63,66,69,72,75
2	1,4,7,10,13,16,19,22,25,28,31,34,37,40,43,46,49,52,55,58,61,64,67,70,7376
3	2,5,8,11,14,17,20,23,26,29,32,35,38,41,44,47,50,53,56,59,62,65,68,71,72,77

После того как уровень MAC пропускает MAC – фрейм, который в локальных беспроводных сетях имеет название PSDU (сокращение от PLCP service data unit), подуровень PLCP добавляет два поля в начало фрейма, чтобы сформировать таким образом фрейм PPDU (элемент данных протокола PLCP). Но рис. 12 представлен формат фрейма FHSS подуровня PLCP.

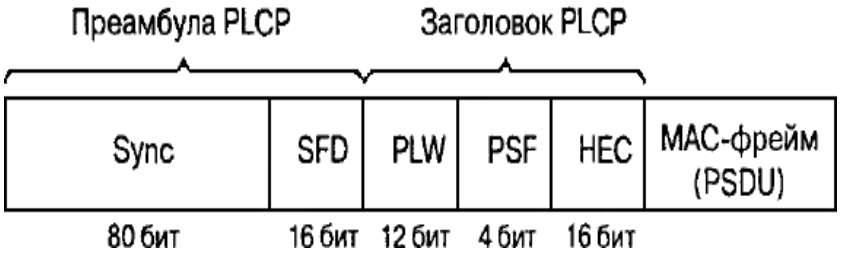


Рис. 12. Формат фрейма FHSS подуровня PLCP

Преамбула PLCP состоит из двух подполей. Подполе Sync размером 80 бит. Строка, состоящая из чередующихся 0 и 1, начинается с нуля. Приемная станция использует это поле, чтобы принять решение о выборе антенны при наличии такой возможности, откорректировать уход частоты (frequency offset) и синхронизировать распределение пакетов (packet timing). Подполе флага начала фрейма (start of frame delimiter, SFD) размером 16 бит. Состоит из специфической строки (0000 1100 1011 1101, крайний слева бит первый), применяется для синхронизации фреймов в приемной станции.

Заголовок фрейма PLCP состоит из трех подполей. PSDU Length Word (PLW)

- слово длины служебного элемента данных PLCP (PSDU), указывает размер фрейма MAC в октетах. Сигнальное поле PLCP (signaling field PLCP, PSF) размером 4 бита. Указывает скорость передачи данных конкретного фрейма.

Подуровень PLCP преобразует фрейм в поток битов и передает его на подуровень PMD. Подуровень PMD технологии FHSS модулирует поток данных с использованием модуляции, основанной на гауссовом переключении частот (Gaussian frequency shift keying, GFSK). Для скорости 1 Мбит/с модулятор использует для передачи 0 и 1, два различных по частоте сигнала рис 4.13.

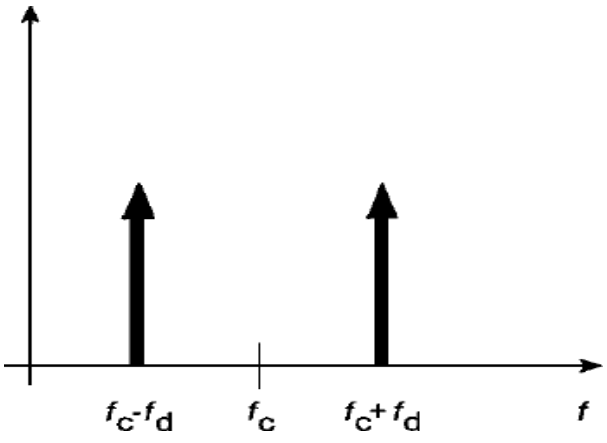


Рис. 13. Модуляция GFSK

Чтобы осуществлять передачу со скоростью 2 Мбит/с используется модуляция 4GFSK, в этом случае 2 бита модулируют сигнал одновременно. Для реализации этого метода требуется четыре различные частоты, в таблице 4.2 представлена карта преобразования символов в частоту.

Таблица 2. Карта преобразования символов в частоту при модуляции 4GFSK

Символ	Частота
01	$f_c + f_{d1}$
11	$f_c + f_{d2}$
01	$f_c - f_{d1}$
00	$f_c - f_{d2}$

Основные недостатки рассматриваемого метода:

- не высокая скорость передачи (максимум 2 Мбит/с);
- нет стандартизированных механизмов которые бы позволял исключать те частотные каналы, на которых помехи особенно ощутимы;
- Нет механизма синхронизации или координации последовательностей переключения частоты для соседствующих точек доступа.

В следствии чего последовательности переключений соседних точек доступа могут перекрываются.

Беспроводные локальные сети, использующие широкополосную модуляцию DSSS с расширением спектра методом прямой последовательности

Как было указано в стандарте 802.11 разработки 1997 года, технология DSSS поддерживает скорости передачи 1 и 2 Мбит/с. Беспроводные локальные сети DSSS используют каналы шириной 22 МГц. Каналы шириной 22 МГц позволяют создать в диапазоне 2,4—2,483 ГГц три не перекрывающихся канала передачи. Аналогично подуровню PLCP, используемому в технологии FHSS, подуровень PLCP технологии DSSS стандарта

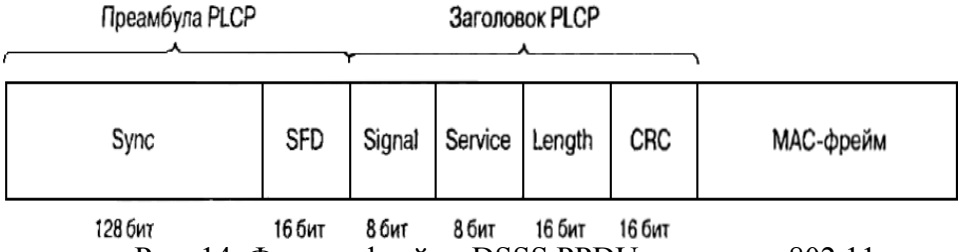


Рис. 14. Формат фрейма DSSS PPDU стандарта 802.11

802.11 добавляет два поля во фрейм MAC, чтобы сформировать PPDU: преамбулу

PLCP и заголовок PLCP. Формат фрейма представлен на рис. 14.

Преамбула PLCP состоит из двух подполей. Подполе Sync шириной 128 бит, представляющее собой строку, состоящую из единиц. Задача этого поля – обеспечить синхронизацию для приемной станции. Подполе SFD шириной 16 бит, содержит специфическую строку 0xF3A0; обеспечивает тайминг для приемной станции

Заголовок PLCP состоит из четырех подполей. Подполе Signal шириной 8 бит, указывает тип модуляции и скорость передачи данного фрейма. Подполе Service шириной 8 бит, зарезервировано. Подполе Length шириной 16 бит, указывает количество микросекунд (из диапазона 16 – 2^{16}-1), необходимое для передачи части MAC фрейма

Подуровень PLCP преобразует фрейм в поток битов и передает данные на подуровень PMD. Весь PPDU проходит через процесс скремблирования с целью рандомизации данных.

Скремблированная преамбула PLCP всегда передается со скоростью 1 Мбит/с, в то время как скремблированный фрейм MPDU передается со скоростью, указанной в подполе Signal. Подуровень PMD модулирует отделенный поток битов, используя следующие методы модуляции.

Двоичная относительная фазовая манипуляция (differential binary phase shift keying, DBPSK) для скорости передачи 1 Мбит/с

- Квадратурная фазовая манипуляция (quadrature phase shift key, QPSK) для скорости передачи 2 Мбит/с

Технологии расширения спектра

При методе **DSSS** каждый информационный символ представляется 11- разрядным кодом Баркера вида 11100010010. Коды Баркера обладают наилучшими среди известных псевдослучайных последовательностей свойствами шумоподобности, что и обусловило их применение в аппаратуре беспроводных сетей. Для передачи единичного и нулевого символов сообщения используются инверсная и прямая последовательности соответственно.

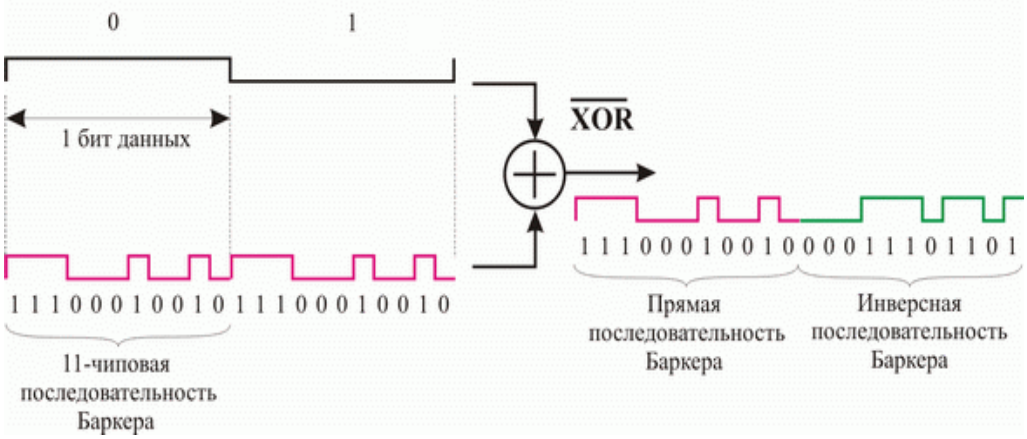


Рис. 15 Расширение спектра по технологии DSSS

Для модуляции несущего колебания в этом случае используются уже не исходные символы сообщения, а прямые или инверсные последовательности Баркера. При использовании **DSSS** происходит "размазывание" мощности сигнала в полосе частот, в 11 раз превышающей полосу исходного узкополосного сигнала. Здесь следует упомянуть о довольно часто встречающемся в литературе тезисе о том, что при переходе к технологии **DSSS** возможна работа на пониженных мощностях передатчика. Это верно только в том смысле, что снижается спектральная плотность мощности излучаемого игналапри неизменной излучаемой передатчиком мощности.

В приемнике полученный сигнал снова складывается по модулю два с кодом Баркера, в результате он становится узкополосным, поэтому его фильтруют в узкой полосе частот, равной удвоенной скорости передачи. Любая помеха, попадающая в полосу исходного широкополосного сигнала, после умножения на код Баркера, наоборот, становится широкополосной, поэтому в узкую информационную полосу попадает лишь часть помехи, примерно в 11 раз меньшая по мощности помехи, действующей на входе приемника. Главной проблемой, возникающей при решении этой задачи, является обеспечение синхронизации приемника по передаваемому сигналу. На уровне физического канала необходимо обеспечить синхронизацию по фазе несущего колебания, тактовой частоте кода Баркера и тактовой частоте сообщения. Для решения этой задачи передатчик не реже, чем один раз за 100 мс передает специальный синхросигнал.

Применение технологии DSSS позволяет также эффективно бороться с интерференционной помехой, возникающей в результате отражения сигнала от стен и местных предметов, что особенно актуально для закрытых помещений.

Двоичная относительная фазовая манипуляция (DBPSK)

Данный вид модуляции используется для передачи информации со скорость 1 Мбит/с. Для модуляции синусоидального несущего сигнала используется относительная двоичная фазовая модуляция (Differential Binary Phase Shift Key, DBPSK). При этом кодирование информации происходит за счет сдвига фазы синусоидального сигнала по отношению к предыдущему состоянию сигнала. Двоичная фазовая модуляция предусматривает два возможных значения сдвига фазы — 0 и π. Тогда логический нуль может передаваться синфазным сигналом (сдвиг по фазе равен 0), а единица — сигналом, который сдвинут по фазе на π. Квадратурная фазовая манипуляция (QPSK)

Для передачи данных на скорости 2 Мбит/с используется относительная квадратурная фазовая модуляция (Differential Quadrature Phase Shiftey). При относительной квадратурной фазовой модуляции сдвиг фаз может принимать четыре различных значения: 0, π/2, π и 3π/2. Используя четыре различных состояния сигнала, можно в одном дискретном состоянии

закодировать последовательность двух информационных бит (дибит) и тем самым в два раза повысить информационную скорость передачи. Дибиту 00 соответствует сдвиг фазы, равный 0; дибиту 01 — сдвиг фазы, равный π/2; дибиту 11 — сдвиг фазы, равный π; дибиту 10 — сдвиг фазы, равный 3π/2.

В заключение рассмотрения физического уровня протокола 802.11 отметим, что при информационной скорости 2 Мбит/с скорость следования отдельных чипов последовательности Баркера остается прежней, то есть 11×10^6 чип/с, а следовательно, не меняется и ширина спектра передаваемого сигнала.

Главным недостатком технологий DSSS и FHSS является низкая скорость передачи. На сегодняшний день технологии являются устаревшими и не используются.

Физический уровень сетей стандарта 802.11b

Появившийся в 1999 году стандарт 802.11b регламентировал правила использования высокоскоростной технологии HR – DSSS, обеспечивающей скорость передачи 5,5 Мбит/с и 11 Мбит/с. Для достижения таких скоростей применялось кодирование с использованием комплементарных кодов (complementary code keying, CCK) или технологии двоичного пакетного сверточного кодирования (packet binary convolution coding, PBCC). В технологии HR-DSSS использовалась та же схема организации каналов что и DSSS – полоса канала 22 МГц, 11 каналов, 3 не перекрывающихся, ISM диапазон 2,4 ГГц.

Подуровень PLCP технологии HR-DSSS стандарта 802.11b

Подуровень PLCP технологии HR-DSSS использует фреймы PPDU двух типов: длинный и короткий. Преамбула и заголовок длинного фрейма всегда передаются со скоростью 1 Мбит/с, для обеспечения обратной совместимости с технологией DSSS. Длинный фрейм HR-DSSS почти такой же как в DSSS но с небольшими отличиями, направленными на повышения скорости передачи:

В подполе Signal могут быть указаны дополнительные скорости передачи данных (0x37 – 5,5 Мбит/с; 0x6E – 11 Мбит/с)

Подполе Service определяет ранее зарезервированные биты (Таблица 43)

Подполе Length по прежнему указывает время в микросекундах, необходимое для передачи PSDU

Таблица 3. Определение битов подполя Service

Бит	Наименование	З ачение

B2	Генераторы синхронизированы (locked clocks)	0 = не сенхранизированы, 1 = задающие генераторы частоты и символов синхронизированы
B3	Выбор модуляции (modulation selection)	0 = CCK; 1 = PBCC
B7	Увеличение длины	Используется подполем длины

Короткий фрейм PLCP PPDU обеспечивает средство для минимизации числа служебных сигналов, все еще позволяющих, передатчику и приемнику связаться с друг другом надлежащим образом. Короткий фрейм показан на рисунке 5.7. Он использует те же заголовок, преамбулу и формат PSDU, но заголовок PLCP передается на скорости 2 Мбит/с, в то время как PSDU передается со скоростью 2; 5,5; 11 Мбит/с. Кроме того его подполя модифицированы следующим образом. Ширина поля Sync сокращена со 128 до 56 битов, оно представляет собой строку состоящую из одних нулей. Поле SFD шириной 16 бит указывает на начало фрейма и на используемый заголовок (короткий или длинный)

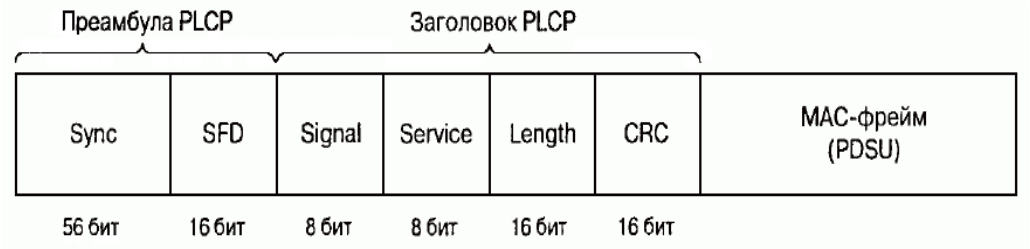


Рис. 16 Короткий PPDU технологии HR-DSSS

Модуляция ССК на подуровне PMD стандарта 802.11b

В стандарте IEEE 802.11b используются комплексные комплементарные 8- чиповые последовательности, определенные на множестве комплексных элементов

{1, –1, j, –j}. Элементы 8-чиповой CCK-последовательности могут принимать одно из следующих восьми значений: 1, –1, j, –j, 1+j, 1–j, –1+j, –1–j. Основное отличие CCK-последовательностей от рассмотренных ранее кодов Баркера заключается в том, что существует не строго заданная последовательность, посредством которой можно было кодировать либо логический нуль, либо единицу, а целый набор последовательностей. Использование CCK-кодов позволяет кодировать 8 бит на один символ при скорости 11 Мбит/с и 4 бит на символ при скорости 5,5 Мбит/с.

Для того, чтобы передавать данные со скоростью 5,5 Мбит/с, нужно сгруппировать скремблированный поток битов в символы по 4 бита (b0, b1, b2 и b3). Последние два бита (b2

и b3) используются для определения 4 последовательностей комплексных чипов, как показано в табл. 4.1, где {cl, c2, c3, c4, c5, c6, c7, c8} представляют чипы последовательности.

Таблица 4. Последовательность чипов CCK

b2,b3	1	2	3	4	5	6	7	8
00				1			1	
01	J	1	j				j	
10	j		j	1	**j**			
11		1			i			

Теперь, имея последовательность чипов, определенную битами (b2, b3), можно использовать первые два бита (b0, b1) для определения поворота фазы, осуществляемого при модуляции по методу DQPSK, который будет применен к последовательности.

Определенное битами вращение фазы применяется по отношению к 8 комплексным чипам символа, затем осуществляется модуляция на подходящей несущей частоте.

Следует иметь ввиду, что речь идет об использовании DQPSK, а не QPSK, и поэтому представленные в таблице изменения фазы отсчитываются по отношению к предыдущему символу или, в случае первого символа PSDU, по отношению к последнему символу предыдущего DQPSK символа.

Для того чтобы передавать данные на скорости 11 Мбит/с, скремблированная последовательность битов разбивается на группы по 8 бит. Последние 6 битов выбирают одну последовательность, состоящую из 8 комплексных чипов из числа 64 возможных последовательностей, первые биты так же как и для скорости 5,5 Мбит/с определяют изменение фазы символов.

Двоичное пакетное сверточное кодирование PBCC

Идея сверточного кодирования заключается в следующем. Входящая последовательность информационных бит преобразуется в специальном сверточном кодере таким образом, чтобы каждому входному биту соответствовало более одного выходного. То есть сверточный кодер добавляет определенную избыточную информацию к исходной последовательности. Если, к примеру, каждому входному биту соответствует два выходных, то говорят о сверточном кодировании со скоростью r = 1/2.

Любой сверточный кодер строится на основе нескольких последовательно связанных

запоминающих ячеек и логических элементов, связывающих эти ячейки между собой. Количество запоминающих ячеек определяет количество возможных состояний кодера. Если, к примеру, в сверточном кодере используется шесть запоминающих ячеек, то в кодере хранится информация о шести предыдущих состояниях сигнала, а с учетом значения входящего бита получим, что в таком кодере используется семь бит входной последовательности. Такой сверточный кодер называется кодером на семь состояний (K = 7).

Выходные биты, формируемые в сверточном кодере, определяются значениями входного бита и битами, хранимыми в запоминающих ячейках, то есть значение каждого формируемого выходного бита зависит не только от входящего информационного бита, но и от нескольких предыдущих битов.

В технологии PBCC используются сверточные кодеры на семь состояний (K =

7) со скоростью r=1/2. Главным достоинством сверточных кодеров является помехоустойчивость формируемой ими последовательности. Дело в том, что при избыточности кодирования даже в случае возникновения ошибок приема исходная последовательность бит может быть безошибочно восстановлена. Для восстановления исходной последовательности битов на стороне приемника применяется декодер Витерби.

Дибит, формируемый в сверточном кодере, используется в дальнейшем в качестве передаваемого символа, но предварительно этот дибит подвергается фазовой модуляции. Причем в зависимости от скорости передачи возможна двоичная, квадратурная или даже восьмипозиционная фазовая модуляция.

Метод пакетного сверточного кодирования опционально предусмотрен как альтернативный метод кодирования в протоколе 802.11b на скоростях передачи 5,5 и 11 Мбит/с. Кроме того, именно данный режим кодирования лег в основу протокола 802.11b+ — расширения протокола 802.11b. Собственно, протокола 802.11b+ как такового официально не существует, однако данное расширение поддержано многими производителями беспроводных устройств. В протоколе 802.11b+ предусматривается еще одна скорость передачи данных — 22 Мбит/с с использованием технологии PBCC.

При скорости передачи 5,5 Мбит/с для модуляции дибита, формируемого сверточным кодером, используется двоичная фазовая модуляция, а при скорости 11 Мбит/с — квадратурная фазовая модуляция. При этом для скорости 11 Мбит/с в каждом символе кодируется по одному входному биту и скорость передачи бит соответствует скорости передачи символов, а при скорости 5,5 Мбит/с скорость передачи битов равна половине скорости передачи символов (поскольку каждому входному биту в данном случае соответствует два выходных символа). Поэтому и для скорости 5,5 Мбит/с, и для скорости 11 Мбит/с символьная скорость составляет 11×10^6 символов в секунду.

Для скорости 22 Мбит/с по сравнению с уже рассмотренной нами схемой PBCC передача данных имеет две особенности. Прежде всего, используется 8- позиционная фазовая модуляция (8-PSK), то есть фаза сигнала может принимать восемь различных значений, что позволяет в одном символе кодировать уже 3 бита. Кроме того, в схему кроме сверточного кодера добавлен пунктурный кодер (Puncture). Смысл такого решения довольно прост: избыточность сверточного кодера, равная 2 (на каждый входной бит приходится два выходных), достаточно высока и при определенных условиях помеховой обстановки является излишней, поэтому можно уменьшить избыточность, чтобы, к примеру, каждым двум входным битам соответствовало три выходных.

Для этого можно, конечно, разработать соответствующий сверточный кодер, но лучше добавить в схему специальный пунктурный кодер, который будет просто уничтожать лишние биты.

Допустим, что пунктурный кодер удаляет один бит из каждых четырех входных битов. Тогда каждым четырем входящим битам будет соответствовать тривыходящих. Скорость такого кодера составляет 4/3.

Если же такой кодер используется в паре со сверточным кодером со скоростью 1/2, то общая скорость кодирования составит уже 2/3, то есть каждым двум входным битам будет соответствовать три выходных.

Таблица 6. Соотношение между скоростями передачи и типом кодирования в стандарте 802.11b

Скорость передачи, Мбит/с		Метод кодирования	Модуляция	Скорость сверточного кодирования	Символьная скорость, 106 символ/с	Коли-чество бит
1	(обязательно)	Код Баркера	DBPSK	-	1	1
2	(обязательно)	Код Баркера	DQPSK	-	1	2
5, 5	(обязательно)	CCK	DQPSK	-	1,375	2
	(опционально)	PBCC	DBPSK	1/2	11	0,5
	(обязательно)	CCK	DQPSK	-	1,375	8

11	(опционально)	PBCC	DQPSK	1/2	11	1

Физический уровень стандарта 802.11g

Стандарт IEEE 802.11g является логическим продолжением стандарта 802.11b и предполагает передачу данных в том же частотном диапазоне, но с более высокими скоростями. Кроме того, стандарт 802.11g полностью совместим с 802.11b, то есть любое устройство 802.11g должно поддерживать работу с устройствами 802.11b. Максимальная скорость передачи в стандарте 802.11g составляет 54 Мбит/с. При разработке стандарта 802.11g рассматривались несколько конкурирующих технологий: метод ортогонального частотного разделения OFDM, предложенный к рассмотрению компанией Intersil, и метод двоичного пакетного сверточного кодирования PBCC, опционально реализованный в стандарте 802.11b и предложенный компанией Texas Instruments. В результате стандарт 802.11g основан на компромиссном решении: в качестве базовых применяются технологии OFDM и CCK, а опционально предусмотрено использование технологии PBCC.

Ортогональное частотное разделение каналов с мультиплексированием Распространение сигналов в открытой среде, коей является радиоэфир, сопровождается возникновением различного рода помех. Классический пример такого рода помех — эффект многолучевой интерференции сигналов, заключающийся в том, что в результате многократных отражений сигала от естественных преград один и тот же сигнал может попадать в приемник различными путями. Но подобные пути распространения имеют и разные длины, а потому для различных путей распространения ослабление сигнала будет неодинаковым. Следовательно, в точке приема результирующий сигнал представляет собой суперпозицию (интерференцию) многих сигналов, имеющих различные амплитуды и смещенных друг относительно друга по времени, что эквивалентно сложению сигналов с разными фазами.

Следствием многолучевой интерференции является искажение принимаемого сигнала. Многолучевая интерференция присуща любому типу сигналов, в результате интерференции определенные частоты складываются синфазно, что приводит к увеличению сигнала, а некоторые, наоборот, — противофазно, вызывая ослабление сигнала на данной частоте.

Говоря о многолучевой интерференции, возникающей при передаче сигналов, различают два крайних случая. В первом случае максимальная задержка между различными сигналами не превосходит времени длительности одного символа и интерференция возникает в пределах одного передаваемого символа. Во втором случае максимальная задержка между различными сигналами больше длительности одного символа, а в результате

интерференции складываются сигналы, представляющие разные символы, и возникает так называемая межсимвольная интерференция (Inter Symbol Interference, ISI).

Наиболее отрицательно на искажение сигнала влияет межсимвольная интерференция. Поскольку символ — это дискретное состояние сигнала, характеризующееся значениями частоты несущей, амплитуды и фазы, то для различных символов меняются амплитуда и фаза сигнала, поэтому восстановить исходный сигнал крайне сложно.

Чтобы частично компенсировать эффект многолучевого распространения, используются частотные эквалайзеры, однако по мере роста скорости передачи данных либо за счет увеличения символьной скорости, либо из-за усложнения схемы кодирования, эффективность использования эквалайзеров падает.

Поэтому при более высоких скоростях передачи применяется принципиально иной метод кодирования данных – ортогональное частотное разделение каналов с мультиплексированием (Orthogonal Frequency Division Multiplexing, OFDM). Идея данного метода заключается в том, что поток передаваемых данных распределяется по множеству частотных подканалов и передача ведется параллельно на всех этих подканалах. При этом высокая скорость передачи достигается именно за счет одновременной передачи данных по всем каналам, а скорость передачи в отдельном подканале может быть и невысокой. Поскольку в каждом из частотных подканалов скорость передачи данных можно сделать не слишком высокой, это создает предпосылки для эффективного подавления межсимвольной интерференции.

При частотном разделении каналов необходимо, чтобы ширина отдельного канала была, с одной стороны, достаточно узкой для минимизации искажения сигнала в пределах отдельного канала, а с другой — достаточно широкой для обеспечения требуемой скорости передачи. Кроме того, для экономного использования всей полосы канала, разделяемого на подканалы, желательно как можно более плотно расположить частотные подканалы, но при этом избежать межканальной интерференции, чтобы обеспечить полную независимость каналов друг от друга. Частотные каналы, удовлетворяющие перечисленным требованиям, называются ортогональными. Несущие сигналы всех частотных подканалов (а точнее, функции, описывающие эти сигналы) ортогональны друг другу.

Важно, что хотя сами частотные подканалы могут частично перекрывать друг друга, ортогональность несущих сигналов гарантирует частотную независимость каналов друг от друга, а, следовательно, и отсутствие межканальной интерференции (рис. 17).

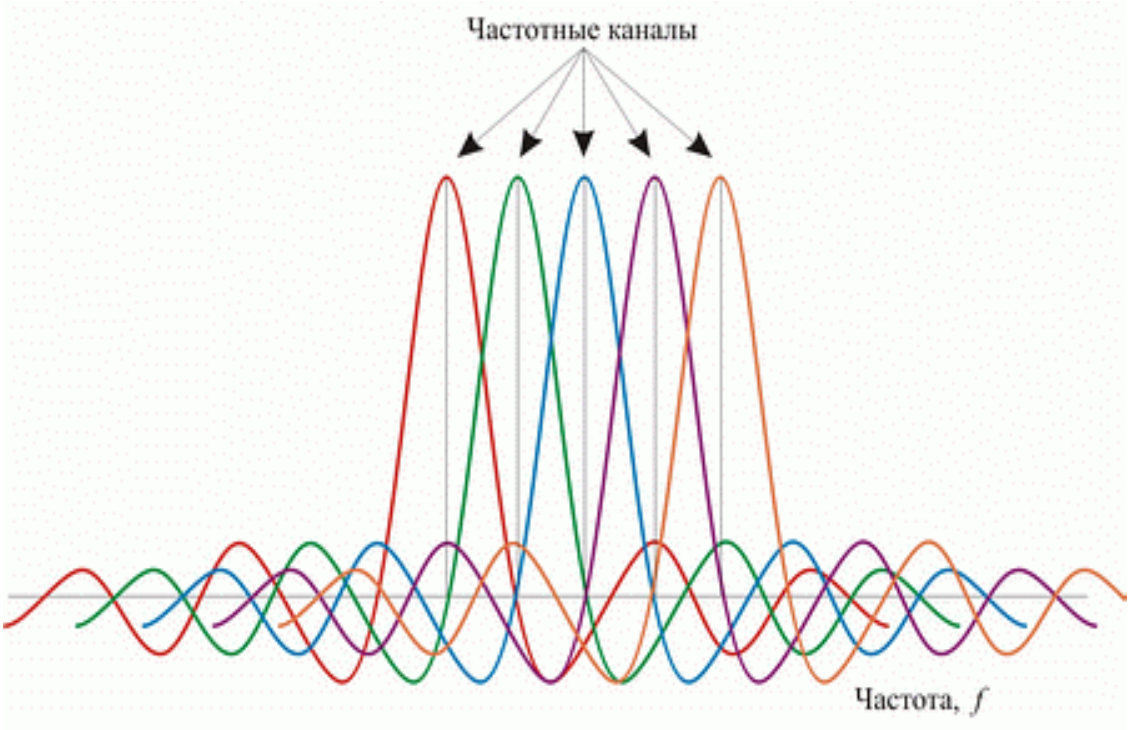


Рис. 17. Пример перекрывающихся частотных каналов с ортогональными несущими

Рассмотренный способ деления широкополосного канала на ортогональные частотные подканалы называется ортогональным частотным разделением с мультиплексированием (OFDM). Одним из ключевых преимуществ метода OFDM является сочетание высокой скорости передачи с эффективным противостоянием многолучевомураспространению. Если говорить точнее, то сама посебе технология OFDM не устраняет многолучевого распространения, но создает предпосылкидля устранения эффекта межсимвольнойинтерференции. Неотъемлемой частью технологии OFDM является охранный интервал (Guard Interval, GI) — циклическое повторение окончания символа, пристраиваемое в начале символа (рис. 18).

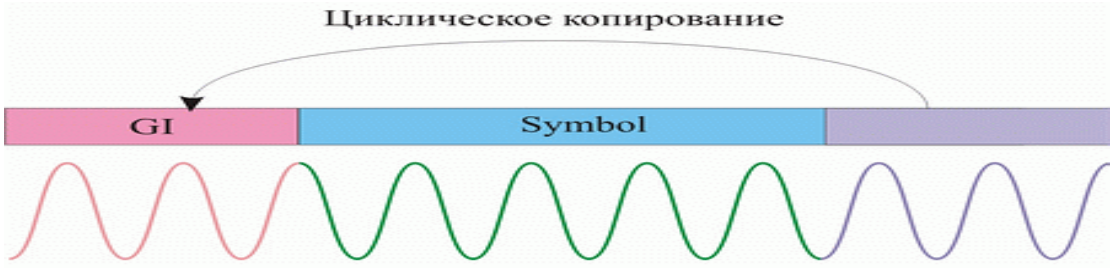


Рис. 18. Охранный интервал GI

Охранный интервал является избыточной информацией и в этом смысле снижает полезную (информационную) скорость передачи, но именно он служит защитой от возникновения межсимвольной интерференции. Эта избыточная информация добавляется к

передаваемому символу в передатчике и отбрасывается при приеме символа в приемнике.

Наличие охранного интервала создает временные паузы между отдельными символами, и если длительность охранного интервала превышает максимальное время задержки сигнала в результате многолучевого распространения, то межсимвольной интерференции не возникает (рис. 19).

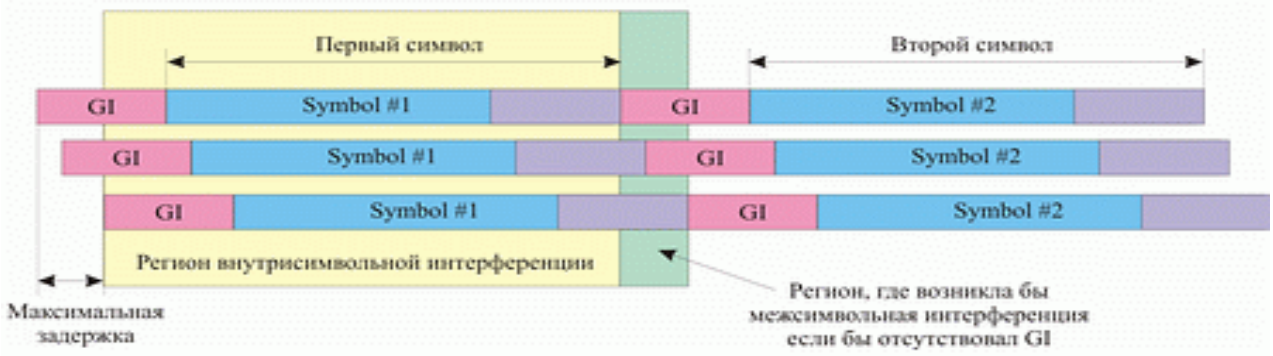


Рис. 19. Избежание межсимвольной интерференции за счет использования охранных интервалов

При использовании технологии OFDM длительность охранного интервала составляет одну четвертую длительности самого символа. При этом сам символ имеет длительность 3,2 мкс, а охранный интервал — 0,8 мкс. Таким образом, длительность символа вместе с охранным интервалом составляет 4 мкс.

Скоростные режимы и методы кодирования в протоколе 802.11g

В протоколе 802.11g предусмотрена передача на скоростях 1, 2, 5,5, 6, 9, 11,

12, 18, 22, 24, 33, 36, 48 и 54 Мбит/с. Обязательными являются скорости передачи 1;

2; 5,5; 6; 11; 12 и 24 Мбит/с, а более высокие скорости передачи (33, 36, 48 и 54 Мбит/с) — опциональными. Как уже отмечалось, протокол 802.11g включает в себя подмножество протоколы 802.11b. Технология кодирования PBCC опционально может использоваться на скоростях 5,5; 11; 22 и 33 Мбит/с. Кроме того, одна и та же скорость может реализовываться при различной технологии кодирования. Соотношение между различными скоростями передачи и используемыми методами кодирования отображено в табл. 7.

Говоря о технологии частотного ортогонального разделения каналов OFDM,

применяемой на различных скоростях в протоколе 802.11g, мы до сих пор не касались вопроса о методе модуляции несущего сигнала.

Перейдем к рассмотрению методов модуляции применяемых стандартом 802.11g.

Напомню, что в протоколе 802.11b для модуляции использовалась либо двоичная (BDPSK), либо квадратурная (QDPSK) относительная фазовая модуляция. В протоколе 802.11g на низких скоростях передачи также используется фазовая модуляция (только не относительная), то есть двоичная и квадратурная фазовые модуляции BPSK и QPSK. При использовании BPSK-модуляции в одном символе кодируется только один информационный бит, а при использовании QPSK- модуляции — два информационных бита. Модуляция BPSK используется для передачи данных на скоростях 6 и 9 Мбит/с, а модуляция QPSK — на скоростях 12 и 18 Мбит/с.

Для передачи на более высоких скоростях используется квадратурная амплитудная модуляция QAM (Quadrature Amplitude Modulation), при которой информация кодируется за счет изменения фазы и амплитуды сигнала. В протоколе 802.11g используется модуляция 16-QAM и 64-QAM. В первом случае имеется 16 различных состояний сигнала, что позволяет закодировать 4 бита в одном символе. Во втором случае имеется уже 64 возможных состояний сигнала, что позволяет закодировать последовательность 6 бит в одном символе. Модуляция 16-QAM применяется на скоростях 24 и 36 Мбит/с, а модуляция 64-QAM — на скоростях 48 и 54 Мбит/с.

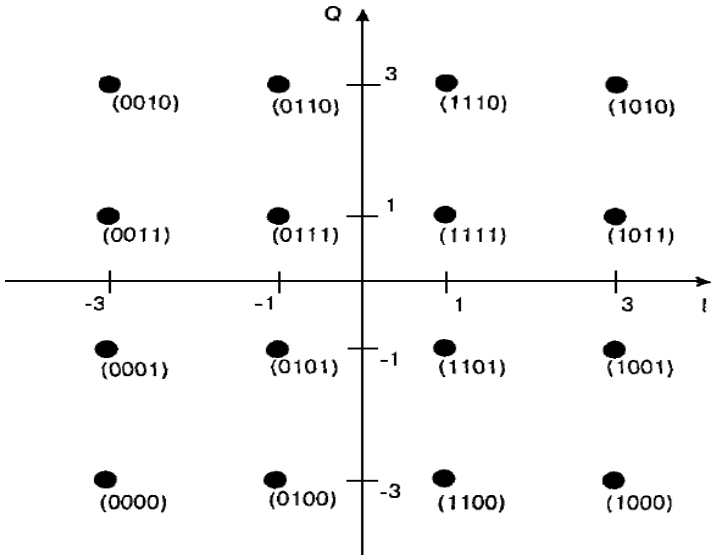


Рис. 20. Представление сигнала при QAM-16

Из таблицы 7 видно, что при одном и том же типе модуляции возможны различные скорости передачи. Рассмотрим как они получаются на примере модуляции BPSK, при которой скорость передачи данных составляет 6 или 9 Мбит/с. При использовании технологии OFDM используется сверточное кодирование с различными пунктурными кодерами, что приводит к различной скорости сверточного кодирования. В результате при

использовании одного и того же типа модуляции могут получаться разные значения информационной скорости

— все зависит от скорости сверточного кодирования. Так, при использовании BPSK-модуляции со скоростью сверточного кодирования 1/2 получаем информационную скорость 6 Мбит/с, а при использовании сверточного кодирования со скоростью 3/4 — 9 Мбит/с.

Таблица 7. Соотношение между скоростями передачи и типом кодирования в стандарте 802.11g

Скорость передачи (Мбит/с)		Метод кодирования	Модуляция
1	(опционально)	Код Баркера	DBPSK
2	(опциональн)	Код Баркера	DQPSK
5.5	(обязательно)	CCK	DQPSK
	(опционально)	PBCC	DBPSK
6	(обязательно)	OFDM	BPSK
	(опционально)	CCK-OFDM	BPSK
9	(опционально)	OFDM, CCK-OFDM	BPSK
11	(обязательно)	CCK	DQPSK
	(опционально)	PBCC	DQPSK
12	(обязательно)	OFDM	QPSK
	(опционально)	CCK-OFDM	QPSK
18	(обязательно)	OFDM, CCK-OFDM	QPSK
22	(опционально)	PBCC	DQPSK
24	(обязательно)	OFDM	16-QAM
	(опционально)	CCK-OFDM	
33	(опционально)	PBCC	
36	(опционально)	OFDM, CCK-OFDM	16-QAM
48	(опционально)	OFDM, CCK-OFDM	16 QAM
54	(опционально)	OFDM, CCK-OFDM	16-QAM

Стандарт также предусматривает применение гибридного кодирования. Для того чтобы понять сущность этого термина, вспомним, что любой передаваемый пакет данных

содержит заголовок/преамбулу со служебный информацией и поле данных. Когда речь идет о пакете в формате CCK, имеется в виду, что заголовок и данные кадра передаются в формате CCK. Аналогично при использовании технологии OFDM заголовок кадра и данные передаются посредством OFDM- кодирования. При применении технологии CCK-OFDM заголовок кадра кодируется с помощью CCK-кодов, но сами данные кадра передаются посредством многочастотного OFDM-кодирования. Таким образом, технология CCK-OFDM является своеобразным гибридом CCK и OFDM. Технология CCK-OFDM — не единственная гибридная технология: при использовании пакетного кодирования PBCC заголовок кадра передается с помощью CCK-кодов и только данные кадра кодируются посредством PBCC.

Безопасность беспроводных LAN

Так как беспроводные сети используют в качестве среды передачи радиоэфир они больше остальных подвержены опасности, любой желающий может получить доступ к информации передаваемой по радиоканалу. Единственным вариантом обеспечения конфиденциальности и целостности информации является применение стойких алгоритмов шифрования и надежных методов аутентификации. В первых редакциях стандарта защите, на мой взгляд, было уделено не достаточно внимания, отсутствовала возможность идентификации пользователя, применялся не стойкий алгоритм шифрования WEP. Однако с тех пор многое изменилось, и по мере повышения пропускной способности и надежности беспроводных сетей совершенствовались и стандарты обеспечения их безопасности. WPA и WPA2 — новейшие протоколы обеспечения безопасности беспроводных сетей, разработанные на основе стандарта IEEE 802.11i, — помогают надежно защитить трафик в беспроводных сетях даже в ситуациях, предъявляющих повышенные требования к безопасности. При правильной настройке системы с поддержкой этих стандартов защищены гораздо надежнее, чем прежние решения, и их можно смело использовать в корпоративных системах среднего размера.

В таблице приведены основные подходы к обеспечению безопасности беспроводных сетей.

Таблица 8. Сравнение подходов к обеспечению безопасности беспроводных сетей

Характеистики	**WPA**	**WPA2**	**WEP**	**VPN**	**IPsec**
Строгая проверка подлинности	Да	Да	нет	Да[1]	Да[2]
Надежное шифрование данных	Да	Да	нет	Да	Да
Прозрачное подключение и восстановление подключения	Да	Да	Да	нет	Нет
Проверка подлинности пользователей	Да	Да	нет	Да	нет
Проверка подлинности компьютеров	Да	Да	Да	Нет	Да
Защита трафика при широковещательной и многоадресной передаче	Да	Да	Да	Да	нет
Потребность в дополнительных сетевых устройствах	Да[3]	Да[3]	Нет	Да[4]	Нет
Защита доступа к беспроводной сети помимо доступа к пакетам	Да	Да	Да	Нет	Нет

1 - если не используется проверка подлинности с помощью общих ключей

2 - если используется проверка подлинности с помощью сертификатов или по протоколу Kerberos

3 - требуются серверы RADIUS

4 - требуются системы VPN и серверы RADIUS

Рассмотрим более подробно каждый из подходов к обеспечению безопасности.

Алгоритм шифрования WEP

Первая Спецификация стандарта 802.11 предусматривает обеспечение защиты данных с использованием алгоритма WEP (Wired Equivalent Protection). Этот алгоритм основан на применении симметричного поточного шифра RC4. Симметричность RC4 означает, что согласованные WEP-ключи размером 40 или 104 бит статично конфигурируются на клиентских устройствах и в точках доступа. Производители оборудования предлагают два способа конфигурирования ключей, ведение в поле «key» n-битного HEX числа или более удобный с точки зрения пользователя способ, введение некоторой последовательности ASCII

символов которая в дальнейшем трансформируется в ключ. Алгоритм WEP был выбран главным образом потому, что он не требует объемных вычислений. WEP — простой в применении алгоритм, для записи которого в некоторых случаях достаточно 30 строк кода. Малые непроизводительные расходы, возникающие при применении этого алгоритма, делают его идеальным алгоритмом шифрования для специализированных устройств.

Чтобы избежать шифрования в режиме ECB (Electronic Code Book – при использовании этого режима один и тот же открытый текст после шифрования преобразуется в один и тот же зашифрованный текст). Этот фактор потенциально представляет собой угрозу для безопасности, поскольку злоумышленники могут получать образцы зашифрованного текста и выдвигать какие-то предположения об исходном тексте), WEP использует 24-разрядный вектор инициализации, который добавляется к ключу перед выполнением обработки по алгоритму RC4. Вектор инициализации должен изменяться пофреймово во избежание коллизий. Коллизии такого рода происходят, когда используются один и тот же вектор инициализации и один и тот же WEP-ключ, в результате чего для шифрования фрейма используется один и тот же ключевой поток. Такая коллизия предоставляет злоумышленникам большие возможности по разгадыванию данных открытого текста путем сопоставления подобных элементов. При использовании вектора инициализации важно предотвратить подобный сценарий, поэтому вектор инициализации часто меняют. Большинство производителей предлагают пофреймовые векторы инициализации в своих устройствах для беспроводных LAN. На рисунке 4.21 показан фрейм зашифрованный с использованием алгоритма WEP.

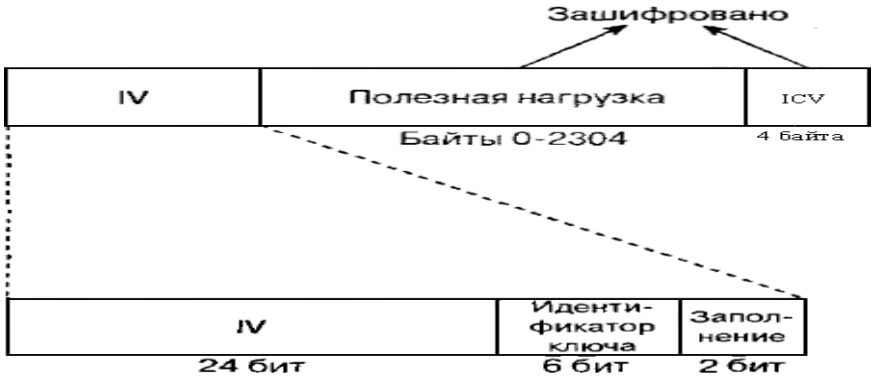


Рис. 21. Фрейм, зашифрованный алгоритмом WEP

Спецификация стандарта 802.11 требует, чтобы одинаковые WEP-ключи были сконфигурированы как на клиентах, так и на устройствах, образующих инфраструк- туру сети. Можно определять до четырех ключей на одно устройство, но одновре- менно для шифрования отправляемых фреймов используется только один из них.WEP-шифрование используется только по отношению к фреймам данных и во время процедуры аутентификации с совместно используемым ключом. По алгоритму WEP шифруются

следующие поля фрейма данных стандарта 802.11. Данные или полезная нагрузка (payload).

Контрольный признак целостности (integrity check value, ICV).

Значения всех остальных полей передаются без шифрования. Вектор инициализации должен быть послан незашифрованным внутри фрейма, чтобы приемная станция могла получить его и использовать для корректнойрасшифровки полезной нагрузки и ICV. На рис. 22 схематично представлен процесс шифрования.

В дополнение к шифрованию данных спецификация стандарта 802.11 предлагает использовать 32-разрядное значение, функция которого — осуществлять контроль целостности. Этот контрольный признак целостности говорит приемнику о том, что фрейм был получен без повреждения в процессе передачи. Контрольный признак целостности вычисляется по всем полям фрейма с использованием 32-разрядной полиномиальной функции контроля и с помощью циклического избыточного кода (CRC-32). Станция отправитель вычисляет это значение и помещает его в поле ICV, приемная сторона расшифровывает фрейм вычисляет значение ICV и сравнивает его со значением в поле ICV. Если значения совпадают считается что фрейм не поддельный, в противном случае фрейм отбрасывается. На рис. 22 и 23 показан процесс дешифрования фреймов и вычисления контрольного признака целостности.

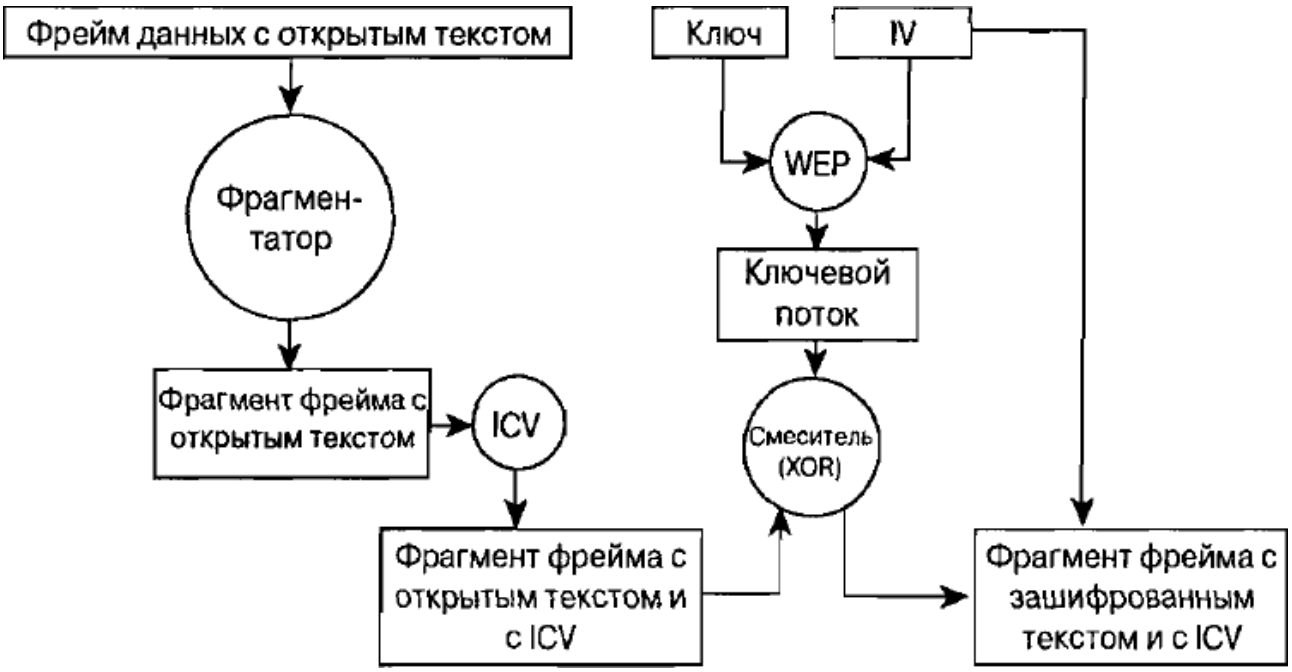


Рис. 22. Шифрование по алгоритму WEP

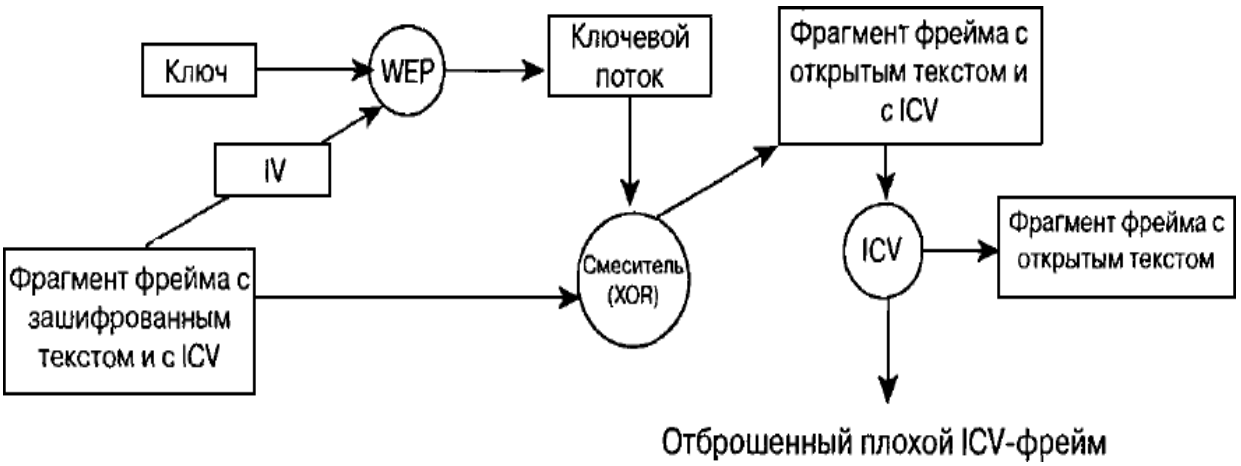


Рис. 23. Дешифрование по алгоритму WEP

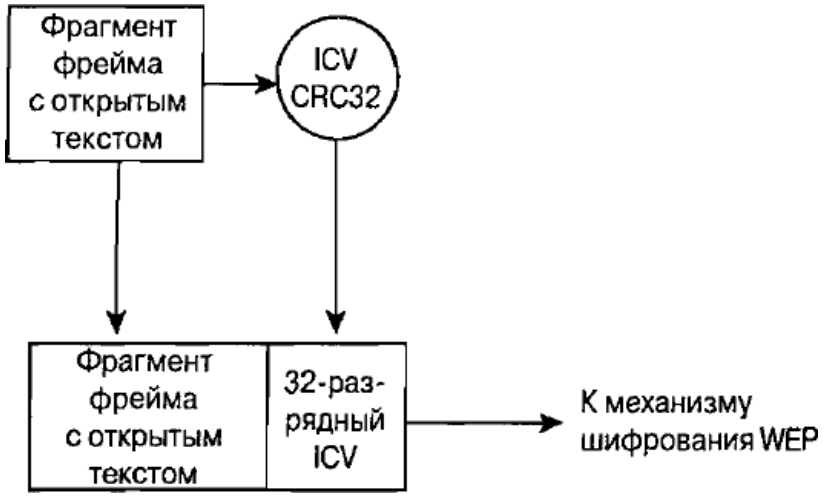


Рис. 24. Диаграмма функционирования механизма ICV

Механизмы аутентификации стандарта 802.11

Спецификация стандарта 802.11 оговаривает два механизма, которые могут применяться для аутентификации клиентов WLAN.

- Открытая аутентификация (open authentication).
- Аутентификация с совместно используемым ключом (shared key authentication).

Открытая аутентификация по сути представляет собой алгоритм с нулевой аутентификацией (null authentication algorithm). Точка доступа принимает любой запрос на аутентификацию. Это может быть просто бессмысленный сигнал, используемый для указания на применение именно этого алгоритма аутентификации, тем не менее открытая аутентификация играет определенную роль в сетях стандарта 802.11. Столь простые требования к аутентификации позволяют устройствам быстро получить доступ к сети.

Контроль доступа при открытой аутентификации осуществляется с использованием заранее сконфигурированного WEP-ключа в точке доступа и на клиентской станции. Эта

станция и точка доступа должны иметь одинаковые ключи, тогда они могут связываться между собой. Если станция и точка доступа не поддерживают алгоритм WEP, в BSS невозможно обеспечить защиту. Любое устройство может подключиться к такому BSS, и все фреймы данных передаются незашифрованными.

После выполнения открытой аутентификации и завершения процесса ассоциирования клиент может начать передачу и прием данных. Если клиент сконфигурирован так, что его ключ отличается от ключа точки доступа, он не сможет правильно зашифровывать и расшифровывать фреймы, и такие фреймы будут отброшены как точкой доступа, так и клиентской станцией. Этот процесс предоставляет собой довольно-таки эффективное средство контроля доступа.

В отличие от открытой аутентификации, при аутентификации с совместно используемым ключом требуется, чтобы клиентская станция и точка доступа были способны поддерживать WEP и имели одинаковые WEP-ключи. Процесс аутентификации с совместно используемым ключом осуществляется следующим образом. Клиент посылает точке доступа запрос на аутентификацию с совместно используемым ключом. Точка доступа отвечает фреймом вызова (challenge frame), содержащим открытый текст. Клиент шифрует вызов и посылает его обратно точке доступа. Если точка доступа может правильно расшифровать этот фрейм и получить свой исходный вызов, клиенту посылается сообщение об успешной аутентификации. Клиент получает доступ WLAN.

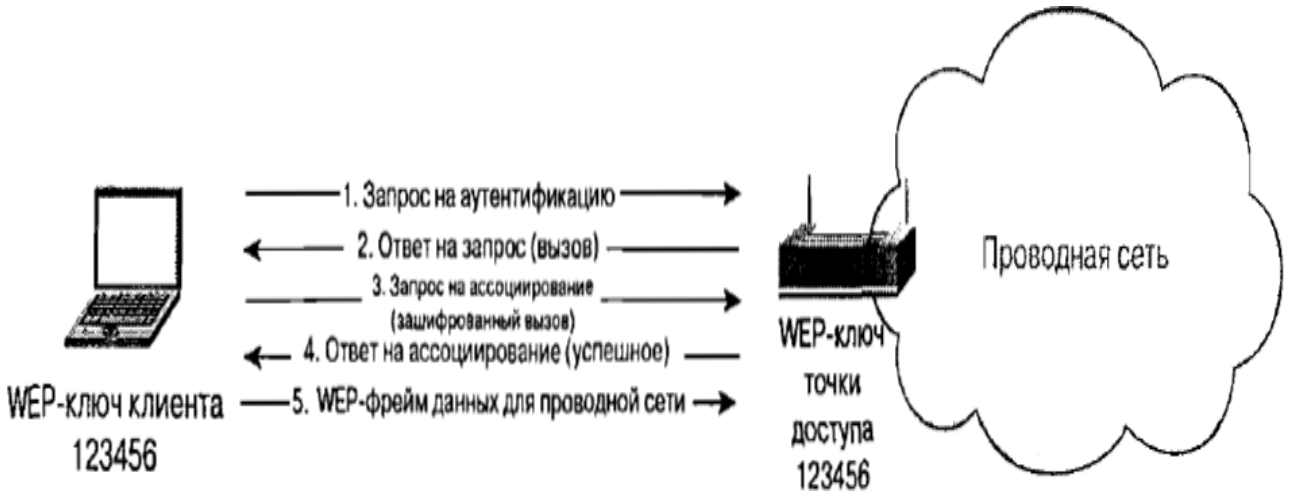


Рис. 25. Процесс аутентификации с совместно используемым ключом

Предпосылки, на которых основана аутентификация с совместно используемым ключом, точно такие же, как и те, которые предполагались при открытой ау- тентификации, использующей WEP-ключи в качестве средства контроля доступа. Разница между этими двумя схемами состоит в том, что клиент не может ассо- циировать себя с точкой доступа при использовании механизма аутентификации с совместно используемым ключом, если его ключ не сконфигурирован должным образом.

Уязвимости алгоритма WEP

Проблемы алгоритма WEP носят комплексный характер и кроются в целой серии слабых мест: механизме обмена ключами (а точнее, практически полном его отсутствии); малых разрядностях ключа и вектора инициализации (Initialization Vector - IV); механизме проверки целостности передаваемых данных; способе аутентификации и алгоритме шифрования RC4.

Процесс шифрования WEP выполняется в два этапа. Вначале подсчитывается контрольная сумма (Integrity Checksum Value - ICV) с применением алгоритма Cyclic Redundancy Check (CRC-32), добавляемая в конец незашифрованного сообщения и служащая для проверки его целостности принимаемой стороной. На втором этапе осуществляется непосредственно шифрование. Ключ для WEP- шифрования - общий секретный ключ, который должны знать устройства на обеих сторонах беспроводного канала передачи данных. Этот секретный 40-битный ключ вместе со случайным 24-битным IV является входной последовательностью для генератора псевдослучайных чисел, базирующегося на шифре Вернама для генерации строки случайных символов, называемой ключевым потоком (key stream). Данная операция выполняется с целью избежания методов взлома, основанных на статистических свойствах открытого текста.

Initialization Vector (IV) используется, чтобы обеспечить для каждого сообщения свой уникальный ключевой поток. Зашифрованное сообщение образуется в результате выполнения операции XOR над незашифрованным сообщением с ICV и ключевым потоком. Чтобы получатель мог прочитать его, в передаваемый пакет в открытом виде добавляется IV. Когда информация принимается на другой стороне, производится обратный процесс.

Таким образом, мы можем получить незашифрованный текст, являющийся результатом операции XOR между двумя другими оригинальными текстами. Процедура их извлечения не составляет большого труда. Наличие оригинального текста и IV позволяет вычислить ключ, что в дальнейшем даст возможность читать все сообщения данной беспроводной сети.

После несложного анализа можно легко рассчитать, когда повторится ключевой поток. Так как ключ постоянный, а количество вариантов IV составляет 2^{24}=16 777 216, то при достаточной загрузке точки доступа, среднем размере пакета в беспроводной сети, равном 1500 байт (12 000 бит), и средней скорости передачи данных, например 5 Mbps (при максимальной 11 Mbps), мы получим, что точкой доступа будет передаваться 416 сообщений в секунду, или же 1 497 600 сообщений в час, т. е. повторение произойдет через 11 ч 12 мин (2^{24}/1 497 600=11,2 ч). Данная проблема носит название "коллизия векторов". Существует большое количество способов, позволяющих ускорить этот процесс. Кроме того, могут

применяться атаки "с известным простым текстом", когда одному из пользователей сети посылается сообщение с заранее известным содержанием и прослушивается зашифрованный трафик. В этом случае, имея три составляющие из четырех (незашифрованный текст, вектор инициализации и зашифрованный текст), можно вычислить ключ. В работе "Intercepting Mobile Communications: The Insecurity of 802.11" было описано множество типов атак, включая довольно сложные, использующие манипуляции с сообщениями и их подмену, основанные на ненадежном методе проверки целостности сообщений (CRC-32) и аутентификации клиентов. С ICV, используемым в WEP-алгоритме, дела обстоят аналогично. Значение CRC-32 подсчитывается на основе поля данных сообщения. Это хороший метод для определения ошибок, возникающих при передаче информации, но он не обеспечивает целостность данных, т. е. не гарантирует, что они не были подменены в процессе передачи. Контрольная сумма CRC-32 имеет линейное свойство: CRC(A XOR B)=CRC(A)XOR CRC(B), предоставляющее нарушителю возможность легко модифицировать зашифрованный пакет без знания WEP-ключа и пересчитать для него новое значение ICV. Появившаяся в 2001 г. спецификация WEP2, которая увеличила длину ключа до 104 бит, не решила проблемы, так как длина вектора инициализации и способ проверки целостности данных остались прежними. Большинство типов атак реализовывались так же просто, как и раньше. На сегодняшний день использование алгоритма WEP для построение защищенных беспроводных сетей не допустимо.

VPN

Сегодня технология VPN (Virtual Private Network - виртуальная частная сеть) завоевала всеобщее признание и практически все компания организовывают VPN- каналы для сотрудников, работающих вне офиса. С помощью VPN можно организовать защищенный виртуальный канал через публичные сети. Зашита трафика основана на криптографии. Наиболее часто используемым алгоритмом кодирования является Triple DES, который обеспечивает тройное шифрование (168 разрядов) с использованием трех разных ключей. Технология включает в себя проверку целостности данных и идентификацию пользователей, задействованных в VPN. Первая гарантирует, что данные дошли до адресата именно в том виде, в каком были посланы. Самые популярные алгоритмы проверки целостности данных

- MD5 и SHA1. Далее система проверяет, не были ли изменены данные во время движения по сетям, по ошибке или злонамеренно. Таким образом, построение VPN предполагает создание защищенных от постороннего доступа туннелей между несколькими локальными сетями или удаленными пользователями. Для построения VPN необходимо иметь на обоих концах линии связи программы шифрования исходящего и дешифрования

входящего трафиков. Они могут работать как на специализированных аппаратных устройствах, так и на ПК с такими операционными системами как Windows, Linux или NetWare. Чтобы организовать надежную защиту передаваемых данных и обеспечить прозрачность для устройств находящихся между концами виртуального туннеля применяется инкапсуляция, т.е. кадр сгенерированный узлом-отправителем шифруется и снабжается дополнительным заголовком содержащим информацию о маршруте. На другом конце туннеля заголовок отбрасывается, кадр дешифруется и доставляется по указанному в нем адресу.

Для формирования туннелей VPN используются протоколы PPTP, L2TP, IPsec, IP-IP. Протокол PPTP - позволяет инкапсулировать IP-, IPX- и NetBEUI- трафик в заголовки IP для передачи по IP-сети, например Internet.

Протокол L2TP - позволяет шифровать и передавать IP-трафик с использованием любых протоколов, поддерживающих режим `точка-точка` доставки дейтаграмм. Например, к ним относятся протокол IP, ретрансляция кадров и асинхронный режим передачи (ATM). Протокол IPsec - позволяет шифровать и инкапсулировать полезную информацию протокола IP в заголовки IP для передачи по IP-сетям.

Для технической реализации VPN, кроме стандартного сетевого оборудования, понадобится шлюз VPN, выполняющий все функции по формированию туннелей, защите информации, контролю трафика, а нередко и функции централизованного управления. Рассмотренная технология является достаточно мощным средством зашиты передаваемого трафика, однако ее применение в беспроводных сетях имеет ряд недостатков. Основной из них: для реализации технологии необходим VPN шлюз, для большого числа клиентов этот участок сети может стать узким местом и снизит пропускную способность. К тому же беспроводным клиентам придется сначала проходить процедуру аутентификации на точке а затем устанавливать VPN соединение, что не совсем удобно. По этой причине рассматривать технологию VPN как вариант зашиты при проектировании беспроводной сети не стоит, технология может применятся лишь в сетях не поддерживающих современные методы зашиты данных (WPA или WPA2) как последняя возможность повышения безопасности без глобального обновления оборудования.

IPSec. Архитектура IPSec

IP Security - это комплект протоколов, касающихся вопросов шифрования, аутентификации и обеспечения защиты при транспортировке IP-пакетов; в его состав сейчас входят почти 20 предложений по стандартам и 18 RFC. Спецификация IP Security (известная сегодня как IPsec) разрабатывается рабочей группой IP Security Protocol IETF. Первоначально IPsec включал в себя 3 алгоритмо-независимые базовые спецификации,

опубликованные в качестве RFC- документов "Архитектура безопасности IP", "Аутентифицирующий заголовок (AH)", "Инкапсуляция зашифрованных данных (ESP)" (RFC1825, 1826 и 1827). Сейчас предложены новые версии этих спецификаций, это RFC2401 - RFC2412. Отмечу, что RFC1825-27 на протяжении уже нескольких лет считаются устаревшими. Кроме этого, существуют несколько алгоритмо-зависимых спецификаций, использующих протоколы MD5, SHA, DES.

Гарантии целостности и конфиденциальности данных в спецификации IPsec обеспечиваются за счет использования механизмов аутентификации и шифрования соответственно. Последние, в свою очередь, основаны на предварительном согласовании сторонами информационного обмена т.н. "контекста безопасности" – применяемых криптографических алгоритмов, алгоритмов управления ключевой информацией и их параметров. Спецификация IPsec предусматривает возможность поддержки сторонами информационного обмена различных протоколов и параметров аутентификации и шифрования пакетов данных, а также различных схем распределения ключей. При этом результатом согласования контекста безопасности является установление индекса параметров безопасности (SPI), представляющего собой указатель на определенный элемент внутренней структуры стороны информационного обмена, описывающей возможные наборы параметров безопасности.

По сути, IPSec, работает на третьем уровне, т. е. на сетевом уровне. В результате передаваемые IP-пакеты защищены прозрачным для сетевых приложений и инфраструктуры образом. В отличие от SSL (Secure Socket Layer), который работает на четвертом (т. е. транспортном) уровне и теснее связан с более высокими уровнями модели OSI, IPSec призван обеспечить низкоуровневую защиту.

К IP-данным, готовым к передаче по виртуальной частной сети, IPSec добавляет заголовок для идентификации защищенных пакетов. Перед передачей по Internet эти пакеты инкапсулируются в другие IP-пакеты. IPSec поддерживает несколько типов шифрования, в том числе Data Encryption Standard (DES) и Message Digest 5 (MD5).

Чтобы установить защищенное соединение, оба участника сеанса должны иметь возможность быстро согласовать параметры защиты, такие как алгоритмы аутентификации и ключи. IPSec поддерживает два типа схем управления ключами, с помощью которых участники могут согласовать параметры сеанса.

С текущей версией IP, IPv4, могут быть использованы или Internet Secure Association Key Management Protocol (ISAKMP), или Simple Key Management for Internet Protocol. С версией IPv6, придется использовать ISAKMP.

Заголовок AH

Аутентифицирующий заголовок (AH) является обычным опциональным заголовком и, как правило, располагается между основным заголовком пакета IP и полем данных. Наличие AH никак не влияет на процесс передачи информации транспортного и более высокого уровней. Основным и единственным назначением AH является обеспечение защиты от атак, связанных с несанкционированным изменением содержимого пакета, и в том числе от подмены исходного адреса сетевого уровня. Протоколы более высокого уровня должны быть модифицированы в целях осуществления проверки аутентичности полученных данных.

Формат AH достаточно прост и состоит из 96-битового заголовка и данных переменной длины, состоящих из 32-битовых слов. Названия полей достаточно ясно отражают их содержимое: Next Header указывает на следующий заголовок, Payload Len

представляет длину пакета, SPI является указателем на контекст безопасности и Sequence Number Field содержит последовательный номер пакета.

Рис. 26**.** Формат заголовка AH

Последовательный номер пакета был введен в AH в 1997 году в ходе процесса пересмотра спецификации IPsec. Значение этого поля формируется отправителем и служит для защиты от атак, связанных с повторным использованием данных процесса аутентификации. Поскольку сеть Интернет не гарантирует порядок доставки пакетов, получатель должен хранить информацию о максимальном последовательном номере пакета, прошедшего успешную аутентификацию, и о получении некоторого числа пакетов, содержащих предыдущие последовательные номера (обычно это число равно 64).

В отличие от алгоритмов вычисления контрольной суммы, применяемых в протоколах передачи информации по коммутируемым линиям связи или по каналам локальных сетей и ориентированных на исправление случайных ошибок среды передачи, механизмы обеспечения целостности данных в открытых телекоммуникационных сетях должны иметь средства защиты от внесения целенаправленных изменений. Одним из таких механизмов является специальное применение алгоритма MD5: в процессе формирования AH последовательно вычисляется хэш-функция от объединения самого пакета и некоторого предварительно согласованного ключа, а затем от объединения полученного результата и

преобразованного ключа.

Заголовок ESP

В случае использования инкапсуляции зашифрованных данных заголовок ESP является последним в ряду опциональных заголовков, "видимых" в пакете. Поскольку основной целью ESP является обеспечение конфиденциальности данных, разные виды информации могут требовать применения существенно различных алгоритмов шифрования. Следовательно, формат ESP может претерпевать значительные изменения в зависимости от используемых криптографических алгоритмов. Тем не менее, можно выделить следующие обязательные поля: SPI, указывающее на контекст безопасности и Sequence Number Field, содержащее последовательный номер пакета. Поле "ESP Authentication Data" (контрольная сумма), не является обязательным в заголовке ESP. Получатель пакета ESP расшифровывает ESP заголовок и использует параметры и данные применяемого алгоритма шифрования для декодирования информации транспортного уровня.

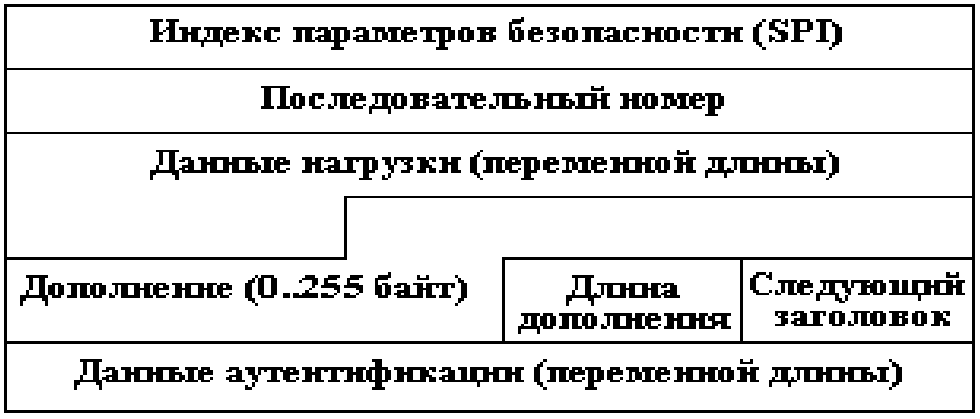


Рис. 27. Формат заголовка ESP

Различают два режима применения ESP и AH - транспортный и туннельный.

Транспортный режим

Транспортный режим используется для шифрования поля данных IP пакета, содержащего протоколы транспортного уровня (TCP, UDP, ICMP), которое, в свою очередь, содержит информацию прикладных служб. Примером применения транспортного режима является передача электронной почты. Все промежуточные узлы на маршруте пакета от отправителя к получателю используют только открытую информацию сетевого уровня и, возможно, некоторые опциональные заголовки пакета (в IPv6). Недостатком транспортного режима является отсутствие механизмов скрытия конкретных отправителя и получателя пакета, а также возможность проведения анализа трафика. Результатом такого анализа может стать информация об объемах и направлениях передачи информации, области интересов абонентов, расположение руководителей.

Туннельный режим

Туннельный режим предполагает шифрование всего пакета, включая заголовок сетевого уровня. Туннельный режим применяется в случае необходимости скрытия информационного обмена организации с внешним миром. При этом, адресные поля заголовка сетевого уровня пакета, использующего туннельный режим, заполняются межсетевым экраном организации и не содержат информации о конкретном отправителе пакета. При передаче информации из внешнего мира в локальную сеть организации в качестве адреса назначения используется сетевой адрес межсетевого экрана. После расшифровки межсетевым экраном начального заголовка сетевого уровня пакет направляется получателю.

Security Associations

Security Association (SA) – это соединение, которое предоставляет службы обеспечения безопасности трафика, который передаѐтся через него. Два компьютера на каждой стороне SA хранят режим, протокол, алгоритмы и ключи, используемые в SA. Каждый SA используется только в одном направлении. Для двунаправленной связи требуется два SA. Каждый SA реализует один режим и протокол; таким образом, если для одного пакета необходимо использовать два протокола (как например AH и ESP), то требуется два SA.

Политика безопасности

Политика безопасности хранится в SPD (База данных политики безопасности). SPD может указать для пакета данных одно из трѐх действий: отбросить пакет, не обрабатывать пакет с помощью IPSec, обработать пакет с помощью IPSec. В последнем случае SPD также указывает, какой SA необходимо использовать (если, конечно, подходящий SA уже был создан) или указывает, с какими параметрами должен быть создан новый SA.

SPD является очень гибким механизмом управления, который допускает очень хорошее управление обработкой каждого пакета. Пакеты классифицируются по большому числу полей, и SPD может проверять некоторые или все поля для того, чтобы определить соответствующее действие. Это может привести к тому, что весь трафик между двумя машинами будет передаваться при помощи одного SA, либо отдельные SA будут использоваться для каждого приложения, или даже для каждого TCP соединения.

IPsec достаточно хорошо противостоит большинству известным сетевым атакам (sniffing, spoofing, hijacking). Благодаря тому что предусмотрен механизм отбраковки пакетов не удовлетворяющих политики безопасности, IPsec не плохо справляется с атаками Denial-Of-Service (DOS). Replay Attack - нивелируется за счет использования Sequence Number.

К сожалению, с использованием протокола IPsec для защиты беспроводных сетей

связаны некоторые проблемы. Протокол IPsec не позволяет защищать трафик при широковещательной или многоадресной передаче, потому что его действие может распространяться только на взаимодействие двух сторон, обменявшихся ключами и выполнивших взаимную проверку их подлинности. Протокол IPsec защищает только сетевые пакеты, но не саму беспроводную сеть. Несмотря на прозрачность протокола IPsec для пользователей, для сетевых устройств он прозрачен не полностью, потому что работает на сетевом уровне, а не на MAC- уровне. Это предъявляет дополнительные требования к правилам для брандмауэров. Все устройства, не поддерживающие IPsec, уязвимы перед зондированием или атаками со стороны любых пользователей, способных осуществлять мониторинг трафика в беспроводной сети. Если протокол IPsec используется в крупной системе не только для защиты трафика беспроводной сети, но и для комплексной защиты трафика других приложений, управлять политиками IPSec будет сложно

Потокол WPA

WPA включает в себя улучшенный механизм аутентификации и шифрования. Эти изменения были внесены в проект стандарта 802.11i, однако Альянс Wi-Fi собрав поднабор компонентов, соответствующих стандарту 802.11i не дожидаясь официального принятия внедрил их поддержку в выпускаемое оборудование. Протокол получил название «защищенный доступ к Wi-Fi» (Wi-Fi Protected Access, WPA).

Защита беспроводных сетей имеет четыре составляющие. Базовая аутентификация (authentication framework). Представляет собой механизм, который усиливает действие алгоритма аутентификации путем организации защищенного обмена сообщениями между клиентом, точкой доступа и сервером аутентификации. Алгоритм аутентификации. Представляет собой алгоритм, посредством которого подтверждаются полномочия пользователя.

Алгоритм защиты данных. Обеспечивает защиту при передаче через беспроводную среду фреймов данных. Алгоритм обеспечения целостности. (data integrity algorithm). Обеспечивает целостность данных при передаче их через беспроводную среду, позволяя приемнику убедиться в том, что данные не были подменены.

Базовая аутентификация

Основные компоненты, обеспечивающие эффективную аутентификацию – это :

- централизованная аутентификация, ориентированная на пользователя;
- динамические ключи;
- управление зашифрованными ключами;
- взаимная аутентификация.

Аутентификация, ориентированная на пользователя, чрезвычайно важна для

обеспечения защиты сети. Аутентификация, ориентированная на устройства, подобная скрытой аутентификации и аутентификации с совместно используемым ключом, не способна воспрепятствовать неавторизованным пользователям воспользоваться авторизованным устройством. Из этого следует, что при потере и краже такого устройства или по окончании работы по найму администратор сети будет вынужден вручную изменять ключи всех точек доступа и клиентов сети стандарта 802.11. При централизованном, ориентированном на пользователя управлении через сервер аутентификации, авторизации и учета (authentication, authorization and accounting, AAA), такой как Radius, администратор может запретить доступ к сети отдельным пользователям, а не их устройствам.

Аутентификация, которая поддерживает создание динамических ключей, хорошо подходит для улучшения защиты беспроводных LAN и модели управления ими. Динамические ключи, индивидуальные для каждого пользователя, освобождают администратора от необходимости использования статически управляемых ключей. Динамические ключи сами назначаются и аннулируются, когда пользователь проходит аутентификацию.

Взаимная аутентификация – это аутентификация, при которой не только сеть аутентифицирует пользователя, но и пользователь сеть. Технология WPA, призванная временно (в ожидании перехода к 802.11i) закрыть бреши WEP, состоит из нескольких компонентов:

- протокол 802.1x - универсальный протокол для аутентификации, авторизации и учета (AAA);
- протокол EAP - расширяемый протокол аутентификации (Extensible Authentication Protocol);
- протокол TKIP - протокол временной целостности ключей, другой вариант перевода - протокол целостности ключей во времени (Temporal Key Integrity Protocol);
- MIC - криптографическая проверка целостности пакетов (Message Integrity Code);
- протокол RADIUS.

Проктокол 802.1X

Протокол 802.1x может выполнять несколько функций. В данном случае нас интересуют функции аутентификации пользователя и распределение ключей шифрования. Необходимо отметить, что аутентификация происходит «на уровне порта» - то есть пока пользователь не будет аутентифицирован, ему разрешено посылать/принимать пакеты, касающиеся только процесса его аутентификации (учетных данных) и не более того. И

только после успешной аутентификации порт устройства (будь то точка доступа или коммутатор) будет открыт и пользователь получит доступ к ресурсам сети. IEEE 802.11x определяет три основных компонента в сетевом окружении: Саппликант (supplicant) – объект которому необходима аутентификация. Сервер аутентификации (authentication server) – объект, обеспечивающий службы аутентификации. В стандарте четко не определено, что должно выступать в качестве сервера аутентификации, но, как правило, им является сервер RADIUS (Remote Access Dial In User Service).

Аутентификатор (authenticator) – объект на конце сегмента "точка--точка" локальной вычислительной сети, который способствует аутентификации объектов. Другими словами, это устройство-посредник, располагаемое между сервером аутентификации и саппликантом. Обычно его роль выполняет беспроводная точка доступа.

Аутентификатор создает логический порт для устройства саппликанта. Этот логический порт имеет два тракта прохождения данных: неконтролируемый и контролируемый. Неконтролируемый порт позволяет проходить через тракт всему трафику аутентификации. Контролируемый тракт блокирует прохождение трафика до тех пор, пока не будет осуществлена успешная аутентификация клиента. См. рисунок 6.8.

Во время аутентификации обмен сообщениями осуществляется следующим образом. Клиент-проситель ассоциируется с аутентификатором точкой доступа. Аутентификатор предоставляет порт просителю. Переводит порт в неавторизованное состояние. Клиент начинает аутентификацию. Аутентификатор отвечает сообщением с EAP запросом на аутентификацию просителю, чтобы удостовериться в идентичности клиента. На сервер аутентификации отправляется пакет, содержащий идентификационные данные клиента.

В завершении посылается пакет RADUIS-ACCEPS, RADIUS-REJECT, направленный от сервера аутентификации к точке доступа. Аутентификатор переводит порт клиента в состояние –авторизован|.

Протокол EAP

Протокол EAP (Extensible Authentication Protocol) был создан с целью упразднения частных механизмов аутентификации и распространения стандартизированных подходов – схем типа "запрос-ответ" (challenge-response) и инфраструктуры, основанной на публичных ключах и пользовательских сертификатах. Стандартизация механизмов EAP позволила сделать процедуру аутентификации прозрачной для серверов доступа различных производителей. Например, при подключении пользователя к серверу удаленного доступа и использовании механизма EAP протокола PPP для аутентификации сам сервер доступа не должен знать или поддерживать конкретные механизмы или алгоритмы аутентификации, его задача в этом случае – лишь передать пакеты EAP-сообщений RADIUS-серверу, на котором

фактически производится аутентификация. В этомслучае сервер доступа исполняет роль посредника между клиентом и RADIUS- сервером, в задачи которого входит передача EAP-сообщений между ними.

Перечислим наиболее распространенные методы аутентификации

LEAP – алгоритм взаимной аутентификации с использованием пароля. Пропреоретарный метод от Cisco systems. Поддерживается оборудованием компании Cisco.

EAP-MD5 - процедура односторонней аутентификации саппликанта сервером аутентификации, основанная на применении хэш-суммы MD5 имени пользователя и пароля как подтверждение для сервера RADIUS. Данный метод не поддерживает ни управления ключами, ни создания динамических ключей. Является простейшим и не стойким методом.

EAP-TLS - процедура аутентификации, которая предполагает использование цифровых сертификатов X.509 в рамках инфраструктуры открытых ключей (Public Key Infrastructure – PKI). EAP-TLS поддерживает динамическое создание ключей и взаимную аутентификацию между саппликантом и сервером аутентификации. Недостатком данного метода является необходимость поддержки инфраструктуры открытых ключей. EAP-TTLS - EAP, разработанный компаниями Funk Software и Certicom и расширяющий возможности EAP-TLS. EAP-TTLS использует безопасное соединение, установленное в результате TLS-квитирования для обмена дополнительной информацией между саппликантом и сервером аутентификации. В результате дальнейший процесс может производиться с помощью других протоколов аутентификации, например таких, как: PAP, CHAP, MS-CHAP или MS-CHAP-V2. EAP-PEAP – этот метод перед непосредственной аутентификацией пользователя сначала образует TLS-туннель между клиентом и сервером аутентификации. А уже внутри этого туннеля осуществляется сама аутентификация с использованием стандартного EAP (MD5, TLS, MSCHAP V2). EAP-MSCHAP V2 - метод аутентификации на основе логина/пароля пользователя в MS-сетях. Данный метод поддерживает функции управления ключами и создания динамических ключей.

Протокол TKIP

Temporal Key Integrity Protocol (TKIP) – протокол, предусмотренный спецификацией WPA. TKIP предназначен для решения основных проблем WEP в области шифрования данных. Для совместимости с существующим аппаратным обеспечением TKIP использует тот же алгоритм шифрования, что и WEP – RC4. TKIP подразумевает несколько способов повышения защищенности беспроводных сетей:

- динамические ключи;
- измененный метод генерации ключей;
- более надежный механизм проверки целостности сообщений;

- увеличенный по длине вектор инициализации (до 48-разрядного);
- нумерация пакетов.

Основные усовершенствования, внесенные протоколом TKIP, следующие. Пофреймовое изменение ключей шифрования. Контроль целостности сообщения (message integrity check, MIC). Обеспечивается эффективный контроль целостности фреймов данных с целью предотвращения проведения тайных манипуляций с фреймами и воспроизведения фреймов.

Основной принцип, на котором основано пофреймовое изменение ключа, состоит в том, что IV, MAC - адрес передатчика и WEP – ключ обрабатывается вместе с помощью двухступенчатой функции перемешивания. Вектор инициализации имеет 48 разрядный размер (в отличие от 24 разрядного в других протоколах) и он разбит на две части – старшие 32 разряда и младшие 16 разрядов.

Пофреймово изменяемый ключ имеет силу только тогда, когда 16-разрядные значения IV не используются повторно. Если 16-разрядные значения IV используются дважды, происходит коллизия, в результате чего появляется возможность провести атаку и вывести ключевой поток. Чтобы избежать коллизий IV, значение ключа 1-ой фазы вычисляется заново путем увеличения старших 32 разрядов IV на 1 и повторного вычисления пофреймового ключа. Процесс пофреймового изменения ключа происходит следующим образом.

Базовый ключ, полученный во время аутентификации и имеющий размерность в 128 разрядов, перемешивается со старшими 32 разрядами 48 разрядного вектора инициализации и 48-разрядным MAC адресом передатчика (TA). Результат этого действия называется ключом первой фазы (80-разрядный). Ключ первой фазы снова перемешивается с IV и TA для выработки значения пофреймового ключа (128-разрядный, первые 16 разрядов – это IV). IV, используемый для передачи фрейма имеет размер 16 битов (0-65535). Пофреймовый ключ используется для шифрования данных. Когда 16-битовое пространство IV оказывается исчерпанным, ключ 1-й фазы отбрасывается и 32 старших разряда увеличиваются на 1. Заново вычисляется значение пофреймового ключа (рис. 29)

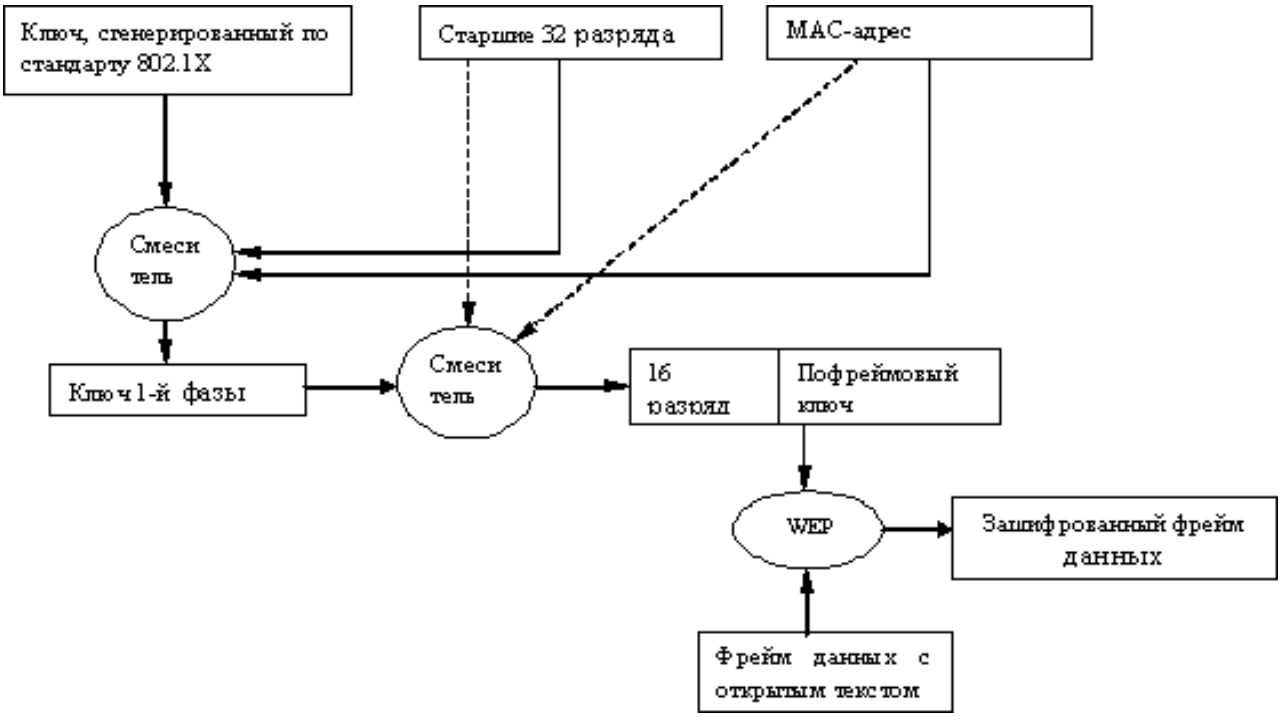


Рис. 29. Пофреймовое изменение ключей

Проверка целостности сообщений MIC

MIC Проверка целостности сообщений (Message Integrity Check, MIC) предназначена для предотвращения захвата пакетов данных, изменения их содержимого и повторной пересылки. MIC построена на базе мощной математической функции, которую применяют отправитель и получатель, а затем сравнивают результат. Если он не совпадает, то данные считаются ложными и пакет отбрасывается.

В отличие от WEP, где для контроля целостности передаваемых данных использовалась CRC-32, TKIP применяет MIC, обеспечивающий криптографическую контрольную сумму от нескольких полей (адрес источника, адрес назначения и поля данных). Так как классические MIC-алгоритмы (например, HMAC-MD5 или HMAC-SHA1) для существующего беспроводного оборудования являлись очень "тяжелыми" и требовали больших вычислительных затрат, то специально для использования в беспроводных сетях Нильсом Фергюсоном (Niels Ferguson) был разработан алгоритм Michael. Для шифрования он применяет 64- битный ключ и выполняет действия над 32-битными блоками данных. MIC включается в зашифрованную часть фрейма между полем данных и полем ICV.

Для обеспечения целостности данных в протоколе TKIP, помимо механизма MIC, предусмотрена еще одна функция, отсутствовавшая в WEP, -- нумерация пакетов. В качестве номера используется IV, который теперь называется TKIP Sequence Counter (TSC) и имеет длину 48 бит, в отличие от 24 бит в WEP. Увеличение длины IV до 48 бит позволяет

избежать коллизии векторов и гарантирует, что они не повторятся на протяжении многих лет.

Основным и самым важным отличием TKIP от WEP является механизм управления ключами, позволяющий периодически изменять ключи и производить обмен ими между всеми участниками сетевого взаимодействия: саппликантом, аутентификатором и сервером аутентификации. В процессе работы и аутентификации на разных этапах взаимодействия и для различных целей генерируются специализированные ключи. На рис. 30 показан механизм работы алгоритма MIC.

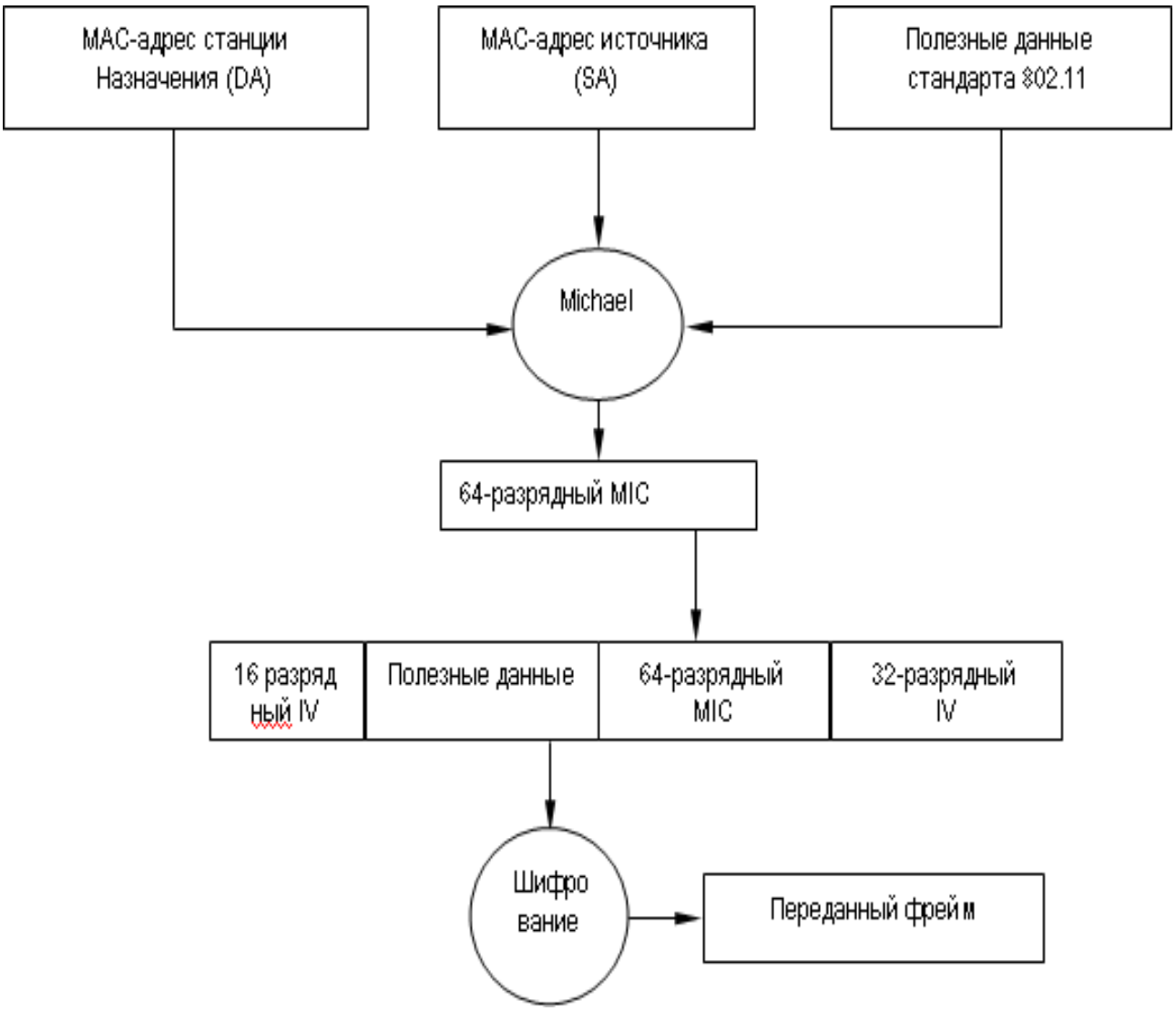


Рис. 30. Работа алгоритма MIC

Итак, зная каким образом происходит пофреймовое изменение ключей, а также понимая принцип работы алгоритма контроля целостности сообщений MIC, можно рассмотреть алгоритм шифрования данных TKIP (рис. 31).

Генерируется пофреймовый ключ. Алгоритм MIC генерирует MIC для фрейма вцелом.

Фрейм фрагментируется в соответствии с установками MAC для фрейма в целом. Фрагменты фрейма шифруются с помощью пофреймового ключа. Осуществляется передача зашифрованных фреймов.

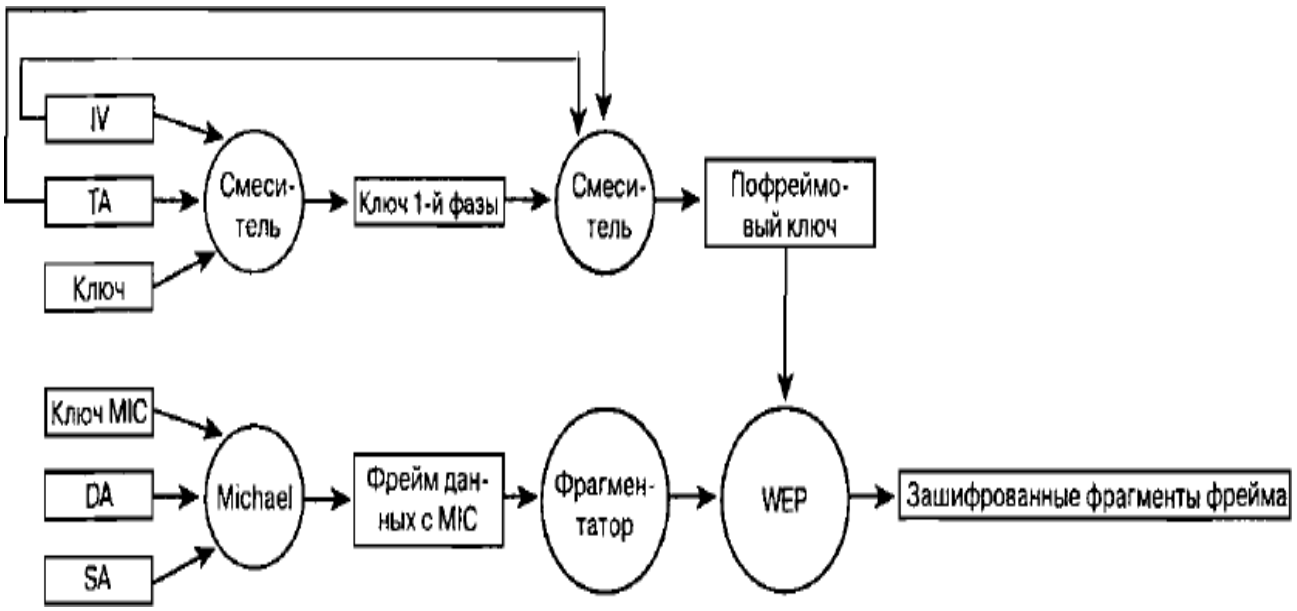


Рис. 31 – Алгоритм шифрования TKIP

Стандарт 802.11i

Стандарт 802.11i или WPA2 был принят в сентябре 2004 года организацией Wi-Fi Alliance и представляет собой сертифицированную совместимую версию полной спецификации IEEE 802.11i, принятой в июне 2004 года. Как и предшествующий ему стандарт, WPA2 поддерживает проверку подлинности по протоколу IEEE 802.1X/EAP или технологию предварительных ключей, но, в отличие от своего предшественника, содержит новый усовершенствованный механизм шифрования AES (Advanced Encryption Standard) со 128 битным ключом.

AES пришел на смену DES, в его основе лежит алгоритм Rijndael. Согласно оценкам, Rijndael не подвержен следующим видам криптоаналитических атак:

1. У алгоритма отсутствуют слабые ключи, а также возможности его вскрытия с помощью атак на связанных ключах.
2. К алгоритму не применим дифференциальный криптоанализ.

3. Алгоритм не атакуем с помощью линейного криптоанализа и усеченных дифференциалов.
4. Square-атака (специфичная атака на алгоритмы со структурой «квадрат», к которым относится и AES) также не применима к алгоритму Rijndael.
5. Алгоритм не вскрывается методом интерполяции.

Сервер устанавливает с клиентом TLS – туннель (в моем случае у клиента имеется сертификат сервера аутентификации. Сервер передает зашифрованный ключ сеанса, клиент используя открытый ключ содержащийся в сертификате и расшифровывает ключ сеанса). Сервер аутентификации внутри сформированного туннеля начинает аутентификацию клиента, для этого посылается запрос на предоставление необходимой для аутентификации информации. Так как используется MSCHAP V2 клиент пересылает свой логин и пароль. Сервер аутентификации проверяет имя пользователя и пароль в Active Directory и после удачной проверки посылает беспроводному коммутатору сообщение RADIUS ACCEPT содержащее динамический ключ для шифрования трафика. Коммутатор передает динамический ключ клиенту используя ключ сеанса. Коммутатор устанавливает с клиентом защищенное VPN соединения и переводит клиентский порт в состояние допускающее перенаправление трафика

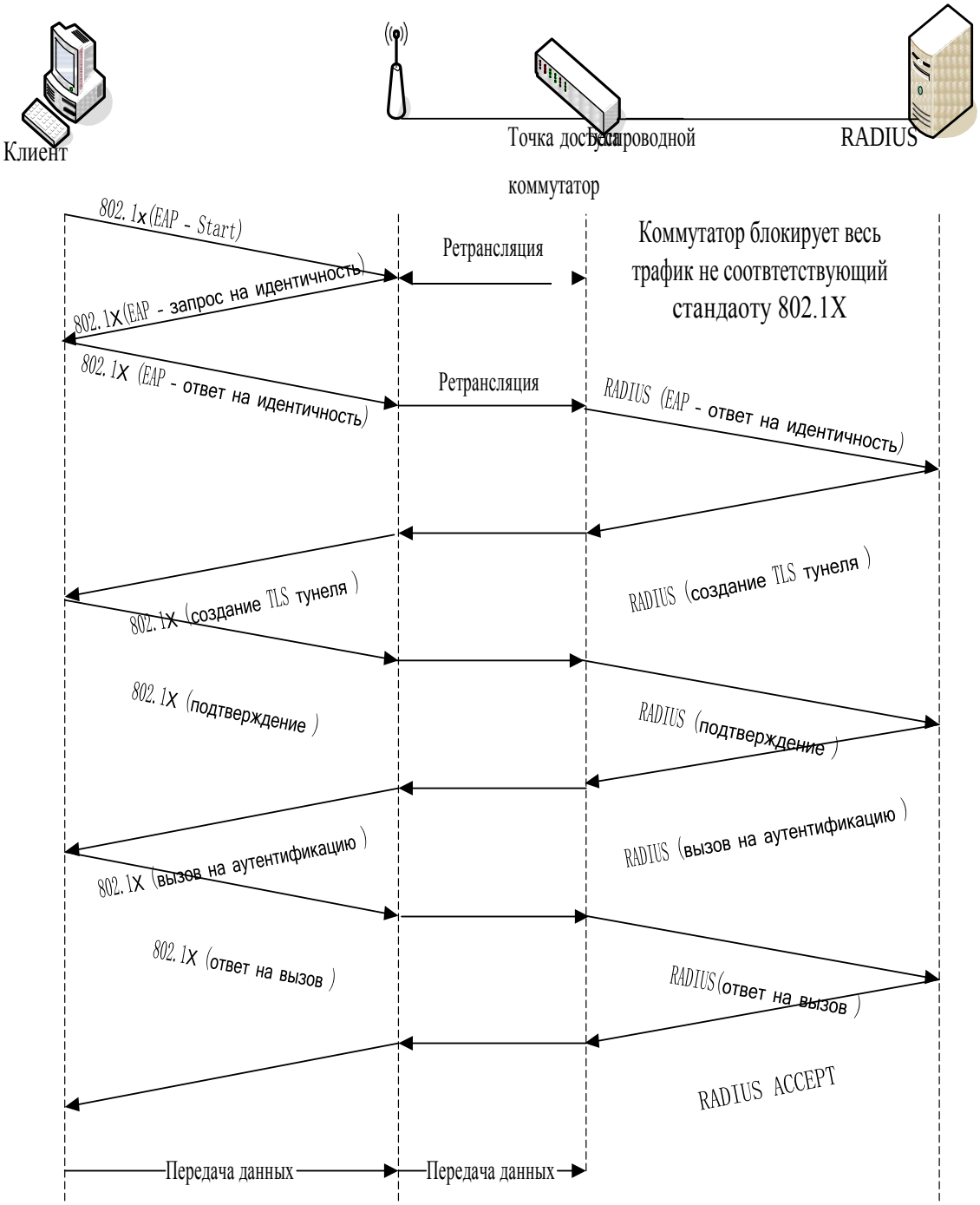


Рис. 37. Процедура прохождения аутентификации EAP-PEAP-MSCHAP V2

Роуминг в сетях 802.11

Роуминг делится на два основных вида:

- бесшовный роуминг (seamless roaming);
- кочевой роуминг (nomadic roaming).

Бесшовный роуминг обеспечивает «незаметный» для абонента переход в зону обслуживания новой базовой станции, т.е. без потери соединения и за небольшой промежуток времени (например, при переходе абонента сети GSM он может продолжать говорить). Кочевой роуминг означает, что абонент должен разорвать текущий сеанс связи найти новую базовую станцию и ассоциироваться с ней. Именно кочевой роуминг может быть организован, в сетях стандарта 802.11 без применения дополнительного оборудования. Для этого на клиентском ПК необходимо настроить соединения с каждой из точек доступа (настроить параметры аутентификации). Однако это не очень удобно так как переходя в зону обслуживания клиент должен будет вновь восстанавливать все сетевые сеансы, к тому же он должен будет повторно проходить процедуру аутентификации которая занимает 10 – 40 секунд. По этому в проектируемой сети будет реализован бесшовный роуминг. Прежде чем переходить к рассмотрению процесса бесшовного роуминга познакомимся с основными понятиями.

Домен роуминга. Под доменом роуминга понимается совокупность точек доступа, относящихся к одному широковещательному домену, и сконфигурированных, так что они имеют одинаковый идентификатор зоны обслуживания (SSID).

Длительность роуминга. Под длительностью роуминга понимается время необходимое для осоциирования абонента с новой точкой доступа. Этот процесс включает следующие фазы: процесс зондирования; процесс аутентификации по стандарту 802.11; процесс ассоциирования по стандарту 802.11; процесс аутентификации по стандарту 802.1X. Суммарная длительность этих процессов и составляет длительность роуминга.

Определения направления движения абонента

Механизм определяющий точку доступа, в направлении которой движется абонент не определен стандартом, каждый производитель решает эту задачу по своему. Можно выделить два варианта реализации. Предварительное обнаружение точки доступа. Обнаружение точки доступа во время перемещения. Каждый из двух вариантов может в свою очередь использовать один из следующих механизмов.

Активное сканирование. Клиент активно ищет точку доступа. Этот процесс обычно включает отправку клиентом зондирующих запросов по каждому из сконфигурированных на нем каналов и ожидание ответов от точек доступа на зондирующие запросы. Затем клиент определяет, какая из точек подходит для него лучше всего.

Пассивное сканирование. Клиент не передает фреймы, а просто прослушивает сигнальные фреймы, передаваемые по каждому из каналов. Клиент продолжает переходить с канала на канал через определенные промежутки времени, как при активном сканировании, но при этом не посылает зондирующие запросы.

Активное сканирование считается более совершенным механизмом поиска точки доступа, потому что при его использовании активно рассылаются запросы по всем частотным каналам. При этом требуется чтобы клиент оставался на одном и том же канале от 10 до 20 мс, ожидая ответ на зондирующий запрос.

При пассивном сканировании клиент медленнее проходит по каналам, чем при активном, так как прослушивает сигнальные фреймы, посылаемые точками доступа с предопределенной частотой (обычно 10 сигнальных фреймов в секунду). Такой клиент должен оставаться на канале дольше чтобы быть уверенным что получил сигнальные фреймы от максимального числа точек доступа для данного канала. Иногда пассивное сканирование не применимо, например, если администратор, в целях безопасности, отключил передачу в сигнальных фреймах имени SSID, клиент не может определить принадлежность точки к домену роуминга.

Предварительное обнаружение точки доступа

Предварительный роуминг — это функция, которая наделяет клиента способностью переходить к обслуживанию предварительно определенной точкой доступа после того, как клиент примет решение перемещаться. Этот процесс требует минимального общего времени роуминга, благодаря чему снижается воздействие роуминга на работу приложений. Однако предварительный роуминг не свободен от недостатков.

Для того чтобы клиент мог определить, к какой точке доступа нужно осуществлять подключение, он должен сканировать точки доступа **в** течение периода нормальной, без роуминга, работы. Когда клиент осуществляет сканирование, он должен переходить с канала на канал, чтобы или прослушивать другие точки доступа, или рассылать зондирующие запросы. Такое изменение может потенциально привести к возникновению двух проблем для клиента, которые могут повлиять на работу приложений.

Клиент не может получать данные от точки доступа, с которой он в данное время ассоциирован, пока он сканирует каналы (активно или пассивно). Если точка доступа посылает данные клиенту в то время, когда он сканирует каналы (предполагается, что клиент работает на другом канале, нежели точка доступа), клиент пропустит эти данные и потребуется повторная передач их точкой доступа.

Приложение клиента может испытать воздействие снижения пропускной способности. Клиент не может передавать данные во время сканирования каналов (активного либо пассивного), поэтому некоторые приложения, выполняемые клиентом, могут ощутить снижение пропускной способности.

Обнаружение точки доступа во время перемещения

Другой вариант обнаружения точки доступа состоит в том, что ее поиск начинается

уже после принятия решения о роуминге. Этот процесс похож на таковой, когда клиент осуществляет начальное включение, за исключением того что запрос на ассоциацию, посылаемый клиентом новой точке доступа, является в действительности фреймом запроса на реассоциацию.

Обнаружение точки доступа во время перемещения не приводит к повышению накладных расходов, характерному для предварительного обнаружения точки доступа (в то время, когда роуминг не осуществляется), потому что клиент не знает, с какой точкой доступа он должен реассоциироваться, но зато больше времени тратится на сам процесс роуминга.

Принцип работы беспроводных коммутаторов

В современной модели беспроводных сетей точки доступа работают как изолированные системы, обеспечивая такие функции стандарта 802.11, как шифрование данных и аутентификация пользователя. В архитектуре, базирующейся на технологии беспроводной коммутации, все интеллектуальные функции, которые выполнялись точками доступа, делегируются центральному беспроводному коммутатору, специально спроектированному для скоростной обработки пакетов. Таким образом, упрощаются задачи точек доступа, которые, по сути, выполняют роль трансиверов. Соединенные непосредственно с беспроводным коммутатором, они становятся как бы его удаленными портами доступа, направляющими пользовательский трафик коммутатору для обработки.

Функции безопасности, например шифрование, аутентификация и управление доступом, реализованы в беспроводном коммутаторе так, что они "отслеживают" пользователя, позволяя ему передвигаться между точками доступа, коммутаторами, виртуальными сетями и подсетями без потери соединения.

Беспроводные коммутаторы обеспечивают также новый подход к автоматизации управления сетями Wi-Fi. Поскольку конфигурации точек доступа хранятся в коммутаторе и запитываются, как правило, также от него (Power over Ethernet -- PoE), то беспроводной коммутатор способен автоматически определить отказавшую точку доступа и дать команду соседним увеличить мощность и изменить настройки каналов, чтобы компенсировать неисправность. Когда вышедшее из строя устройство заменяется, коммутатор регистрирует это событие и конфигурирует новую точку доступа. Беспроводной коммутатор постоянно выполняет мониторинг эфира с целью определения подключенных пользователей и загрузки сети и в соответствии с маршрутами передвижения пользователей динамически настраивает полосу пропускания, управляет доступом, качеством обслуживания и другими параметрами.

Архитектура

Для выполнения расширенного набора функций стандартные уровни 2 и 3 (канальный и сетевой, соответственно) стека протоколов в системе, базированной на беспроводных

коммутаторах, пополняются тремя уникальными блоками:

- mobility management (управление мобильностью);
- security management (управление безопасностью);
- air traffic management (управление радиотрафиком).

Блок управления мобильностью объединяет протоколы Mobile IP и DHCP (Dynamic Host Configuration Protocol) с такими функциями блока управления безопасностью,какаутентификация пользователя и мобильный брандмауэр, политики управления доступом, мониторинг состояния беспроводных соединений. Статусы активных пользователей содержатся в глобальной базе данных (Active User Database), что позволяет непрерывно поставлять необходимые сервисы в процессе их перемещений с соблюдением соответствующих политик безопасности. Уровень безопасности в дополнение к процедуре аутентификации и защите с помощьюмобильногобрандмауэра выполняеттакже

VPN-шифрование для каждого порта, гарантируя конфиденциальность беспроводной передачи данных. Работая совместно с блоком управления радиотрафиком, он блокирует трафик от неисправных точек доступа.

Уровень управления радиотрафиком обеспечивает обнаружение сигнала в зоне покрытия. Он регулирует полосу пропускания и предоставляет необходимый класс обслуживания беспроводным клиентам. Все инструменты, включающие автоматическое обнаружение и калибровку точек доступа, беспроводной удаленный мониторинг (RMON) и захват пакетов данных,строятся вокругуровня управления радиотрафиком.

Алгоритм работы

Дальность действия радиосистемы. Для обеспечения качественной связи мобильных устройств с сетью во всех требуемых участках помещения, радиосистема должна обеспечить достаточное для уверенного приема сигналов покрытие радиоизлучением. Стандарты 802.11b и 802.11g примерно одинаково подготовлены к работе в условиях многолучевого распространения сигналов. Покрытие любого помещения беспроводной сетью требует не столько инженерского расчета, сколько большого количества замеров.

Скорость передачи информации. Требования к скорости передачи данных беспроводной сети являются одними из основных. Они определяются требованиями к скорости доступа ко всем используемым сервисам и ресурсам сети (к базам данных, терминальным и файловым серверам). Из рассмотренных выше стандартов, оптимальным с точки зрения скорости, является стандарт передачи данных 802.11g, позволяющий передавать информацию со скорость до 54 Мбит/с.

Безопасность и защищенность сети. Для корпоративной сети, ключевой задачей является обеспечение требуемого уровня безопасности информации, циркулирующей в сети.

Вопросы информационной и технической безопасности беспроводной сети становятся основополагающими при проектировании такой системы. Острота этой проблемы связана, прежде всего, с используемой средой передачи данных - радиоэфиром. Осуществить перехват информации в радиоэфире намного проще, чем в проводных сетях, - достаточно иметь комплект пользовательского оборудования и специализированный софт. Обеспечение безопасности радиосети, как и любой другой коммуникационной системы, сводится к решению трех проблем – защиты от подключения к сети нелегальных пользователей, предотвращения несанкционированного доступа к ресурсам сети зарегистрированных потребителей и гарантированной поддержки целостности и конфиденциальности данных, передаваемых по радиоканалам. Выбираемый стандарт, в равной степени, как и программно-аппаратный комплекс, должны обеспечить решение этих проблем. Для решения первых двух задач сегодня применяются процедуры аутентификации, авторизации и учета, для решения третьей проблемы применяются процедуры шифрования, проверки целостности пакетов и т.д.

Аутентификация представляет собой процесс установления подлинности абонента.

Авторизация обеспечивает контроль над доступом легальных пользователей к ресурсам сети. Успешно пройдя данную процедуру, потребитель получает только те права, которые предоставлены ему администратором сети.

Система учета фиксирует все события, происходящие в сети. Эта система регистрирует количество ресурсов, потребляемых каждым пользователем, время его работы в сети и т. д., что необходимо в первую очередь для управления сетью, в том числе для контроля доступа. Шифрация данных производится с помощью специальных алгоритмов, защищенных кодовыми ключами, с предусмотренными процедурами динамической смены ключей шифрования и т.п.

На основе сформулированных критериев можно выбрать подходящий стандарт. Сразу исключаем из рассмотрения стандарт 802.11a так как он использует не разрешенный в России частотный диапазон. Из двух оставшихся стандартов наиболее перспективным является 802.11g так как он обеспечивает большую скорость передачи, оборудование соответствующее этому стандарту поддерживаетспецификацию WPA2, которая в свою очередь обеспечивает надежную защиту передаваемой по радиоканалу информации (используется алгоритм шифрования AES) и разнообразные методы надежной аутентификации.

Описание и выбор сервера аутентификации

Для предоставления доступа правомочных пользователей к проектируемой сети будет применяться RADIUS сервер. В его задачи входит проверка подлинности и авторизация

пользователей, зашита сети от несанкционированного доступа, протоколирование событий. Работа сервера основана на протоколе RADIUS (Remote Authentication Dial-In User Service) — это отраслевой стандартный протокол, описанный в документах RFC 2865 «Remote Authentication Dial-in User Service (RADIUS)» и RFC 2866 «RADIUS Accounting». Протокол RADIUS используется для осуществления проверки подлинности, авторизации и учета. Клиент RADIUS (обычно сервер удаленного доступа, VPN-сервер или точка доступа к беспроводной сети) посылает учетные данные пользователя и параметры подключения в форме сообщения RADIUS на сервер RADIUS. Сервер RADIUS проверяет подлинность и авторизует запрос клиента RADIUS, а затем посылает обратно ответное сообщение RADIUS. Клиенты RADIUS посылают на серверы RADIUS также сообщения учета RADIUS. Кроме того стандарт RADIUS поддерживает использование прокси-серверов RADIUS. Прокси-сервер RADIUS — это компьютер, пересылающий сообщения RADIUS между компьютерами, поддерживающими протокол RADIUS.

Для передачи сообщений RADIUS используется протокол UDP (User Datagram Protocol). Для сообщений проверки подлинности RADIUS используется UDP-порт 1812, а для сообщений учета RADIUS — UDP-порт 1813. Некоторые серверы доступа к сети могут использовать UDP-порт 1645 для сообщений проверки подлинности RADIUS и UDP-порт 1646 для сообщений учета RADIUS. В документах RFC 2865 и RFC 2866 определены следующие типы сообщений RADIUS.

Access-Request (запрос доступа) Посылается клиентом RADIUS для

запроса проверки подлинности и авторизации попытки подключения. Access-Accept (предоставление доступа) Посылается сервером RADIUS в ответ на сообщение запроса доступа. Это сообщение информирует клиента RADIUS о том, что для попытки подключения клиента была выполнена проверка подлинности и авторизация. Access-Reject (запрещение доступа) Посылается сервером RADIUS в ответ на сообщение запроса доступа. Это сообщение информирует клиента RADIUS о том, что попытка подключения клиента была отклонена. Сервер RADIUS посылает это сообщение в том случае, если недействительны учетные данные или не авторизована попытка подключения.

Access-Challenge (запрос уточнения) Посылается сервером RADIUS в ответ на сообщение запроса доступа. Это сообщение является запросом дополнительной информации клиента RADIUS, который требует ответа. Accounting-Request (запрос учета) Посылается клиентом RADIUS для указания учетных сведений о разрешенном подключении. Accounting-Response (ответ учета) Посылается сервером RADIUS в ответ на сообщение запроса учета. Это сообщение подтверждает успешное получение и обработку сообщения запроса учета.

Сообщение RADIUS состоит только из заголовка RADIUS или из заголовка RADIUS и

одного или нескольких атрибутов RADIUS. Каждый атрибут RADIUS содержит определенные сведения о попытке подключения. Например, имеются атрибуты RADIUS для имени пользователя, пароля пользователя, типа услуг, запрашиваемых пользователем, и IP-адреса сервера доступа. Атрибуты RADIUS используются для передачи информации между клиентами RADIUS, прокси- серверами RADIUS и серверами RADIUS. Например, список атрибутов в сообщении запроса доступа включает информацию об учетных данных пользователя и параметрах попытки подключения. В отличие от этого сообщение предоставления доступа содержит информацию о типе подключения, котороеможет быть осуществлено, ограничениях подключения и имеющихся особых атрибутах вендора (Vendor-Specific Attribute, VSA).

На сегодняшний день существует большое множество RADIUS серверов, реализованных как программно, так и аппаратно. Большинство из них – это коммерческие продукты. Для выбора более подходящего продукта сформулирую два основных критерия. Продукт должен иметь сертификат соответствия требованиям Гостехкомиссии России, в области зашиты информации от НСД. Продукт должен иметь как можно меньшую стоимостью, при этом обладать достаточной функциональностью.

Использование аппаратных RADIUS серверов для небольших сетей не оправдано из-за их высокой стоимости. Свободно распространяемые продукты не имеют сертификатов соответствия, их использование может быть не безопасным (программа может содержать вредоносный код, не гарантируется конфиденциальность и криптографическая защита информации с которой взаимодействует программа). Подходящим вариантом является использование включенного в состав Windows server 2003 Enterprise Edition RADIUS – сервера (служба IAS). Операционная система имеет сертификат соответствия (№112-0938 выдан 23.10.06 центром безопасности связи ФСБ России) и может применятся в составе автоматизированных информационных систем, работающих с информацией не содержащей государственную тайну. Для различных решений могут быть созданы различные конфигурации службы Internet Authentication Service (IAS):

- Беспроводной доступ.
- Удаленный доступ организаций через коммутируемое подключение или виртуальную частную сеть (VPN).
- Удаленный коммутируемый или беспроводной доступ через внешних поставщиков.
- Доступ к Интернету.
- Доступ с проверкой подлинности к ресурсам экстрасети для деловых партнеров

Я буду использовать службу IAS для авторизации клиентов беспроводной сети. Основные возможности службы. Поддерживаются разнообразные методы проверки подлинности. Поддерживаются протоколы PPP проверки подлинности с паролем, такие как протокол PAP (Password Authentication Protocol), протокол CHAP (Challenge Handshake Authentication Protocol), протокол MS-CHAP (Microsoft Challenge Handshake Authentication Protocol) и MS-CHAP версии 2 (MS-CHAP v2). Протокол EAP Инфраструктура, основанная на стандартах Интернета и разрешающая дополнительные произвольные методы проверки подлинности, такие как смарт-карты, сертификаты, одноразовые пароли и генераторы кода доступа. Способ проверки подлинности, в котором применяется инфраструктура EAP, является способом типа EAP. В службу IAS включена поддержка способов EAP- Message Digest 5 (MD5) и EAP-Transport Level Security (EAP-TLS).

Поддерживаются различные способы авторизации. Протокол DNIS (Dialed Number Identification Service). Авторизация попытки подключения на основе набираемого номера. Служба DNIS показывает набранный номер получателю вызова. Эта возможность предоставляется большинством обычных телефонных компаний. Протокол ANI/CLI (Automatic Number Identification/Calling Line Identification). Авторизация попытки подключения на основе номера телефона, с которого выполняется вызов. Служба ANI/CLI показывает получателю вызова номер телефона, с которого выполняется вызов. Эта возможность предоставляется большинством обычных телефонных компаний. Авторизация для гостей. Учетная запись гостя применяется для идентификации пользователя при установлении подключения без учетных данных пользователя (имени пользователя и пароля).

Неоднородные серверы доступа. Служба IAS поддерживает серверы доступа, реализованные на основе документов RADIUS RFC 2865 и 2866. Помимо серверов удаленного доступа служба IAS поддерживает следующие возможности. Точки доступа к беспроводной сети. Применение политик удаленного доступа и параметров порта Wireless-IEEE 802.11 позволяет использовать службу IAS в качестве сервера RADIUS для точек доступа к беспроводной сети, в которых проверка подлинности и авторизация для беспроводных узлов производится с помощью RADIUS.

Коммутаторы с проверкой подлинности. Применение политик удаленного доступа и параметров порта Ethernet позволяет использовать службу IAS в качестве сервера RADIUS для коммутаторов сети Ethernet, в которых проверка подлинности и авторизация производится с помощью RADIUS. Интеграция со службой маршрутизации и удаленного доступа. Службы IAS и маршрутизации и удаленного доступа используют общие политики удаленного доступа и возможности ведения файла журнала. Такая интеграция обеспечивает

согласованную работу служб IAS и маршрутизации и удаленного доступа. Это позволяет развертывать службу маршрутизации и удаленного доступа на небольших узлах, не предъявляя требований к наличию отдельного централизованного IAS-сервера. Обеспечивается также возможность масштабирования модели централизованного управления удаленным доступом, когда в организации появятся несколько серверов маршрутизации и удаленного доступа. Служба IAS совместно с серверами маршрутизации и удаленного доступа используют одну точку администрирования для удаленного доступа к сети через внешнего поставщика, вызова по требованию и доступа через VPN. Политики службы IAS большого центрального сайта можно экспортировать на независимый сервер маршрутизации и удаленного доступа малого сайта.

Прокси-сервер RADIUS. Служба IAS позволяет пересылать входящие запросы RADIUS на другие RADIUS-серверы для проверки подлинности и авторизации или учета. Действуя в качестве прокси-сервера RADIUS, служба IAS может быть применена всякий раз когда возникает необходимость маршрутизации запроса RADIUS на другой RADIUS-сервер. Служба IAS позволяет пересылать запросы, основанные на имени пользователя, получать доступ к IP-адресу сервера, идентификатору сервера и другим параметр.

Обеспечение удаленного и беспроводного доступа в сеть через внешнего поставщика. При удаленном доступе через внешнего поставщика заключается договор между организацией (заказчиком) и поставщиком услуг Интернета (ISP). Поставщик услуг Интернета обеспечивает подключение сотрудников организации к своей сети перед установлением туннеля VPN в частную сеть организации. Когда сотрудник подключается к серверу NAS поставщика услуг Интернета, на сервер IAS, расположенный в организации, пересылаются записи проверки подлинности и использования. Сервер IAS позволяет организации управлять проверкой подлинности пользователей, отслеживать использование сети поставщика услуг Интернета и управлять доступом сотрудников к ней.Преимущество доступа через внешнего поставщика заключается в потенциальной экономии. Использование маршрутизаторов, серверов сетевого доступа и доступа к каналам глобальной сети, предоставленных поставщиком услуг, вместо приобретения собственных, позволяет получить значительную экономию на затратах, связанных с оборудованием (инфраструктурой). Международные подключения через поставщика услуг Интернета позволяют существенно сократить счета организации за междугородние телефонные звонки. Благодаря перекладыванию на поставщика забот по поддержке сети исключаются расходы на ее администрирование.Кроме того, через внешнего поставщика можно осуществлять и беспроводной доступ. Поставщик может обеспечить беспроводной доступ с удаленной территории и, используя имя пользователя, пересылать запрос на подключение для проверки

подлинности и авторизации на тот RADIUS-сервер, который находится под управлением организации. Хорошим примером служит доступ к Интернету в аэропортах.

Централизованная проверка подлинности и авторизация пользователей. При проверке подлинности запроса на подключение служба IAS сверяет учетные данные подключения с учетными записями пользователей в локальном диспетчере учетных записей безопасности (SAM) домена Microsoft® Windows NT® Server 4.0 или домена Active Directory®. Для домена Active Directory в службе IAS имеется поддержка использования основных имен пользователей (User Principal Name, UPN) Active Directory и универсальных групп. Для авторизации запроса на подключение в службе IAS применяются параметры входящих звонков для учетной записи пользователя, соответствующие как учетным данным подключения, так и политикам удаленного доступа. Управление разрешением удаленного доступа осуществляется относительно просто, однако такой подход не обеспечивает масштабирования по мере роста организации. Политики удаленного доступа обеспечивают более мощное и гибкое управление разрешениями удаленного доступа. Авторизация доступа в сеть может производиться на основе различных параметров, включая описанные далее. (Вхождение учетной записи пользователя в группу, Время суток или день недели, Тип устройства, с помощью которого производится подключение (например беспроводное устройство, коммутатор Ethernet, модем или туннель VPN, Номер вызываемого телефона, Сервер доступа, с которого был получен запрос, Интервал времени бездействия, Максимальная продолжительность одного сеанса, Выбор применяемых способов проверки подлинности, Применение шифрования и степень его стойкости).

Централизованное администрирование всех серверов доступа организации. Поддержка стандарта RADIUS позволяет службе IAS управлять параметрами подключения для любого сервера NAS, использующего стандарт RADIUS. Стандарт RADIUS также позволяет отдельным поставщикам удаленного доступа создавать собственные расширения, называемые особыми атрибутами вендора (Vendor-Specific Attribute, VSA). Служба IAS объединяет расширения, предоставленные несколькими поставщиками, в один словарь. Дополнительные атрибуты VSA могут быть внесены в профиль отдельных политик удаленного доступа.

IAS в качестве RADIUS-сервера

В данной работе служба Internet Authentication Service будет использоваться в качестве RADIUS – сервера. Сервер RADIUS будет выполнять проверки подлинности, авторизацию и учет клиентов RADIUS. В моем случае клиентом радиус клиентами RADIUS будут точки доступа. Для авторизации подключения IAS-сервер применяет параметры входящих звонков учетной записи пользователя и политику удаленного доступа, запросы учета будут сохранятся для анализа в локальном файле журнала. На рисунке 4.39 показан IAS-сервер в качестве сервера RADIUS для клиентов беспроводного доступа. Сервер IAS использует домен Active Directory для проверки подлинности учетных данных пользователя в поступающих сообщениях запросов доступа RADIUS.

Если IAS-сервер используется как сервер RADIUS, сообщения RADIUS обеспечивают проверку подлинности, авторизацию и учет подключений к сети следующим образом. Серверы доступа, например серверы удаленного доступа к сети, VPN-серверы и точки

доступа к беспроводной сети, получают запросы подключения от клиентов доступа.

Сервер доступа, настроенный для использования RADIUS в качестве протокола проверки подлинности, авторизации и учета, создает сообщение запроса доступа и посылает его на IAS-сервер. Сервер IAS оценивает сообщение запроса доступа. При необходимости IAS-сервер посылает запрос уточнения на сервер доступа. Сервер доступа обрабатывает запрос уточнения и посылает обновленный запрос доступа на IAS-сервер.

Производится проверка учетных данных пользователя, а также получение параметров входящих звонков учетной записи пользователя через безопасное соединение с контроллером домена. Попытка подключения авторизуется с учетом параметров входящих звонков учетной записи пользователя и политики удаленного доступа. Если для попытки подключения проверка подлинности и авторизация выполнена, IAS-сервер посылает сообщение предоставления доступа на сервер доступа. Если попытка подключения не прошла проверку подлинности или авторизацию, IAS-сервер посылает сообщение запрещения доступа на сервер доступа. Сервер доступа завершает процесс подключения с

клиентом доступа и посылает сообщение запроса учета на IAS-сервер, на котором сообщение записывается в журнал. Сервер IAS посылает ответ учета на сервер доступа

Выбор оборудования для проектируемой сети

Проектируемая сеть строится на основе беспроводного коммутатора Netgear ProSafe Smart WFS709TP. Его описание приведено в таблице 4.12. Коммутатор способен работать с точками доступа следующих моделей: NETGEAR ProSafe 802.11a/g Dual Band Light Wireless Access Point (WAGL102); NETGEAR ProSafe 802.11g Light Wireless Access Point (WGL102); и NETGEAR WG102 и WAG102. Модели WG102 и WGL102 имеют одинаковые физические характеристики и отличаются лишь программным обеспечением функционирующим на них. Модели WAGL102 и WAG102 также имеют одинаковые физические характеристики. Точки WG102 и WAG102 выпущены раньше беспроводного коммутатора и в своей первоначальной конфигурации не могут взаимодействовать с беспроводным коммутатором, однако производители выпустили свежую прошивку. Ее можно свободно скачать с сайта компании NETGEAR. Выбор будем производить из двух моделей WG102 и WAG102, более новые модели не рассматриваются так как при одинаковых физических характеристиках с более старыми точками их цена превышает последние более чем на 1000 рублей. Характеристики точек приведены в таблицах 4.13 и 4.14 соответственно. Из ходя из приведенных в таблицах данных было решено что для решаемой задачи наиболее подходящей является модель NETGEAR WG102. WG102 поддерживает технологию Power over Ethernet (POE), следовательно отпадает необходимость в прокладке электрической сети в места установки точек. Еще один не мало важный плюс этой технологии является возможность управлять питанием включать/выключать точки доступа с помощью беспроводного коммутатора (если точка доступа по каким то причинам повиснет администратор сможет перезагрузить ее не вставая с рабочего мета). Точки доступа WG102 полностью соответствую стандарту 802.11g.

Порядок выполнения работы

Настройка точек доступа

Для того чтобы перейти к настройке точки доступа необходимо подключить ее к ПК по средствам Ethernet и подключится к ней по используя telnet или WEB – интерфейс. Я буду использовать WEB – интерфейс, он более прост и нагляден. По умолчанию точки доступа D-Link Dir 300, имеют IP – адрес 192.168.0.1, имя пользователя –admin| и пароль –password|.

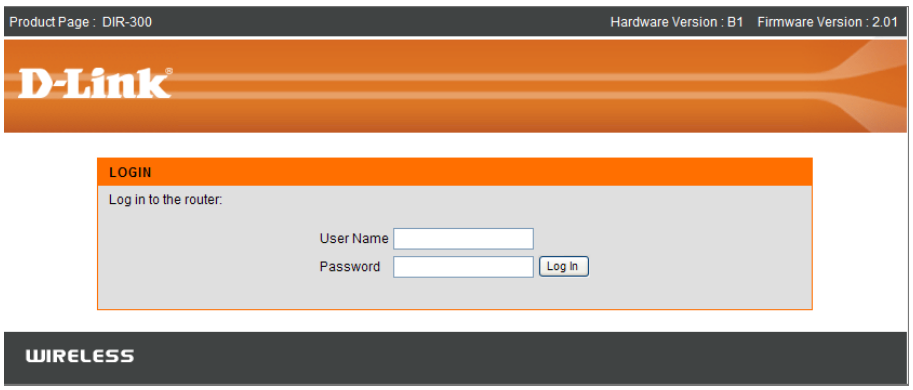


Рис. 40. Начало настройки маршрутизатора

Необходимо настроить точку доступа. Для этого заходим на закладку Setup – Internet Setup.

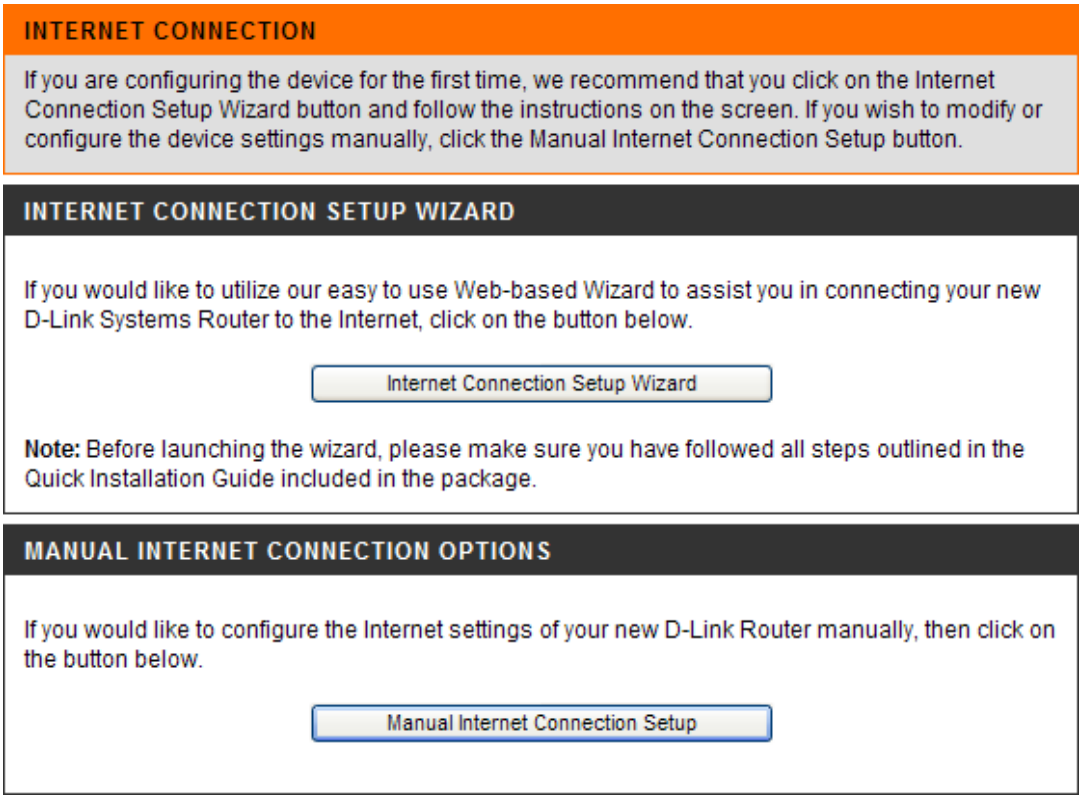
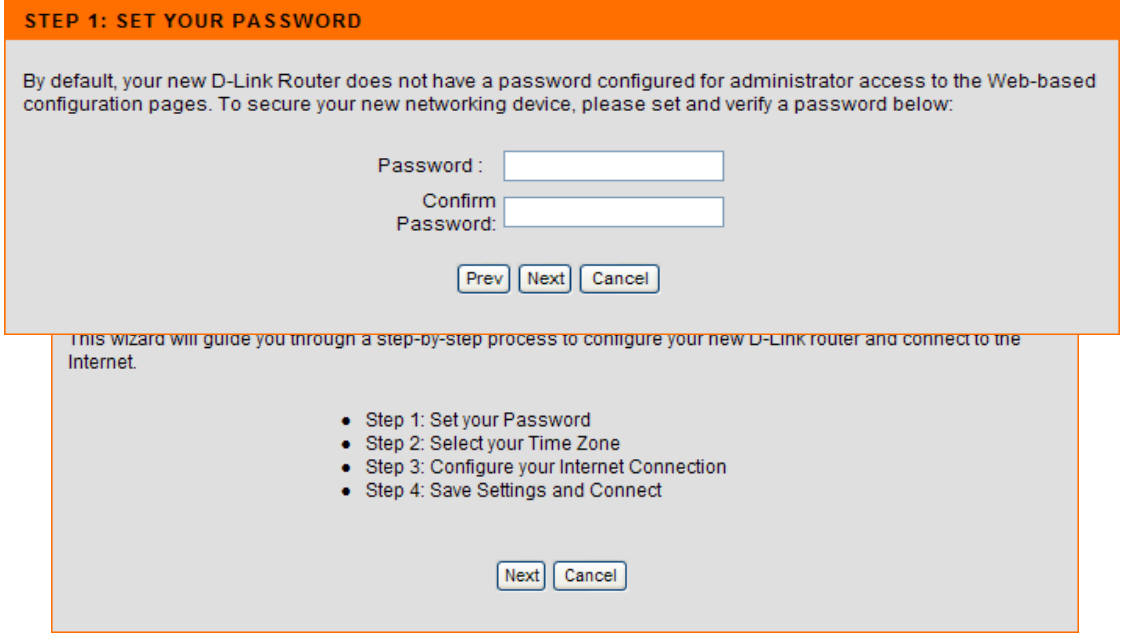


Рис. 41. Настройка Internet.



Для настройки Internet необходимо выбрать одну из предлагаемых функций: Internet connection Setup Wizard (автоматическая настройка) или Manual Internet Connection Setup (ручная настройка). Будем использовать Internet connection Setup Wizard.

Необходимо будет пройти 4 шага настройки. Т.к. Интерфейс настройки маршрутизатора достаточно понятен, то настройка маршрутизатора не представляет особых затруднений.

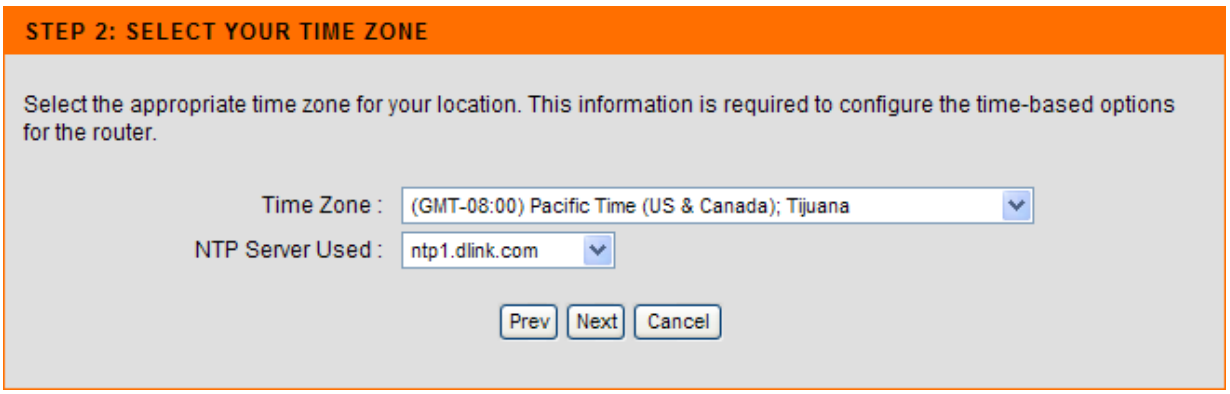
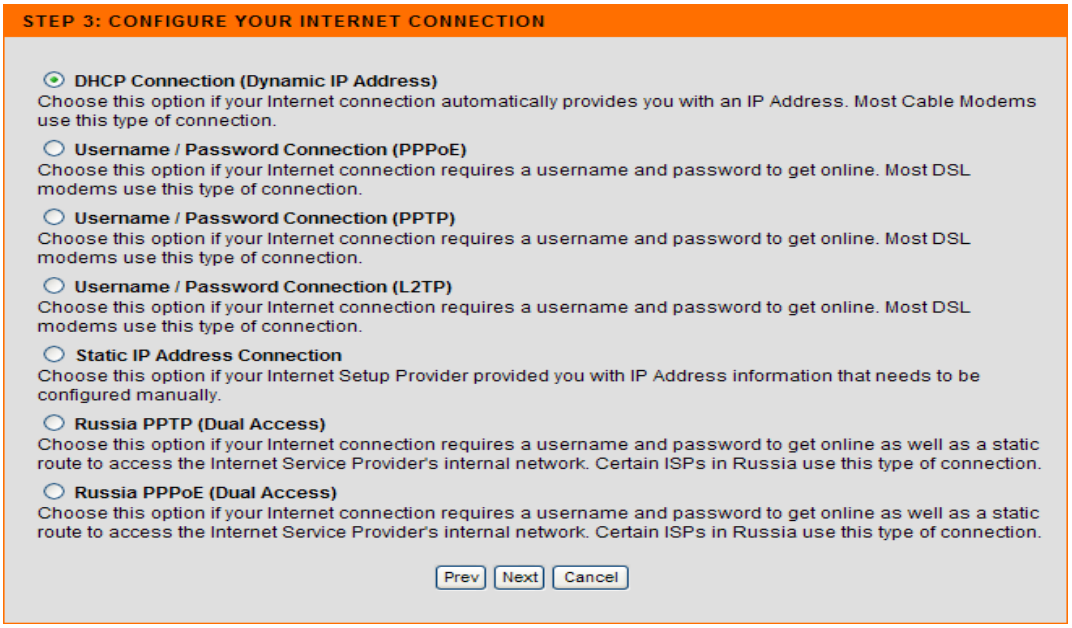


Рис. 44. Третий шаг Затем выбрать соответствующий часовой пояс.

Последним этапом настройки является выбор интернет соединения. В нашем случает это DHCP Connection (Dynamic IP Address).



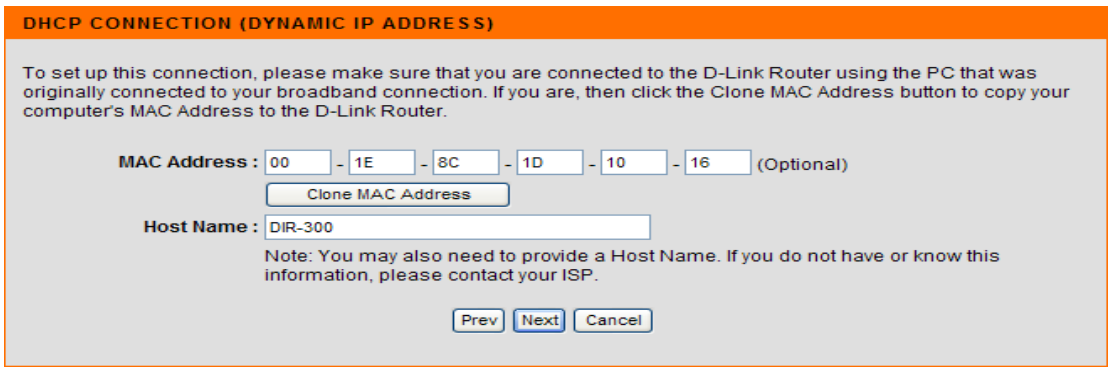


Рис. 46. Проверка MAC адреса

Далее будет предложено проверить мак адрес соединения и ввести Host Name.

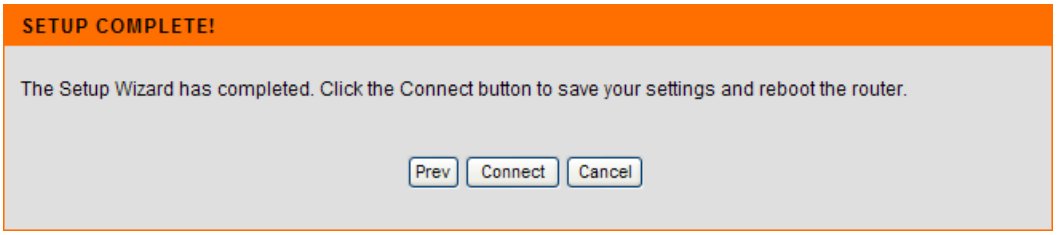


Рис. 47. Завершение настройки Поле нажатия Connect будет установлено соединения.

Проведения испытаний

Оценка производительности точек доступа

Данный тест направлен на оценку производительности используемых в работе точек доступа D-link DIR-300. Под производительностью в данном случае понимается скорость передачи между LAN и WAN (внутренним и внешним) портами устройства, т.е. на сколько быстро микропроцессор точки доступа может обрабатывать поток данных, проходящий сквозь него.

Не смотря на то, что все выпускаемое оборудование соответствует стандарту 802.11g, реальная пропускная способность при работе точки доступа с различным клиентским оборудованием оказывается различной. Проектируемая сеть будет работать с большим числом клиентских адаптеров, выпушенных различными производителями, по этому целесообразно провести тестирование только точек доступа. Именно точки доступа являются связующим звеном между проводной и беспроводной сетью, и по этому, даже если клиентское оборудование может обеспечить большую скорость передачи, максимальная скорость передачи будет ограничена именно возможностями точки доступа.

Для тестирования будет применятся программный пакет NetIQ Chariot. Пакет представляет собой консоль управления (которая может находиться на любом компьютере) и набор сенсоров. Последние являются программами, которые устанавливаются на хостах-

генераторах и осуществляют генерацию и мониторинг трафика. Сенсоры существуют под множество ОС, из которых нас интересует Windows XP SP3. Схема тестирования приведена на рисунке 6.13. В помещении, где проводится тестирование, нет оборудования работающего в диапазоне 2.4 ГГц.

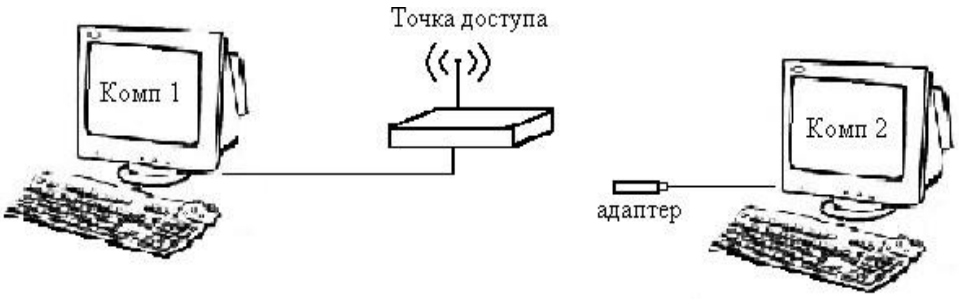


Рис. 52. Тестовый стенд для определения максимальной пропускной способности.

Методика тестирования

Осуществляется передача трафика, сгенерированного программой NetIQ Chariot, между узлами Комп1 и Комп2. В ходе тестирования направление передачи и количество потоков трафика будет меняться:

1. Передача трафика от узла Comp1 к узлу Comp2 с длинной пакета:
   a. Пакеты максимального размера (байт);
   b. Пакеты размера 512 байт;Пакеты размера 64 байта;

Проведем настройку программы NetIQ Chariot. На рис. 53 представлен интерфейс программы.

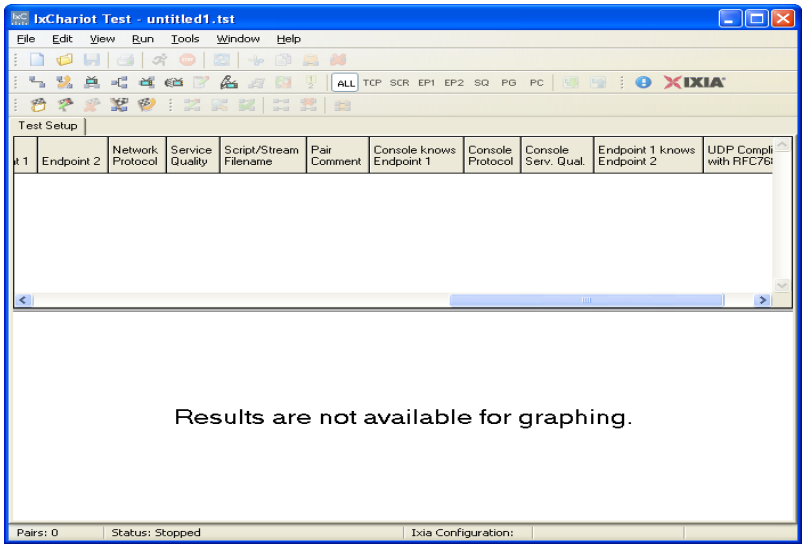


Рис. 53. Интерфейс IXChariot

Перед началом измерений необходимо убедиться , что на компьютере запущена служба «Ixia Perfomance Endpoint» (Пуск -> Настройка -> Панель Управления -> Администрирование -> Службы). Затем зайдите в программу IxChariot и открыть окно Add an Endpoint Pair.

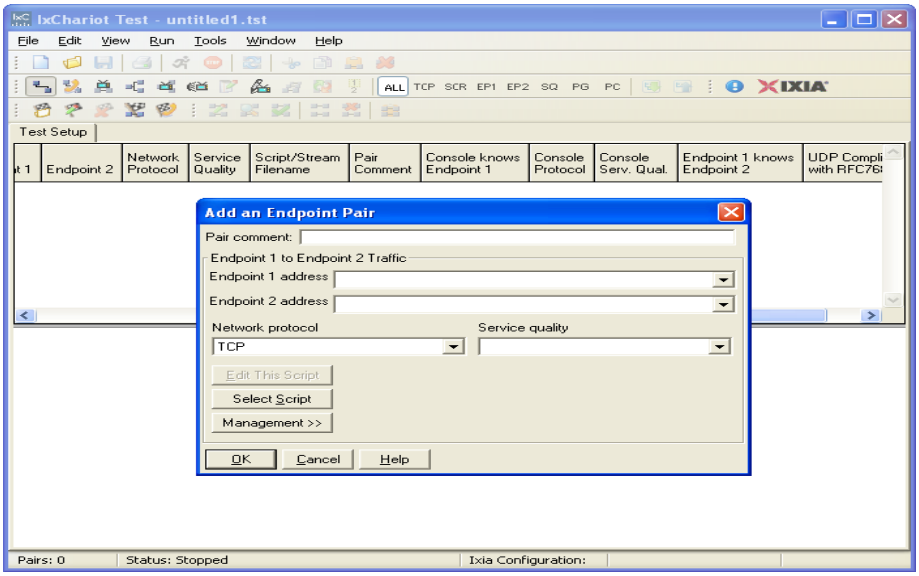


Рис. 54. Окно Add an Endpoint Pair

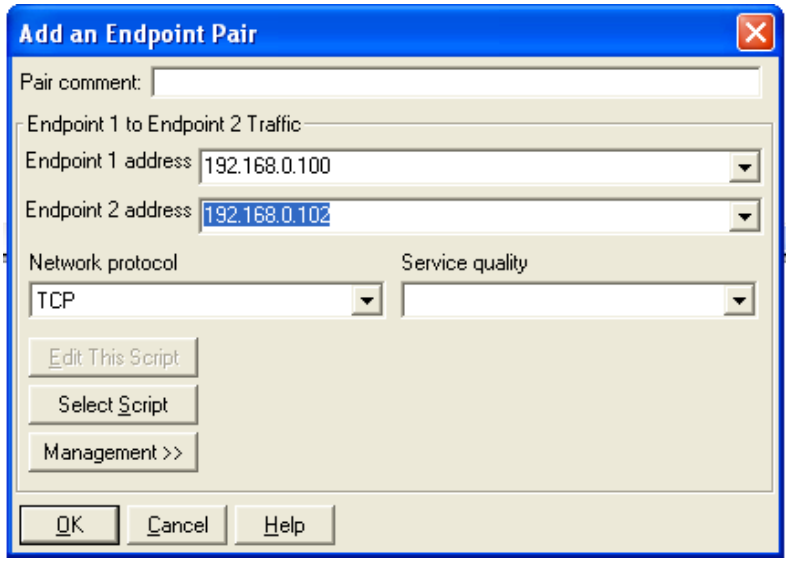


Рис. 55. Ввод IP адресов тестируемых устройствДалее выбираем Select Script и выбираем throughput.

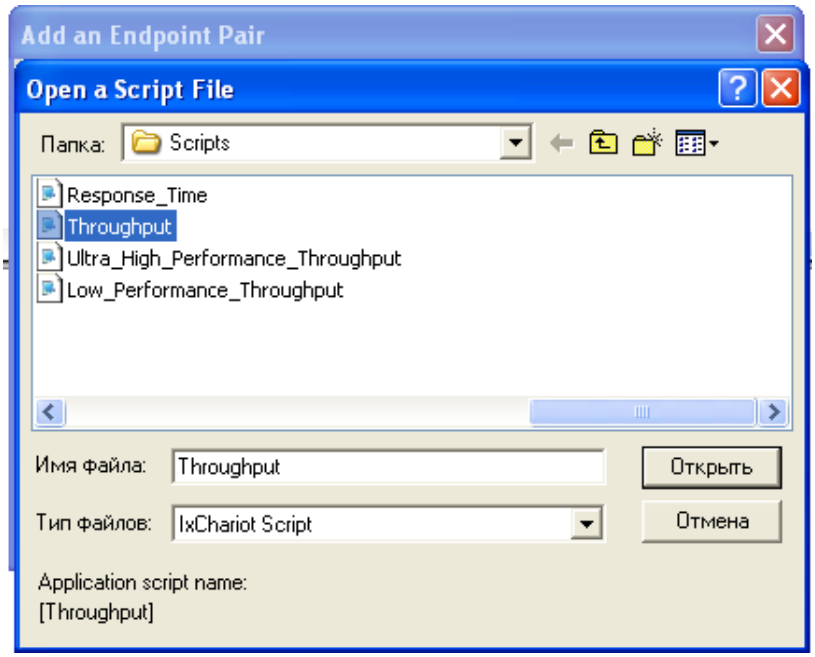


Рис. 56. Выбор скрипта

Произведем настройку скрипта для проведения измерений с различной длиной пакета. Для этого в поле size_file указываем нужное число.

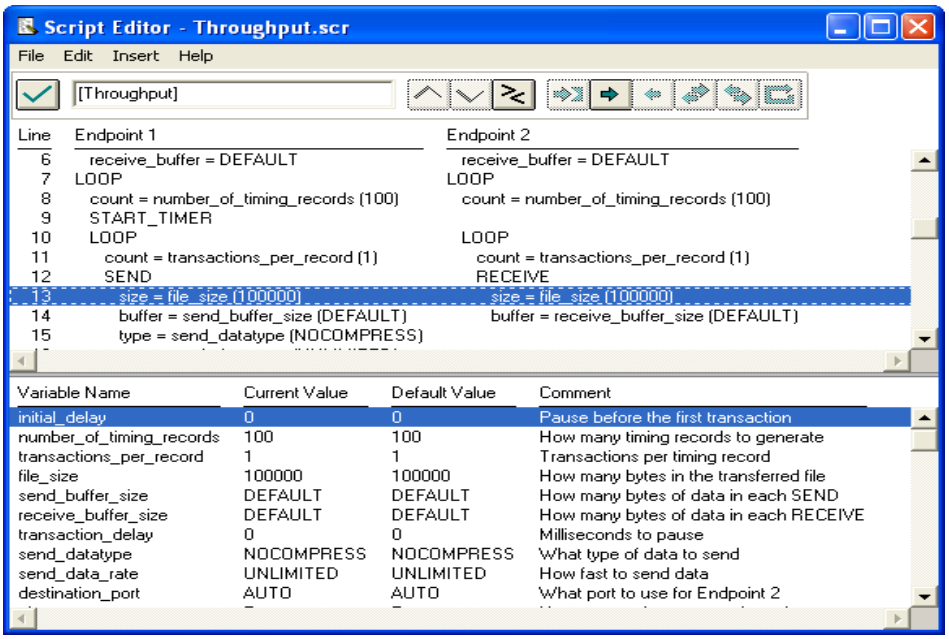


Рис. 57. Настройка скриптаРезультаты измерений.

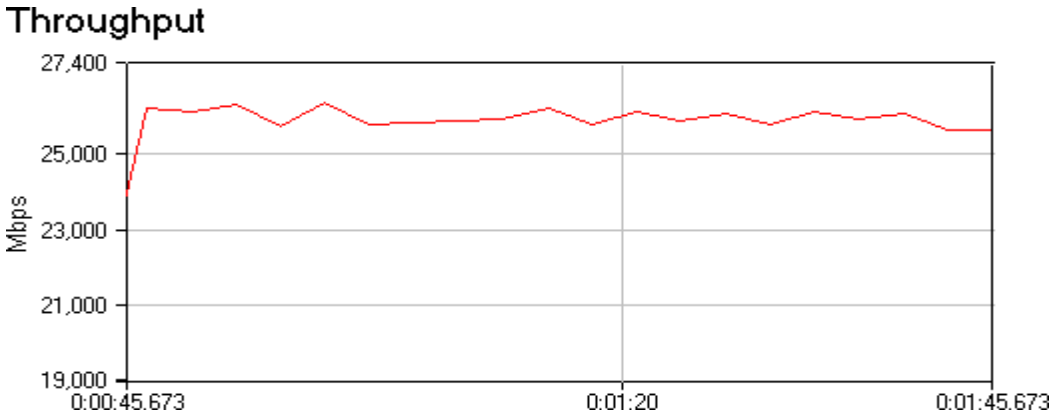


Рис. 58. Размер пакета 1500 байт.

Рис. 59. Размер пакета 512 байт.

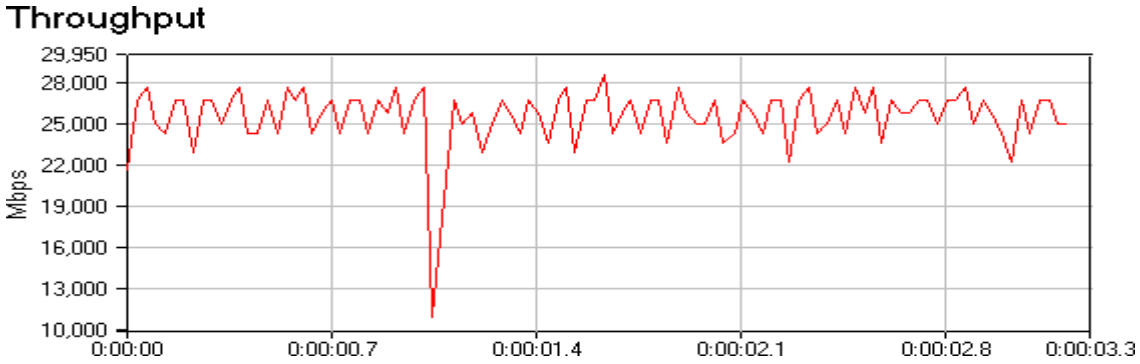


Рис. 60. Размер пакета 64 байта

При проведении всех тестов измерялось среднее время отклика, для этого в течении всего времени тестирования с помощью команды ping от к comp1 к comp2 посылались запросы. Среднее время откликов для каждого из проведенных тестов приведено в таблице 9.

Таблица 9. Результаты измерения времени отклика

№ теста	Время отклика, мс
1	17
2	16
3	9

Оценка накладных расходов связанных с шифрованием

Шифрование как известно, требует значительных вычислений, в результате падает пропускная способность и увеличивается задержки при передаче пакетов, данный тест будет направлен на оценку пропускной способности точки доступа при использовании различных алгоритмов шифрования (WEP, TKIP и AES).

Методика тестирования

Как и в предыдущем случае между конечными точками будет пересылаться сгенерированный программой NetIQ Chariot трафик, будет измеряться скорость передачи и среднее время отклика. При проведении тестирования будем использовать тестовый стенд изображенный на рисунке

6.13. Чтобы провести сравнительный анализ влияния шифрования на пропускную способность как и в предыдущем тесте будем пересылать пакеты с размером 1500 и используя для генерации скрипт throughput.scr. Измерение скорости производится в течении 2 минут.

Настройка оборудования

Оставляем все настройки сделанные для проведения первого теста. Для настройки точки доступа заходим на вкладку Wireless Setup и изменяем метод шифрования.

Без шифрования

Рис. 61. Настройка маршрутизатора для проведения измерений

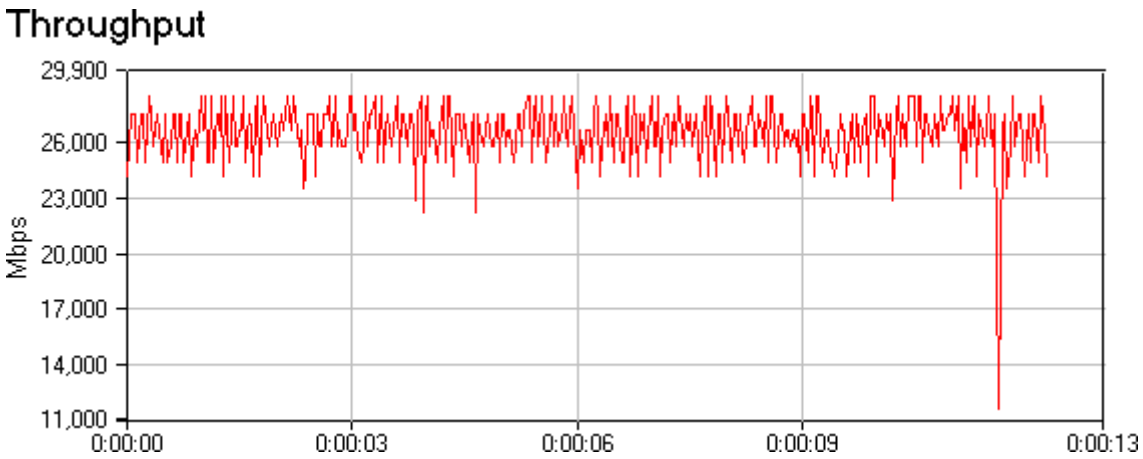
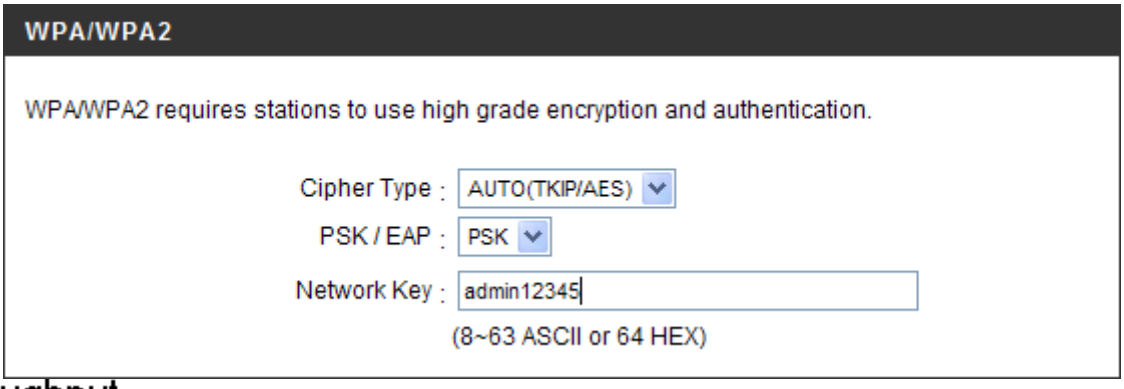


Рис. 62. Результаты измерений в режиме без шифрования WPA/WPA 2 PSK



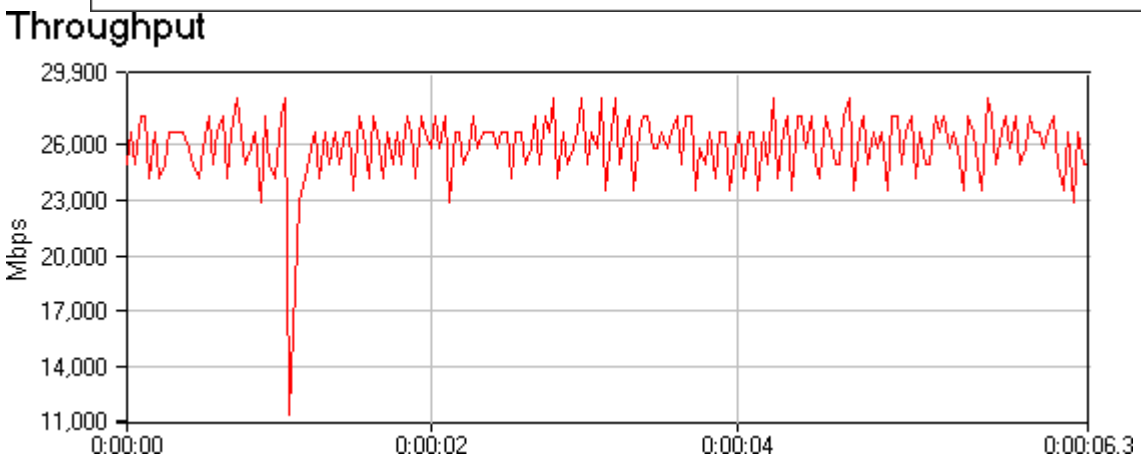


Рис. 64. Результаты измерений режима WPA/WPA 2 PSK

AES

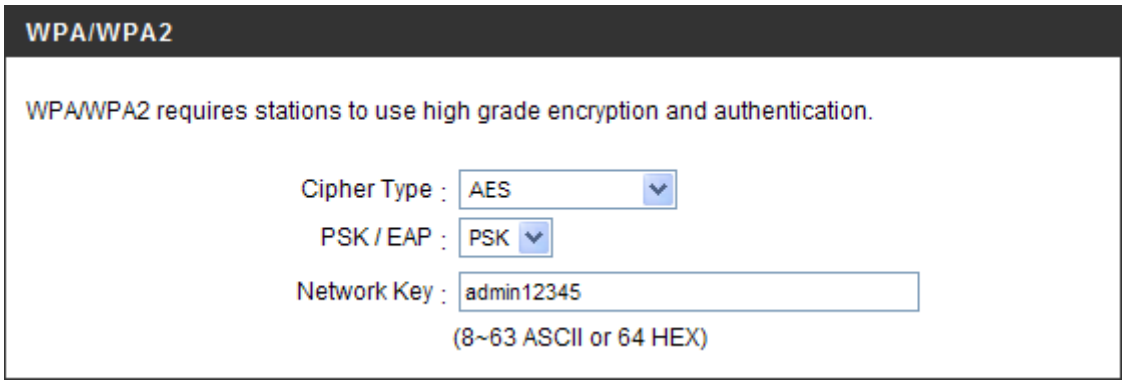


Рис. 65. Настройка маршрутизатора для режима шифрования AES

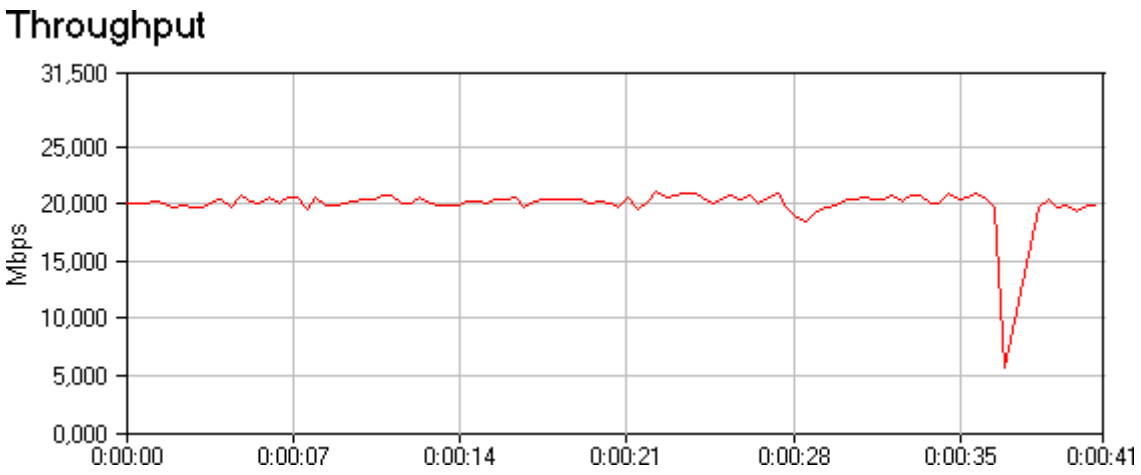


Рис. 66. Результаты измерений в режиме AES

Таблица 10. Результаты измерения времени отклика

№ теста	Время отклика, мсек
Без шифрования	9
TKIP	10
AES	13

Фрагментация фреймов

Данный эксперимент направлен на определение зависимости скорости передачи от длины поля данных в передаваемом пакете.

Методика тестирования

Как и в предыдущих тестах, трафик сгенерированный программой NetIQ Chariot, пересылается между узлами Комп1 и Комп2 (рис. 52), при этом в настройках точки изменяется значение поля данных (Fragmentation) в диапазоне 1500 – 2346 бит. Измерение скорости производится в течении 2 минут, фиксируется среднее значение. По результатам тестирования строится график зависимости скорости передачи от длины поля данных

Настройка оборудования

Оставляем без изменения настройки ПК, выключаем шифрование на точках. Для настройки длины поля данных необходимо перейти на вкладку Advanced Wireless, в поле Fragmentation ввести соответствующее значение.

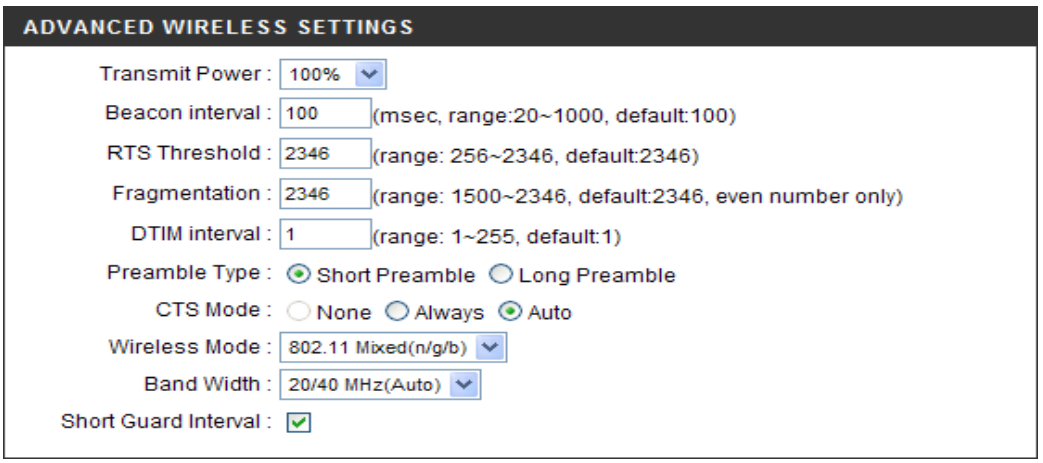


Рис. 67. Настройка длины поля данных передаваемого фрейма Результаты тестирования

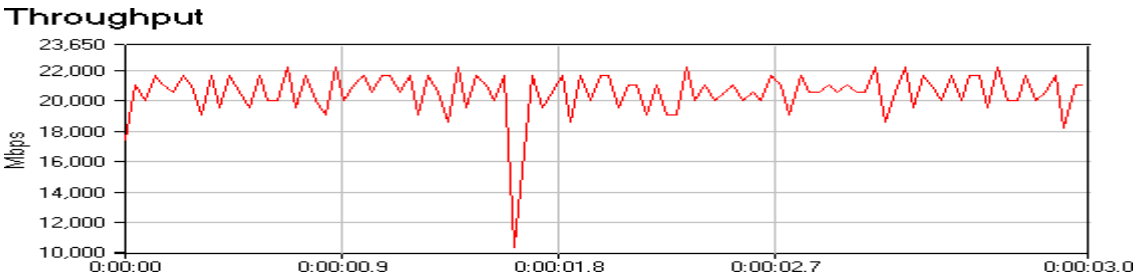


Рис. 68. Длина поля данных 1500 бит

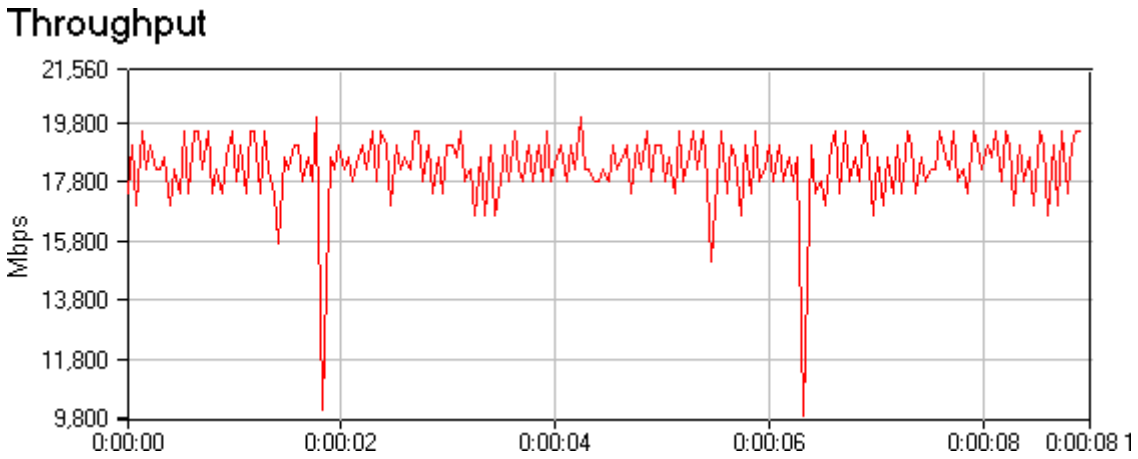


Рис. 69. длина поля данных 2000 бит

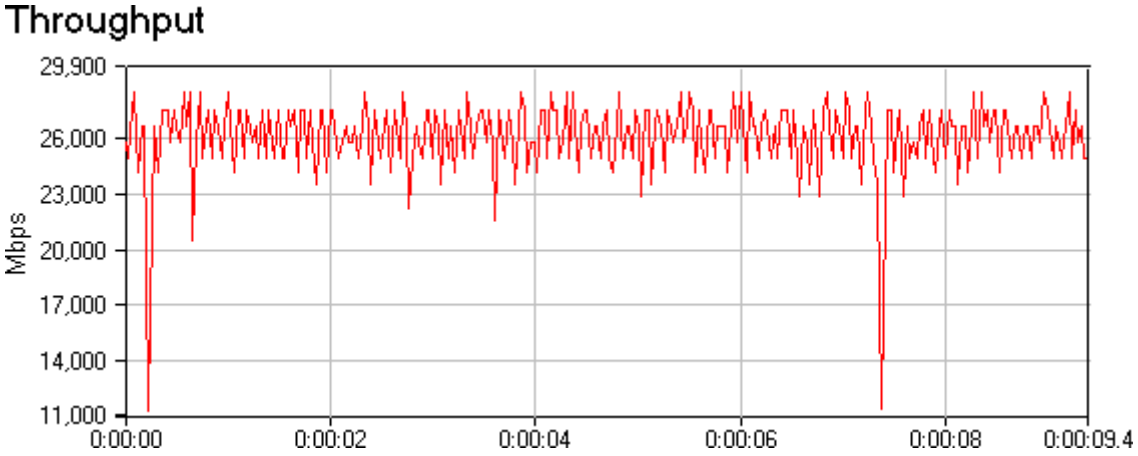


Рис. 70. длина поля данных 2346 бит

Оценка взаимного влияния точек работающих на одном канале

Оценка взаимного влияния точек работающих на одном канале. Тестовый стенд изображен на Рис.2. Точки доступа переводятся на один частотный канал, в первый случае. Между узлами comp1 и comp2, comp3 и comp4 осуществляется передача трафика сгененрированого программой NetIQ Chariot. При тестировании расстояние между точкой 1

и точкой 2 изменяется в пределах от 1 до 30 метров. Для каждого из выбранных значений расстояния L, для пары узлов comp1 и comp2 измеряется среднее значение скорости передачи, времени отклика, количество потерянных пакетов в течении 5 минут. Настройка DSL-2640U на работу в режиме Bridging (режим прозрачного моста).

1. В разделе «Advanced Setup» выберите пункт «WAN», и нажмите кнопку «Add» для создания нового соединения.

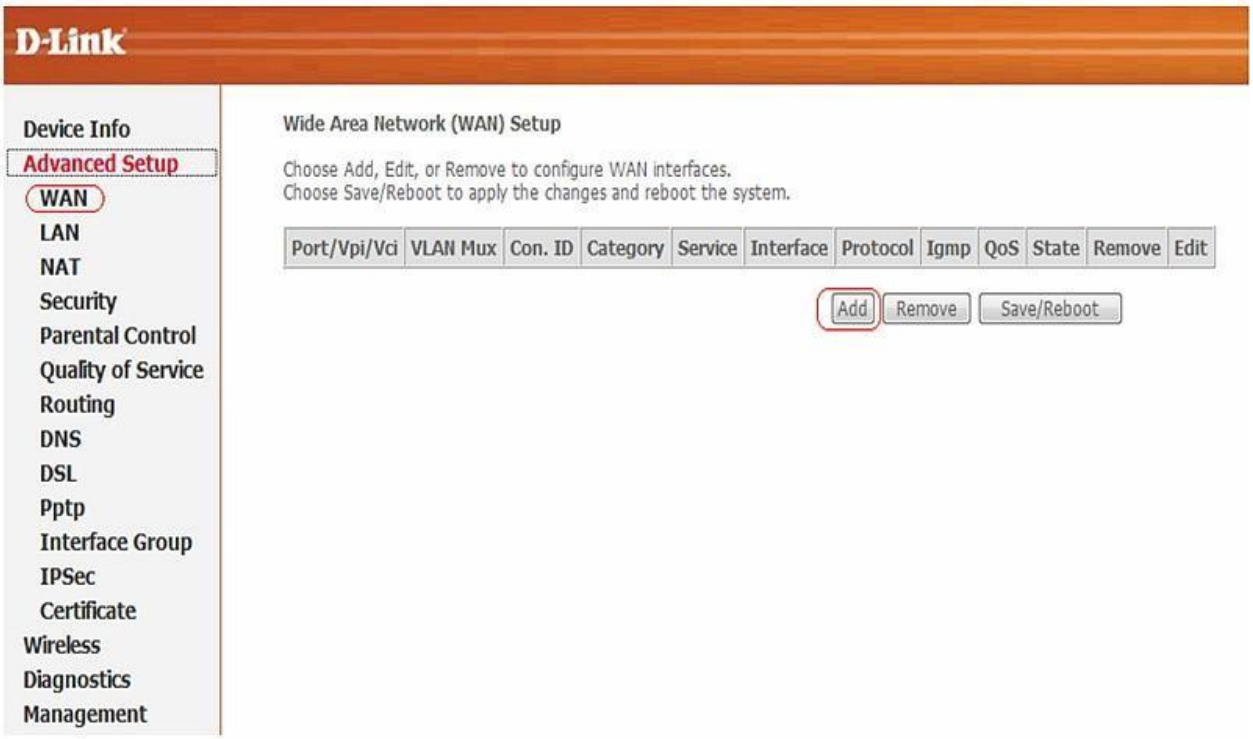


Рис. 71. Создание нового соединения

2. На появившейся странице укажите значения параметров VPI и VCI (значения данных параметров предоставляются провайдером) и нажмите кнопку «NEXT».

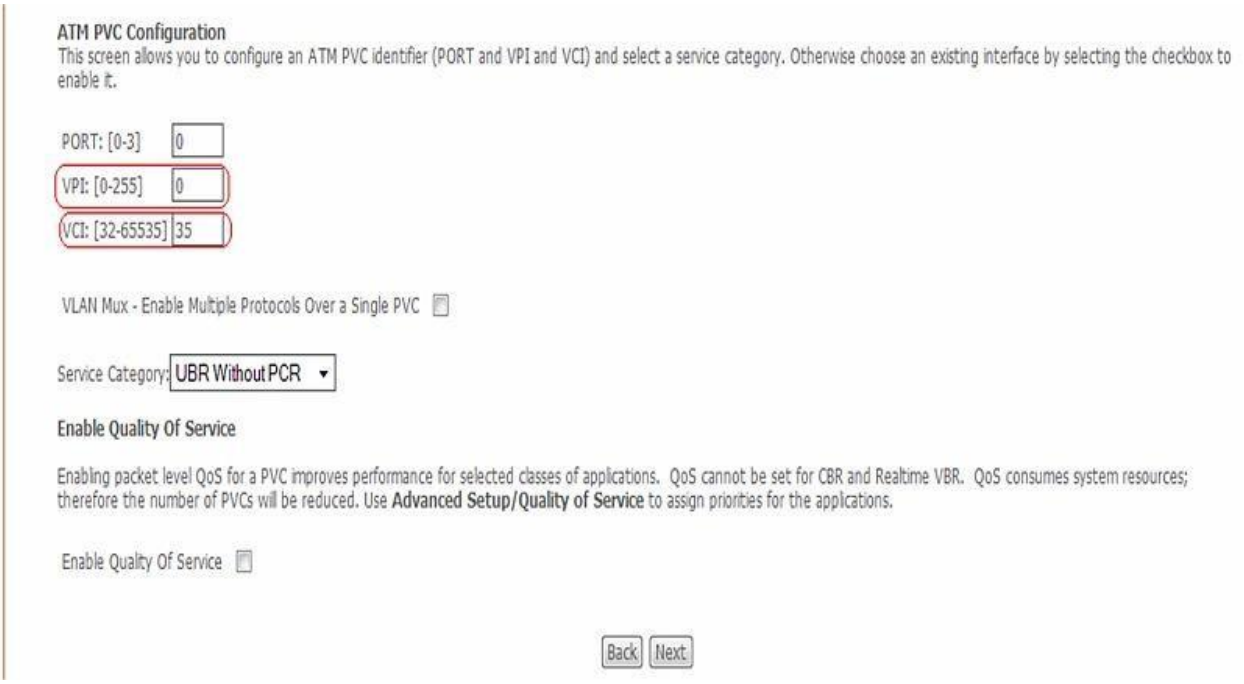


Рис. 72. Значение VPI и VCI

3. На следующей странице в разделе Connection Type установите «Bridging» и нажмите кнопку «NEXT».

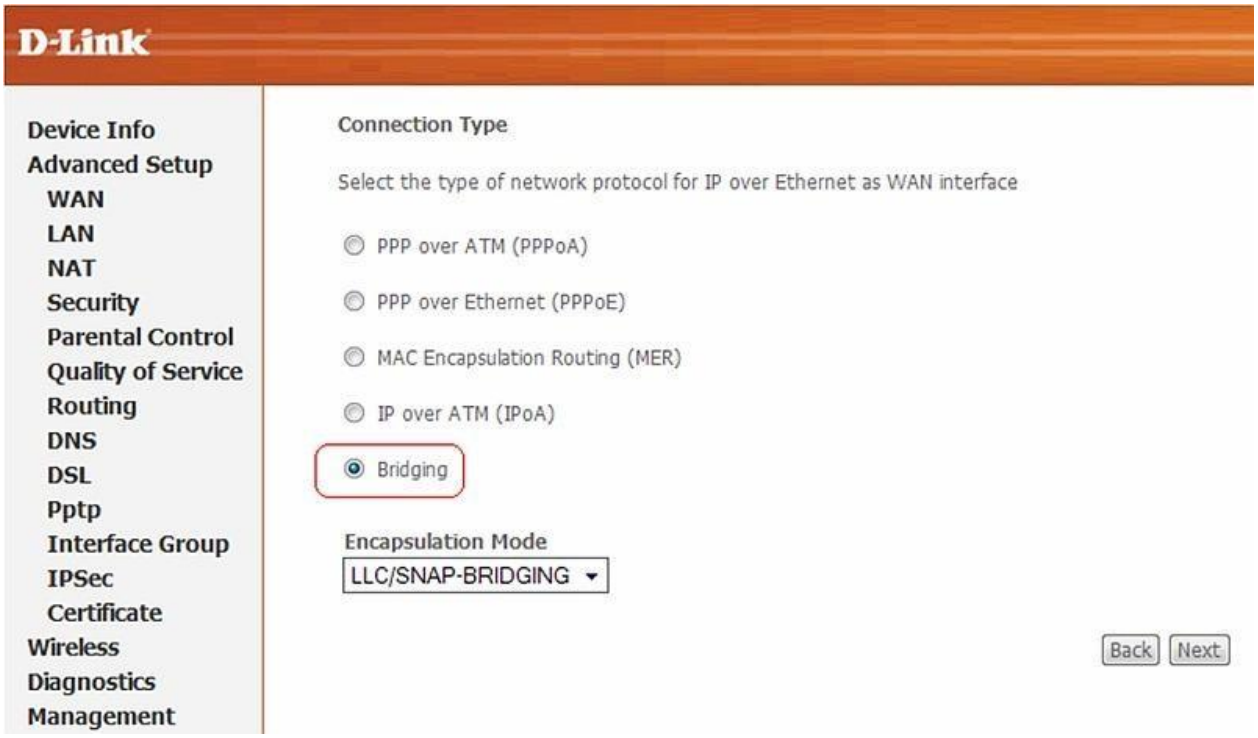


Рис. 73. Установка режим моста

На следующей странице оставьте все настройки по умолчанию и нажмите кнопку «NEXT».

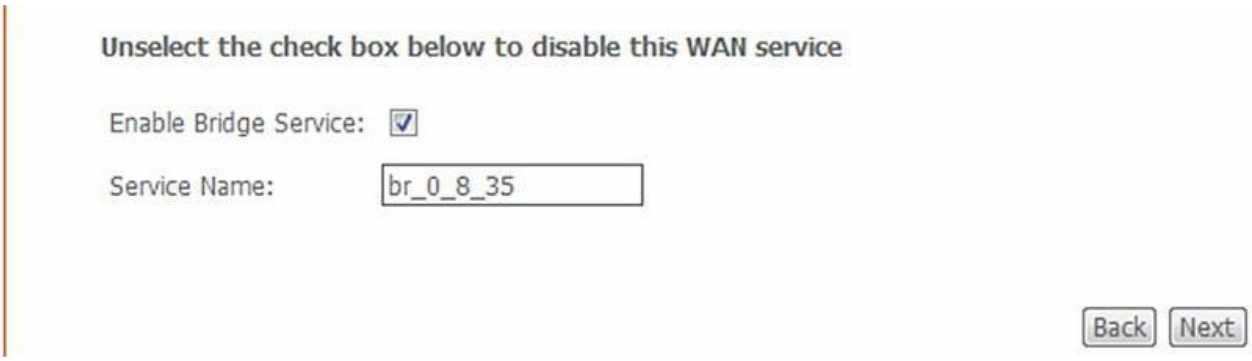


Рис. 74. Создаем имя моста

4. На следующей странице нажмите кнопку «Save».

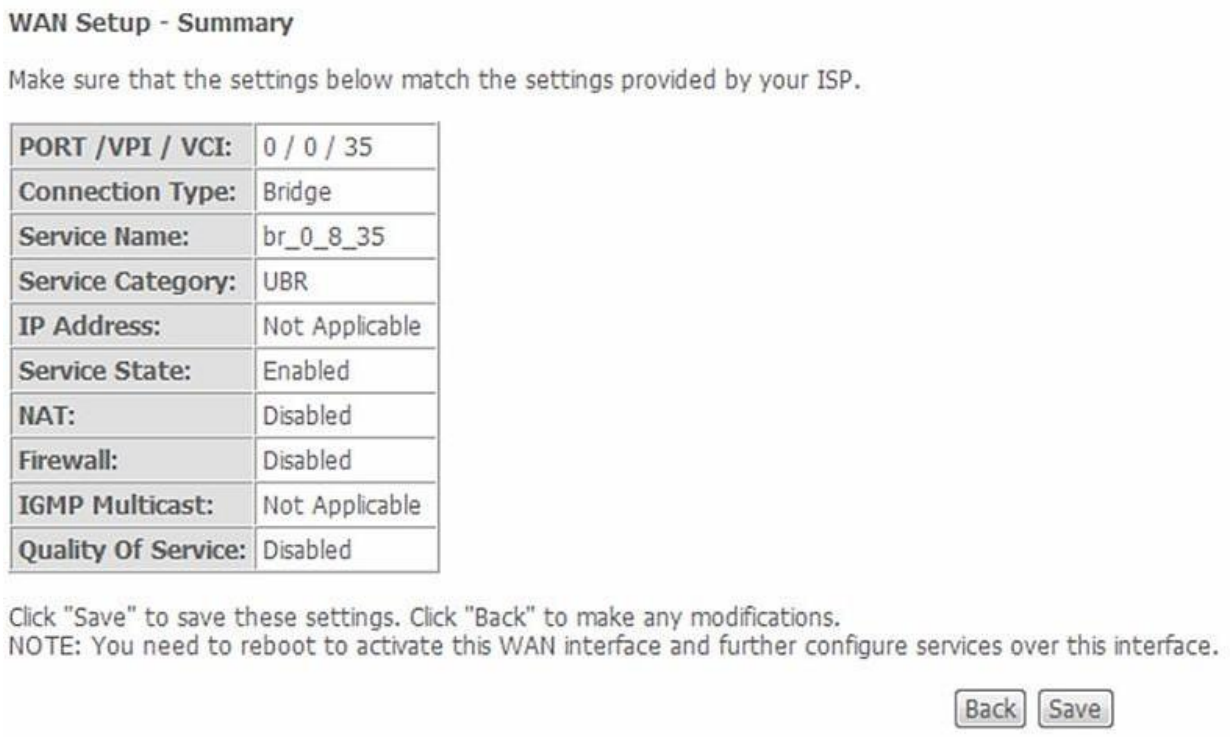


Рис. 75. Проверка настроек

5. После нажатия кнопки «Save» перейдите на страницу «Advanced Setup» > «WAN», где увидите созданное Bridge соединение. Нажмите кнопку «Save/Reboot» для применения параметров и перезагрузки устройства.

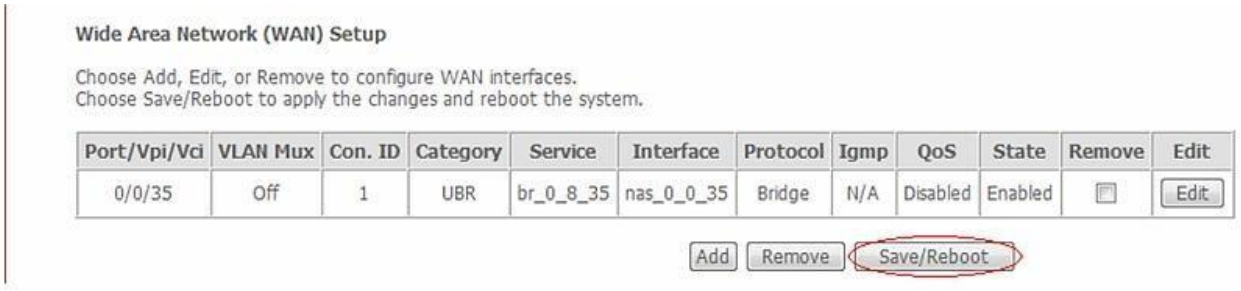


Рис. 76. Перезагрузка устройства

6. Перезагрузка устройства

Рис. 77. Окончание настройки

На этом настройка устройства закончена.

На обеих точках выключается шифрование трафика. Точки переводятся на работу в первый частотный канал. Точкам назначаются разные SIDD, точка один имеет SIDD «dlink», точка 2 «dlink2». Узлам comp1 и comp2, comp3 и comp4 назначаются адреса из одной подсети, конфигурируется тест, по аналогии с предыдущими тестами для генерации трафика используется скрипт throughput.scr, размер пакета максимален. Изначально точки удаленны друг от друга на расстояние 30 метров, с помощью программы Netstumbler 4.0, установленной на узле comp2 осуществляется контроль за уровнем сигнала.Результаты тестирования

Таблица 11. Результаты измерения

Расстояние между точками L, м	Скорость передачи Мбит/с	Среднее время отклика, мс	Количество потерянных пакетов, %
Точка № 2 выключена	45	12	0
30	43	12	0
20	36	13	0

15	32	13	0.01
10	31	14	0.05
8	30.5	15	0.1
5	30.5	15	0.6
3	29.5	18	1.5
1	30	23	3

Как и ожидалось обе точки сохранили работоспособность, не смотря на то что находились в непосредственной близости друг от друга. Используемый для предотвращения коллизий механизм распределенной координации заставляет точки конкурировать за среду, предотвращая тем самым одновременную передачу фреймов обоими точками.

Перед проведением эксперимента я полагал что скорость передачи должна была снизится более чем на 50% при размещении точек в непосредственной близости. Однако наблюдалось уменьшение скорости всего на 30%. При этом скорость передачи между узлами comp3 и comp4 равнялась 28-30 Мбит/с. Суммарная скорость двух систем работающих на одном канале оказалась равной 58-60 Мбит/с, чего в принципе не могло быть. Чтобы объяснить происходящее был детально исследован процесс включения точек. При включении второй точки (первая работала) скорость передачи между узлами comp3 и comp4 составляла около 5-8 Мбит/с, через 8-10 секунд скорость возрастала до 28-30 Мбит/с. При запуске сетевого сканера Netstumbler 4.0 оказалась что точка номер два использует по переменно несколько каналов рисунок 15.19. В точки D-Link Dir - 320 встроена утилита AutoCell которая способна автоматически выбирать не занятые каналы подстраивать мощность передатчика, она отключена, но при конфликтах самостоятельно активируется.

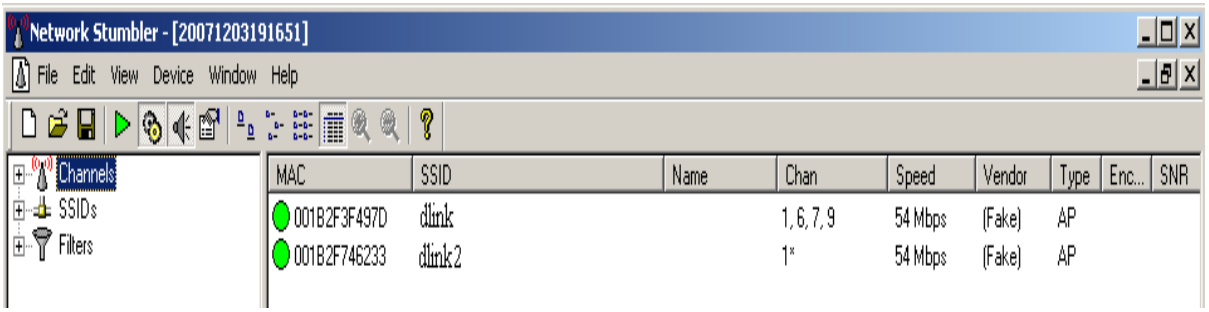


Рис. 78. Влияние точек доступа

Взлом ключей шифрования для стандарта IEEE 802.11

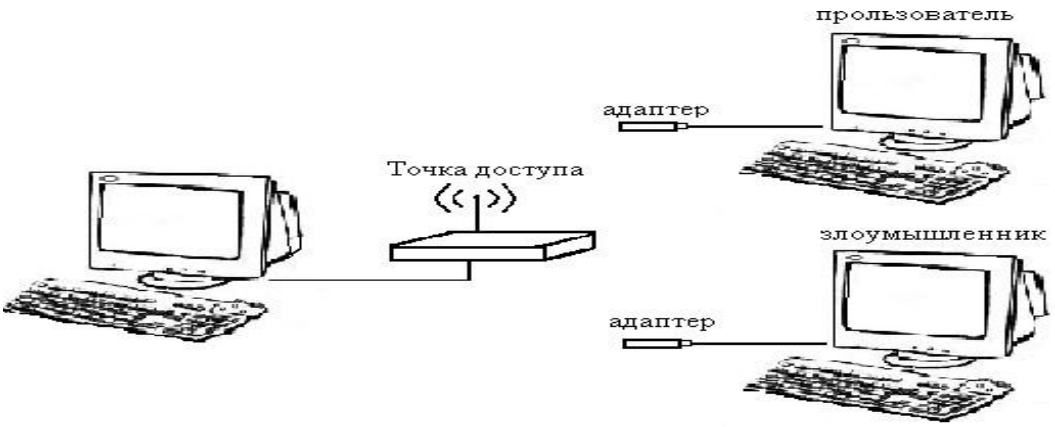


Рис. 79. Тестовый стенд для проверки методов шифрования Настроим точку доступа на режим шифрования как показано в пункте 7.

Затем произведем подключение адаптера к нашему компьютеру.

a. Получения ключа WEP шифрования. Для проведения данного рода атаки необходимо:

Перевести адаптер в режим мониторинга

```
Interface       Chipset         Driver

wlan0           Broadcom        b43 - [phy0]
                                (monitor mode enabled on mon1)
mon0            Broadcom        b43 - [phy0]
```

Рис. 80. Перевод адаптера в режим мониторинга

b. Заменить MAC-адрес адаптера (это делается для того чтобы показать что данная схема защиты не является эффективной)

```
root@dlink-01:~# macchanger --mac 00:11:22:33:44:55 wlan0
Current MAC: 00:11:22:33:44:55 (Cimsys Inc)
Faked MAC:   00:11:22:33:44:55 (Cimsys Inc)
It's the same MAC!!
```

Рис. 81. Замена MAC адреса

Затем поменяем MAC-адрес нашего адаптера. Нужно это для того, что бы показать, что данная схема защиты, т.е привязка по MAC-адресу уже не является функцией защиты.

c. Произвести поиск сети с шифрование данных WEP

После того как мы проделали данную работу можно приступить к поиску сети с шифрованием данных WEP. Для этого в операционной системе.

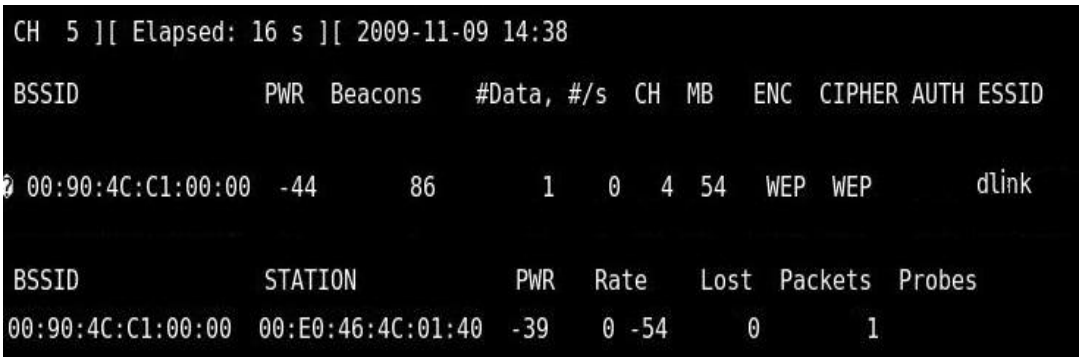


Рис. 82. Поиск сети

Произвести набор пакетов от 10000 до 25000 (это необходимо для дальнейшего анализа пакетов и получения ключа) и при помощи программы aircrack-ng произвести подбор ключа

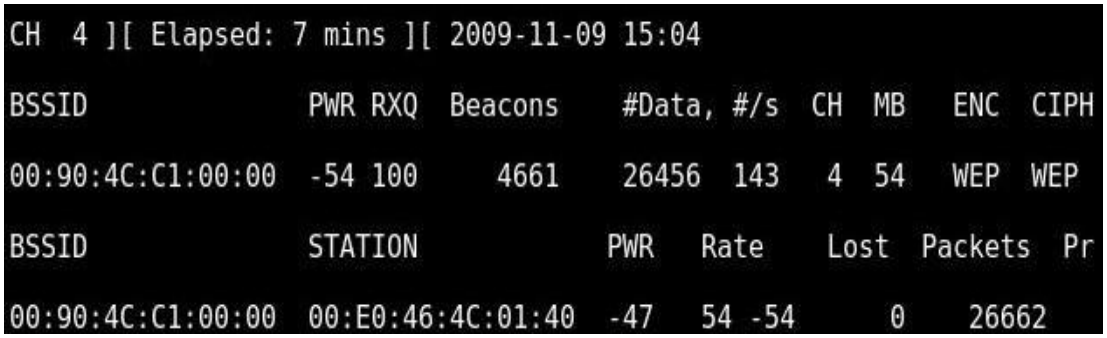


Рис. 83. Сбор пакетов

Для осуществления подбора ключа нам достаточно набрать от 10 000 до 25 000 пакетов. Дождавшись нужного количества пакетов, можно приостановить запись и приступить к перебору пароля. Программа aircrack-ng предназначенная для взлома ключей шифрования, которая перебирает комбинации до того момента, пока конечная сумма не совпадет. Так же она использует еще один метод, это подбор по словарю, но первый метод считается наиболее эффективным и быстрым.

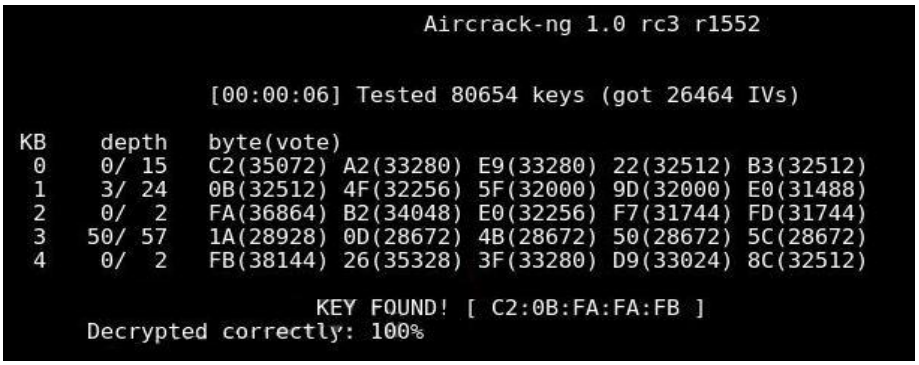


Рис. 84. Нахождение ключа

Подбор ключа занял 15 минут. Т.е. злоумышленнику не составит труда проникнуть в беспроводную сеть.

При изучении программного кода программы aircrack-ng было замечена незначительная ошибка в проверке пакетов, полученных при сборе из эфира. То есть в программе не была описана проверка пакетов на их точное шифрование, т.е если в начале программа проверяла, что пакеты именно ARP пакеты и записывала их в отдельный файл, то при дальнейшей работы программа не проверяла ни длину пакета ни его содержимое, а просто записывала их в отдельный файл. Что бы защитить сеть на WEP шифровании, надо внедрить в эфир пакеты с WPA шифрованием. Так сказать запутать программу, что бы злоумышленник применял методы атак для другого метода шифрования. Для этого нам понадобится еще один компьютер с wi-fi адаптером, который бы выкидывал ‒мусорный трафик‖ под точно таким же MAC-адресом как у точки, как было описано раньше, подделать MAC-адрес не так уж и сложно.

Для получения ключа WPA/WPA2 шифрования, пойдет упор на лобовой метод атаки, то есть перебор всех возможных вариантов ключа. Но мы же не знаем где начало пакетов, я имею ввиду тот счетчик который отправляет, пакеты по очередности. Что бы скинуть счетчик, непосредственно нужно провести атаку на пользователя, тогда же точке придется повторно авторизировать пользователя методом 4 этапного рукопожатия.

Нам не надо собирать множество пакетов из эфира - достаточно поймать первый кадр в котором передана информация о том, что пользователь авторизировался правильным ключом и может работать, принимая и расшифровывая пакеты. В первом же пакете и собранна вся информация о ключе. Тогда и проводить атаку мы будем непосредственно на пойманный пакет

2. Получение ключа WPA/WPA2 шифрования. Для проведения данного рода атак необходимо:

a. Задать самостоятельно ключ шифрования в настройках точки доступа

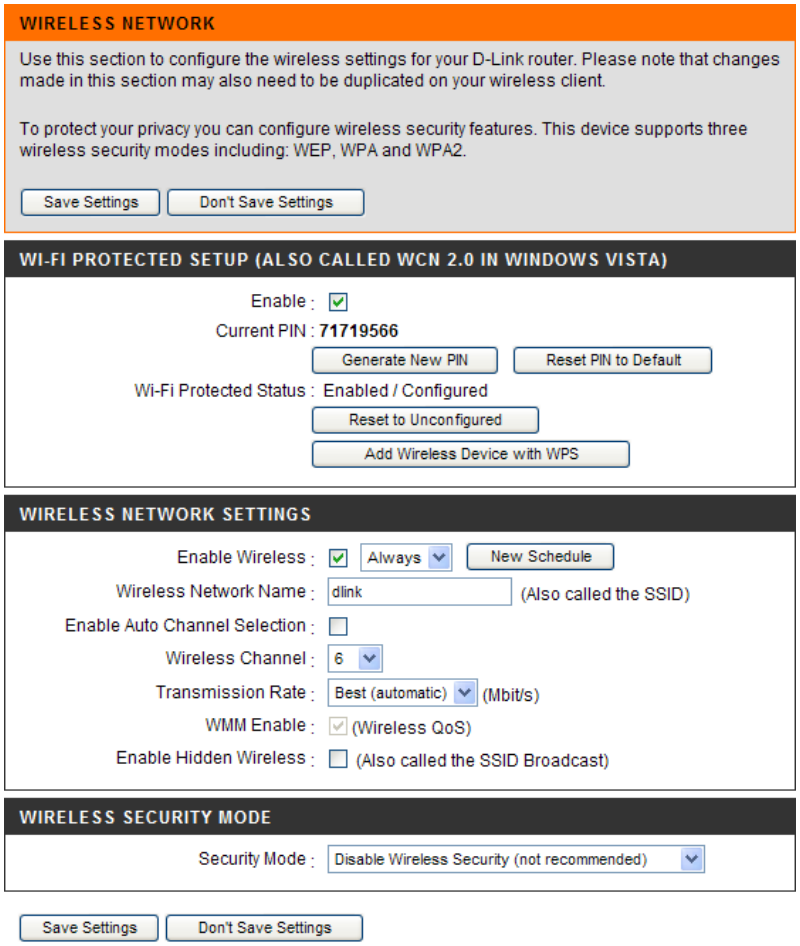


Рис. 85. Настройка точки доступа

Защита беспроводных сетей.

Большинство беспроводных сетей никак не защищены от проникновения злоумышленника. Для обеспечения защиты беспроводного соединения необходимо учитывать множество факторов. Поскольку оборудования для беспроводных соединений постепенно дешевеет, то для большего числа пользователей становится возможным подключение к этой сети.

1. Максимальный уровень безопасности обеспечит применение VPN — используйте эту технологию в корпоративных сетях.

2. Если есть возможность использовать 802.1X (например, точка доступа поддерживает, имеется RADIUS-сервер) — воспользуйтесь ей (впрочем, уязвимости есть и у 802.1X).

3. Перед покупкой сетевого устройства внимательно ознакомьтесь с документацией. Узнайте, какие протоколы или технологии шифрования ими

поддерживаются. Проверьте, поддерживает ли эти технологии шифрования ваша ОС. Если нет, то скачайте апдейты на сайте разработчика. Если ряд технологий не поддерживается со стороны ОС, то это должно поддерживаться на уровне драйверов.

4. Обязательно включать шифрование трафика.

5. Управлять доступом клиентов по MAC-адресам (Media Access Control, в настройках может называться Access List). Хотя MAC-адрес и можно подменить, тем не менее это дополнительный барьер на пути злоумышленника.

6. Запретить трансляцию в эфир идентификатора SSID, используйте эту возможность (опция может называться «closed network»), но и в этом случае SSID может быть перехвачен при подключении легитимного клиента.

7. Располагать антенну как можно дальше от окна, внешней стены здания, а также ограничивайте мощность радиоизлучения, чтобы снизитьвероятность подключения «с улицы».

8. Используйте направленные антенны, не используйте радиоканал по умолчанию.

9. При установке драйверов сетевых устройств предлагается выбор между технологиями шифрования WEP, WEP/WPA (средний вариант), WPA, выбирайте WPA (в малых сетях можно использовать режим Pre-Shared Key (PSK)).

10. Всегда используйте максимально длинные ключи. 128-бит — это минимум (но если в сети есть карты 40/64 бит, то в этом случае с ними вы не сможете соединиться). Никогда не прописывайте в настройках простые, «дефолтные» или очевидные ключи и пароли (день рождения, 12345), периодически их меняйте (в настройках обычно имеется удобный выбор из четырѐх заранее заданных ключей — сообщите клиентам о том, в какой день недели какой ключ используется).

11. Не давайте никому информации о том, каким образом и с какими паролями вы подключаетесь (если используются пароли). Искажение данных или их воровство, а также прослушивание траффика путем внедрения в передаваемый поток — очень трудоемкая задача при условиях, что применяются длинные динамически изменяющиеся ключи. Поэтому хакерам проще использовать человеческий фактор.

12. Если вы используете статические ключи и пароли, позаботьтесь об их частой смене. Делать это лучше одному человеку — администратору.

13. Обязательно используйте сложный пароль для доступа к настройкам точки доступа.

14. По возможности не используйте в беспроводных сетях протокол TCP/IP

для организации папок, файлов и принтеров общего доступа. Организация разделяемых ресурсов средствами NetBEUI в данном случае безопаснее. Не разрешайте гостевой доступ к ресурсам общего доступа, используйте длинные сложные пароли.

15. По возможности не используйте в беспроводной сети DHCP — вручную распределить статические IP-адреса между легитимными клиентами безопаснее.

16. На всех ПК внутри беспроводной сети установите файерволлы, старайтесь не устанавливать точку доступа вне брандмауэра, используйте минимум протоколов внутри WLAN (например, только HTTP и SMTP). Дело в том, что в корпоративных сетях файерволл стоит обычно один — на выходе в интернет, взломщик же, получивший доступ через Wi-Fi, может попасть в LAN, минуя корпоративный файерволл.

17. Регулярно исследуйте уязвимости своей сети с помощью специализированных сканеров безопасности (в том числе хакерских типа NetStumbler), обновляйте прошивки и драйвера устройств, устанавливайте заплатки для Windows.

RADIUS-протокол предназначен для работы в связке с сервером аутентификации, в качестве которого обычно выступает RADIUS-сервер. В этом случае беспроводные точки доступа работают в enterprise-режиме.

Если в сети отсутствует RADIUS-сервер, то роль сервера аутентификации выполняет сама точка доступа - так называемый режим WPA-PSK (pre-shared key, общий ключ). В этом режиме в настройках всех точек доступа заранее прописывается общий ключ. Он же прописывается и на клиентских беспроводных устройствах. Такой метод защиты тоже довольно секьюрен (относительно WEP), очень не удобен с точки зрения управления. PSK-ключ требуется прописывать на всех беспроводных устройствах, пользователи беспроводных устройств его могут видеть. Если потребуется заблокировать доступ какому-то клиенту в сеть, придется заново прописывать новый PSK на всех устройствах сети и так далее. Другими словами, режим WPA-PSK подходит для домашней сети и, возможно, небольшого офиса, но не более того.Для того, чтобы пользователи проектируемой сети имели разграниченный доступ (в зависимости от логина и пароля), а также для того, чтобы избежать атак извне, необходимо иметь отдельный сервер авторизации (AAA-сервер). В качестве такого сервера, в нашей сети будет выступать RADIUS сервер.

3. Порядок выполнения работы

1. Ознакомится с теорией по беспроводным сетям стандарта IEEE 802.11
2. Взять у преподавателя ключа шифрования для точки доступа;
3. Исследование производительности точки доступа:

3.1. Запустить программу NetIQ Chariot.

3.2. Открыть окно Add an Endpoint Pair.

3.3 В окне Add an Endpoint Pair в строках Endpoint 1 и Endpoint 2 написать MAC адреса компьютеров производящих измерения.

3.3. Выбрать скрипт throughput.

3.4. В настройках скрпита выбираем поле size_file и изменяем его значение согласно заданию.

3.5. Произвести измерения с различными значениями size_file и записать их в таблицу.

Размер поля size_file				
Скорость передачи данных				
Время отклика				

3.6. Построить графики зависимости скорости передачи данных от величины передаваемого пакета.

3.7. Сделать выводы.

3.8. .Шифрование:

4.1. Запустить программу NetIQ Chariot.

4.2. Сделать размер отправляемого файла 1500 бит.

4.3. Зайти в настройки точки доступа.

4.4. Включит режим шифрования в соответствии с заданием.

4.5. Произвести измерения.

4.6. Поменять режим шифрования.

4.7. Повторить пункты 4.4-4.6 в соответствии с заданием

4.8. По полученным результатам заполнить таблицу:

Режим шифрования				
Скорость передачи данных				
Время отклика				

4.10. Построить на одном графике скорости передачи данных для различных режимов шифрования.

4.11. Сделать выводы.

5. Фрагментация фреймов:

5.1. Открыть настройки точки доступа.

5.2. Перейти на вкладку Advanced Wireless, в поле Fragmentation ввести соответствующее значение.

5.3. По полученным результатами заполнить таблицу:

Размер фрейма				
Скорость передачи данных				
Время отклика				

5.4 Построить график зависимости скорости передачи данных от размера фрейм.

6. Сделать выводы.

7. Взлом ключа шифрования WEP:

7.1. Ввести в настройках точки доступа ключ шифрования.

7.2. Открыть программу aircrack-ng.

7.3. Перевести адаптер в режим мониторинга.

6.6. Заменить MAC-адрес адаптера.

6.7. Произвести поиск сети с шифрование данных WEP .

6.8. Произвести набор пакетов от 10000 до 25000.

6.9. Произвести подбор ключа.

6.10. Произвести анализ полученных данных

7 Взлом ключа шифрования WPA/WPA2:

7.1. Перевести адаптер в режим мониторинга.

7.2. Выбрать пользователя для атаки и посылать пакеты к точке доступа под MAC – адреса пользователя

7.3. Перехватить покаты авторизации

7.4. При помощи программы aircrack-ng произвести подбор ключа.

7.5. Произвести анализ полученных данных

4.Рекомендуемая литература

1. Педжман Рошан, Джонатан Лиэри Основы построения беспроводных локальных сетей стандарта 802.11. – М.: Издательский дом –Вильямс‖, 2004. – 304 с.

2. Wi-Fi. Беспроводная сеть / Джон Росс ; пер. с англ. В. А. Ветлужских. - М. : НТ Пресс, 2007. - 320 с.

3. Владимиров А.А., Гавриленхо К.В., Михайловский А.А. Wi-Фу: «боевые» приемы взлома и защиты беспроводных сетей. НТ Пресс. 2005.

Лабораторная работа 3. Исследование методов аналогового скремблирования

Вступление человечества в 21 век знаменуется бурным развитием информационных технологий во всех сферах общественной жизни. Информация все в большей мере становится стратегическим ресурсом государства, производительной силой и дорогим товаром. Это не может не вызывать стремления государств, организаций и отдельных граждан получить преимущества за счет овладения информацией, недоступной оппонентам, а также за счет нанесения ущерба информационным ресурсам противника (конкурента) и защиты своих информационных ресурсов.

Безопасность связи при передаче речевых сообщений основывается на использовании большого количества различных методов закрытия сообщений, меняющих характеристики речи таким образом, что она становится неразборчивой и неузнаваемой для подслушивающего лица, перехватившего закрытое речевое сообщение. При этом главной целью при разработке систем передачи речи является сохранение тех ее характеристик, которые наиболее важны для восприятия слушателем [1].

В речевых системах связи известно два основных метода закрытия речевых сигналов, различающихся по способу передачи по каналам связи:

— аналоговое скремблирование;

— цифровое скремблирование (дискретизация речи с последующим шифрованием) [2].

Каждый из этих методов имеет свои достоинства и недостатки, но рассмотрим аналоговое скремблирование

В последнее время сфера применения скремблирующих алгоритмов значительно сократилась. Это объясняется в первую очередь снижением объемов побитной последовательной передачи информации, для защиты которой были разработаны данные алгоритмы. Практически повсеместно в современных системах применяются сети с коммутацией пакетов, для поддержания конфиденциальности которой используются блочные шифры, а их криптостойкость превосходит, и порой довольно значительно, криптостойкость скремблеров. Тем не менее, знать основы функционирования скремблеров, как этап в истории защиты речевой информации, необходимо. Во-первых, аналоговые до сих пор используются там, где невозможно, по ряду причин, использовать другие средства. Во-вторых, фундаментальные принципы и понятия, заложенные в скремблирующие алгоритмы, также распространяются и на другие методы защиты речевых сообщений [2].

Аналоговые скремблеры

Под аналоговым скремблированием понимается изменение характеристик речевого сигнала так, чтобы полученный сигнал, обладая свойствами речевой неразборчивости, занимал такую же полосу частот, что и исходный открытый сигнал. При использовании этого метода в

закрытом сигнале присутствуют фрагменты исходного открытого речевого сообщения, преобразованные в частотной или временной областях. Это означает, что злоумышленники могут попытаться перехватить и проанализировать передаваемую информацию на уровне звуковых сигналов. Поэтому ранее считалось, что, несмотря на высокое качество и разборчивость восстанавливаемой речи, аналоговые скремблеры могут обеспечивать лишь низкую или среднюю, по сравнению с цифровыми системами, степень закрытия. Однако новейшие алгоритмы аналогового скремблирования способны обеспечить не только средний, но очень высокий уровень закрытия [1].

Системы скремблирования подразделяются на два класса:

— статические, схема шифрования которых остается неизменной в течение всей передачи сообщения; такие системы не обладают сколько-нибудь значительной стойкостью, но вполне приемлемы как модели реальных систем скремблирования;

— динамические, с дополнительным повышением уровня закрытия информации за счет изменения параметров преобразования сигнала во времени при постоянном генерировании кодовых подстановок в ходе передачи/приема; такие скремблеры принято обозначать термином роллинговые скремблеры.

Аналоговое скремблирование обеспечивает меньшую степень закрытия речевых сигналов по сравнению с цифровыми методами шифрования, однако при практической реализации аналоговые скремблеры более просты, дешевы, применимы в большинстве случаев в стандартных телефонных каналах с полосой 3 кГц и обеспечивают коммерческое качество восстановления речевого сигнала с гарантией достаточно высокой стойкости закрытия речи, передаваемой по каналу связи.

Большинство структур безопасности оснащено профессиональными средствами УКВ радиосвязи зарубежных фирм таких, как Motorola, Kenwood, Icom и др., использующими аналоговые виды модуляции сигнала (частотный или фазовый). Для подобного рода радиосредств в подавляющем большинстве в качестве устройств защиты информации применяются аналоговые речевые скремблеры.

Аналоговые скремблеры преобразуют исходный речевой сигнал посредством изменения его амплитудных, частотных и временных параметров в различных комбинациях. Скремблированный сигнал может быть передан по каналу связи в той же полосе частот, что и исходный, открытый [1].

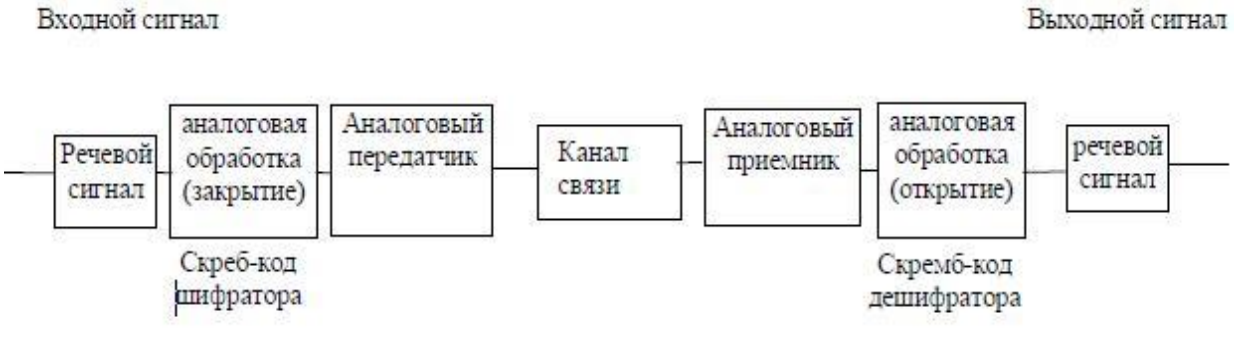


Рис.1 – Обобщенная структурная схема аналогового скремблера

Виды преобразований аналоговых скремблеров

При скремблировании возможно преобразование речевого сигнала по трем параметрам: амплитуде, частоте и времени. Однако в системах подвижной радиосвязи практическое применение нашли в основном частотные и временные методы преобразования сигнала, а также их комбинации. Возможные помехи в радиоканале существенно затрудняют точное восстановление амплитуды речевого сигнала, в связи с чем амплитудные преобразования при скремблировании практически не применяются [1].

При частотных преобразованиях сигнала в средствах подвижной радиосвязи чаще всего используются следующие виды скремблирования:

— частотная инверсия сигнала (преобразование спектра сигнала с помощью гетеродина и фильтра);

— разбиение полосы частот речевого сигнала на несколько поддиапазонов и частотная инверсия спектра в каждом относительно средней частоты поддиапазона;

— разбиение полосы частоты речевого сигнала на несколько поддиапазонов и их частотные перестановки;

— разбиение полосы частоты речевого сигнала на несколько поддиапазонов, их частотные перестановки и частотная инверсия спектра в каждом относительно средней частоты поддиапазона [1].

При временных преобразованиях производится разбиение сигнала на речевые сегменты и применение к ним операций инверсии и перестановок во времени. При этом используются следующие способы закрытия:

— инверсия по времени протяженных сегментов речи;

— временные перестановки коротких фрагментов в сегментах речевого сигнала;

— временные перестановки коротких фрагментов и их инверсия в сегментах речевого сигнала [1].

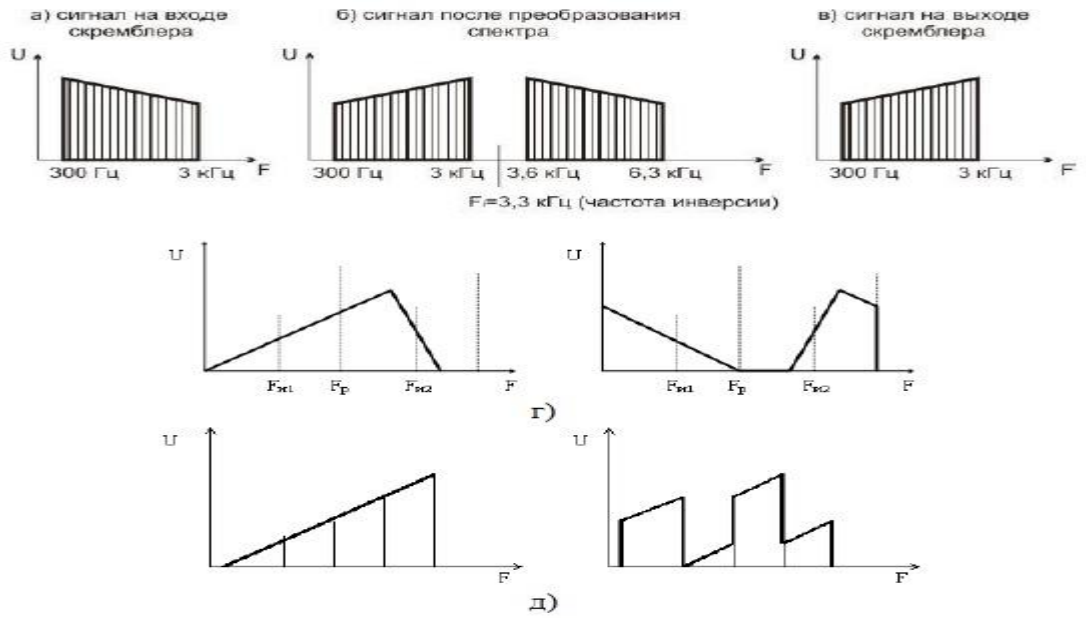


Рис. 2. Инверсия спектра при скремблировании сигнала – а), б), в); последовательность преобразований; – г); частотные перестановки фрагментов спектра сигнала

В скремблерах с временной перестановкой сигнал делится на сегменты и фрагменты (см. рисунок 3.2) над которыми осуществляется перестановка или инверсия, причем сегмент (кадр) может быть, как фиксированным, так и скользящим. Такие скремблеры обеспечивают ограниченный уровень закрытия, зависящий от длительности фрагментов в сегментах, а также создают значительные поддержки при работе, требуют дополнительной синхронизации, поэтому их практическое использование затруднено, но они весьма полезны в системах, где требует простота устройства [1].

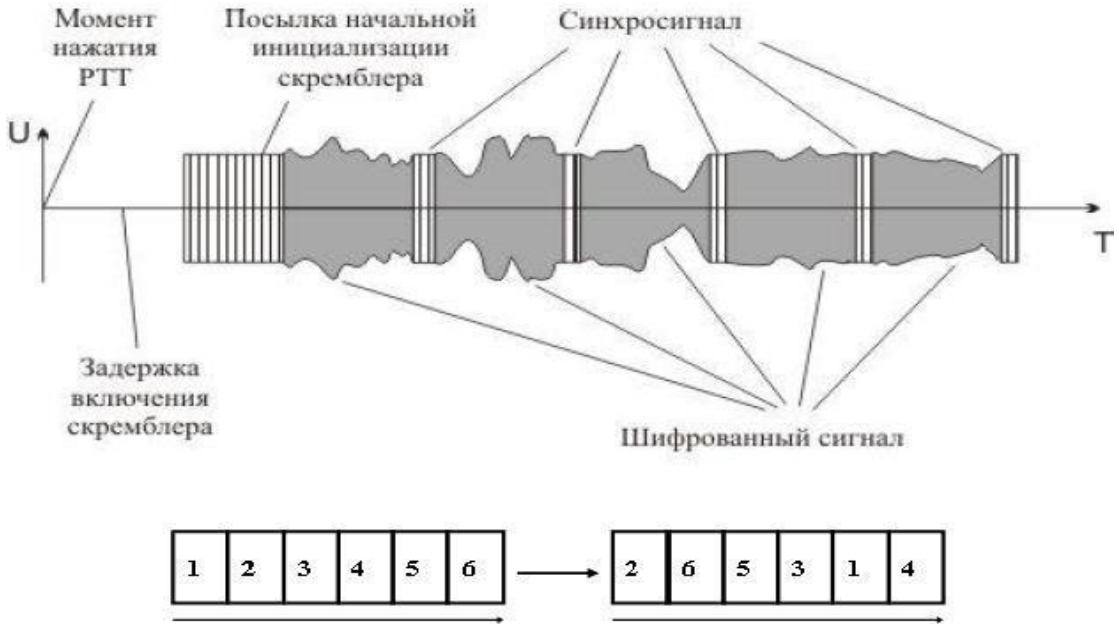


Рис. 3. Скремблированный сигнал с перестановками во времени фрагментов сегмента речевого сигнала

Комбинированные методы преобразования сигнала предполагают использование одновременно нескольких различных способов скремблирования (как частотных, так и

временных), число которых ограничивается, как правило, возможностями технической реализации аналоговых скремблеров [6].

Динамические скремблеры существенно дороже скремблеров с фиксированными параметрами преобразования сигнала, сильнее влияют на характеристики радиосредств и требуют начальной синхронизации. Однако их применение действительно затрудняет возможности перехвата переговоров, в особенности в реальном масштабе времени. Это объясняется тем, что изменение ключевых параметров во времени теоретически делает возможным резкое увеличение количества ключей. Ключом может быть начальное значение генератора псевдослучайной последовательности, в соответствии с которой меняется определенный ключевой параметр [6].

Временные преобразования сигнала в сочетании с изменением ключевых параметров во времени достаточно сложны для реализации и требуют относительно длительной синхронизации, поэтому они пока не нашли свое применение в роллинговых скремблерах. Для способов частотного преобразования сигнала изменяемыми ключевыми параметрами могут быть частота инверсии (для частотного инвертора), частота разбиения полосы сигнала (для полосно-сдвигового инвертора), комбинация частотной перестановки поддиапазонов сигнала (для полосового скремблера). Большинство известных моделей роллинговых скремблеров используют наиболее простой принцип спектрального преобразования – частотный инвертор с изменением частоты инверсии сигнала во времени [2].

Технические характеристики

Основными техническими характеристиками аналоговых скремблеров являются уровень закрытия информации, остаточная разборчивость и качество восстановления сигнала.

Наиболее важной характеристикой скремблера для пользователя, желающего обеспечить защиту информации в своих каналах связи, является уровень закрытия информации. Для сложных цифровых систем передачи речи и данных понятие уровня закрытия строго регламентируется и определяется криптографической стойкостью информации, то для аналоговых скремблеров (особенно в системах подвижной радиосвязи) данное понятие носит условный характер, так как к настоящему времени на этот счет не выработано четких стандартов или правил. В ряде случаев в качестве критериев уровня закрытия информации при сравнении различных средств подвижной радиосвязи с аналоговым скремблированием можно использовать количество ключевых параметров и количество возможных ключей скремблера [1].

Под ключевым параметром аналогового скремблера обычно понимают какой-либо параметр преобразования речевого сигнала, значение которого необходимо знать для осуществления обратного преобразования сигнала на приемной стороне. Ключом аналогового скремблера (по аналогии с цифровыми системами шифрования), как правило, называют конкретное секретное состояние некоторых параметров преобразования речевого сигнала. Количество ключей скремблера определяется множеством всевозможных значений ключа. Для скремблеров с одним ключевым параметром оно определяется числом возможных состояний

этого параметра, для скремблеров с несколькими ключевыми параметрами - количеством возможных комбинаций значений этих параметров (как правило, произведением чисел состояний всех ключевых параметров) [1].

Обзор известных моделей скремблеров

Наибольшее количество известных моделей скремблеров реализуют частотную инверсию сигнала. Все они имеют близкие параметры. Одними из первых на отечественном рынке появились модели скремблеров фирмы Selectone (ST-20 и ST-022), работающие в диапазоне частот 300-2400 Гц и обеспечивающие инверсию сигнала относительно 8 возможных номиналов частот в диапазоне от 2,6 до 3,7 КГц (частота инверсии устанавливается программно).

Простейшие модели скремблеров фирмы Transcrypt SC20-400 и SC20-401 обладают характеристиками, аналогичными ST-20 и ST-022; речевой диапазон частот, 4 варианта частоты инверсии [1].

Сравнительная характеристика скремблеров по основным параметрам приведена в таблице 4.1.

Более сложное преобразование сигнала предлагают полосно-сдвиговые инверторы, разработанные НТЦ "ИНТЕР-ВОК" Принцип работы микросборок 04ХК011 ("Сонет"), 04ХК012, 04ХК014А, 04ХК015А, 04ХК017А состоит в разделении речевого спектра на две части, низкочастотную и высокочастотную, каждая из которых разворачивается вокруг своих средних частот. Все они работают в диапазоне речевых частот - 300-3400 Гц. Указанные скремблеры обладают повышенной по сравнению с частотными инверторами степенью закрытия информации. В технических данных указывается, что скремблеры обеспечивают остаточную разборчивость речи не более 10 %. В то же время гарантируется сохранение высокого качества речи при прослушивании с помощью радиостанции, оснащенной аналогичным скремблером (сохранение 1 класса разборчивости при измерении по методике ГОСТ 16600-72) [1].

Известны скремблеры для эффективной защиты телефонных переговоров в сетях, работающих по GSM стандарту. Специально разработанный скремблер GUARD GSM, будучи эконом-вариантом, отлично маскирует речь, передаваемую по каналам GSM связи. Данное устройство соединяется с сотовым телефоном по проводной гарнитуре и имеет небольшие размеры [1].

Принцип работы данного скремблера основан на первоначальном разрушении и временной перестановки звука на передающей стороне с его последующим восстановлением на принимающей стороне. Этот процесс дуплексный. Начало разговора, как правило, начинается в открытом режиме и далее по обоюдной команде устройства, переключаются в режим скремблирования [1].

Программная реализация виртуальной модели скремблера

Программную реализацию виртуальной модели скремблера можно выполнить в среде LabVIEW, Simulink или на одном из языков объектно-ориентированного программирования. Приведенная реализация программной модели выполнена в виде виртуальных приборов, созданных в среде LabVIEW. Данная программная система моделирует скремблер работающий с телефонным каналом связи на частоте от 200 Гц до 3,4 КГц. В модели представлены несколько видов операций скремблирования [1]:

— временной статический скремблер, производящий операции над блоками фиксированного размера с фиксированным порядком перестановки;

— временной скремблер с инверсией;

— полосовой частотный статический скремблер, производящий операции

— над блоками фиксированного размера с фиксированным порядком перестановки, использует фильтрацию, инверсию спектра, преобразование частоты;

— полосовой частотный статический скремблер, производящий операции над блоками фиксированного размера с фиксированным порядком перестановки, использует прямое и обратное БПФ;

— инвертирующий частотный скремблер, производящий операции над блоками фиксированного размера, использующий прямое и обратное БПФ, инверсия идет относительно средней точки спектральной последовательности.

В качестве исходных сигналов скремблера использованы звуковые файлы в формате WAV, записанные с частотой дискретизации 8 КГц в формате моно. Скремблер может выполнять загрузку звуковых файлов в формате WAV, их скремблирование или дескремблирование по одному из нескольких алгоритмов с изменяемыми параметрами, запись результата в файлы в формате WAV, а также визуализировать и озвучить как исходный, так и обработанный звук [1].

Временное скремблирование

Разработан виртуальный прибор для осуществления временных видов скремблирования/дескремблирования, лицевая панель которого для осуществления скремблирования речевого сигнала во временной области на основе его инверсии приведена на рис.5, а фрагмент диаграммной панели – на рис .6. На лицевую панель прибора выведены: временные диаграммы входного сигнала, скремблированного сигнала, все необходимые регулировочные ручки для настроек параметров скремблера и органы индикации параметров речевого сигнала.

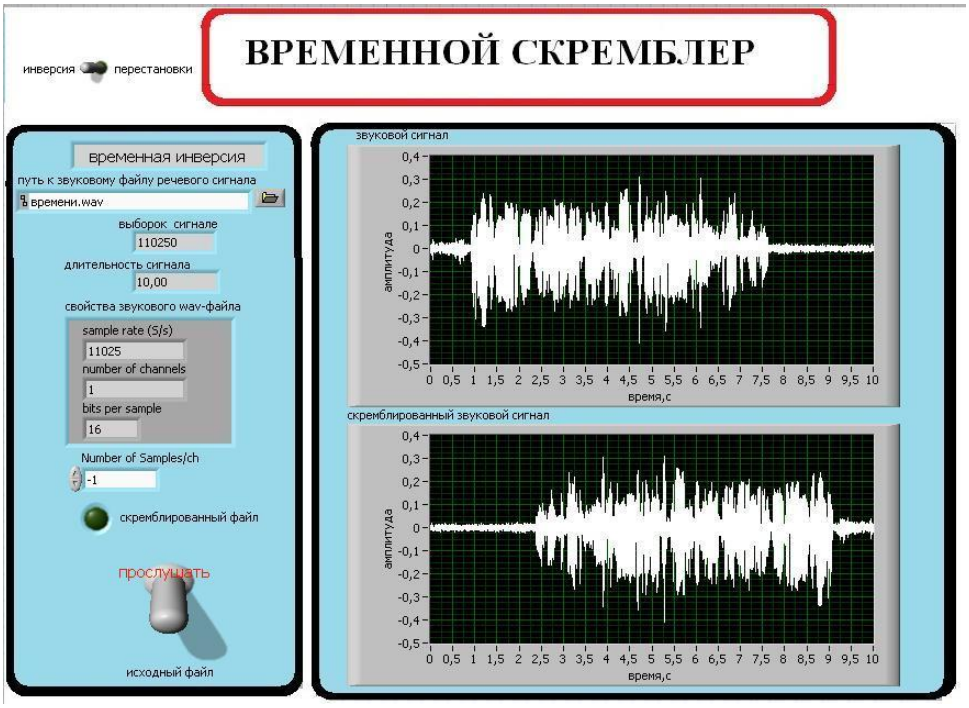


Рис. 4 – Лицевая панель виртуального прибора для осуществления скремблирования речевого сигнала на основе временной инверсии

Как видно, на диаграммной панели использованы вложенные приборы для чтения звукового файла с диска и для записи скремблированного сигнала в файл, а также блоки для преобразований типов данных для осуществления временной инверсии. Лицевая панель виртуального прибора при переключении тумблера для осуществления скремблирования речевого сигнала во временной области на основе перестановок временных сегментов сигнала приведена на рис.3, а фрагмент диаграммной панели – на рис.4. Как видно, на диаграммной панели использованы вложенные приборы для чтения звукового файла с диска, осуществления временных перестановок с фиксированным ключом и для записи скремблированного сигнала в файл. Временные перестановки на приведенном виртуальном приборе на рисунке 3 выбраны с фиксированным ключом: 87214365, где цифры обозначаю номер временного фрагмента в сегменте исходного речевого сигнала [1].

При программировании алгоритма на диаграммной панели можно использовать case-структуру для выбора временной инверсии и временных перестановок. Дальнейшая модернизация скремблера предусматривает задание ключей скремблирования при перестановке временных сегментов с помощью case-структуры. Это же касается и модели дескремблера.

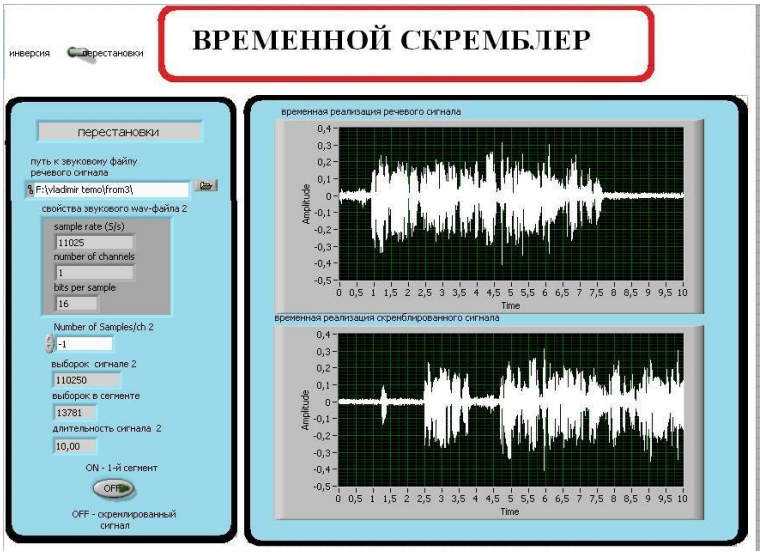


Рис. 5 – Лицевая панель виртуального прибора для осуществления временного скремблирования речевого сигнала с перестановками

Виртуальный прибор позволяет при каскадном наращивании разработанных библиотечных модулей временного скремблирования/ дескремблирования реализовать код скремблирования любой сложности.

— Необходимо учитывать при разработке прибора, что скремблирование и дескремблирование вносит задержки в передаче речевого сигнала.

— Основным источником шума при скремблировании и дескремблировании является длительность элементарного временного сегмента при разбиении, которая в пределе равна шагу дискретизации сигнала.

— При учете всех выше сказанных особенностях и должных настроек элементов виртуального прибора, обеспечивается хорошее закрытие информации, а затем её восстановление при дескремблировании с хорошей словесной разборчивостью [1].

Частотное скремблирование

Реализовать виртуальные приборы для осуществления частотного полосового скремблирования можно различными способами: параллельно-последовательной обработкой с преобразованием частоты и фильтрацией, параллельной обработкой с преобразованием частоты и фильтрацией, параллельной обработкой с использованием БПФ и др. Приведем некоторые варианты реализации первых двух способов.

Параллельно-последовательная обработка при осуществлении частотно скремблирования предполагает разбиение частотного диапазона спектра сигнала на две полосы, осуществление их перестановок и инверсии спектра, а затем последовательно к каждому частотному диапазону применения аналогичных преобразований. Таким образом, можно последовательно увеличивать число частотных полос при разбиении спектра в 2 раза (2 полосы, 4, 8, 16, и т.д.), тем самым, увеличивая количество ключей скремблирования. Созданный виртуальный прибор, как один из вариантов для осуществления заданного вида (разбиение на 4

полосы) частотного полосового скремблирования речевого сигнала, позволяет отображать временные реализации сигналов и их спектров, а также прослушивать речевой сигнал как до скремблирования, так и после осуществления скремблирования и дескремблирования [1].

Лицевая панель виртуального прибора для осуществления скремблирования речевого сигнала в частотной области в диапазоне частот от 300Гц до 3400Гц приведена на рисунке 7.7, а диаграммная панель – на рисунке 7.8.

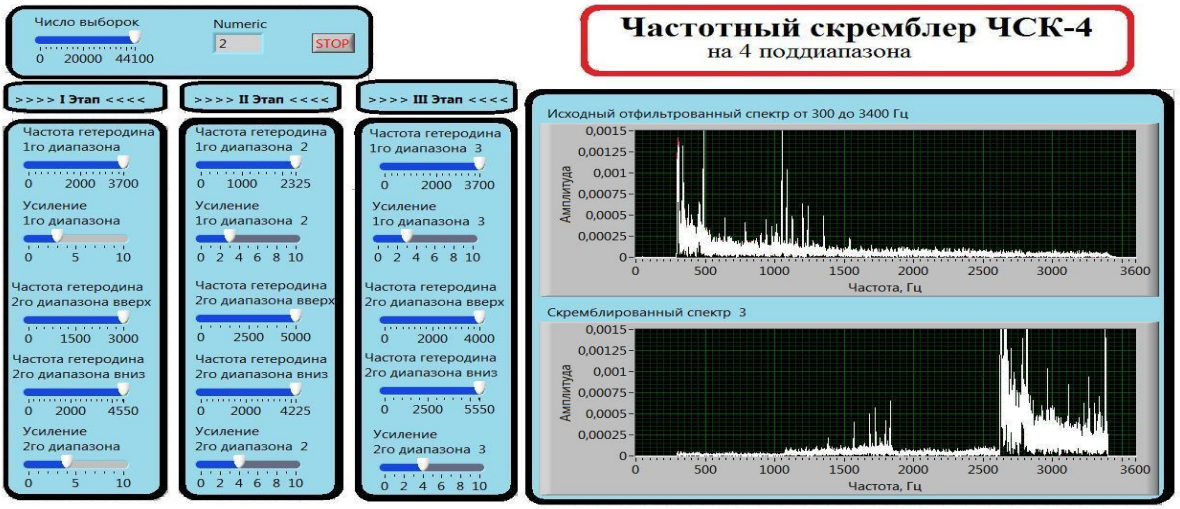


Рис. 6. Лицевая панель виртуального прибора частотного скремблирования речевого сигнала

На лицевую панель прибора выведены: спектр входного сигнала, отфильтрованного от 300Гц до 3400Гц; спектр скремблированного сигнала и все необходимые регулировочные ручки для настроек параметров скремблера. Как видно, на диаграммной панели использованы вложенные приборы для чтения звукового файла с диска, для осуществления преобразования частоты, для расчета спектра, для осуществления частотной фильтрации и для записи скремблированного сигнала в файл. Скремблер состоит из трёх последовательно соединенных смесителей с подключенными регулировочными ручками.

В качестве фильтра выбран эллиптический фильтр 6-го порядка из-за высокой крутизны АЧХ, сопровождающейся колебательным характером плоской вершины в полосе пропускания, и наличием боковых лепестков в полосе заграждения.

Каждый смеситель (см. рисунок 7.9) делит входной сигнал на два диапазона частот. На 1 этапе сигнал делится по 1550Гц. Первый диапазон (300Гц-1850Гц) инвертируется и перемещается (1850Гц-3400Гц) с помощью гетеродина с частотой 3700Гц (см. рисунок 7.10) [1].

Второй диапазон (1850Гц- 3400Гц) перемещается (300Гц-1850Гц) без инвертирования, с помощью двух гетеродинов с частотами 3000Гц и 4550Гц.

На выходе 1-го смесителя два диапазона складываются. В результате получается скремблированный сигнал I этапа на частотах от 300Гц до 3400Гц.

Далее сигнал поступает на вход второго смесителя, где делится на два диапазона. Первый диапазон (2625Гц-3400Гц) перемещается (300Гц-1075Гц) без инверсии, с помощью гетеродина с частотой 2325Гц.

Второй диапазон (300 Гц-2625Гц) перемещается (1075 Гц-3400Гц) без инверсии, с помощью двух гетеродинов с частотами 5000Гц и 4225Гц.

На выходе 2-го смесителя два диапазона складываются. В результате получается скремблированный сигнал II этапа на частотах от 300Гц до 3400Гц.

Далее сигнал поступает на вход третьего смесителя, где делится на два диапазона. Первый диапазон (300Гц-1850Гц) перемещается (1850Гц-3400Гц) с инверсией, с помощью гетеродина с частотой 3700Гц.

Второй диапазон (1850Гц-3400Гц) перемещается (300 Гц-1850Гц) без инверсии, с помощью двух гетеродинов с частотами 4000Гц и 5550Гц [1].

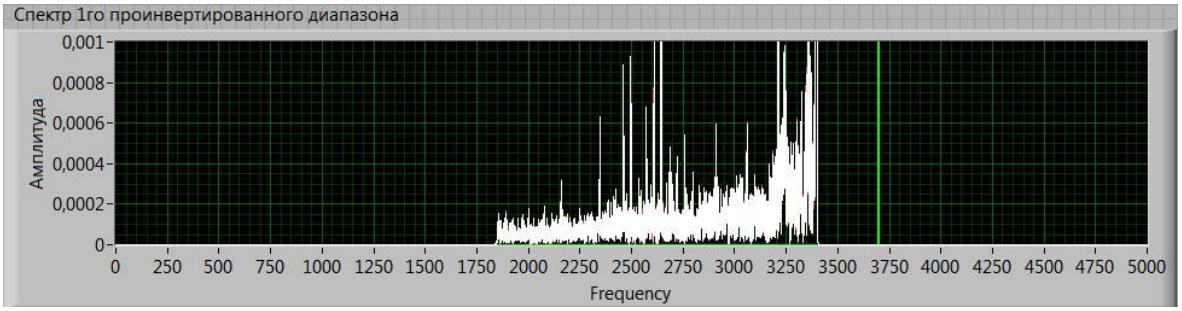


Рис. 7. Спектр первого проинвертированного диапазона

На выходе 3-го смесителя два диапазона складываются. В результате получается скремблированный сигнал III этапа на частотах от 300Гц до 3400Гц – спектр результирующего скремблированного сигнала (см. рисунок 6.11).

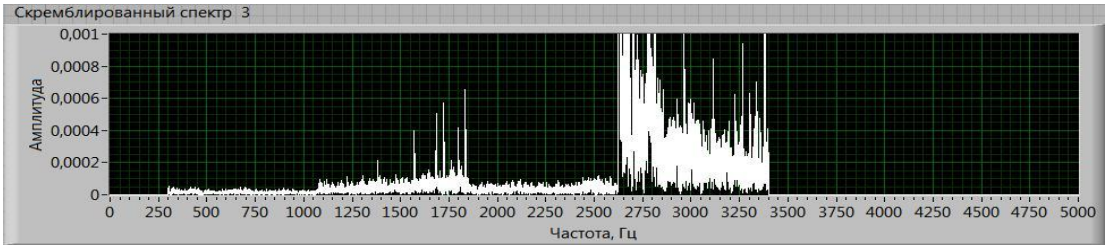


Рис. 8. Спектр скремблированного сигнала третьего этапа

Дескремблер. Для восстановления скремблированного речевого сигнала был спроектирован частотный дескремблер. На лицевую панель прибора выведены: спектр входного сигнала, отфильтрованного от 300Гц до 3400Гц; спектр дескремблированного

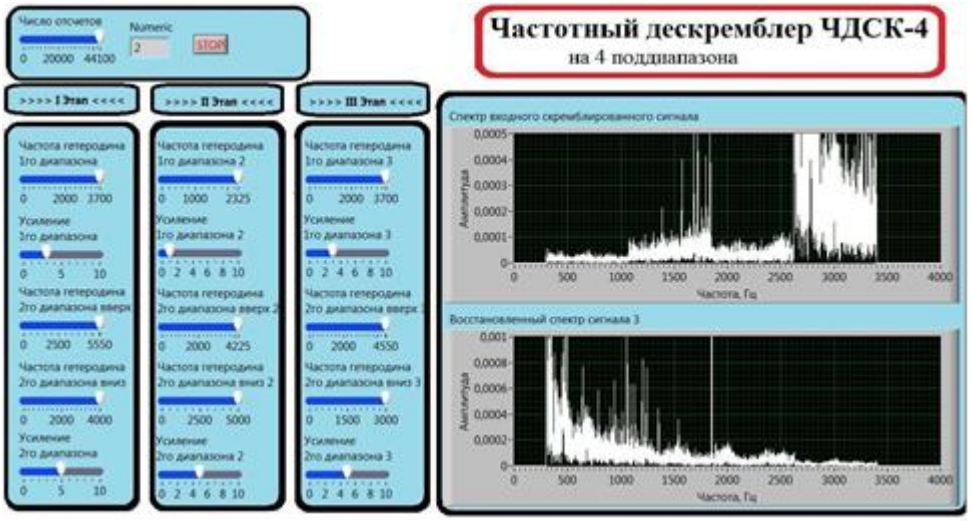


Рис. 9. Лицевая панель виртуального прибора дескремблера: три последовательно соединенных разделителя с регулировочными ручками

Каждый разделитель делит входной сигнал на два диапазона частот (см. рисунок 6.13). Сигнал поступает на вход первого разделителя, где первый диапазон (1850 Гц- 3400 Гц) инвертируется и перемещается (300 Гц-1850 Гц) с помощью гетеродина с частотой 3700Гц.

Второй диапазон (300 Гц-1850 Гц) перемещается (1850Гц-3400Гц) без инвертирования при помощи двух гетеродинов с частотами 5550 Гц и 4000 Гц

На выходе 1-го разделителя два диапазона складываются. В результате получается дескремблированный сигнал I этапа на частотах от 300Гц до 3400 Гц.

Далее сигнал поступает на вход второго разделителя, где делится на два диапазона. Первый диапазон (300Гц-1075Гц) перемещается (2625Гц-3400Гц) без инверсии, при помощи гетеродина с частотой 2325Гц.

Второй диапазон (1075Гц-3400Гц) перемещается (300 Гц-2625Гц) без инверсии, с помощью двух гетеродинов с частотами 4225 Гц и 5000 Гц [1].

На выходе 2-го разделителя два диапазона складываются. В результате получается дескремблированный сигнал II этапа на частотах от 300Гц до 3400Гц.

Далее сигнал поступает на вход третьего разделителя, где делится на два диапазона. Первый диапазон (1850Гц-3400Гц) перемещается (300 Гц-1850 Гц) с инверсией, с помощью гетеродина с частотой 3700 Гц.

Второй диапазон (300 Гц-1850Гц) перемещается (1850 Гц-3400Гц) без инверсии, с помощью двух гетеродинов с частотами 4550Гц и 3000Гц.

На выходе 3-го разделителя два диапазона складываются. В результате получается дескремблированный сигнал III этапа на частотах от 300Гц до 3400Гц.

Виртуальные приборы, осуществляющие аналоговое частотное скремблирование речевых

сигналов, а также библиотечные модули (вложенные виртуальные приборы) для частотного скремблирования и дескремблирования с перестановками и инверсией, позволяют при каскадном наращивании смесителей и разделителей, реализовать код скремблирования любой сложности.

Параллельная обработка при осуществлении частотно скремблирования предполагает разбиение частотного диапазона спектра сигнала на заданное число полос, осуществление их перестановок и инверсии спектра. Созданный виртуальный прибор, как один из вариантов для осуществления заданного вида (разбиение на 8 полос) частотного полосового скремблирования речевого сигнала, позволяет отображать временные реализации сигналов и их спектров, а также прослушивать речевой сигнал как до скремблирования, так и после осуществления скремблирования и дескремблирования [1].

Исходный спектр речевого сообщения разбивается на 8-поддиапазонов, как изображено на рисунок

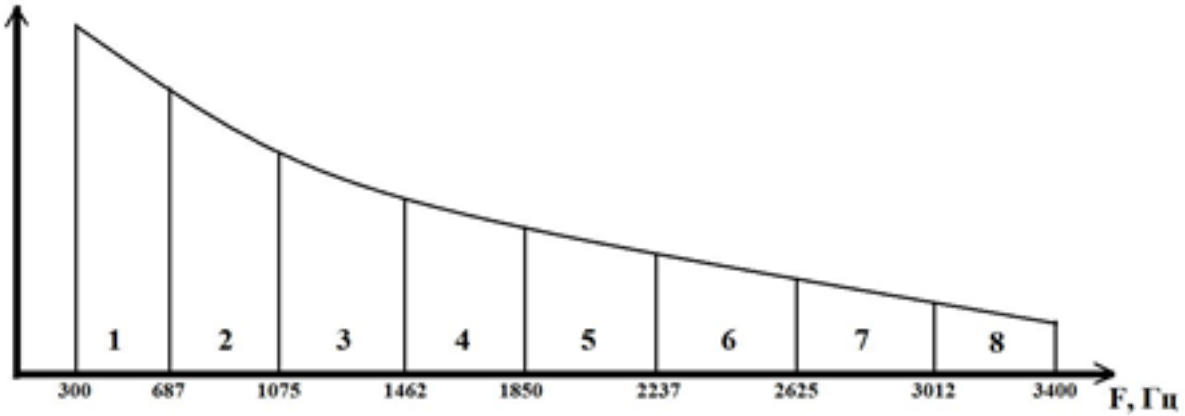


Рис. 9. Разбиение сигнала на 8 поддиапазонов

В зависимости от кода скремблера, диапазоны инвертируются и расставляются в определенном порядке, например, как показано на рисунке 6.16

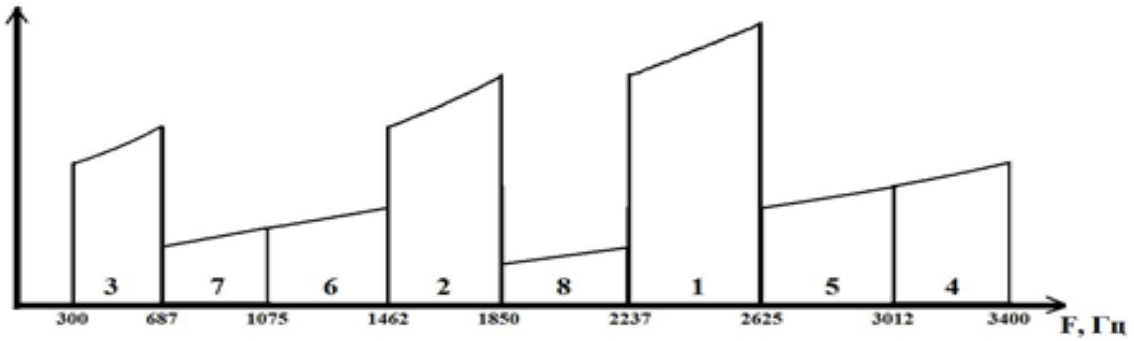


Рис. 10. Структура спектра после скремблирования

Диаграммная панель виртуального прибора для осуществления скремблирования речевого сигнала в частотной области в диапазоне частот от 300Гц до 3400Гц приведена на рисунке 7.17. На лицевую панель прибора выведены: спектр входного сигнала, отфильтрованного от 300Гц до 3400Гц; спектр скремблированного сигнала и все необходимые регулировочные ручки для настроек параметров скремблера [1]. Как видно, на диаграммной панели использованы вложенные приборы для чтения звукового файла с диска, для осуществления преобразования

частоты, для расчета спектра, для осуществления частотной фильтрации и для записи скремблированного сигнала в файл

Исходный сигнал подается на 8 полосовых эллиптических фильтров 7-го порядка, после чего, для того, чтобы проинвертировать спектр и перенести его в диапазон 2237 Гц – 2625 Гц, используется гетеродинное преобразование частоты с частотой генератора 2925 Гц, в результате. Теперь, чтобы отделить необходимую часть спектра, сигнал пропускается через полосовой эллиптический фильтр 6-го порядка. Параметры 2-го фильтра выбираются с меньшим порядком и большим частотным захватом фильтруемого спектра, чтобы меньше искажать форму сигнала [1].

Элемент (SubVI) является вложенным виртуальным прибором, который выполняет фильтрацию и перестановку поддиапазонов, формируя на выходе два канала. После усиления они объединяются в один канал, и сигнал записывается в файл. Диаграммная панель вложенного виртуального прибора представлена на рисунке

На выходе вторых фильтров используются сумматоры для объединения 1, 2, 4 и 7-го поддиапазонов во второй канал и объединения 3, 5, 6 и 8-го поддиапазонов в первый канал.

На рисунке представлена лицевая панель виртуального прибора скремблера, на котором видно, что поддиапазоны в скремблированном сигнале не взаимодействуют

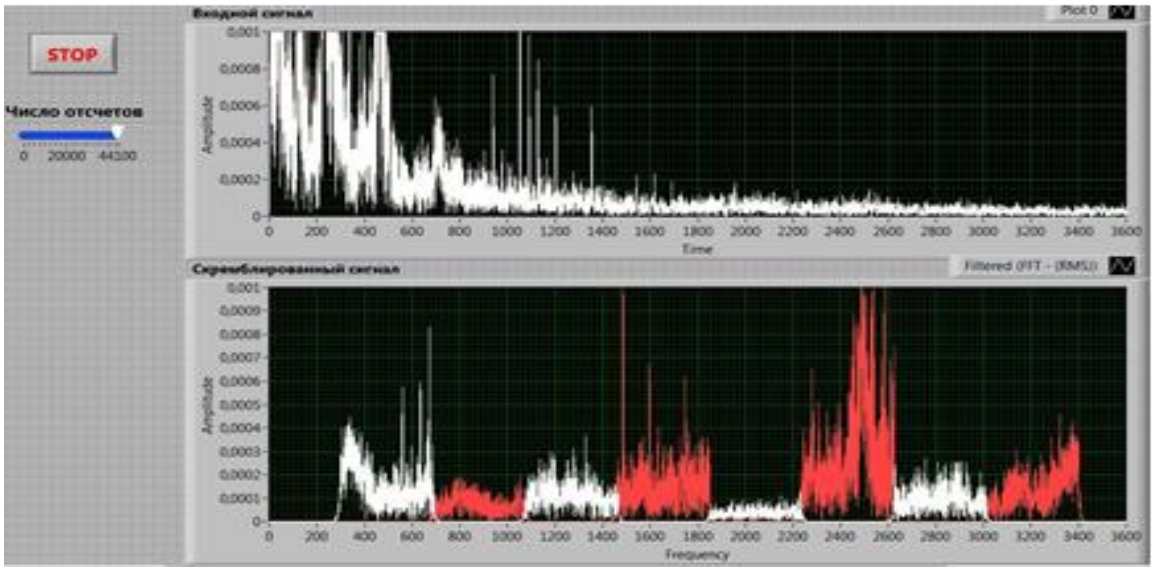


Рис. 11. Лицевая панель виртуального прибора скремблера

Анализ качества и криптостойкости скремблеров

Наиболее важной характеристикой скремблера для пользователя, желающего обеспечить защиту информации в своих каналах связи, является уровень закрытия информации. Для сложных цифровых систем передачи речи и данных понятие уровня закрытия строго регламентируется и определяется криптографической стойкостью информации, то для аналоговых скремблеров (особенно в системах подвижной радиосвязи) данное понятие носит условный характер, так как к настоящему времени на этот счет не выработано четких стандартов или правил.

В ряде случаев в качестве критериев уровня закрытия информации при сравнении различных средств подвижной радиосвязи с аналоговым скремблированием можно использовать

количество ключевых параметров и количество возможных ключей скремблера.

Под ключевым параметром аналогового скремблера обычно понимают какой-либо параметр преобразования речевого сигнала, значение которого необходимо знать для осуществления обратного преобразования сигнала на приемной стороне. Ключом аналогового скремблера (по аналогии с цифровыми системами шифрования), как правило, называют конкретное секретное состояние некоторых параметров преобразования речевого сигнала [1].

Количество ключей скремблера определяется множеством всевозможных значений ключа. Для скремблеров с одним ключевым параметром оно определяется числом возможных состояний этого параметра, для скремблеров с несколькими ключевыми параметрами - количеством возможных комбинаций значений этих параметров (как правило, произведением чисел состояний всех ключевых параметров). В связи с вышесказанным, лучше всего речь закрывает мозаичный скремблер с шестнадцатью возможными положениями ключа и инверсией, и перестановками по времени, на втором месте по защищенности – шестнадцати диапазонный скремблер также с шестнадцатью возможными положениями ключа, но с отсутствием скремблирования по времени. Замыкает тройку частотный четырех диапазонный скремблер. Временные скремблеры, в данном определении уровня закрытия речевой информации, расположились на последнем месте, по той причине, что они статичны и у них отсутствует возможность изменения ключей. Справедливости ради стоит отметить, что на слух, временной скремблер более лучше закрывает информацию, чем скажем четырех диапазонный частотный скремблер. Оценка разборчивость речи мной согласно ГОСТу Р 50840–95 затруднительна, так как требует специальных знаний, средств и обученных людей [1].

Был разработан программный комплекс, позволяющий проводить аналоговое скремблирование. Таким образом, из описанных моделей скремблеров/дескремблеров следуют следующие выводы:

— даже при разделении сигнала на четыре поддиапазона, скремблированный сигнал имеет низкую словесную разборчивость, что указывает на сильное закрытие информации виртуальным прибором;

— так как в данном устройстве используются гетеродины, к ним должны предъявляться жесткие требования, иначе вследствие нестабильности их частоты полезный сигнал будет подавлен фильтром, что снизит качество восстанавливаемого сигнала;

— в результате гетеродинного преобразования полезный сигнал теряет часть энергии, в виду этого необходимо производить усиление в каждом диапазоне на всех этапах скремблирования и дескремблирования;

— необходимо учитывать при разработке прибора, что скремблирование и дескремблирование вносит задержки в передаче речевого сигнала;

— Основным источником шума при скремблировании и дескремблировании являются эллиптические фильтры

— Также при проектировании прибора необходимо учитывать, что фильтр с высоким порядком является высокодобротной системой и имеет долгий незатухающий отклик - «звон», что влечет за собой появление помехи

Виртуальные приборы, осуществляющие аналоговое временное, частотное скремблирование речевых сигналов, а также библиотечные модули (вложенные виртуальные приборы) для частотного, временного скремблирования и дескремблирования с перестановками и инверсией, позволяют при каскадном наращивании смесителей и разделителей, реализовать код скремблирования любой сложности.

Исследование аналогового временного скремблера

Временные скремблеры основаны на двух основных способах закрытия: инверсии по времени сегментов речи и их временной перестановке. В скремблерах с временной инверсией речевой сигнал делится на последовательность временных сегментов и каждый из них передается инверсно во времени - с конца. Такие скремблеры обеспечивают ограниченный уровень закрытия, зависящий от длительности сегментов. Для достижения неразборчивости медленной речи необходимо, чтобы длина сегмента составляла около 250 мс. Это означает, что задержка системы будет равна примерно 500 мс, что может оказаться неприемлемым для некоторых приложений.

Для повышения уровня закрытия прибегают к способу перестановки временных отрезков речевого сигнала в пределах фиксированного кадра (рисунок 1). Правило перестановок является ключом системы, изменением которого можно существенно повысить степень закрытия речи. Остаточная разборчивость зависит от длительностей отрезков сигнала и кадра и с увеличением последнего уменьшается.

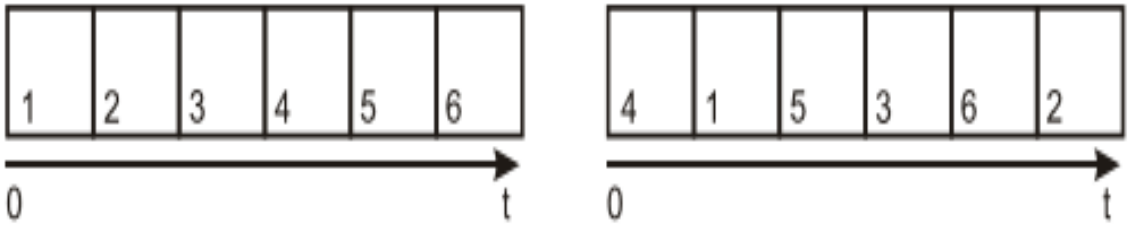


Рис. 12. Схема работы временного скремблера с перестановкам
и в фиксированном кадре

Главным недостатком скремблера с фиксированным кадром является большая величина времени задержки системы, равная удвоенной длительности кадра. Этот недостаток устраняется в скремблере с перестановкой временных отрезков речевого сигнала со скользящим окном. В нем число комбинаций возможных перестановок ограничено таким образом, что задержка любого отрезка не превосходит установленного максимального значения. Каждый отрезок исходного речевого сигнала как бы имеет временное окно, внутри которого он может занимать произвольное место при скремблировании. Это окно скользит во времени по мере поступления в него каждого нового отрезка сигнала. Задержка при этом снижается до длительности окна.

Ход работы

Для проведения лабораторной работы понадобится звуковой файл в формате wav, для его создания необходимо открыть программу Audacity, рисунок

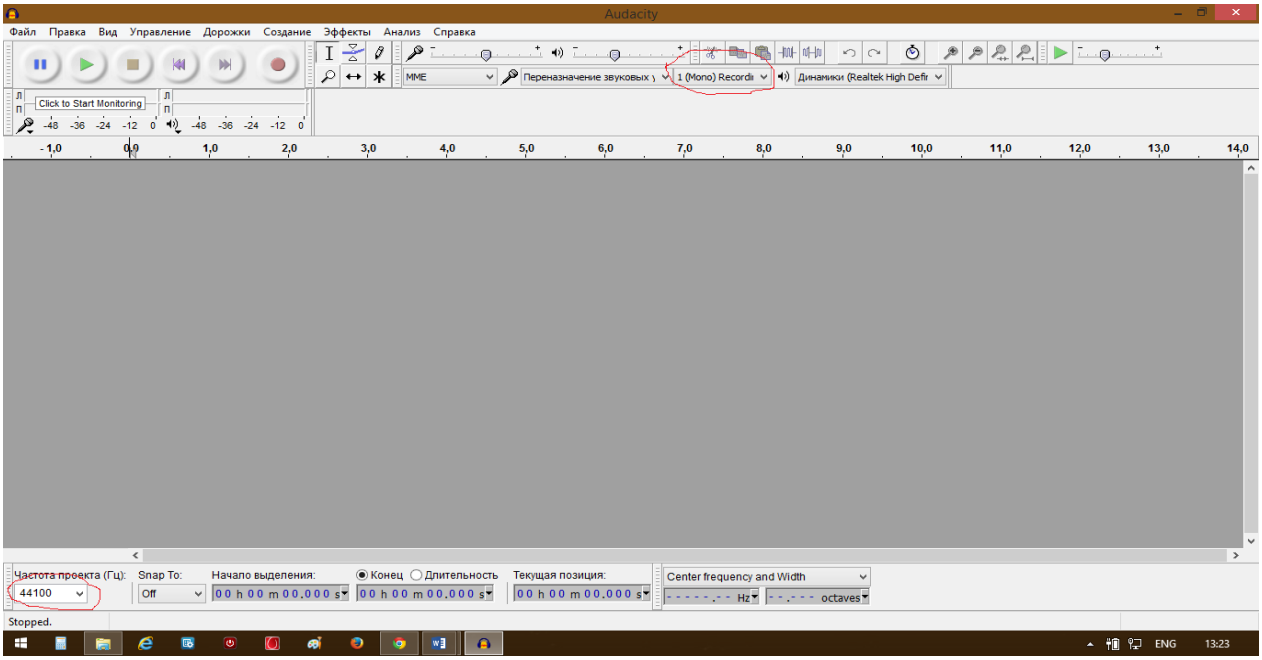


Рис. 13. Окно программы Audacity с нужными настройками (выделено красным).

После этого нужно нажать кнопку запись (круглая кнопка с красным кругом в центре), и записать.

Затем нужно нажать на копку стоп. В меню нажать Файл->Export Audio, в появившемся окне нужно выбрать место куда следует сохранить файл, задать имя файла и убедиться что в поле тип файла выбрано значение: WAV (Microsoft) signed 16-bit PCM.

Для начала работы нужно запустить файл test.vi, запустить программу, установить количество сэмплов, и нажать кнопку старт, в появившемся окне следует выбрать файл, который был записан с помощью программы Audacity.

После этого сигналы исходного и скремблированного файла отображатся на соответствующих экранах, после этого появится окно для выбора места сохранения скремблированного файла.

Инверсный скремблер

Исходный файл был создан в программе “Audacity”, его продолжительность составляет 8 секунд, а размер 697 кб.

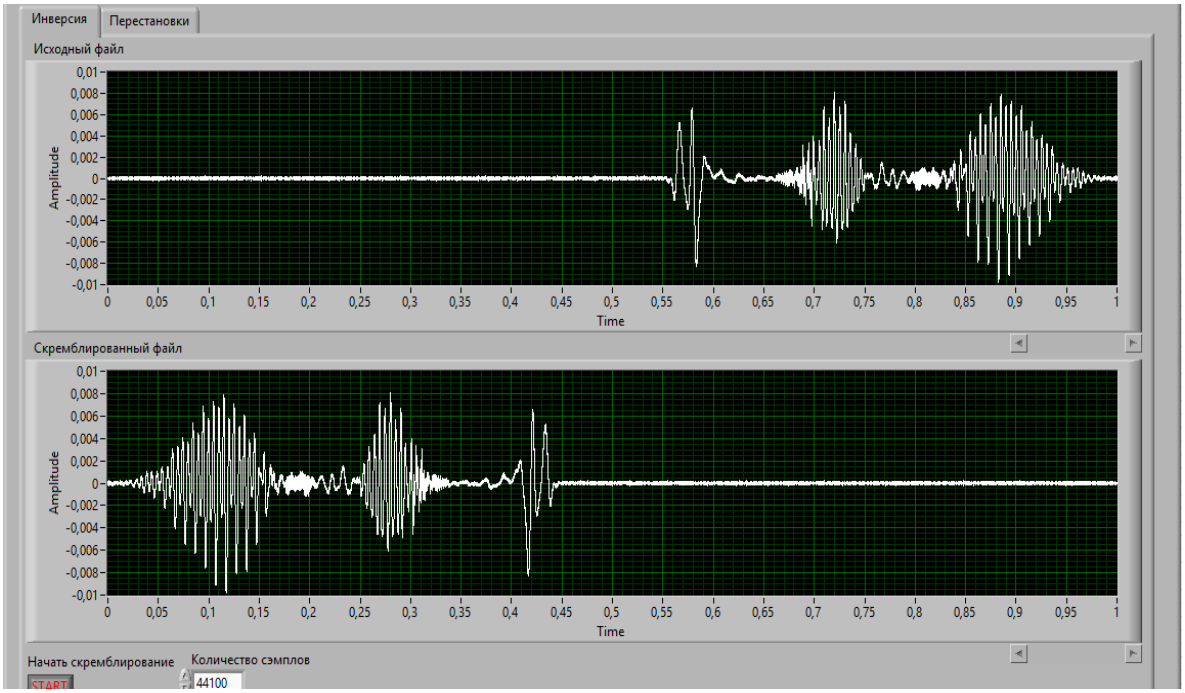


Рис. 14. Результат работы инверсного скремблера с количеством семплов 44100.

Параметры выходного файла: длительность 1 секунда, размер файла 86,1 кб.

Скремблирование прошло со значительными потерями так как оно завершилось, примерно, на 87% раньше. Как следствие обратное преобразование не дало исходного файла.

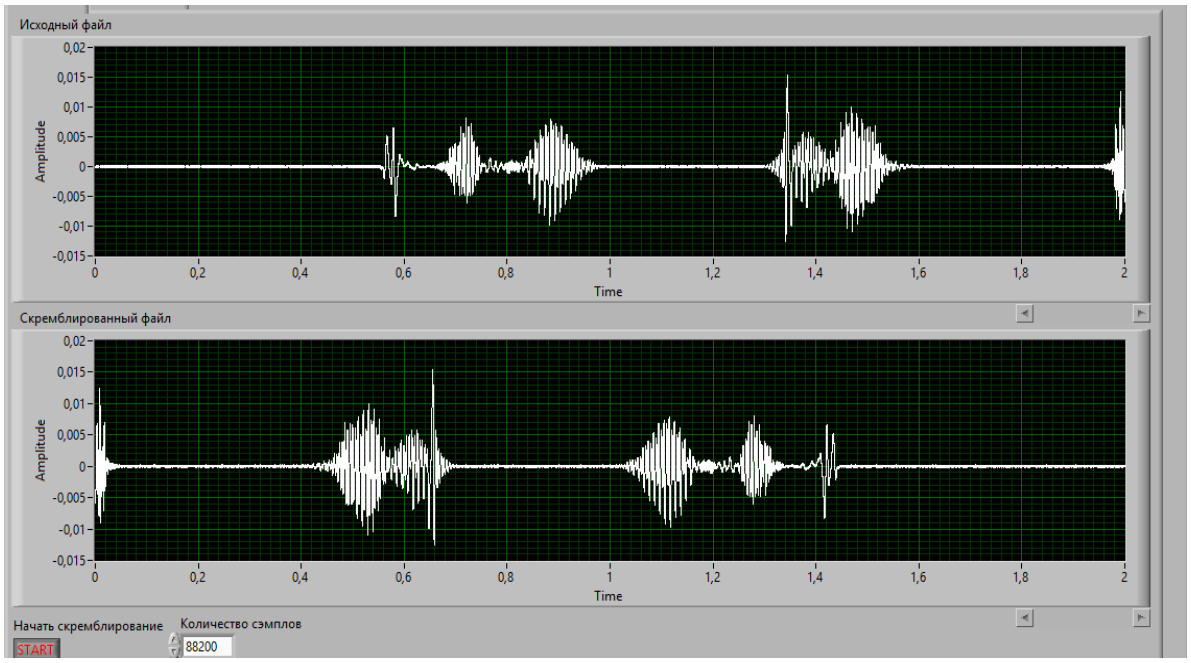


Рис. 15. Результат работы инверсного скремблера с количеством семплов 88200.

Параметры выходного файла: длительность 2 секунды, размер файла 172,2 кб.

Скремблирование прошло со значительными потерями так как оно завершилось, примерно, на 75% раньше. Как следствие обратное преобразование не дало исходного файла

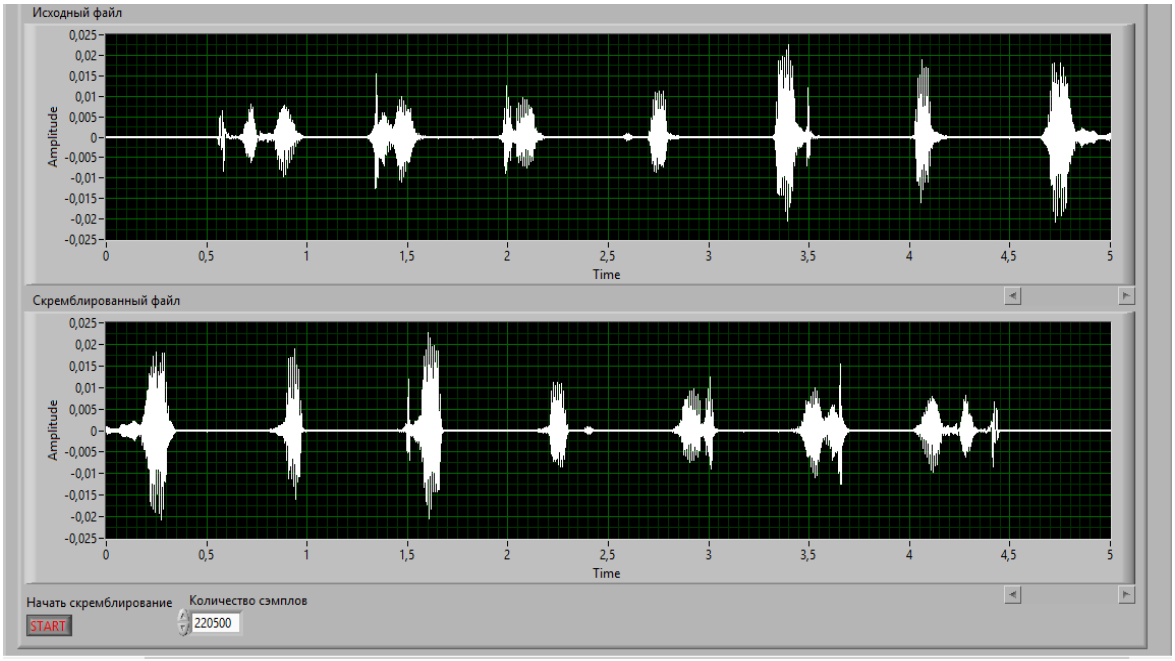


Рис. 16. Результат работы инверсного скремблера с количеством семплов 220500.

Параметры выходного файла: длительность 5 секунд, размер файла 430 кб.

Скремблирование прошло со значительными потерями так как оно завершилось, примерно, на 37% раньше. Как следствие обратное преобразование не дало исходного файла.

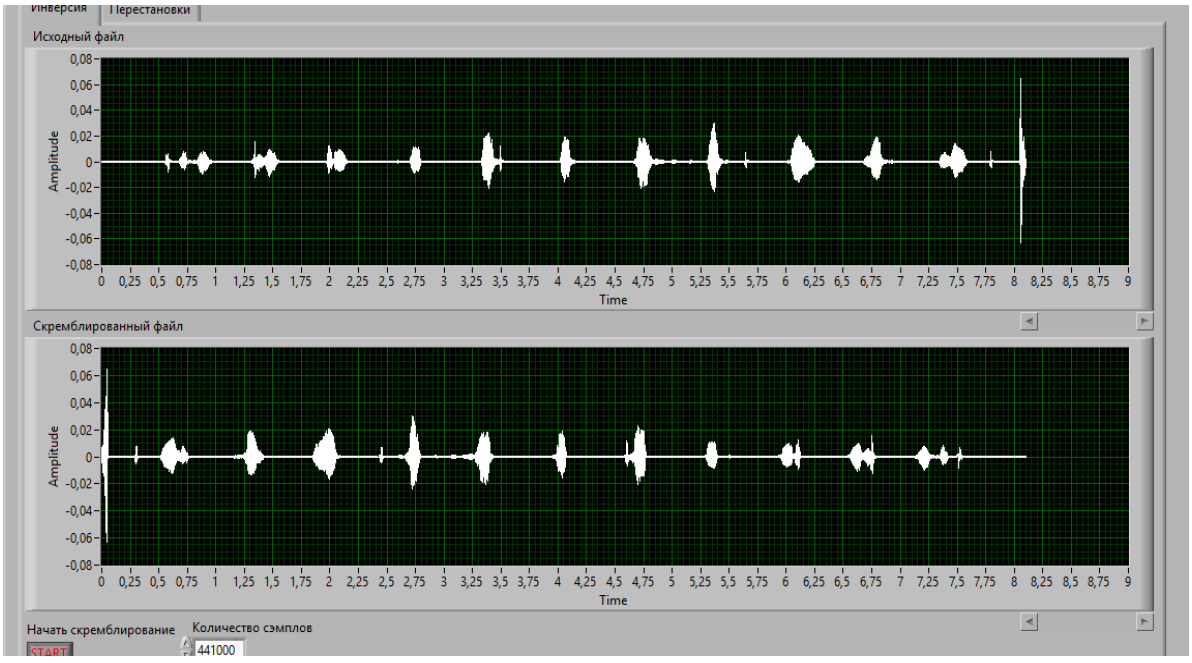


Рис. 17. Результат работы инверсного скремблера с количеством семплов 441000.

Параметры выходного файла: длительность 8 секунд, размер файла 697 кб.

Скремблирование прошло без потерь так как процесс скремблирования длился, примерно, на 25% больше. Как следствие обратное преобразование дало исходный файл. Так же стоить отметить что дополнительное время скремблирования не повлияло на размер файла.

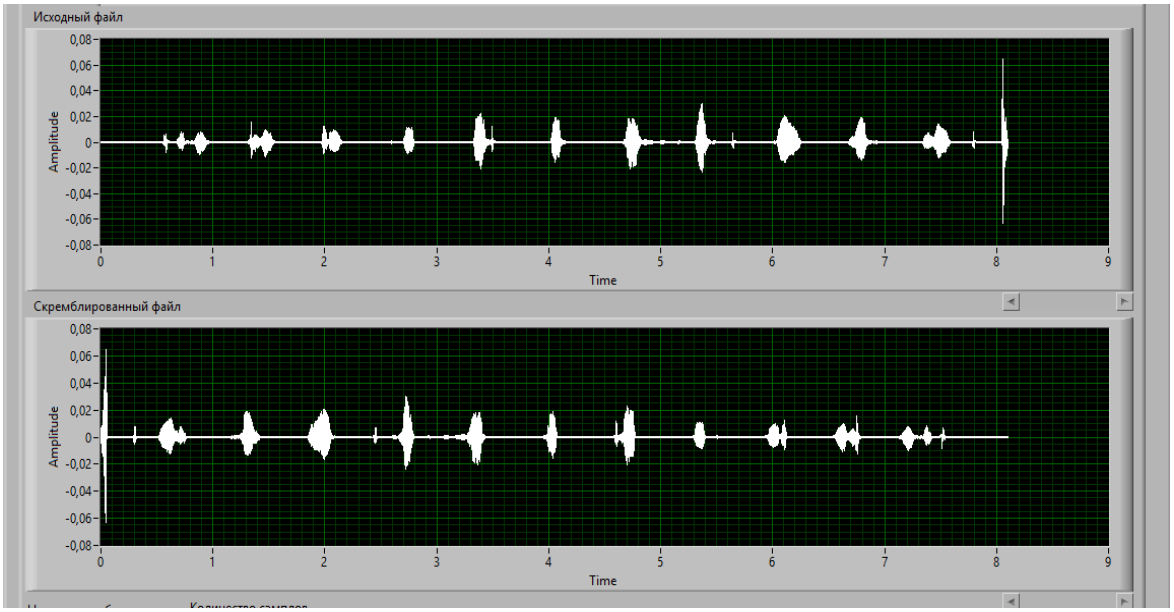


Рис. 18. Результат работы инверсного скремблера с количеством семплов 661500.

Параметры выходного файла: длительность 8 секунд, размер файла 697 кб.

Скремблирование прошло без потерь так как процесс скремблирования длился, примерно, на 87% больше. Как следствие обратное преобразование дало исходный файл. Так же стоить отметить что дополнительное время скремблирования не повлияло на размер файла.

Исходя из полученных данных видно, что количество семплов зависит от продолжительности файла и от частоты. Таким образом следует что количество семплов должно быть равно f*(t+1), где t-длительность сигнала в секундах, а f его частота в Гц. Единичка прибавляется для того что бы не потерять часть данных в случае если длительность файла, например, 8.2 секунды.

Скремблер перестановки

Задавая количество семплов 44100*n где n=1,2,5,10,15 посмотрим, как изменится выходной файл.

Исходный файл был создан в программе “Audacity”, его продолжительность составляет 8 секунд, а размер 697 кб.

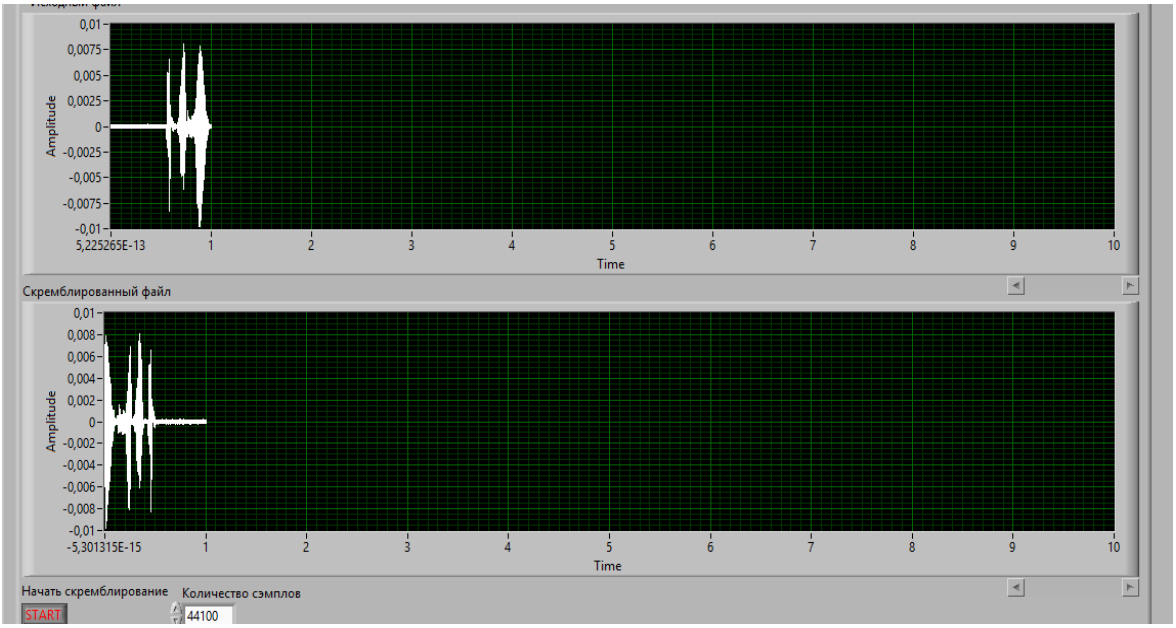


Рис. 19. Результат работы скремблера перестановки с количеством семплов 44100.

Параметры выходного файла: длительность 1 секунда, размер файла 81,1 кб.

Скремблирование прошло со значительными потерями так как оно завершилось, примерно, на 87% раньше. Как следствие обратное преобразование не дало исходного файла.

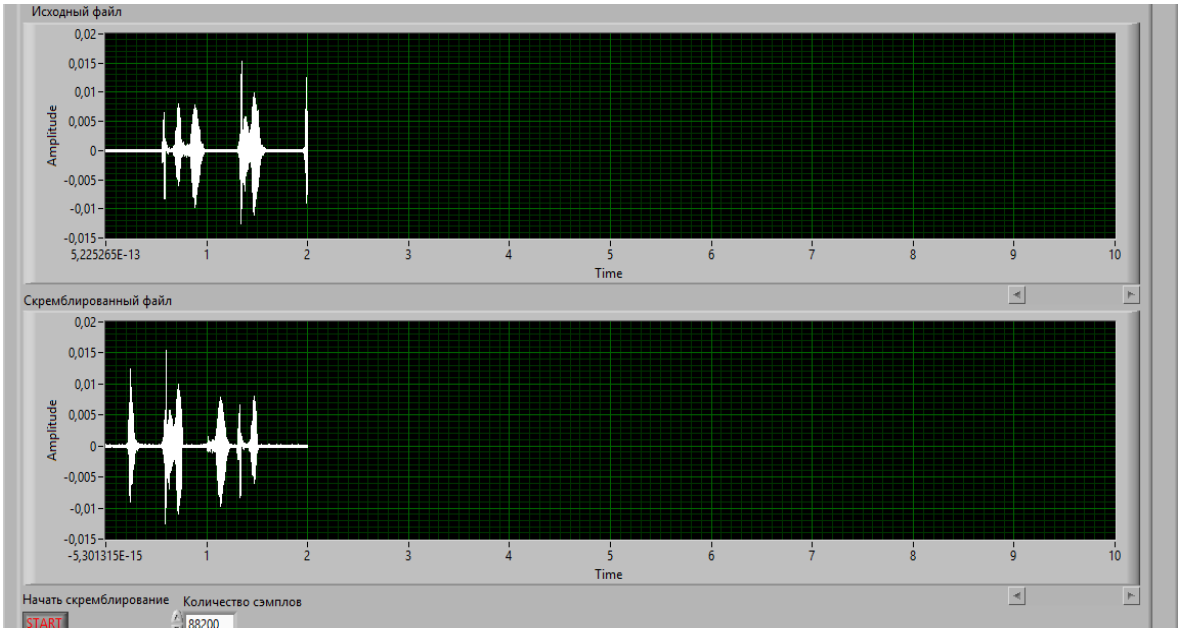


Рис. 20. Результат работы скремблера перестановки с количеством семплов 88200.

Параметры выходного файла: длительность 2 секунды, размер файла 172,2 кб.

Скремблирование прошло со значительными потерями так как оно завершилось, примерно, на 75% раньше. Как следствие обратное преобразование не дало исходного файла.

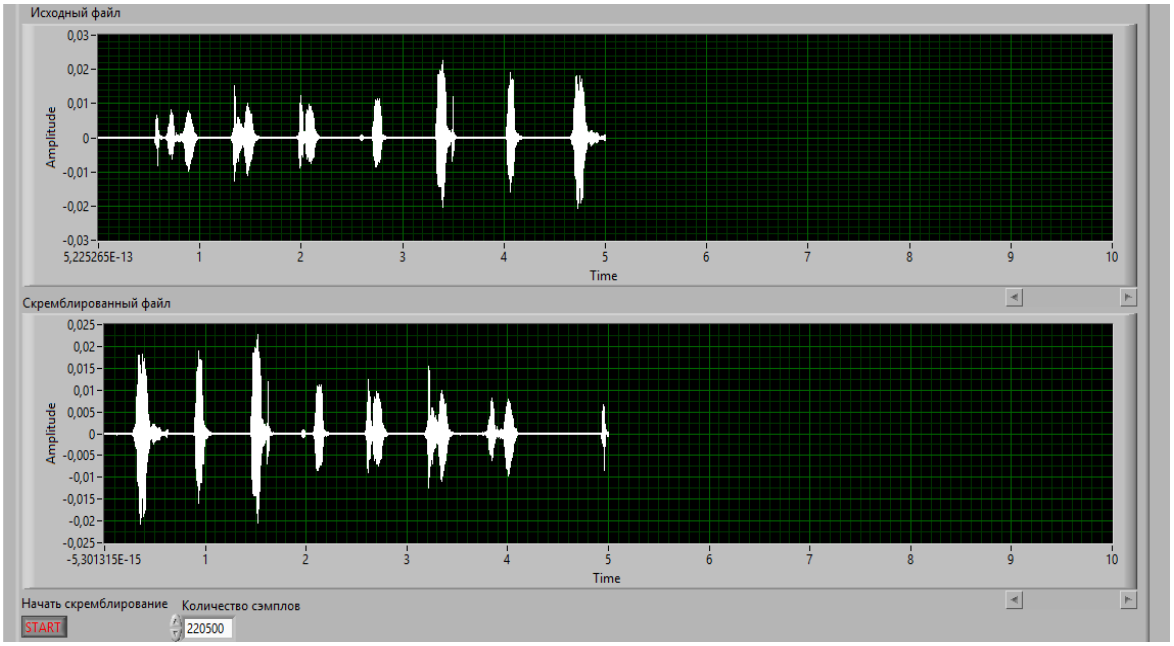


Рис. 21. Результат работы скремблера перестановки с количеством семплов 220500.

Параметры выходного файла: длительность 5 секунд, размер файла 430 кб.

Скремблирование прошло со значительными потерями так как оно завершилось, примерно, на 37% раньше. Как следствие обратное преобразование не дало исходного файла.

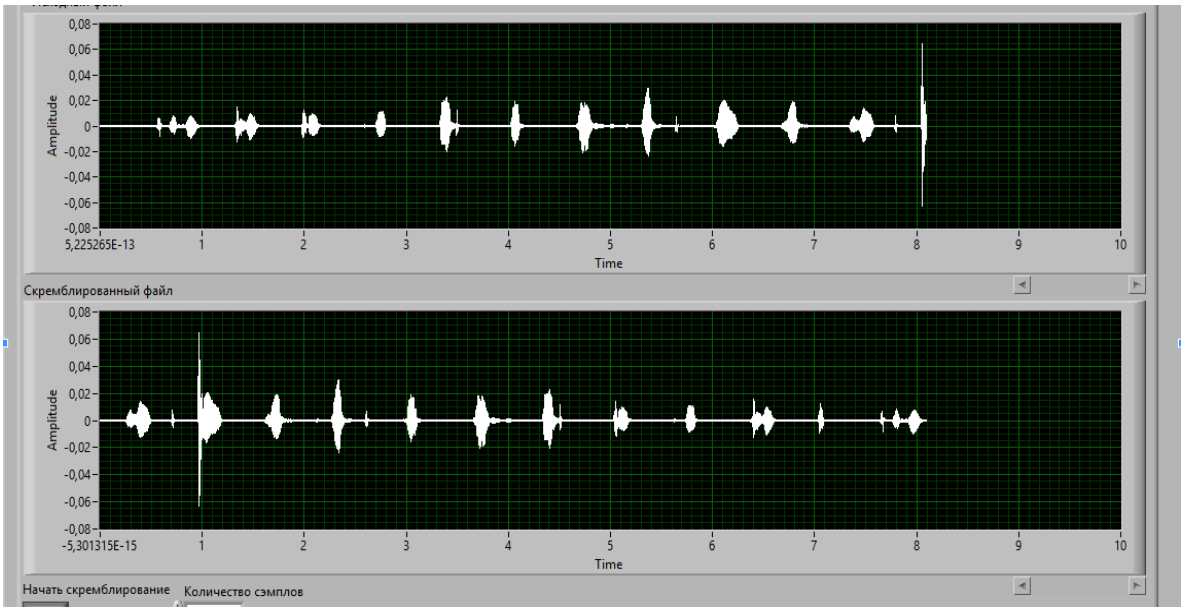


Рис. 22. Результат работы скремблера перестановки с количеством семплов 441000.

Параметры выходного файла: длительность 8 секунд, размер файла 497 кб.

Скремблирование прошло без потерь так как процесс скремблирования длился, примерно, на 25% больше. Как следствие обратное преобразование дало исходный файл. Так же стоить отметить что дополнительное время скремблирования не повлияло на размер файла.

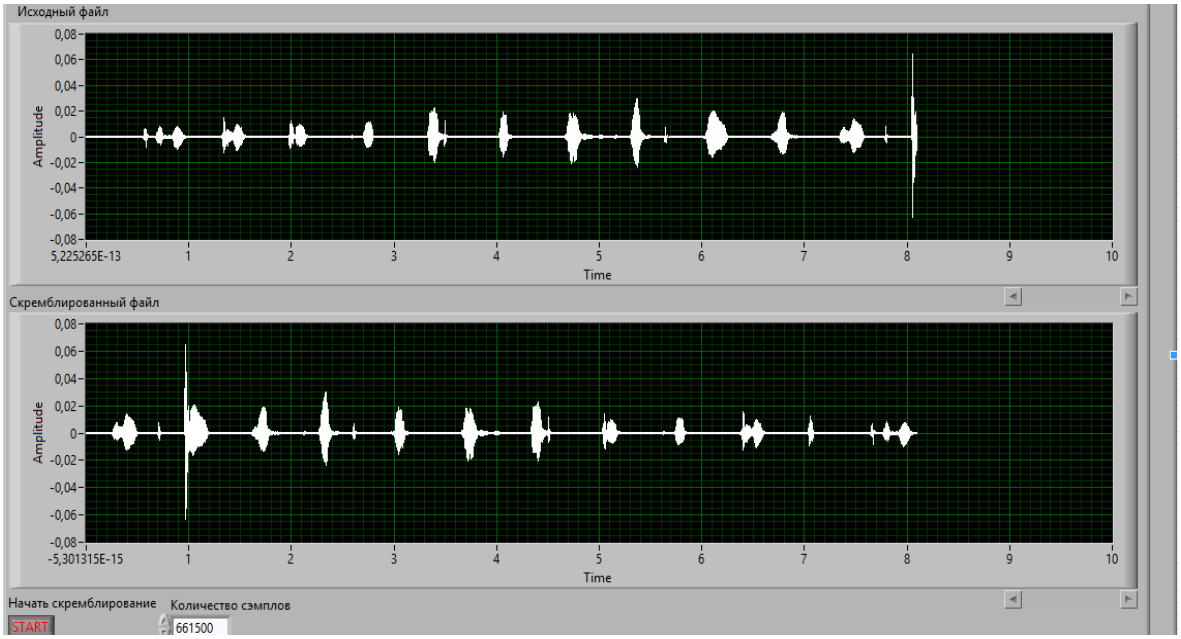


Рис. 23. Результат работы скремблера перестановки с количеством семплов 661500.

Параметры выходного файла: длительность 8 секунд, размер файла 497 кб.

Скремблирование прошло без потерь так как процесс скремблирования длился, примерно, на 87% больше. Как следствие обратное преобразование дало исходный файл. Так же стоить отметить что дополнительное время скремблирования не повлияло на размер файла.

Исходя из полученных данных видно, что количество семплов зависит от продолжительности файла и от частоты. Таким образом следует что количество семплов должно быть равно f*(t+1), где t-длительность сигнала в секундах, а f его частота в Гц. Единичка прибавляется для того что бы не потерять часть данных в случае если длительность файла, например, 8.2 секунды.

Лабораторная работа. 4. Скремблирования аудиосигнала с использованием Вейвлет преобразования

Запись аудио сигнала

Для записи аудиосигнала использовались встроенные средства программы MatLab. Изначально для записи голосового сообщения необходимо знать состояние системы и ID подключенных устройств.

Воспользовавшись следующим программным кодом:

```
devinfo = audiodevinfo;

disp('Input devices');
for i = 1 : size(devinfo.input, 2) devinfo.input(i)
end

disp('Output devices');
for i = 1 : size(devinfo.output, 2) devinfo.output(i)
end
```

Получаем сведения о системе представленные на рисунке 1.

```
ans =

            Name: 'Первичный звуковой драйвер (Windows DirectSound)'
    DriverVersion: 'Windows DirectSound'
               ID: 2


ans =

            Name: 'Динамики (Realtek High Definition Audio) (Windows DirectSound)'
    DriverVersion: 'Windows DirectSound'
               ID: 3


ans =

            Name: 'Realtek Digital Output (Realtek High Definition Audio) (Win...'
    DriverVersion: 'Windows DirectSound'
               ID: 4


ans =

            Name: '1 - LG IPS FULLHD (AMD High Definition Audio Device) (Windo...'
    DriverVersion: 'Windows DirectSound'
               ID: 5


ans =

            Name: 'Realtek Digital Output(Optical) (Realtek High Definition Au...'
    DriverVersion: 'Windows DirectSound'
               ID: 6
```

Рис.1. Сведения о системе

Далее зная параметры системы возможно произвести запись аудиосигнала с помощью встроенных в MatLab функций. Для этого был написан следующий программный код:

```
Fs = 8000; % Количество отсчетов nBits = 16; % Битов
на отсчет nChannels = 2; % Количество каналов
deviceID = 1; % ID микрофона подключенного к компьютеру recObj =
audiorecorder(Fs, nBits, nChannels, deviceID); get(recObj)

nSeconds = 10;

% Запись голоса и графическое представление записанного сигнала
% Запись в течении nSeconds секудн disp('Start
speaking.') recordblocking(recObj, nSeconds); disp('End
of Recording.');

% Проигрышь записанного голосового собщения. play(recObj);

% Получение  аудиоданных myRecording =
getaudiodata(recObj);

% Графическое представление
plot(myRecording);
%Сохранение каналов
x1=myRecording(:,1);
x2=myRecording(:,2); save Record1;
save Chanel1 x1; save Chanel2
x2;
```

В результате выполнения программы на экран будет выведен график отображающий записанные аудиоданные.

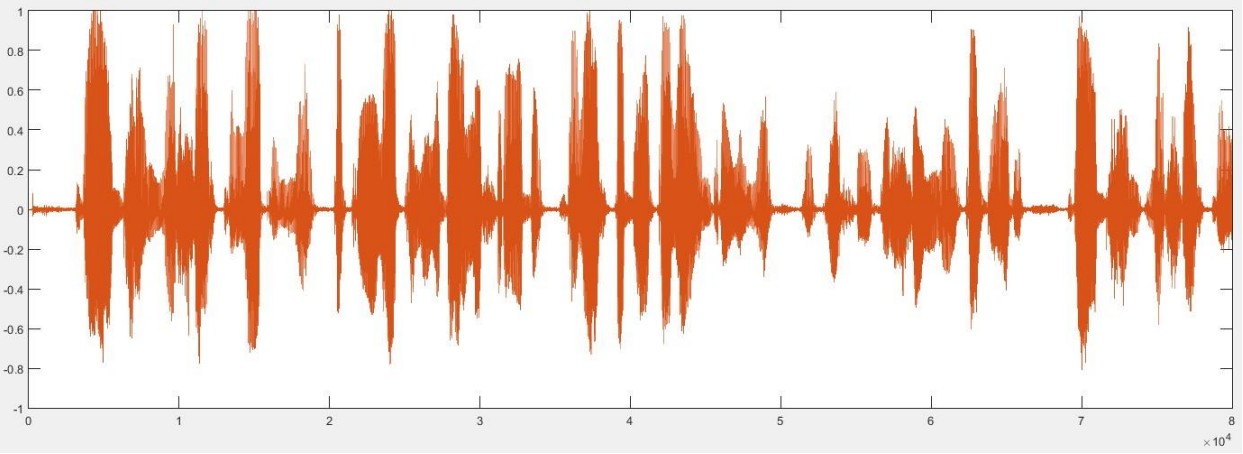


Рис.2. Записанные аудиоданные

Быстрое вейвлет преобразование сигнала

Благодаря своим частотно-временным свойствам вейвлет- преобразование предоставляет широкий спектр возможностей для работы с различного рода сигналами. Помимо классического применения в виде фильтрации и сжатия, вейвлет преобразования являются удобным аппаратом для работы с сигналами в области информационной безопасности. Например, вейвлет преобразование достаточно часто упоминается в различных разделах стеганографии. Так же на основе БВП возможно выполнить сокрытие аудио информации одновременно во временной и частотной области.

Для выполнения быстрого вейвлет-преобразования был разработан следующий код:

```
%Загружаем файл с одним из каналов
load('Chanel1.mat');
%имя вейвлета
wname='sym4'; lev=4;
x=x1';
[dec,struct]=wavedec(x1,lev,wname);
% Вектор dec содержит столбец данных состоящий последовательно приписанных
% уровенй разложения, struct содержит информацию о кол-ве элементов в
% разложении для выделения определенного разложения из dec
% Извлечение коэффициентов разложения sa4
= appcoef (dec, struct, wname,4); sd4= detcoef
(dec, struct, 4);
sd3= detcoef (dec, struct, 3); sd2=
detcoef (dec, struct, 2); sd1= detcoef
(dec, struct, 1);
% Графическая поддержка
subplot (711)
plot (x1), title ('Исходный сигнал') subplot
(712)
plot (sd1), ylabel ('sd1') subplot
(713)
plot (sd2), ylabel ('sd2') subplot
(714)
plot (sd3), ylabel ('sd3') subplot
(715)
plot (sd4), ylabel ('sd4') subplot
(716)
plot (sa4), ylabel ('sa3')
x2 = waverec (dec, struct, wname);
% Рисуем восстановленный сигнал
subplot (717);
plot (x2), title ('Восстановленый сигнал'); save
wav_dec;
```

На рисунке 3. изображено разложение и восстановление аудиосигнала при помощи БВП с использованием симлета 4.

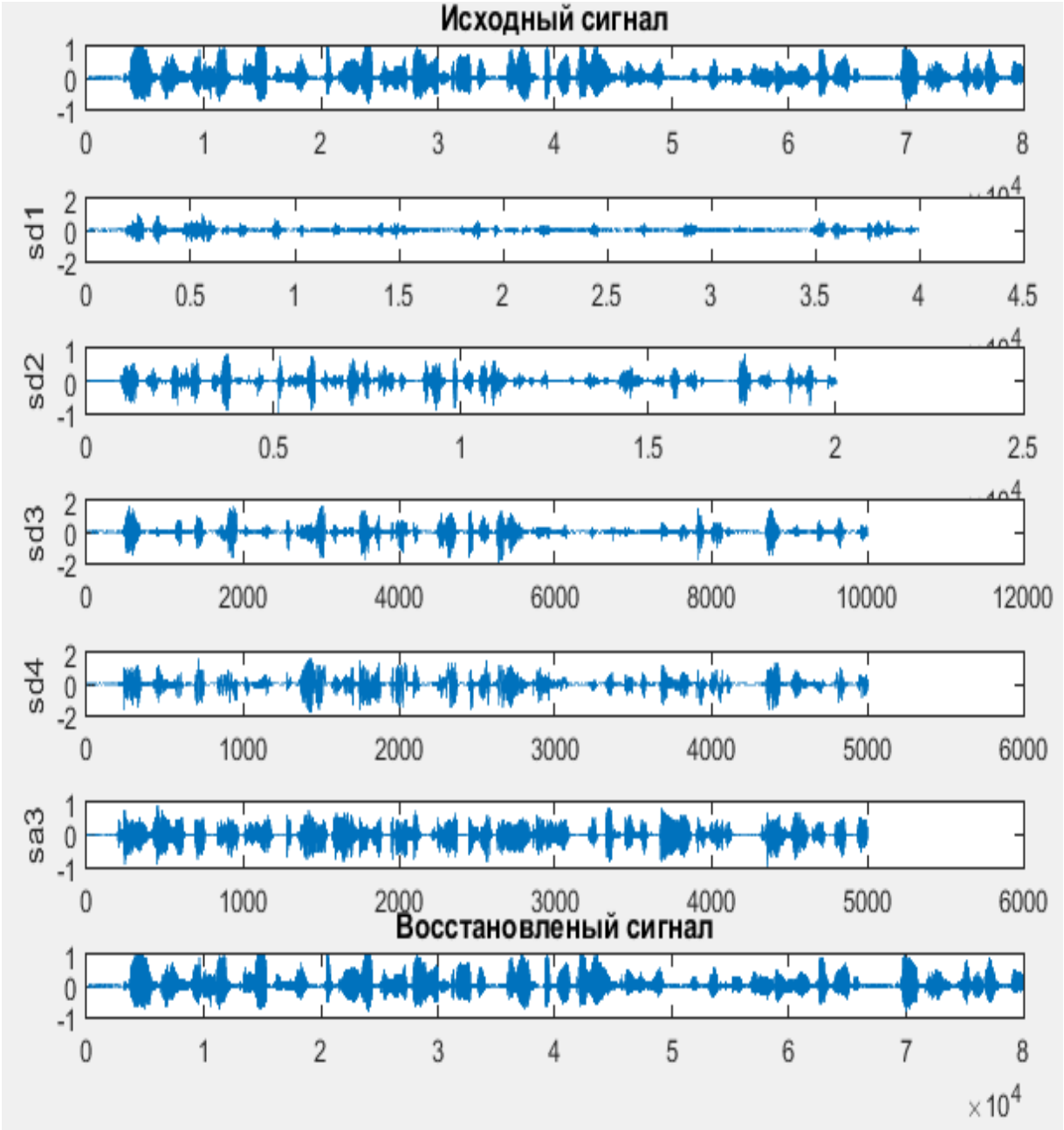


Рис.3. Быстрое вейвлет преобразование примененное к аудиосигналу

Скремблирование сигнала

Для того чтобы скрыть информацию в аудиосигнале, достаточно перемешать коэффициенты различных уровней разложения между собой по определенному алгоритму. Благодаря свойствам вейвлет-спектра подобное воздействие на вейвлет коэффициенты приведет к изменению сигнала как в частотной, так и во временной области.

В программе MatLab декомпозиция сигнала представлена в следующем виде

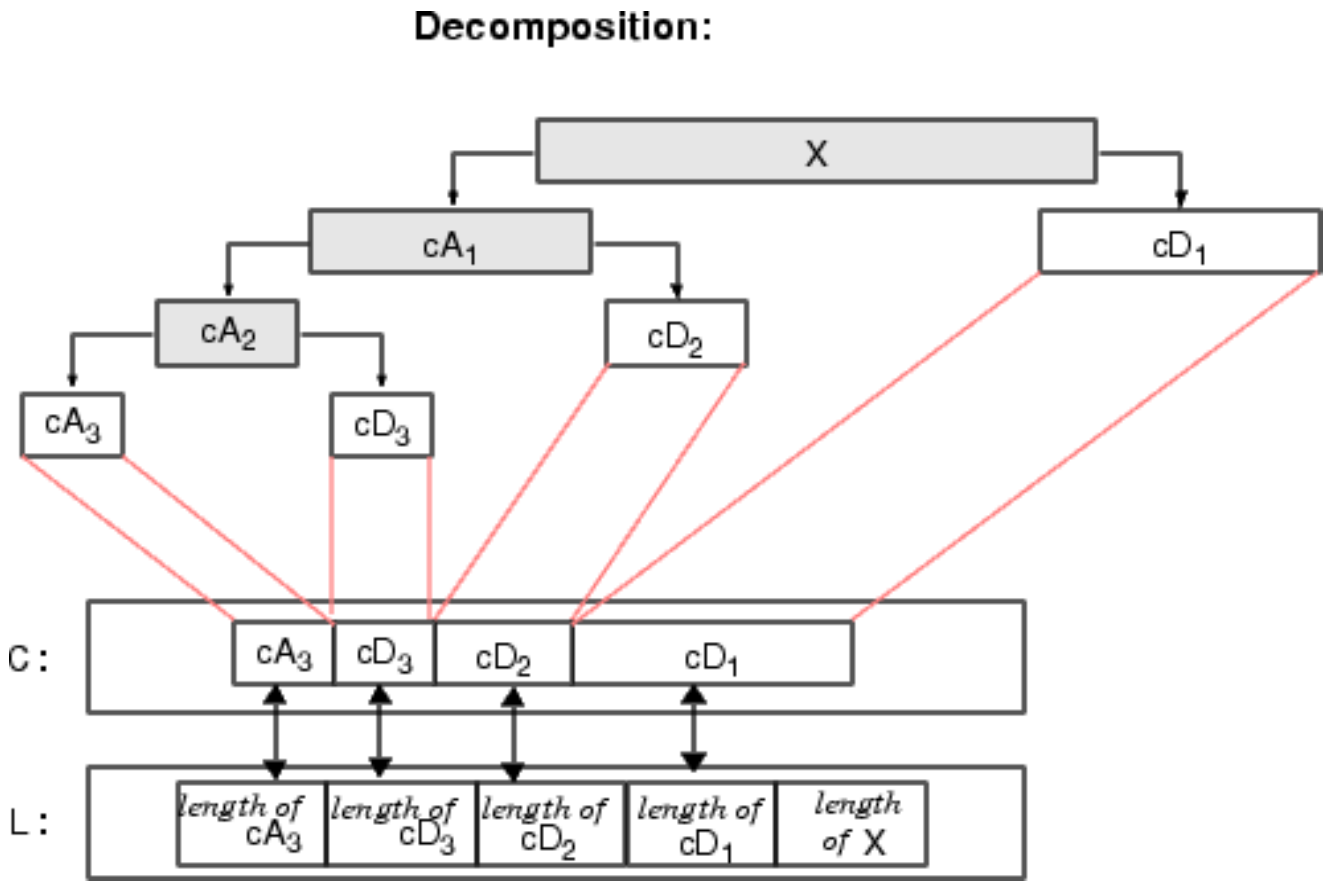


Рис.4. Результат выполнения БВП в MatLab

Как видно из рисунка на выходе имеется вектор вейвлет коэффициентов составленный из коэффициентов на всех уровнях, последовательным приписыванием каждого уровня к предыдущему начиная с минимального. Данный вид представления позволяет выполнить перемежение вейвлет коэффициентов простым переобазначением индексов массива.

В дальнейшем восстановив из перемешанного спектра сигнал, получается заскремблированные аудиоданные как в частотной так и во временной области.

Для перемежения коэффициентов спектра быстрого вейвлет преобразования и последующего восстановления скремблированного сигнала был разработан следующий код:

```
%загрузка
коэффициентов
load('wav_dec.mat');

for i=1:1:10000
new_dec(i)=dec(40000+i-1);% от 40000 до 50000 /10000
new_dec(10000+i)=dec(60000+i-1); % от 60000 до 70000 /20000
new_dec(20000+i)=dec(i); % от 0 до 10000 /30000
new_dec(30000+i)=dec(70000+i-1); % от 70000 до 80000 /40000
```

```
new_dec(40000+i)=dec(10000+i-1); % от 10000 до 20000 /50000
new_dec(50000+i)=dec(30000+i-1); % от 30000 до 40000 /60000
new_dec(60000+i)=dec(20000+i-1); % от 20000 до 30000 /70000
new_dec(70000+i)=dec(50000+i-1); % от 50000 до 60000 /80000
end
for i=80000:1:80026
new_dec(i)=dec(i); % от 50000 до 60000 /80000
end
new_dec=new_d
ec';
save ScrDecomp new_dec;
% Извлечение коэффициентов разложения
new_sa4 = appcoef (new_dec, struct, wname,4);
new_sd4= detcoef (new_dec, struct, 4); new_sd3=
detcoef (new_dec, struct, 3); new_sd2= detcoef
(new_dec, struct, 2); new_sd1= detcoef (new_dec,
struct, 1);
% Графическая
поддержка subplot
(711)
plot (x1), title ('Исходный сигнал')
subplot (712)
plot (new_sd1), ylabel ('sd1')
subplot (713)
plot (new_sd2), ylabel ('sd2')
subplot (714)
plot (new_sd3), ylabel ('sd3')
subplot (715)
plot (new_sd4), ylabel ('sd4')
subplot (716)
plot (new_sa4), ylabel ('sa3')
scrembl_sign = waverec (new_dec, struct, wname);
% Рисуем восстановленный
сигнал subplot (717);
plot (scrembl_sign), title ('Скремблированный сигнал'); save
Scr_sig scrembl_sign;
load('Record1.mat');
Voice_sound(:,1)=scrembl_sign(:,1);
Voice_sound(:,2)=scrembl_sign(:,1);
player = audioplayer(Voice_sound, Fs, nBits); start
= 1;
stop = player.SampleRate * nSeconds;
play(player, [start stop]);
%pause(player)
%resume(player)
```

При выполнении данного кода были получены следующие результаты:

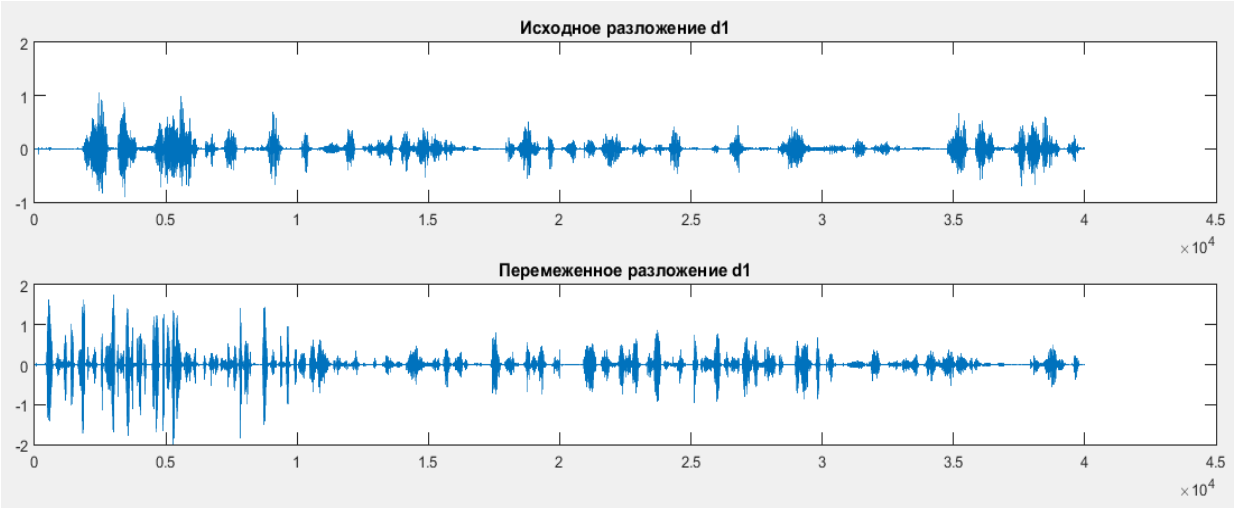


Рис. 5. Разложение на уровне d1

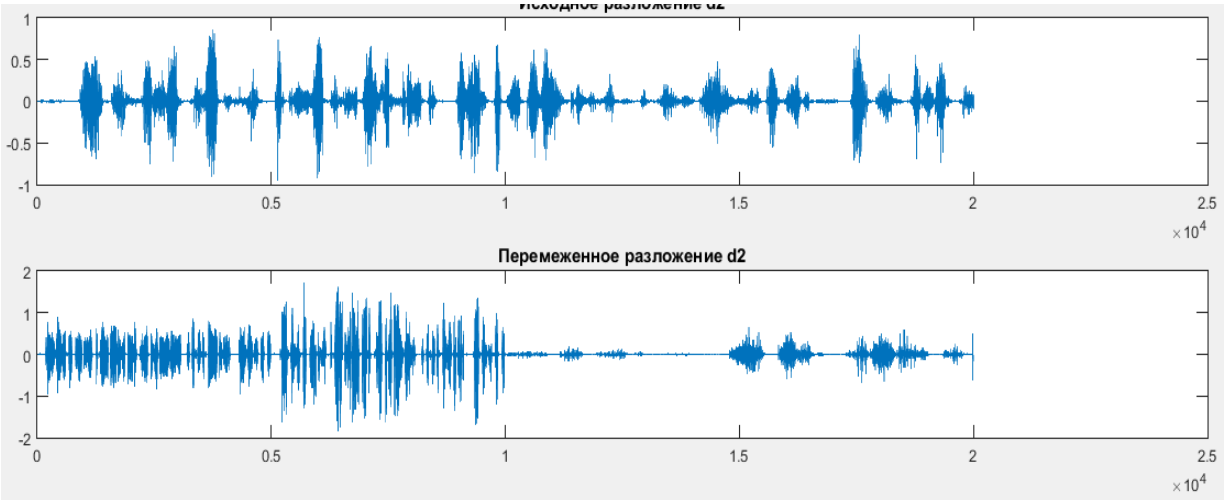


Рис.6. Разложение на уровне d2

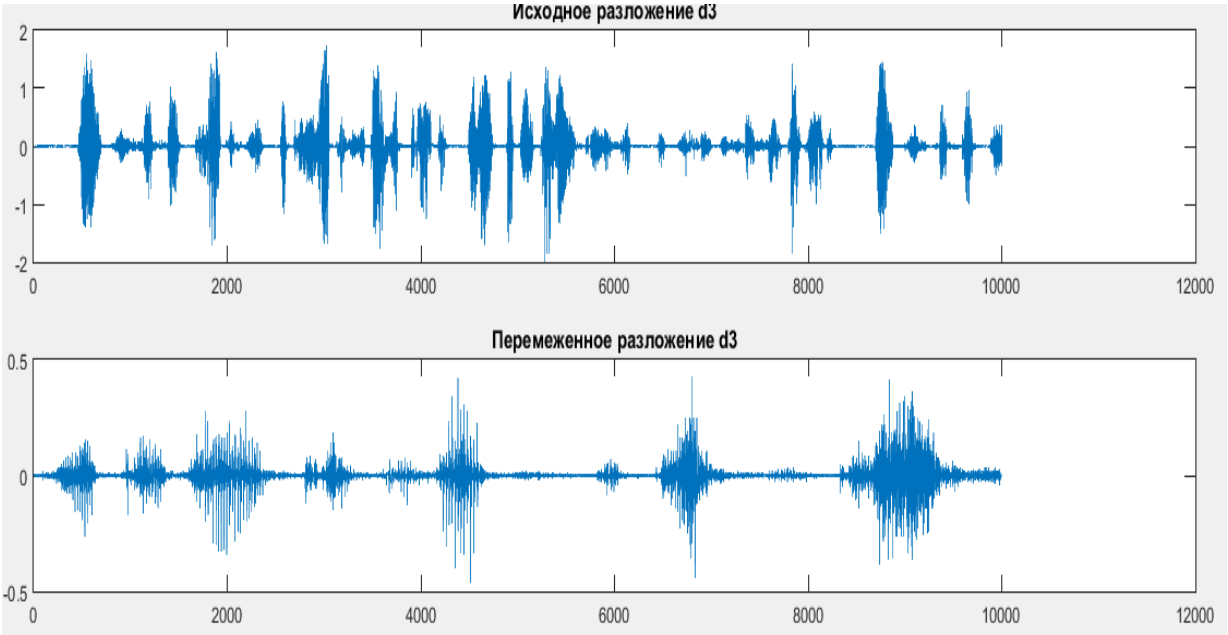


Рис.7. Разложение на уровне d3

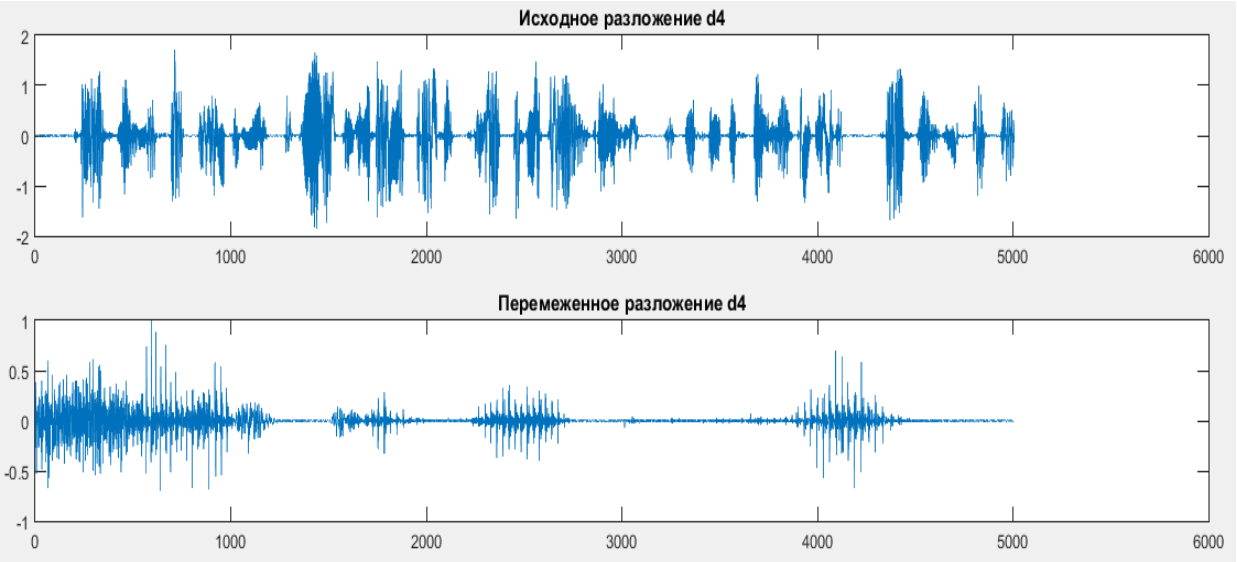


Рис.8. Разложение на уровне d4

При этом из полученный сигнал не похож на исходной в достаточной степени, чтобы говорить о защищенности информации.

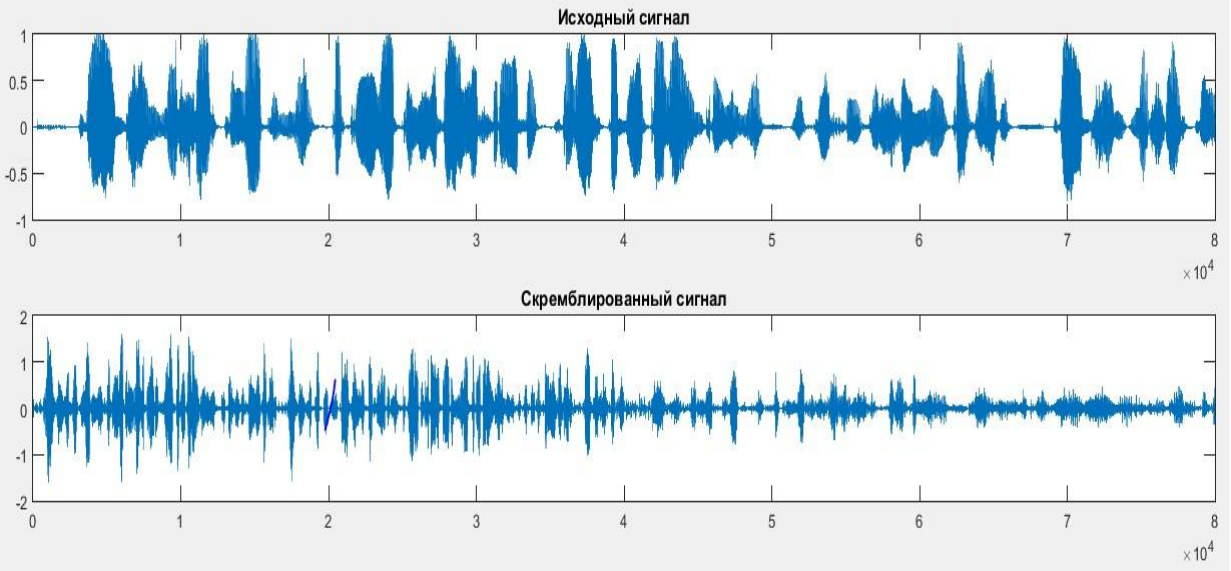


Рис. 9. Исходный и заскремблированный сигналы.

Восстановление исходного сигнала

Для восстановления исходного сигнала скремблированный сигнал подвергается быстрому вейвлет преобразованию. Полученные коэффициенты вейвлет-спектра по алгоритму, обратному скремблирующему, перемешиваются, для получения исходного спектра. На основании полученного спектра происходит восстановление сигнала. При должном навыке и практических исследованиях возможно добиться восстановления сигнала без искажений. На рисунке 10 представлен восстановленный сигнал имеющий небольшие искажения в следствии

несовершенных алгоритмов перемежения спектра.

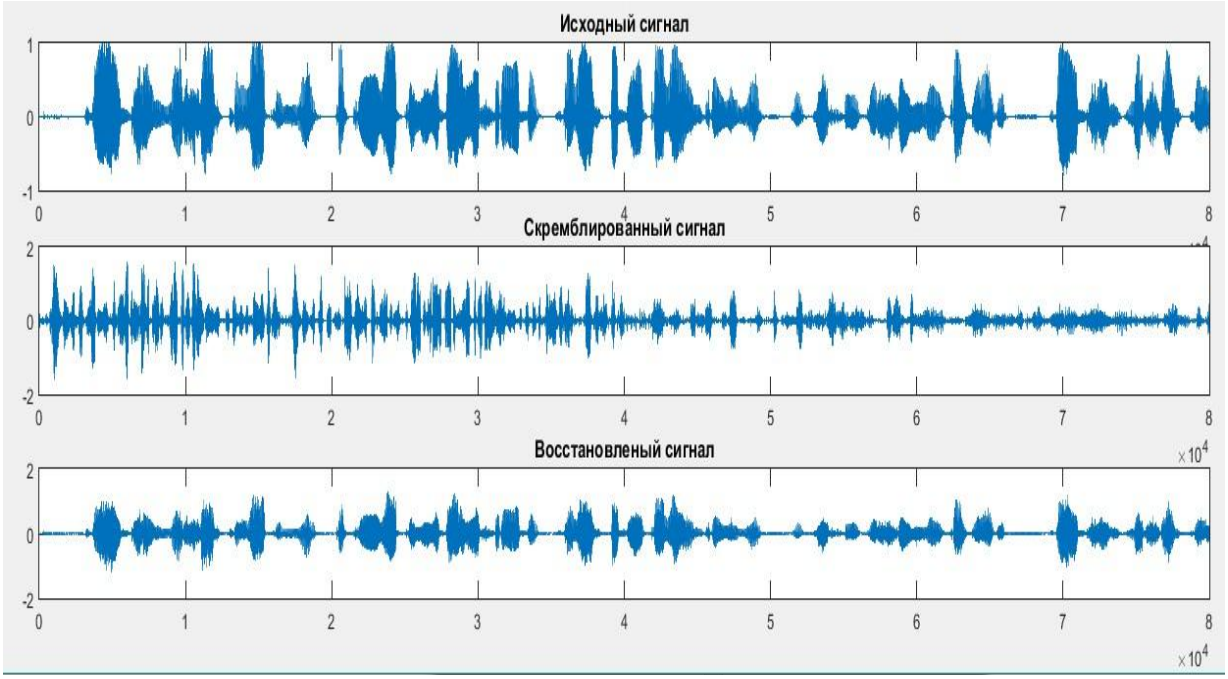


Рис.10. Исходный, заскремблированный и восстановленный сигналы На рисунке 2.11 представлено разложение на уровне d1, как видно восстановленный спектр довольно точно повторяет исходный.

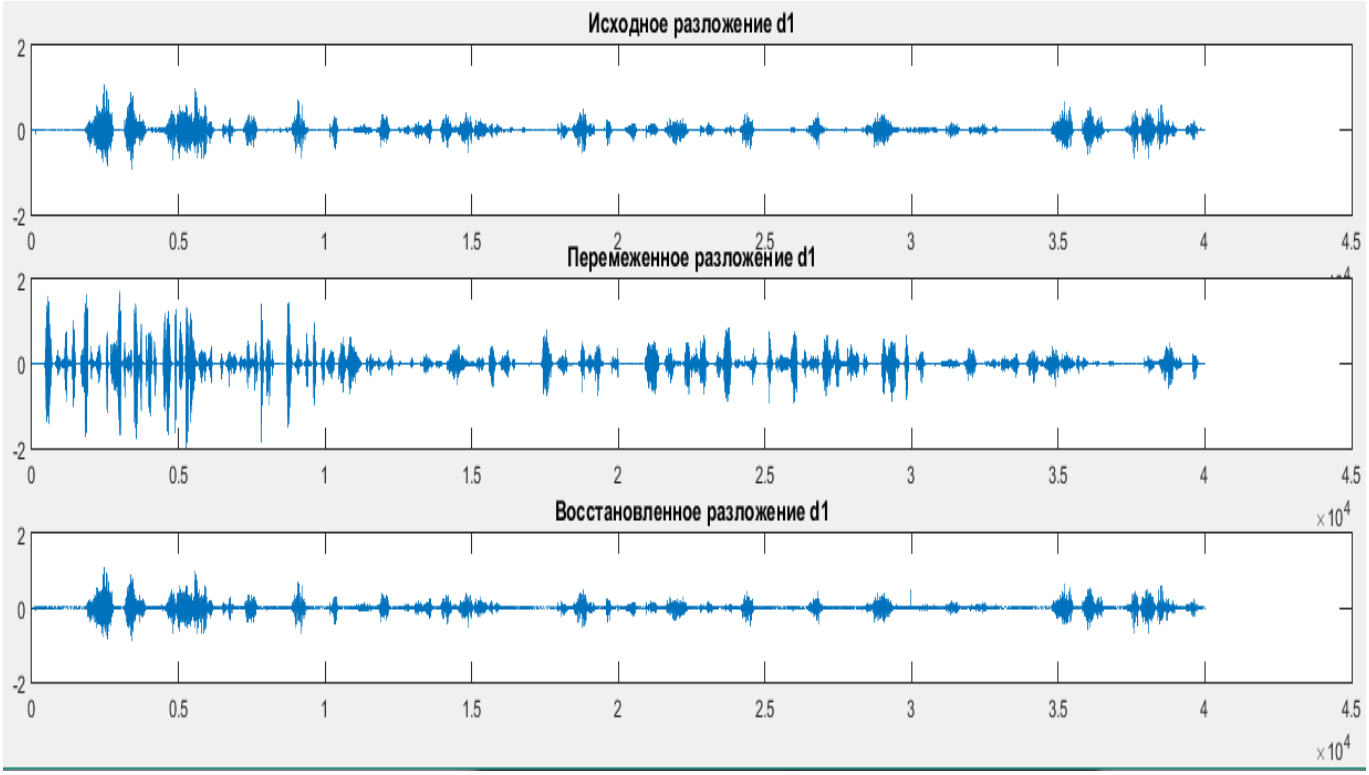


Рис. 11. Исходный, заскремблированный и восстановленный уровни разложения d1

На рисунках 12-14 изображены разложения на уровнях d2, d3 и d4 соответственно.

Рис.12. Исходный, заскремблированный и восстановленный уровни разложения d2

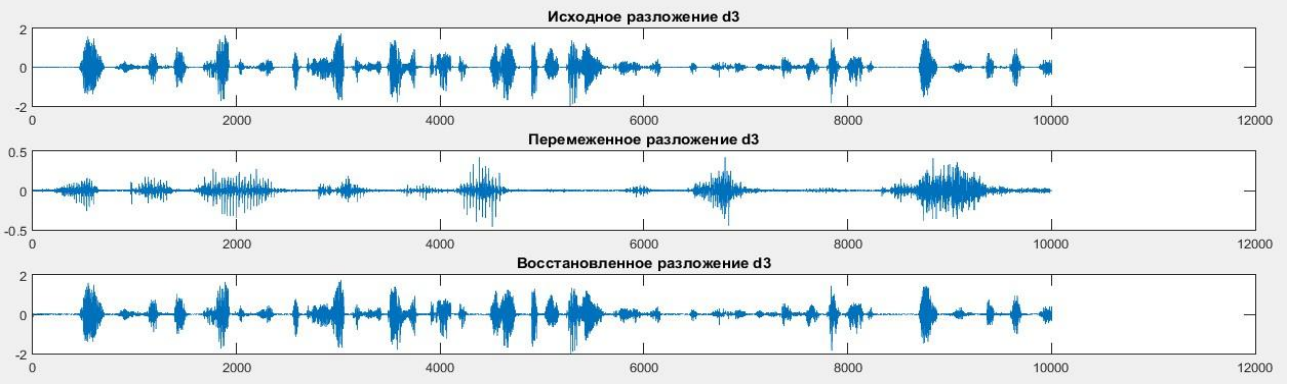


Рис. 13. Исходный, скремблированный и восстановленный уровни разложения d3

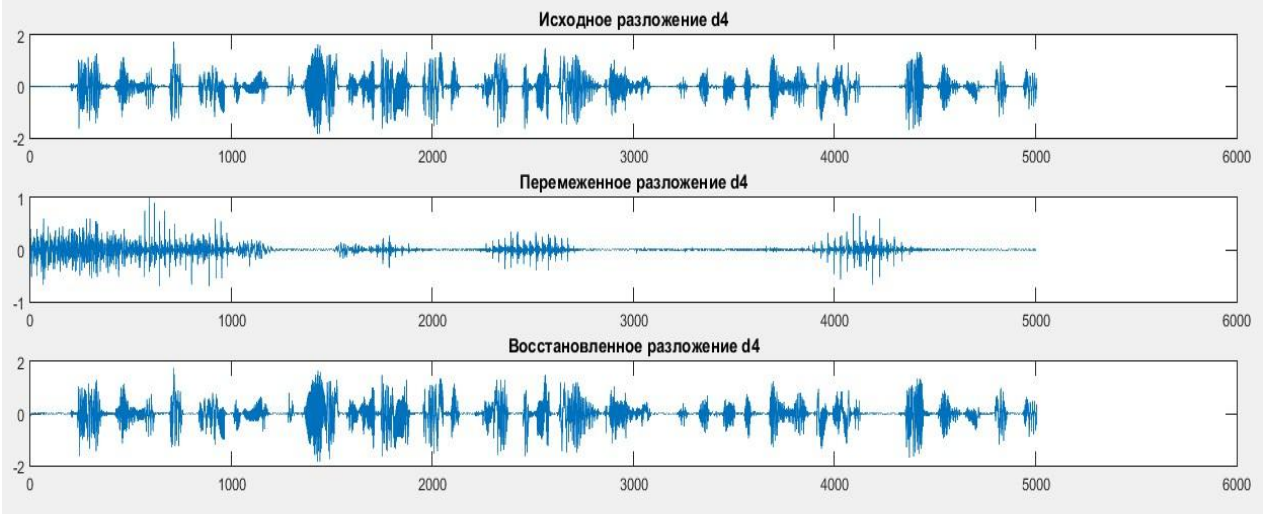


Рис.14. Исходный, скремблированный и восстановленный уровни разложения d4

В лабораторной работе исследовано скремблирование аудиосигнала с помощью вейвлет преобразования. Установлено, что вейвлет преобразование позволяет выполнить как частотное так и временное скремблирование одновременно, что повышает крипто стойкость. Восстановленный сигнал в достаточной степени

соответствует исходному, при практических исследования и должном навыке возможно полное восстановление сигнала без искажений.

ЛИТЕРАТУРА

1. Яковлев А.Н. Введение в вейвлет-преобразования: Учеб. пособие. –Новосибирск: Изд-во НГТУ, 2003. – 104 с.

2. Дьяконов В.П. Абраменкова И. MATLAB. Обработка сигналов и изображений. Специальный справочник. – СПб.: Питер, 2002, 608 с.

3. Дьяконов В.П, Вейвлет преобразования от теории к практике– СПб.: Питер, 2005, 439 с

4. Дьяконов В.П, MATLAB6 Учебный курс– СПб.: Питер, 2001

Лабораторная работа 5. Защищенная IP АТС на базе программного обеспечения ASTERISK

Asterisk — свободное решение компьютерной телефонии (в том числе, VoIP) с открытым исходным кодом от компании Digium, первоначально разработанное Марком Спенсером. Благодаря коммерческой поддержке Его компании и лицензии GNU GPL Asterisk активно развивается и поддерживается тысячами людей со всей планеты.

Asterisk может работать как с аналоговыми линиями (FXO/FXS модули), так и цифровыми (ISDN BRI и PRI — потоки T1/E1). С помощью компьютерных плат (наиболее известными производителями которых являются Digium, Sangoma, OpenVox, Rhino, AudioCodes) Asterisk можно подключить к высокопропускным линиям T1/E1, которые позволяют работать с десятками и сотнями телефонных линий.

Общие принципы IP телефонии

«Классические» телефонные сети основаны на технологии коммутации каналов (рисунок 1.1), которая для каждого телефонного разговора требует выделенного физического соединения. Следовательно, один телефонный разговор представляет собой одно физическое соединение телефонных каналов. Основным недостатком телефонных сетей с коммутацией каналов является неэффективное использование полосы канала – во время пауз в речи канал не несет никакой полезной нагрузки.

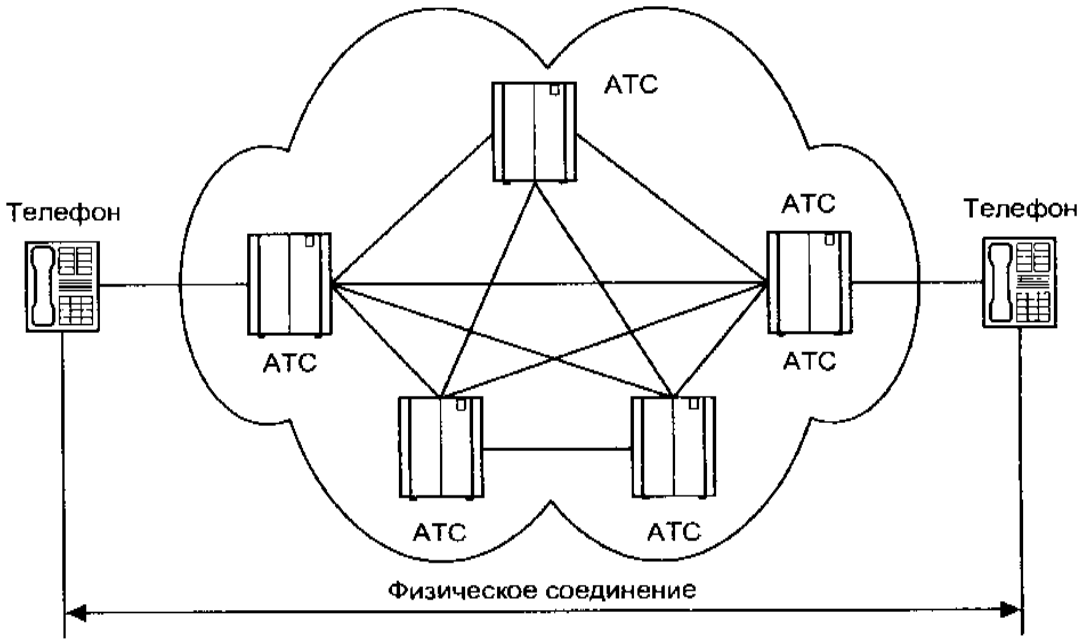


Рисунок 1.1 – Соединение в «классической» телефонной сети с коммутацией каналов.

Переход от аналоговых к цифровым технологиям стал важным шагом для возникновения современных цифровых телекоммуникационных сетей. Одним из таких шагов в развитии цифровой телефонии стал переход к пакетной коммутации. В сетях пакетной коммутации по каналам связи передаются единицы информации, которые не

зависят от физического носителя. Такими единицами могут быть пакеты, кадры или ячейки (в зависимости от протокола), но в любом случае они передаются по разделяемой сети (рисунок 1.2), более того - по отдельным виртуальным каналам, не зависящим от физической среды. Каждый пакет идентифицируется заголовком, который может содержать информацию об используемом им канале, его происхождении (то есть об источнике или отправителе) и пункте назначения (о получателе или приемнике).

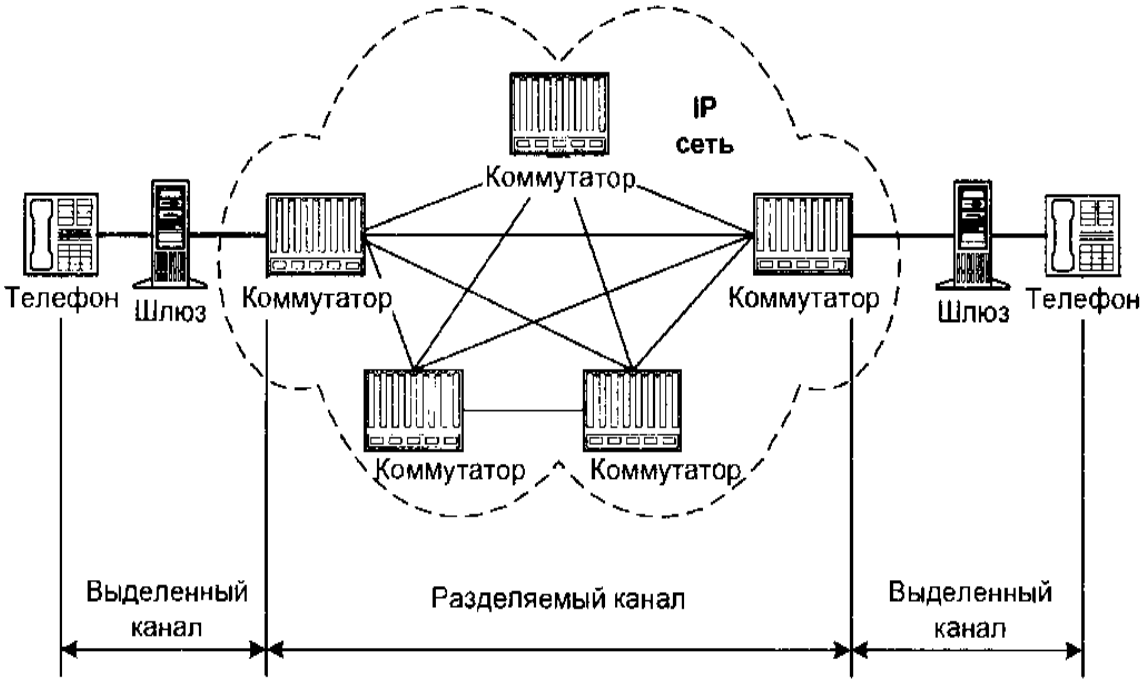


Рисунок 1.2 – Соединение в сети с коммутацией пакетов.

В сетях на основе протокола IP все данные - голос, текст, видео, компьютерные программы или информация в любой другой форме - передаются в виде пакетов. Любой компьютер и терминал такой сети имеет свой уникальный IP-адрес, и передаваемые пакеты маршрутизируются к получателю в соответствии с этим адресом, указываемом в заголовке. Данные могут передаваться одновременно между многими пользователями и процессами по одной и той же линии. При возникновении проблем IP-сети могут изменять маршрут для обхода неисправных участков. При этом протокол IP не требует выделенного канала для сигнализации.

Процесс отправки голоса по IP-сети состоит из нескольких этапов [1]:

1. Оцифровка голоса;
2. Анализ и обработка с целью уменьшения объема данных (подавление фонового шума и ненужных пауз, компрессирование);
3. Накопление информации и разбивка на пакеты;

4. Прикрепление протокольной информации к каждому пакету (адрес получателя, порядковый номер пакета на случай, если они будут доставлены не последовательно, и дополнительные данные для коррекции ошибок);

Извлечение переданной голосовой информации из полученных пакетов также происходит в несколько этапов:

1. Прием и накопление пакетов;

2. Проверка количества пакетов. В случае отсутствия пакета отсутствующие данные, как правило аппроксимируются либо заполняются шумом;

3. Проверка порядковой последовательности пакетов (IP-сети не гарантируют время доставки, пакеты могут прийти не по порядку);

4. Последовательность данных декомпрессируется и преобразуется в аудио-сигнал, несущий голосовую информацию.

Таким образом, с большой степенью вероятности, полученная информация не соответствует исходной (искажена) и задержана (обработка на приёмной и передающей сторонах требует промежуточного накопления). Однако в некоторых пределах избыточность голосовой информации позволяет мириться с такими потерями.

Абонент, оплативший полосу 64 кбит/с, использует канал в среднем лишь на 25 %. Значит, оператор способен продать имеющийся у него ресурс в четыре раза большему числу пользователей, не перегружая свою сеть. Это выгодно обеим сторонам – и клиенту, и продавцу, - поскольку оператор увеличивает свои доходы и уменьшает абонентскую плату за счёт снижения издержек.

В IP-телефонии существует два основных способа передачи голосовых пакетов по IP-сети:

- через глобальную сеть Интернет (Internet-телефония);

- через сети передачи данных на базе выделенных каналов (IP-телефония);

В Internet-телефонии полоса пропускания напрямую зависит от загруженности сети Интернет пакетами, содержащими данные, голос, графику, а значит, задержки при прохождении пакетов могут быть самыми разными. При использовании же выделенных каналов исключительно для голосовых пакетов можно гарантировать фиксированную (или почти фиксированную) скорость передачи. Ввиду широкого распространения сети Интернет особый интерес вызывает реализация системы Интернет-телефонии, хотя в этом случае качество телефонной связи оператором не гарантируется.

Для того чтобы осуществить междугородную (международную) связь с помощью телефонных серверов, оператор услуги должны иметь по серверу в тех местах, куда и откуда планируются звонки. Стоимость такой связи на порядок меньше стоимости телефонного

звонка по обычным телефонным линиям.

Общий принцип действия телефонных серверов Интернет-телефонии таков: с одной стороны, сервер связан с телефонными линиями и может соединиться с любым телефоном мира. С другой стороны, сервер связан с Интернетом и может связаться с любым компьютером в мире. Сервер принимает стандартный телефонный сигнал, оцифровывает его (если он исходно не цифровой), значительно сжимает, разбивает на пакеты и отправляет через Интернет по назначению с использованием протокола IP. Для пакетов, приходящих из сети на телефонный сервер и уходящих в телефонную линию, операция происходит в обратном порядке. Обе составляющие операции (вход сигнала в телефонную сеть и его выход из телефонной сети) происходят практически одновременно, что позволяет обеспечить полнодуплексный разговор. На основе этих базовых операций можно построить много различных конфигураций. Например, звонок «телефон-компьютер» или «компьютер-телефон» может обеспечивать один телефонный сервер. Для организации связи телефон (факс)-телефон (факс) нужно два сервера.

С точки зрения масштабируемости (если отвлечься от проблем с неконтролируемым ухудшением качества при росте нагрузки на сеть) IP-телефония представляется вполне законченным решением. Во-первых, поскольку соединение на базе протокола IP может начинаться (и заканчиваться) в любой точке сети от абонента до магистрали. Соответственно, IP-телефонию в сети можно вводить участок за участком, что, кстати, на руку и с точки зрения миграции, так как ее можно проводить «сверху вниз», «снизу вверх» или по любой другой схеме. Для решений IP-телефонии характерна определенная модульность: количество и мощность различных узлов - шлюзов, gatekeeper («привратников» - так в терминологии VoIP именуются серверы обработки номерных планов) - можно наращивать практически независимо, в соответствии с текущими потребностями [2].

Межсетевой протокол IP

В настоящее время наиболее эффективная передача потока любых дискретных (цифровых) сигналов, в том числе и несущих речь (голос), обеспечивается цифровыми сетями электросвязи, в которых реализована пакетная технология IP [2].

Протокол IP – основной протокол сетевого уровня, позволяющий реализовывать межсетевые соединения.

Следует подчеркнуть, что протокол IP реализуется не только в глобальной сети Интернет, для которой он был первоначально разработан, он может быть применен и в других цифровых телекоммуникационных сетях.

Основным сдерживающим фактором на пути масштабного внедрения IP-телефонии является отсутствие в протоколе IP механизмов обеспечения гарантированного качества

услуг, что делает его пока не самым надежным транспортом для передачи голосового трафика. Протокол IP обрабатывает каждый IP-пакет как независимую единицу, не имеющую связи ни с какими другими IP-пакетами. Сам протокол IP не гарантирует доставку пакетов, а также время их доставки, что вызывает такие проблемы, как «рваный голос» и просто провалы в разговоре. В протоколе IP нет механизмов, обычно применяемых для увеличения достоверности конечных данных: отсутствует квитирование – обмен подтверждениями между отправителем и получателем, нет процедуры упорядочения, повторных передач или других подобных функций. Если во время продвижения пакета произошла какая-либо ошибка, то протокол IP по своей инициативе ничего не предпринимает для исправления этой ошибки. Например, если на промежуточном маршрутизаторе пакет был отброшен по причине истечения времени жизни или из-за ошибки в контрольной сумме, то модуль IP не пытается заново послать испорченный или потерянный пакет. Все вопросы обеспечения надежности доставки данных по составной сети в стеке TCP/IP решает протокол TCP, работающий непосредственно над протоколом IP.

Администратор сети присваивает оконечным устройствам IP-адреса в соответствии с тем, к каким IP-сетям они подключены. Для IP-адреса первоначально выбрали размер в 32 бита для удобства его обработки в 32 – разрядном регистре компьютера. Для обеспечения свойства иерархичности адрес содержит две части: номер сети и номер узла (рисунок 1.3). Число бит, отводимых для этих номеров, может быть переменным [6].

Описание основных протоколов систем IP телефонии

Стандарт H.323

Набор рекомендаций МСЭ-Т H.323 определяет сетевые компоненты, протоколы и процедуры, позволяющие организовать мультимедиа-связь в пакетных сетях, в том числе в ЛВС Ethernet. Они определяют порядок функционирования абонентских терминалов в сетях с разделяемым ресурсом, не гарантирующих качества обслуживания QoS. H.323-совместимые устройства могут применяться для телефонной связи (IP-телефония), передачи звука и видео (видеотелефония), а также звука, видео и данных (мультимедийные конференции).

В связи с появлением множества аппаратно-программных средств организации телефонной связи по протоколу IP потребовалось внести изменения в спецификации H.323, так как эти средства зачастую оказывались несовместимыми друг с другом. В частности, понадобилось обеспечить взаимодействие телефонных устройств на базе ПК и обычных телефонов для сетей, функционирующих по принципу коммутации каналов. Стандарт H.323 входит в семейство рекомендаций H.32x, описывающих порядок организации мультимедиа-связи в сетях различных типов:

- H.320 - узкополосные цифровые коммутируемые сети, включая -ISDN;
- H.321 - широкополосные сети ISDN и ATM;
- H.322 - пакетные сети с гарантированной полосой пропускания;
- H.324 - телефонные сети общего пользования (ТфОП).

Одна из основных целей разработки стандарта H.323 - обеспечение взаимодействия с другими типами сетей мультимедиа-связи (рисунок 2.1). Данная задача реализуется с помощью шлюзов, осуществляющих трансляцию сигнализации и форматов данных. Стандарт H.323 позволяет создать надежные решения для организации коммуникаций по ненадежным сетям с переменной задержкой. При условии соответствия стандарту устройства с различными возможностями могут и взаимодействовать друг с другом. Например, терминалы с видео средствами могут участвовать в аудиоконференции. В совокупности с другими стандартами МСЭ-Т на мультимедийную связь и телеконференции рекомендации H.323 применимы для любых видов соединений - от многоточечных до соединений «точка-точка» [1]. Основные компоненты этого стандарта приведены в таблице 1.

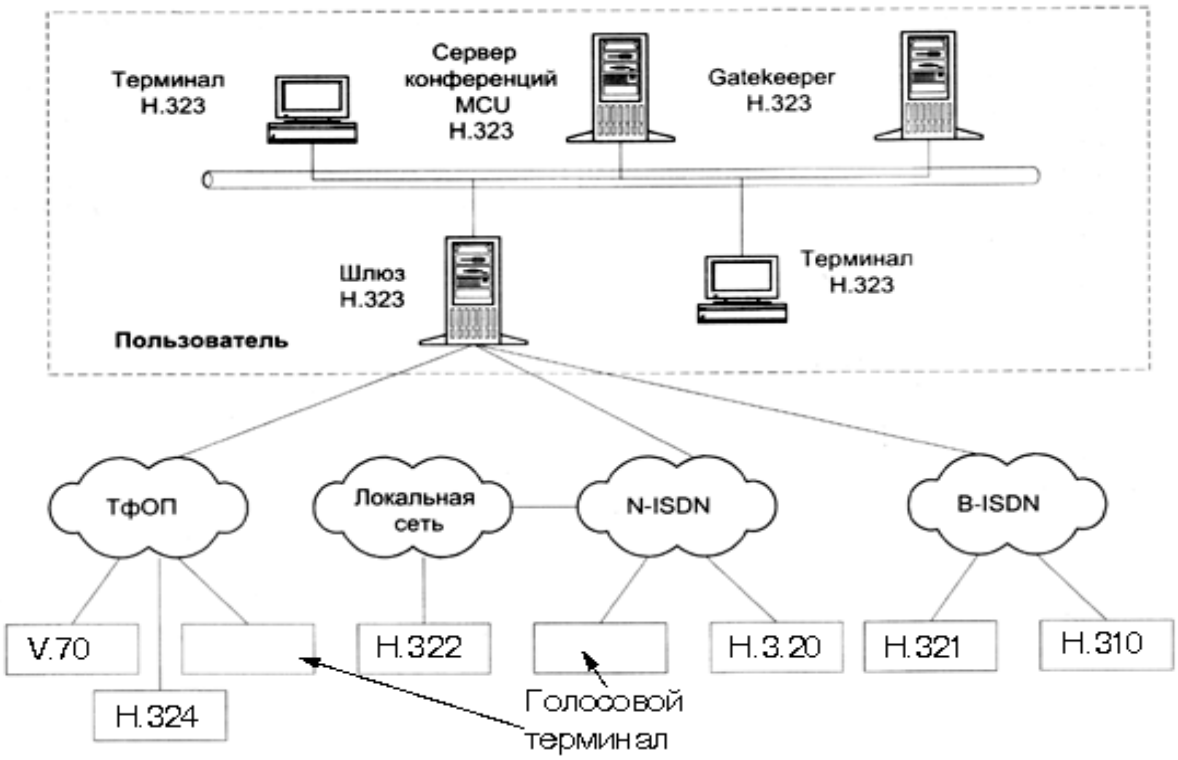


Рисунок 2.1 – Конфигурация сети на базе стандарта H.323

Стандарт H. 323 определяет также порядок взаимодействия с оконечными устройствами других стандартов. Наиболее часто такая задача возникает при сопряжении телефонных сетей с коммутацией пакетов и коммутацией каналов. Сети стандарта H.323 совместимы и с другими типами H.32x-сетей. Межсетевое взаимодействие различных H.32x-сетей определяет рекомендация H.246. На следующем этапе развития IP-телефонии к

спецификациям H.323, соответствующим нижним уровням эталонной модели взаимодействия открытых систем (ЭМВОС), будут добавлены новые. Они зафиксируют возможности обеспечения классов (class-of-service, CoS) и качества обслуживания (quality-of-service, QoS), т. е. услуг, относящихся, соответственно, ко второму (канальному) и третьему (сетевому) уровням [1].

Протокол инициирования сеансов связи (SIP)

За годы работы с протоколом H.323 накоплен большой опыт использования, который позволил выявить как его положительные черты, так и недостатки, которые были учтены при разработке протокола SIP.

Протокол инициирования сеансов – Session Initiation Protocol (SIP) является протоколом прикладного уровня и предназначается для организации, модификации и завершения сеансов связи: мультимедийных конференций, телефонных соединений и передачи данных. Пользователи могут принимать участие в существующих сеансах связи, приглашать других пользователей и быть приглашенными ими к новому сеансу связи.

Приглашения могут быть адресованы определенному пользователю, группе пользователей или всем пользователям [3].

Протокол SIP разработан группой MMUSIC (Multiparty Multimedia Session Control) комитета IETF (Internet Engineering Task Force), а спецификации протокола представлены в документе RFC 2543.

В основу протокола рабочая группа MMUSIC заложила следующие принципы:

- Персональная мобильность пользователей.

Пользователи могут перемещаться без ограничений в пределах сети, поэтому услуги связи должны предоставляться им в любом месте этой сети. Пользователю присваивается уникальный идентификатор, а сеть предоставляет ему услуги связи вне зависимости от того, где он находится. Для этого пользователь с помощью специального сообщения – REGISTER – информирует о своих перемещениях сервер определения местоположения.

- Масштабируемость сети.

Она характеризуется, в первую очередь, возможностью увеличения количества элементов сети при ее расширении. Серверная структура сети, построенной на базе протокола SIP, в полной мере отвечает этому требованию.

- Расширяемость протокола.

Она характеризуется возможностью дополнения протокола новыми функциями при введении новых услуг и его адаптации к работе с различными приложениями.

Расширение функций протокола SIP может быть произведено за счет введения новых заголовков сообщений. При этом, если SIP-сервер принимает сообщения с неизвестными ему

полями, то он просто игнорирует их и обрабатывает лишь те поля, которые он знает.

Для расширения возможностей протокола SIP могут быть также добавлены и новые типы сообщений.

- Интеграция в стек существующих протоколов Internet.

Протокол SIP является частью глобальной архитектуры мультимедиа, разработанной комитетом IETF. Эта архитектура включает в себя также протокол резервирования ресурсов (Resource Reservation Protocol - RSVP), транспортный протокол реального времени (Real-Time Transport Protocol - RTP), протокол передачи потоковой информации в реальном времени (Real-Time Streaming Protocol - RTSP). Однако функции протокола SIP не зависят ни от одного из этих протоколов.

- Взаимодействие с другими протоколами сигнализации.

Протокол SIP может быть использован совместно с протоколом H.323. Возможно даже взаимодействие протокола SIP с системами сигнализации ТфОП – DSS1 и ОКС7. Для упрощения такого взаимодействия сигнальные сообщения протокола SIP могут переносить не только специфический SIP-адрес, но и телефонный номер формата E.164 или любого другого формата. [4]

Одной из важнейших особенностей протокола SIP является его независимость от транспортных технологий. Но, в то же время, предпочтение отдается технологии маршрутизации пакетов IP и протоколу UDP. При этом, правда, необходимо создать дополнительные механизмы для надежной доставки сигнальной информации. К таким механизмам относятся повторная передача информации при ее потере, подтверждение приема и др.

Здесь же следует отметить то, что сигнальные сообщения могут переноситься не только протоколом транспортного уровня UDP, но и протоколом TCP. Протокол UDP позволяет быстрее, чем TCP, доставлять сигнальную информацию (даже с учетом повторной передачи неподтвержденных сообщений), а также вести параллельный поиск местоположения пользователей и передавать приглашения к участию в сеансе связи в режиме многоадресной рассылки.

Таблица 2 – Место протокола SIP в стеке протоколов TCP/IP

Протокол инициирования сеансов связи (SIP)	Прикладной уровень
Протоколы TCP и UDP	Транспортный уровень
Протоколы IPv4 и IPv6	Сетевой уровень

PPP, ATM, Ethernet	Уровень звена данных
UTP5, SDH, PDH, V.34 и др	Физический уровень

По сети с маршрутизацией пакетов IP может передаваться пользовательская информация практически любого вида: речь, видео и данные, а также любая их комбинация, называемая мультимедийной информацией. При организации связи между терминалами пользователей необходим механизм обмена информацией о том, какие сервисы может использовать вызываемая\вызывающая стороны. Для этой цели используется протокол SDP (Session Description Protocol) - протокол описания сессии. Данный протокол позволяет определить, какие звуковые (видео и другие) кодеки и иные возможности может использовать удаленная сторона.

Для передачи речевой информации комитет IETF предлагает использовать протокол RTP (Real-time Transport Protocol, протокол транспортировки в реальном времени). Таким образом, сам протокол SIP непосредственного участия в передаче голосовых, видео и других данных не принимает, он отвечает только за установление связи (по протоколам SDP, RTP и др.), поэтому под SIP-телефонией понимается не передача голоса по протоколу SIP, а передача голоса с использованием протокола SIP. Использование протокола SIP предоставляет новые возможности установления соединений (а также возможность беспроблемного расширения данных возможностей), а не непосредственной передачи голосового и других видов трафика.

В глобальной информационной сети Интернет уже довольно давно функционирует экспериментальный участок Mbone, который образован из сетевых узлов, поддерживающих режим многоадресной рассылки мультимедийной информации. Важнейшей функцией Mbone является поддержка мультимедийных конференций, а основным способом приглашения участников к конференции стал протокол SIP. Протокол SIP дает возможность присоединения новых участников к уже существующему сеансу связи, т.е. двусторонний сеанс может перейти в конференцию.

Предназначенный для инициации сеансов протокол SIP обеспечивает определение адреса пользователя и установления соединения с ним. Кроме этого, он служит основой для применения других протоколов, реализующих функции защиты, аутентификации, описания канала мультимедийной связи и т.д [3].

Для организации взаимодействия с существующими приложениями IP-сетей и для обеспечения мобильности пользователей протокол SIP использует адрес, подобный адресу электронной почты. В качестве адресов рабочих станций используются специальные

универсальные указатели ресурсов - URL (Universal Resource Locators), так называемые SIP URL.

SIP-адреса бывают четырех типов:

• имя@домен;

• имя@хост;

• имя@IP-адрес;

• №телефона@шлюз.

Таким образом, адрес состоит из двух частей. Первая часть - это имя пользователя, зарегистрированного в домене или на рабочей станции. Если вторая часть адреса идентифицирует какой-либо шлюз, то в первой указывается телефонный номер абонента.

Во второй части адреса указывается имя домена, рабочей станции или шлюза. Для определения IP-адреса устройства необходимо обратиться к службе доменных имен - Domain Name Service (DNS). Если же во второй части SIP-адреса размещается IP-адрес, то с рабочей станцией можно связаться напрямую.

В начале SIP-адреса ставится слово «sip:», указывающее, что это именно SIP-адрес, т.к. бывают и другие (например, «mailto:»). Ниже приводятся примеры SIP-адресов:

sip: als@rts.loniis.ru

sip: user1@192.168.100.152

sip: 294-75-47@gateway.ru

SIP использует обычные текстовые сообщения и очень напоминает HTTP протокол (практически базируется на нем). Архитектура сети SIP базируется на клиент-серверном взаимодействии (рисунок 2.2).

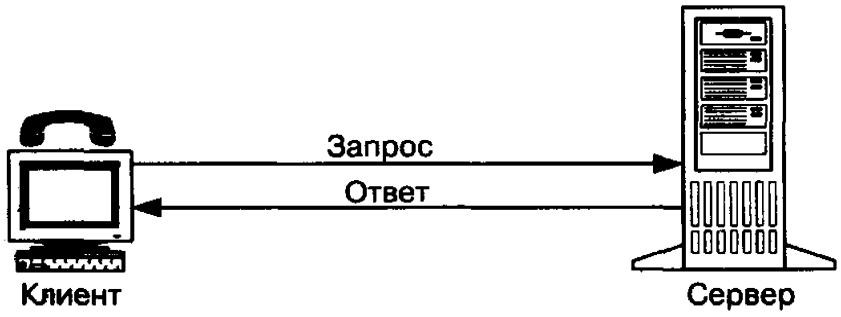


Рисунок 3.2 – Архитектура "клиент-сервер".

Стандартными элементами в SIP-сети являются:

1. User Agent: по протоколу SIP устанавливаются соединения "клиент-сервер". Клиент устанавливает соединения, а сервер принимает вызовы, но так обычно телефонный аппарат (или программный телефон) может, как устанавливать, так и принимать звонки, то получается, что он одновременно играет роль и клиента и сервера (хотя в реализации протокола это не является обязательным критерием) - в этом случае его называют User Agent

(UA) или терминал.

В составе UA выделяются две логические составляющие:

- агент-клиент (UAC - user agent client) - посылает запросы и получает ответы;
- агент-сервер (UAS - user agent server) - принимает запросы и посылает ответы.

Ввиду того, что большинству устройств необходимо как передавать, так и принимать данные, в реальных устройствах присутствует как UAC, так и UAS.

2. Прокси-сервер: прокси-сервер принимает запросы и производит с ним некоторые действия (например, определяет местоположение клиента, производит переадресацию или перенаправление вызова и др.). Он также может устанавливать собственные соединения. Зачастую прокси-сервер совмещают с сервером определения местоположения (Register-сервер), в таком случае его называют Registrar-сервером.

3. Сервер определения местоположения или сервер регистрации (Register): данный вид сервера служит для регистрации пользователей. Регистрация пользователя производится для определения его текущего IP-адреса, для того чтобы можно было произвести вызов user@IP-адрес. В случае если пользователь переместится в другое место и/или не имеет определенного IP-адреса, его текущий адрес можно будет определить после того, как он зарегистрируется на сервере регистрации. Таким образом, клиент останется доступен по одному и тому же SIP-адресу вне зависимости от того, где на самом деле находится.

4. Сервер переадресации (Redirect): обращается к серверу регистрации для определения текущего IP-адреса пользователя, но в отличие от прокси-сервера только «переадресует» клиента, а не устанавливает собственные соединения [4].

В результате SIP архитектура выглядит следующим образом (рисунок 2.3):

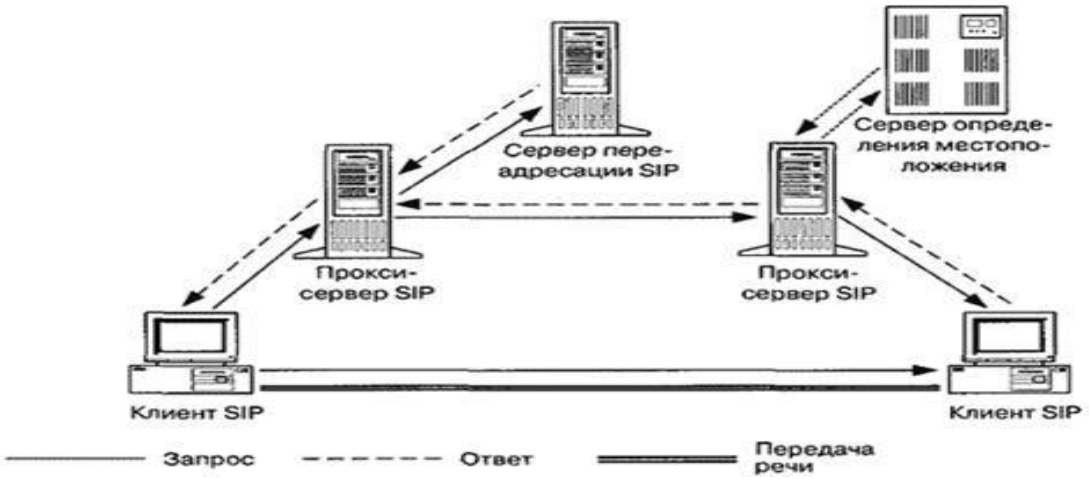


Рисунок 3.3 – Архитектура сети на базе протокола SIP.

Asterisk

Asterisk — свободное решение компьютерной телефонии (в том числе, VoIP) с открытым исходным кодом от компании Digium, первоначально разработанное Марком Спенсером. Приложение работает на операционных системах Linux, FreeBSD, OpenBSD и Solaris. Имя проекта произошло от названия символа «*» (англ. asterisk — «звездочка»).

Asterisk в комплексе с необходимым оборудованием обладает всеми возможностями классической АТС, поддерживает множество VoIP-протоколов и предоставляет богатые функции управления звонками, среди них:

- Голосовая почта.
- Конференции.
- Интерактивное голосовое меню (IVR).
- Центр обработки вызовов (постановка звонков в очередь и распределение их по агентам используя различные алгоритмы).
- Запись (Call Detail Record).

Для создания дополнительной функциональности можно воспользоваться собственным языком Asterisk для написания плана нумерации, написав модуль на языке Си, либо воспользовавшись AGI — гибким и универсальным интерфейсом для интеграции с внешними системами обработки данных. Модули, выполняющиеся через AGI, могут быть написаны на любом языке программирования.

Asterisk распространяется на условиях двойной лицензии, благодаря которой одновременно с основным кодом, распространяемым по открытой лицензии GNU GPL, возможно создание закрытых модулей, содержащих лицензируемый код.

Asterisk может работать как с аналоговыми линиями (FXO/FXS модули), так и цифровыми (ISDN, BRI и PRI — потоки T1/E1). С помощью определённых компьютерных плат (наиболее известными производителями которых являются Digium, Sangoma, OpenVox, Rhino, AudioCodes) Asterisk можно подключить к высокопропускным линиям T1/E1, которые позволяют работать параллельно с десятками и сотнями телефонных соединений. Полный список поддерживаемого оборудования для соединения с телефонной сетью общего пользования определяется поддержкой оборудования в модулях ядра.

Для создания дополнительной функциональности можно воспользоваться собственным языком Asterisk для написания плана нумерации, написав модуль на языке C, либо воспользовавшись AGI - гибким и универсальным интерфейсом для интеграции с внешними системами обработки данных. Модули, выполняющееся через AGI, могут быть написаны на любом языке программирования.

Asterisk распространяется на условиях двойной лицензии, благодаря которой

одновременно с основным кодом, распространяемым по открытой лицензии GNU GPL, возможно создание закрытых модулей, содержащих лицензируемый код: например, модуль для поддержки кодека G.729.

Благодаря свободной лицензии Asterisk активно развивается и поддерживается тысячами людей со всей планеты. В течение последних двух лет рынок Asterisk-приложений активно развиваются в США и уже заняли прочное место на рынке IT-технологий (более 1000 компаний, центры поддержки, online-консультации). В Россию данный продукт попал позже, но интерес российского потребителя растёт, и в первую очередь, благодаря открытости системы. Многие компании применяют Asterisk в своих серийных VoIP-устройствах, например компании Linksys, Nateks.

Поддерживаются следующие протоколы:

- SIP,
- H.323,
- IAX2,
- MGCP,
- Skinny/SCCP,
- XMPP (Google Talk),
- Unistim,
- Skype, через коммерческий канал.

Настройка и программирование производится с помощью нескольких механизмов:

- диалплан, который пишется на специальном языке. Доступна как старая версия, так и новая — AEL, а также на языке Lua.
- AGI.
- AMI.
- Конфигурация из баз данных.

IP-АТС на основе Asterisk обладает возможностями:

- Запись телефонных разговоров
- Конференц-комнаты с использованием виртуальных номеров
- Голосовая почта и пересылка на e-mail
- Поддержка протоколов SIP, IAX2, H.323, MGCP, Skinny
- Инструменты разработчика для создания расширений, предоставляющие новые услуги
- Поддержка кодеков: ADPCM, G.711 (A-Law и μ-Law), G.722, G.723.1, G.726, G.728, G.729, GSM, ILBC, Speex.

- Виртуальный секретарь - IVR
- Поддержка аналоговых интерфейсов FXS / FXO
- Голосовой синтез речи
- Поддержка цифровых интерфейсов (E1/T1/J1) и протоколов PRI/BRI/R2/SS7
- Автоконфигурация IP-телефонов
- АОН определитель номера
- Программное эхоподавление
- Работа с несколькими операторами связи
- Маршрутизация входящих и исходящих вызовов по различным правилам
- Поддержка Видеотелефонов
- Интерфейс обнаружения телефонного оборудования
- Поддержка групповой переадресации вызовов
- DHCP сервер для распределения динамических IP адресов
- Панель оператора. Оператор может видеть всю телефонную деятельность в виде графиков и выполнять простые операции по управлению телефонными звонками
- Поддержка протокола пейджинга (intercom) и домофонов
- Веб-панель управления
- Поддержка временных условиях
- Парковка и перехват звонка
- Запрет вызова по PIN коду
- Call Detail Record (CDR) отчеты
- Прямой доступ в систему (DISA)
- Биллинг, отчеты, статистика, анализ по использованию
- Поддержка обратного звонка
- Поддержка динамических очередей

Asterisk, благодаря гибкой системе настроек, позволяет строить различные решения голосовой связи, в зависимости от требований.

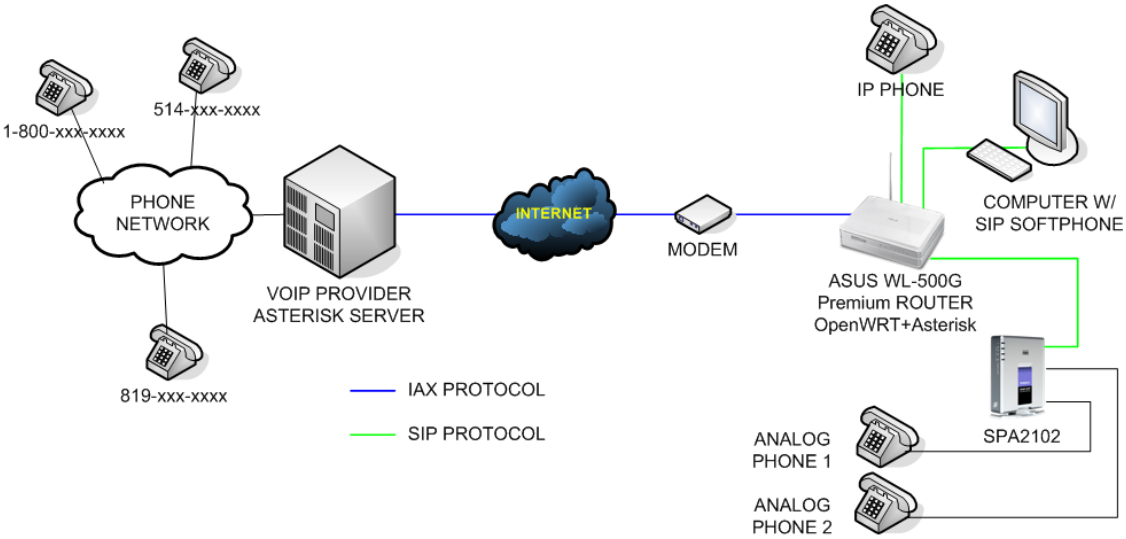


Рисунок 5.1 – Пример сетевого решения на базе Asterisk.

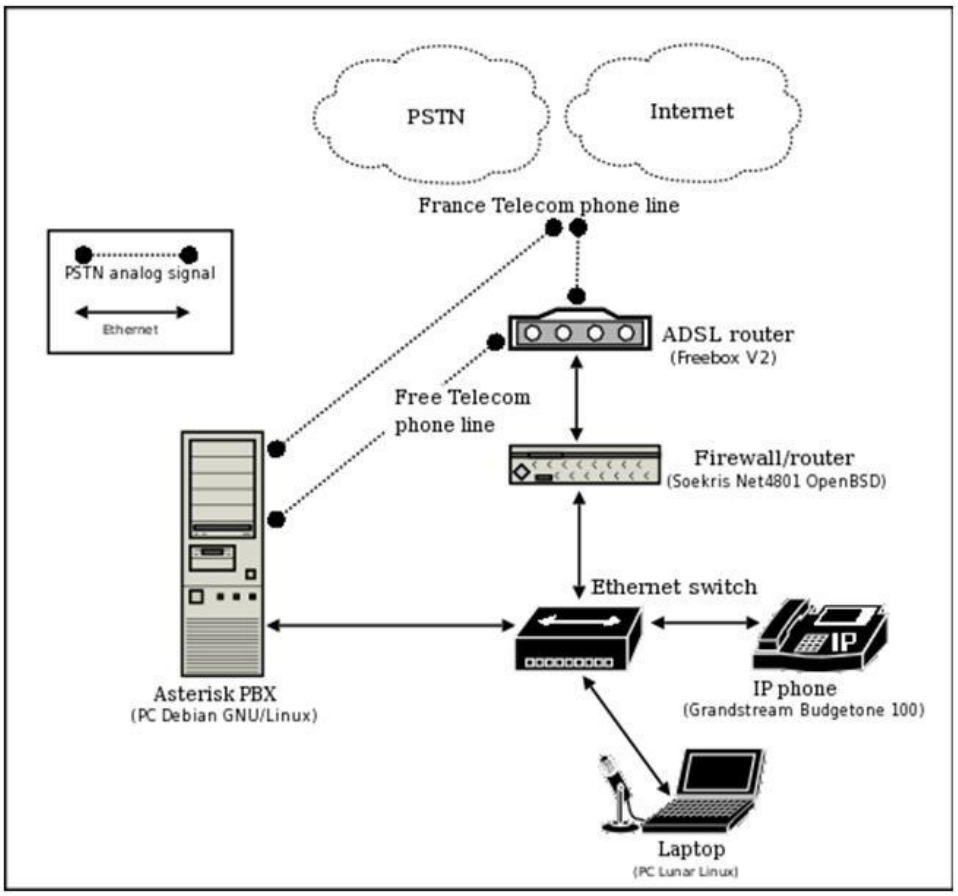


Рисунок 5.2 – Структурная схема сетевого решения на базе Asterisk.

Методические указания по настройке Asterisk

Работа с сервером. Настройка Asterisk

Asterisk разработан для работы на UNIX-образных операционных системах, например Ubuntu, CentOS, Debian и пр. Если имеется возможность выделить отдельный сервер, то Asterisk можно установить на сервер под управлением любой из этих операционных систем. Однако, если такой возможности нет, то Asterisk можно установить на виртуальной машине и при соответствующих настройках компьютер с виртуальной машиной становится одновременно IP-АТС сервером (Asterisk на виртуальной машине с UNIX) и IP-АТС абонентом (софтофон на Windows).

В первую очередь необходимо установить виртуальную машину. В папке с сопутствующими программами имеется exe установочный файл виртуальной машины Virtual Box. После открытия установочного файла появляется окно (рисунок 4.1).

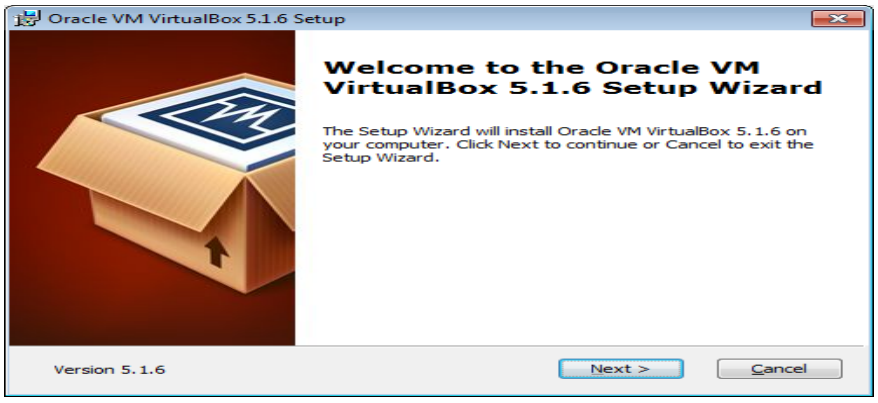


Рисунок 4.1 – Окно установки VirtualBox.

Выполняя требования установочной программы по умолчанию, VirtualBox будет установлен. Далее необходимо установить и настроить сервер. Настроенный сервер имеется в папке с сопутствующими программами. Процесс установки занимает много времени. Если есть возможность, то следует воспользоваться готовым настроенным сервером AsteriskVideo (рисунок 4.3). Если такой возможности нет, то в Приложении А процесс настройки сервера Asterisk показан.

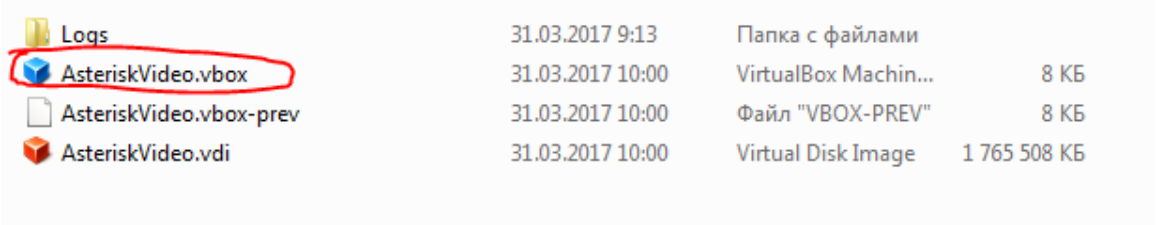


Рисунок 4.2 – Папка с образом виртуальной машины.

К файлу с сервером для виртуальной машины (vbox) прилагается файл виртуального жесткого диска (vdi), без которого сервер работать не будет. Открытие файла vbox приводит к запуску сервера на CentOS 6.4 minimal. Графическая оболочка на сервере отсутствует.

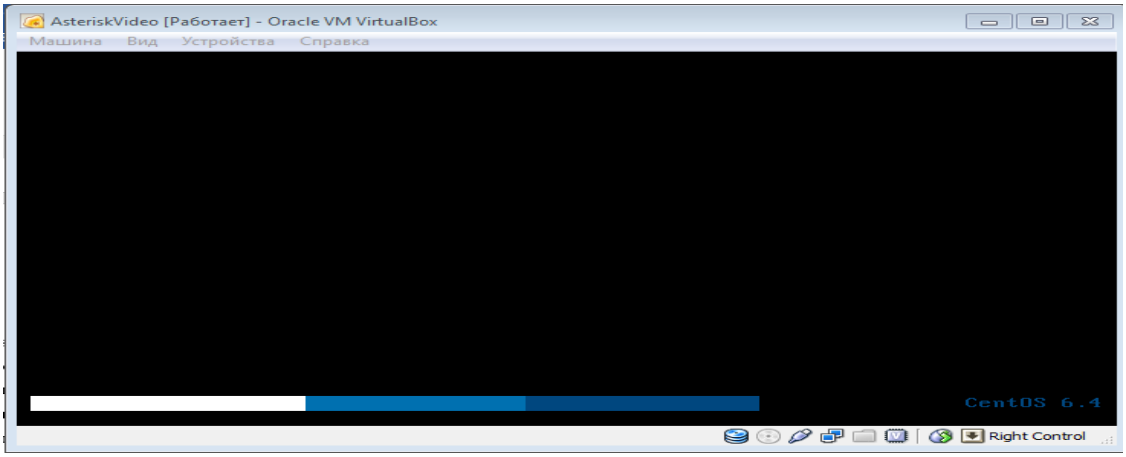


Рисунок 4.3 – Процесс запуска сервера на виртуальной машине.

После запуска сервер потребует ввода логина и пароля.

Логин сервера: ***root***

Пароль сервера: ***123456***

После ввода логина и пароля сервер начинает работу.

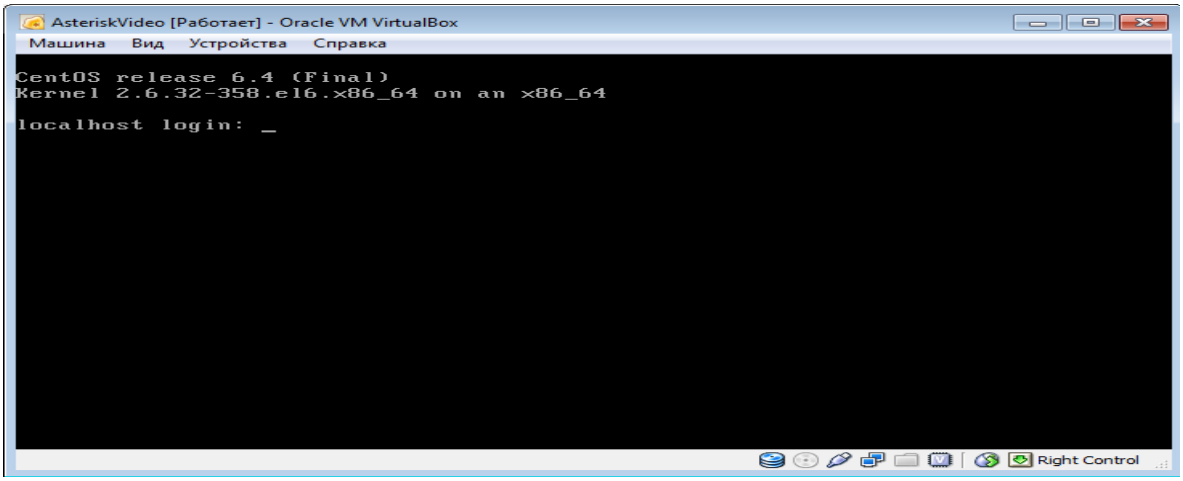


Рисунок 4.4 – Сервер ожидает ввода логина и пароля.

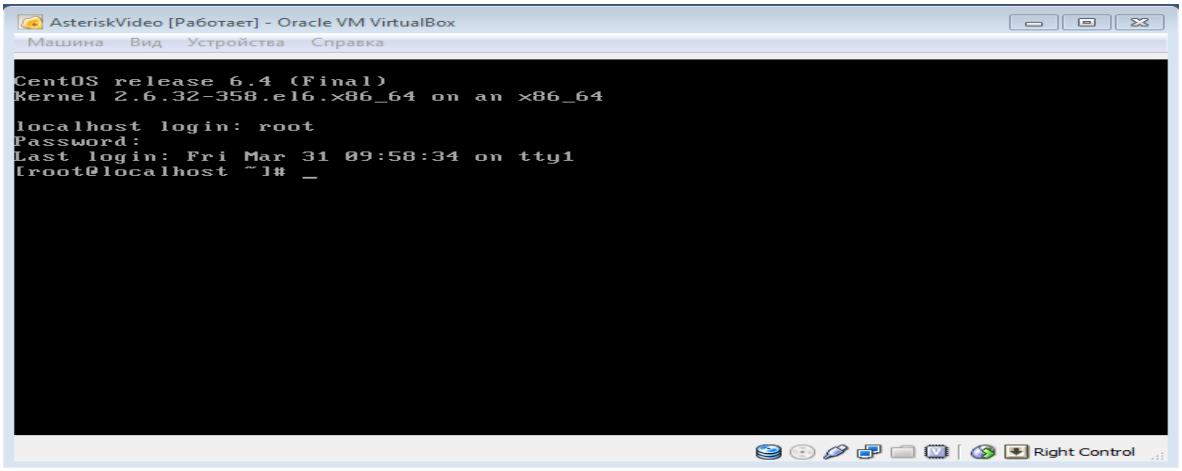


Рисунок 4.5 – Сервер после ввода логина и пароля.

Далее необходимо установить необходимые сетевые настройки для виртуальной машины. Для этого машину нужно поставить на паузу (Машина > Пауза)

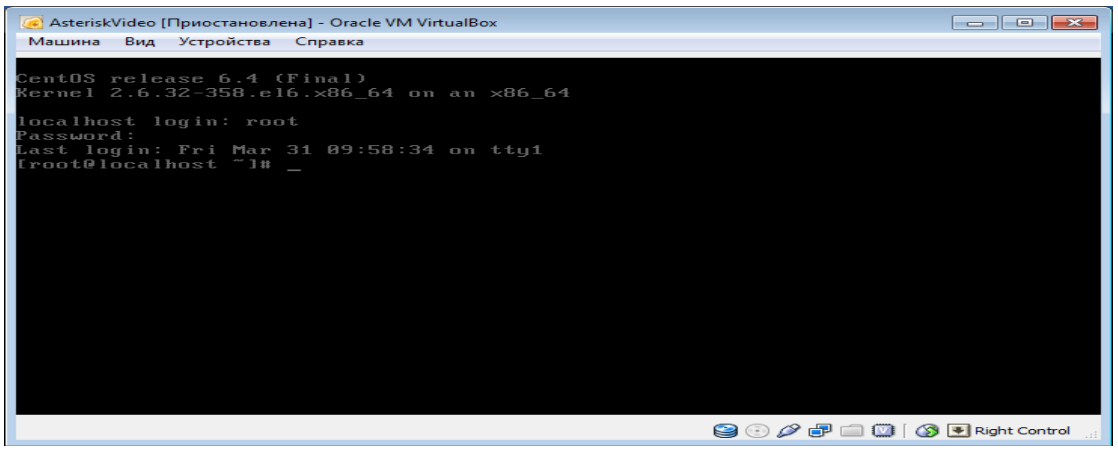


Рисунок 4.6 – Виртуальная машина на паузе.

Теперь возможна настройка сетевых адаптеров (Устройства > Сетевые адаптеры…). По умолчанию Адаптер 1 настроен в режим NAT, а Адаптер 2 – в режим виртуального хоста (рисунок 4.7).

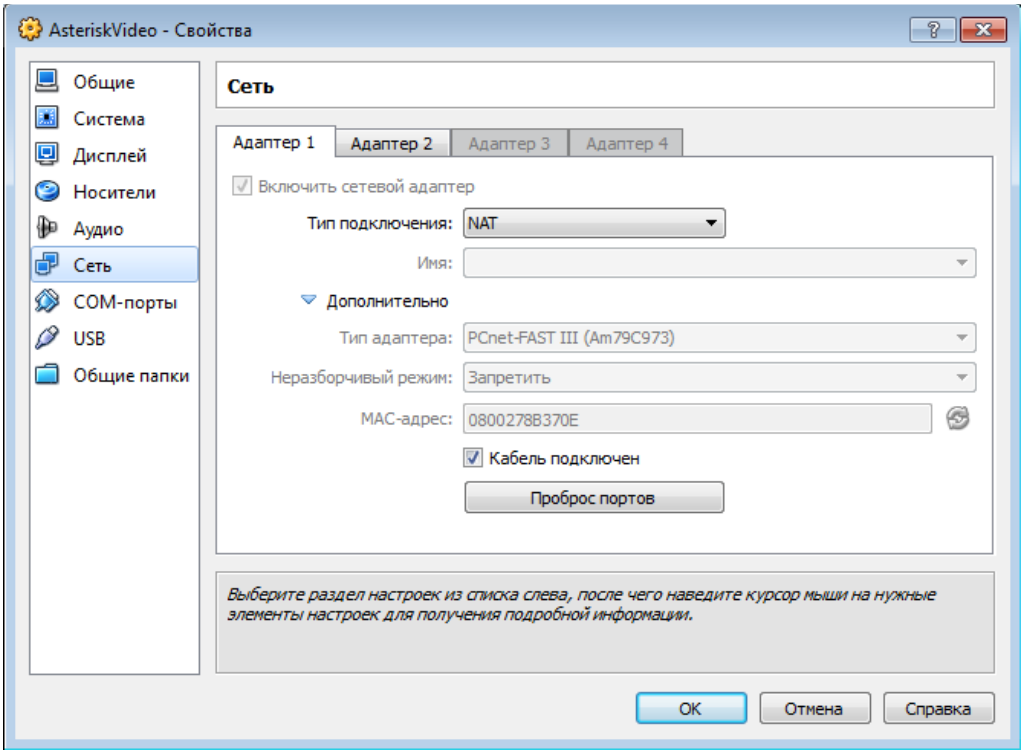


Рисунок 4.7 – Сетевые настройки виртуальной машины по умолчанию.

Адаптер 1 нужно перевести в режим сетевого моста (рисунок 4.8). В соединении типа "Сетевой мост" виртуальная машина работает также, как и все остальные компьютеры в сети. В этом случае адаптер выступает в роли моста между виртуальной и физической сетями. Со стороны внешней сети имеется возможность напрямую соединяться с гостевой операционной системой.

Помимо этого, нужно убедиться, что в пункте «Имя» выбран физический сетевой адаптер (например, Ethernet). Неразборчивому режиму нужно разрешить всё. После этого виртуальная машина видна для маршрутизатора как отдельное полноценное сетевое

устройство.

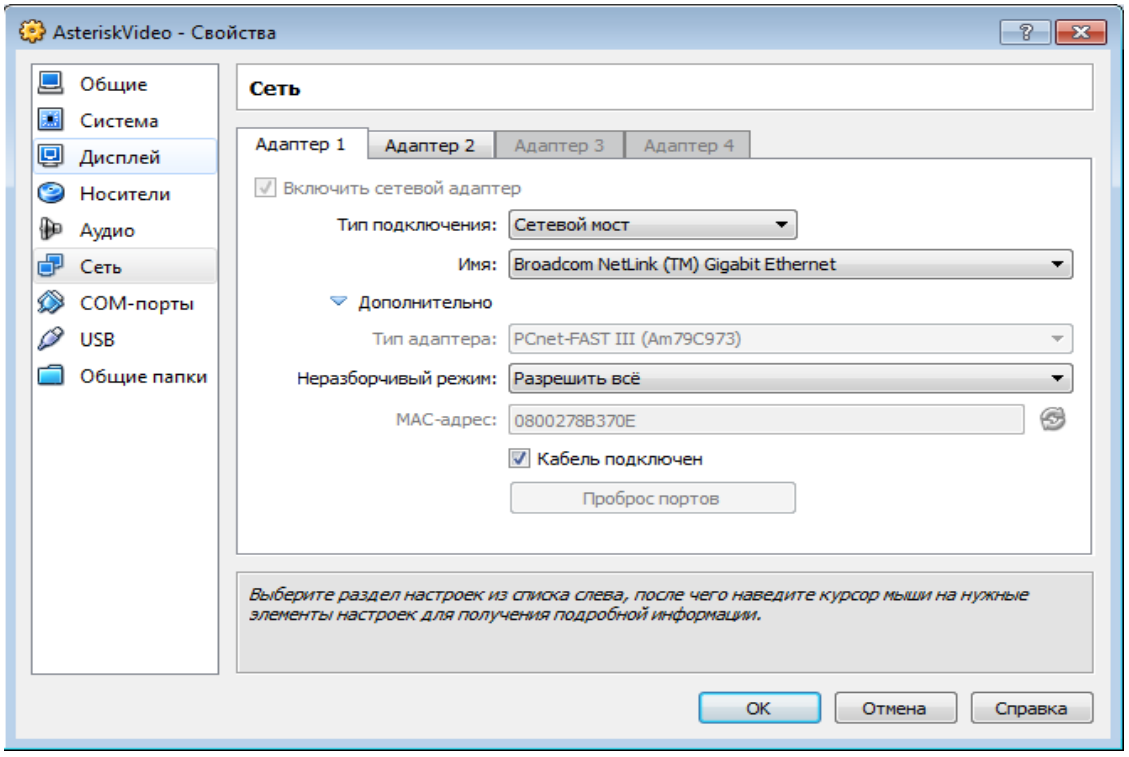


Рисунок 4.8 – Сетевые настройки виртуальной машины после редактирования Адаптера 1.

Для сохранения настроек Адаптера 1 и отключения Адаптера 2 необходимо выключить сервер командой (рисунок 4.9):

poweroff

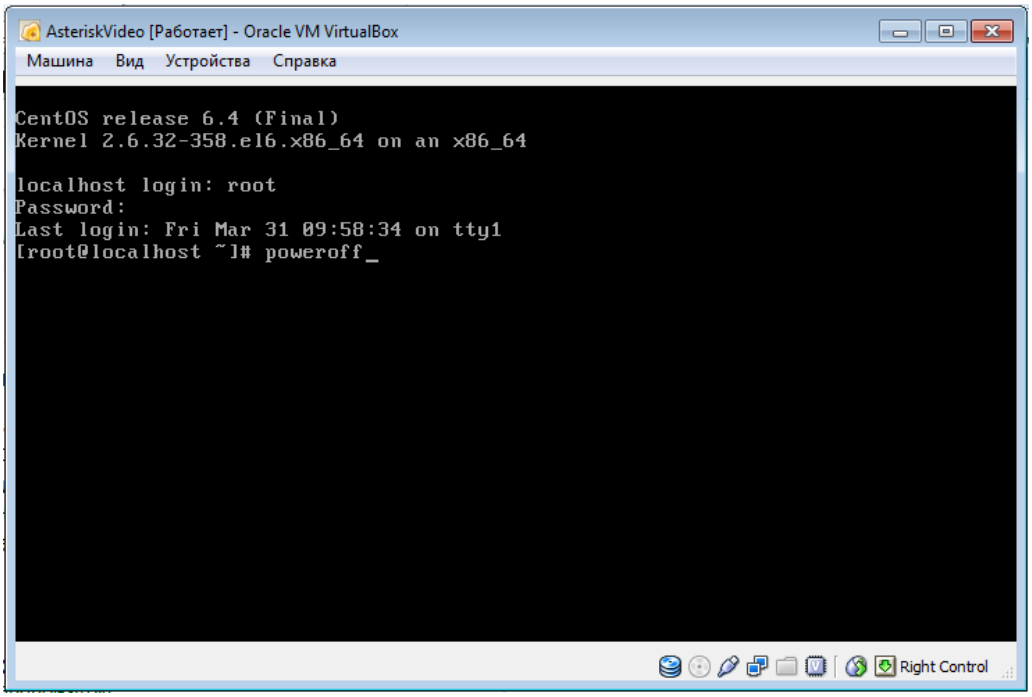


Рисунок 4.9 – Отключение сервера.

Настроить или включить сервер можно через окно программы VirtualBox (рисунок

4.10). Нажатие на кнопку «Свойства» при выборе машины AsteriskVideo открывает окно настроек (рисунок 4.11).

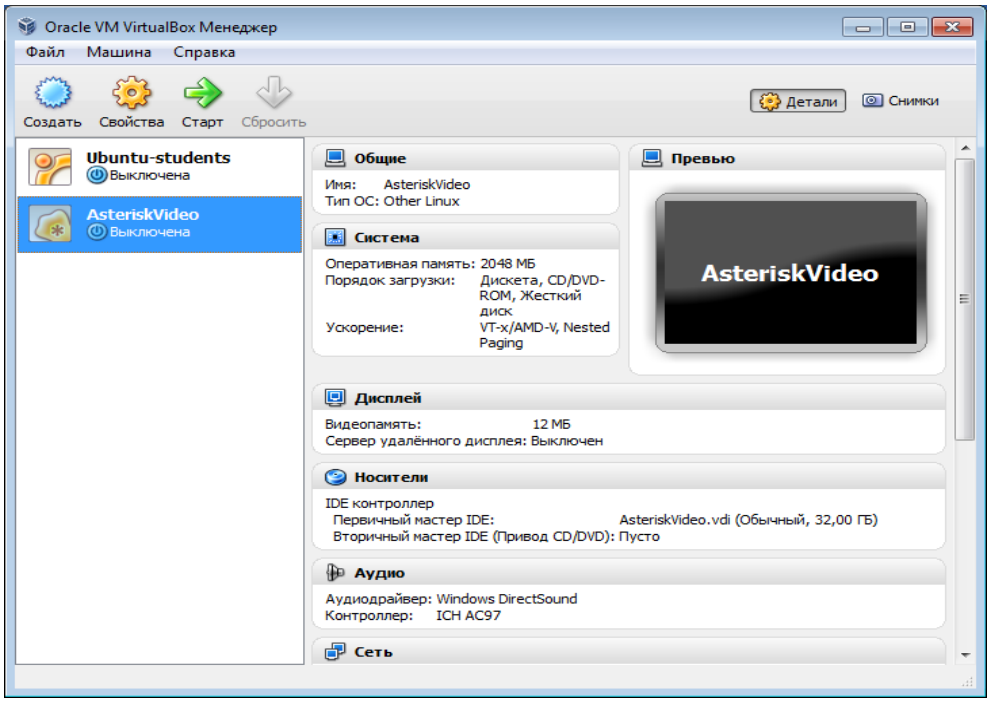


Рисунок 4.10 – Окно программы VirtualBox.

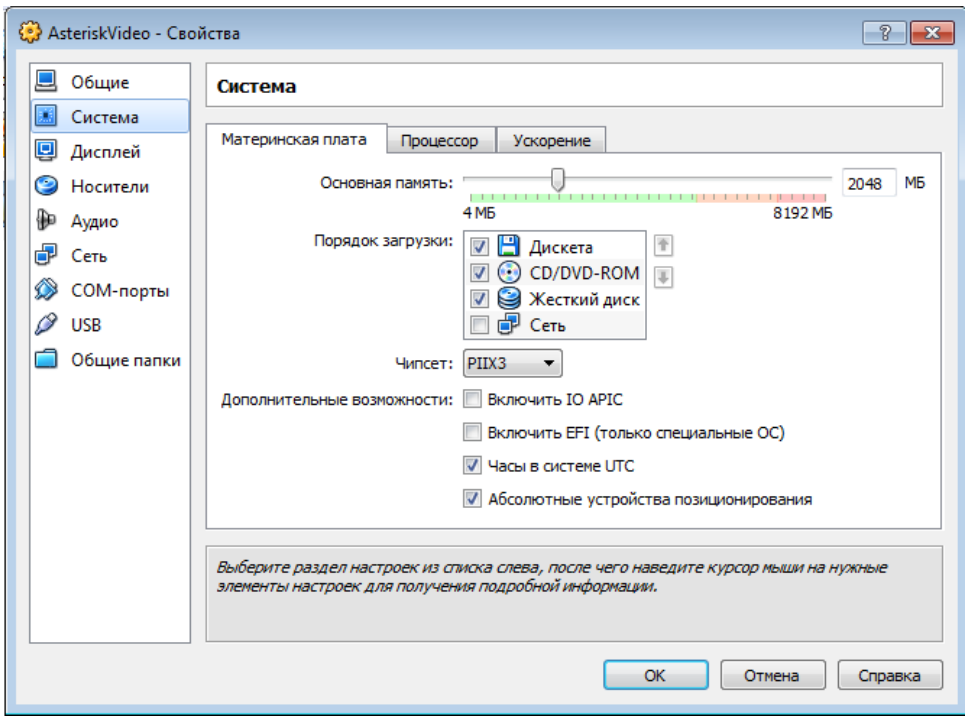


Рисунок 4.11 – Окно настроек «Система» VirtualBox.

В настройках «Система» нужно проверить, чтобы на вкладках «Материнская плата» и «Процессор» все ползунки были в зеленой зоне. В таком случае виртуальная машина не перегружает ресурсы компьютера.

То же самое нужно сделать в настройках «Дисплей».

В настройках «Сеть» нужно выключить Адаптер 2 (рисунок 4.12) убрав соответствующую галочку.

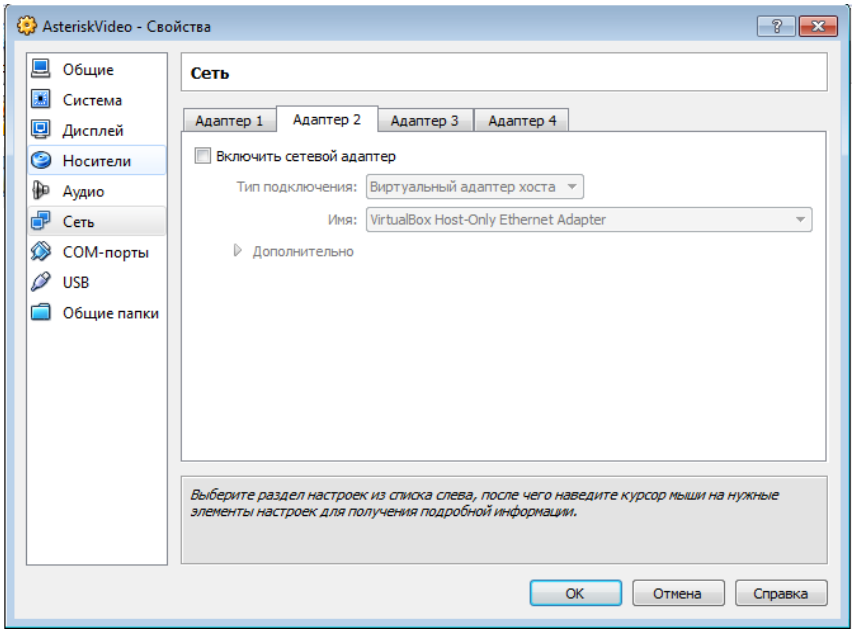


Рисунок 4.12 – Отключение Адаптера 2.

Далее можно запускать виртуальную машину двойным щелчком AsteriskVideo. Основное окно менеджера VirtualBox после запуска можно закрыть.

Работа в консоли без графического интерфейса достаточно проблематична. Например, в консоль виртуальной машины нельзя скопировать команду из основной операционной системы. Эту проблему решает сопутствующая программа putty.exe (рисунок 4.13). Она позволяет удаленно администрировать любую машину из сети через свой интерфейс, поддерживающий копирование команд.

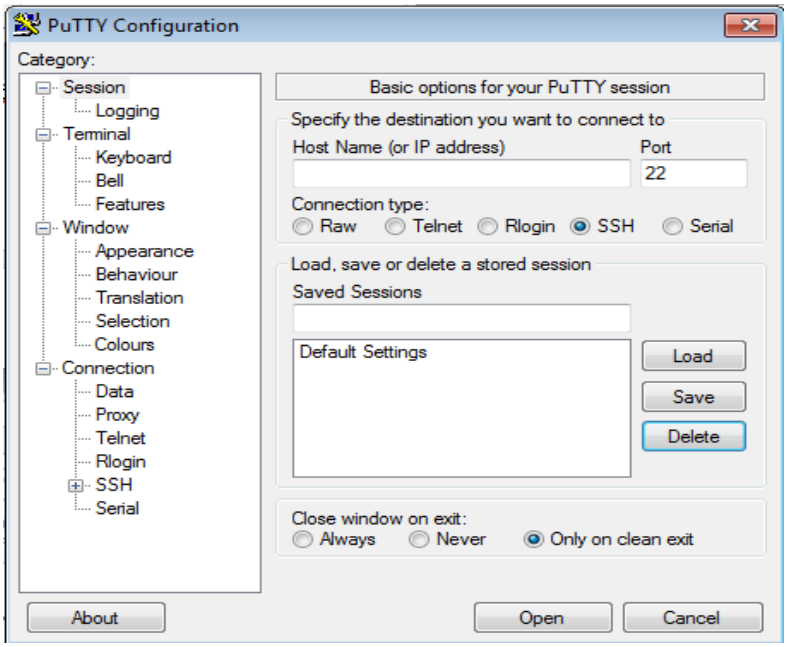


Рисунок 4.13 – Окно программы putty.

Чтобы узнать IP-адрес сервера, на виртуальной машине нужно после повторного ввода

логина/пароля (root/123456) ввести команду результат действия которой показан (рисунок 4.14):

ifconfig –a

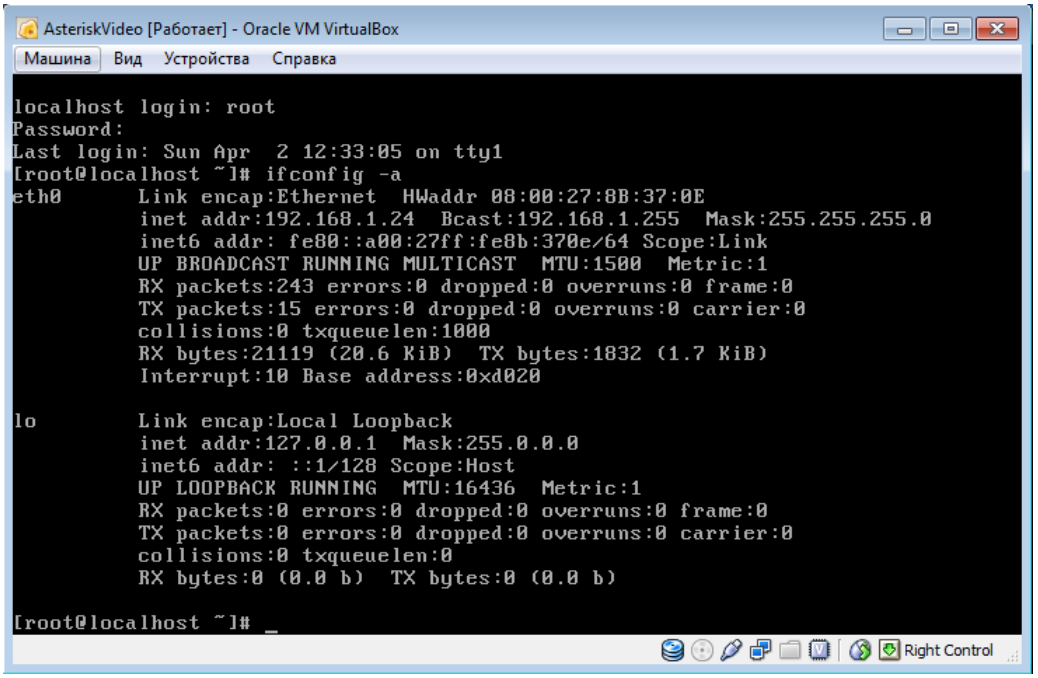


Рисунок 4.14 – Результат запроса ifconfig -a.

Данные от адаптера eth0 содержат в том числе IP-адрес сервера виртуальной машины. Вводим данный IP-адрес и удобное название в интерфейс putty (рисунок 4.15), затем нажимаем Save, чтобы данные сохранились и Open, чтобы получить доступ к серверу через интерфейс putty.

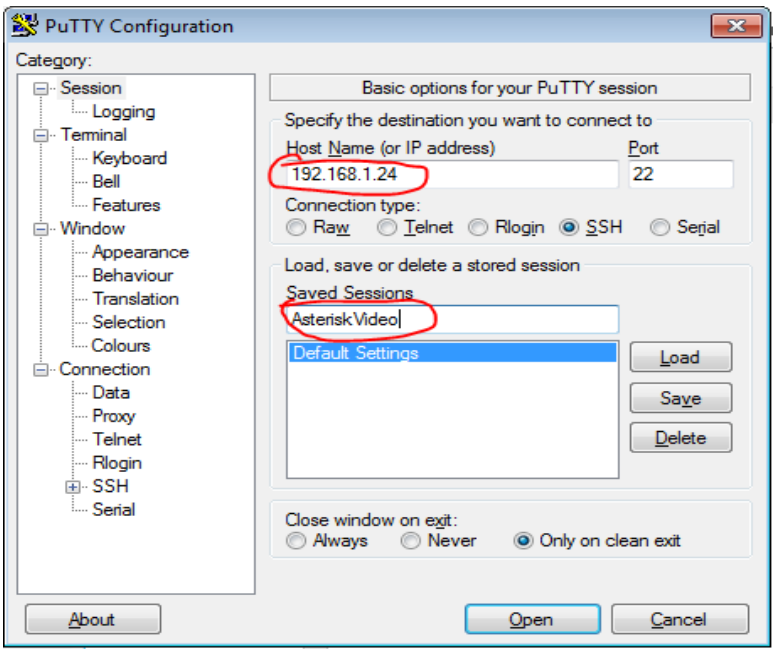


Рисунок 4.15 – Ввод IP-адреса и имени подключения в программу putty.

Результат – доступ к серверу через putty. Ввода логина/пароля (root/123456) позволит

управлять сервером.

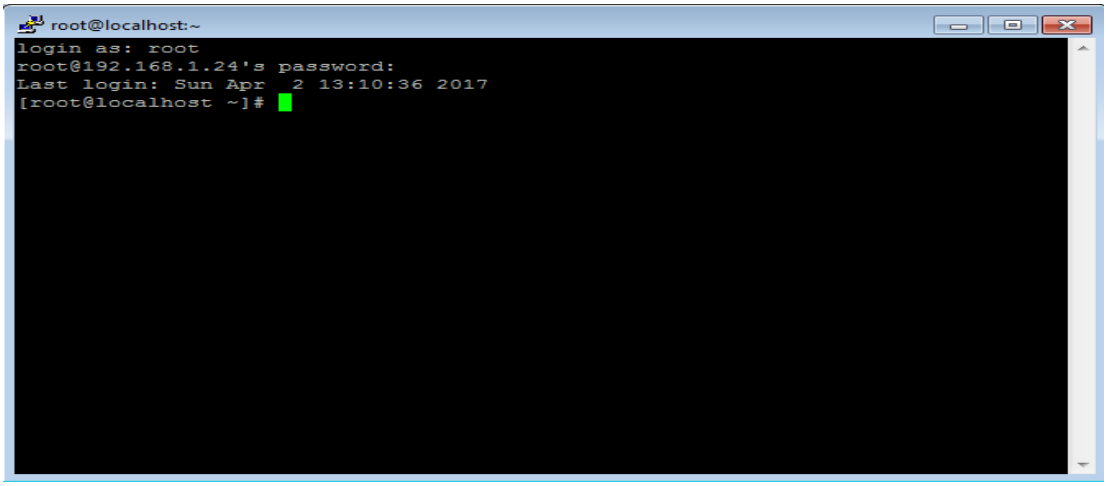


Рисунок 4.16 – Окно программы putty с введенными логином и паролем.

Проверить работу Asterisk можно командой (рисунок 4.17):

asterisk -r

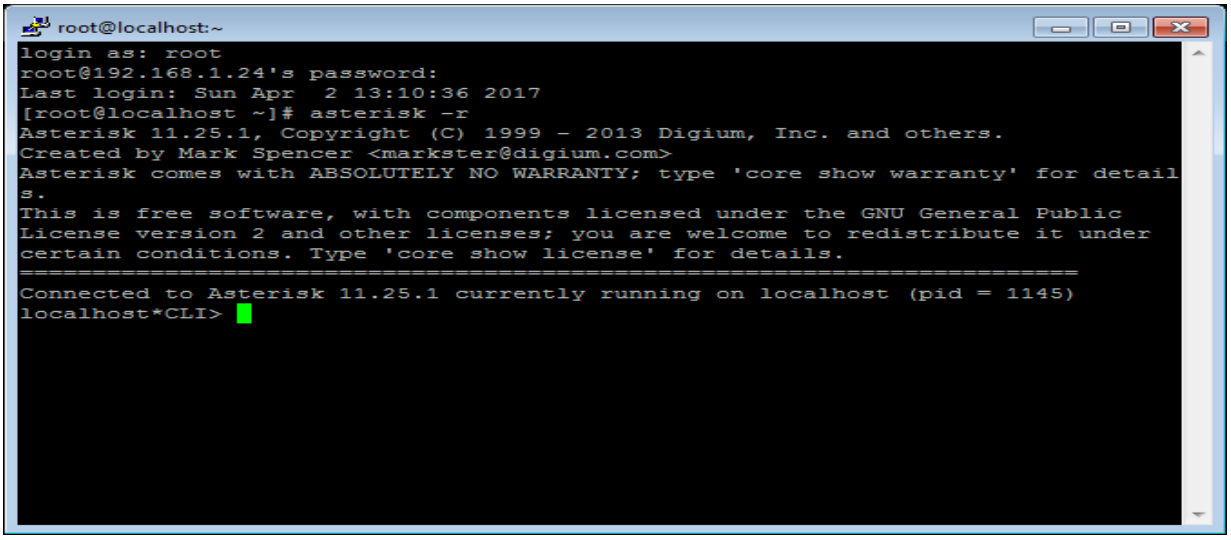


Рисунок 4.17 – Результат входа в Asterisk.

Если результат такой же, как на рисунке 4.17, то Asterisk работает корректно. Вернуться к серверу можно командой (рисунок 4.18):

exit

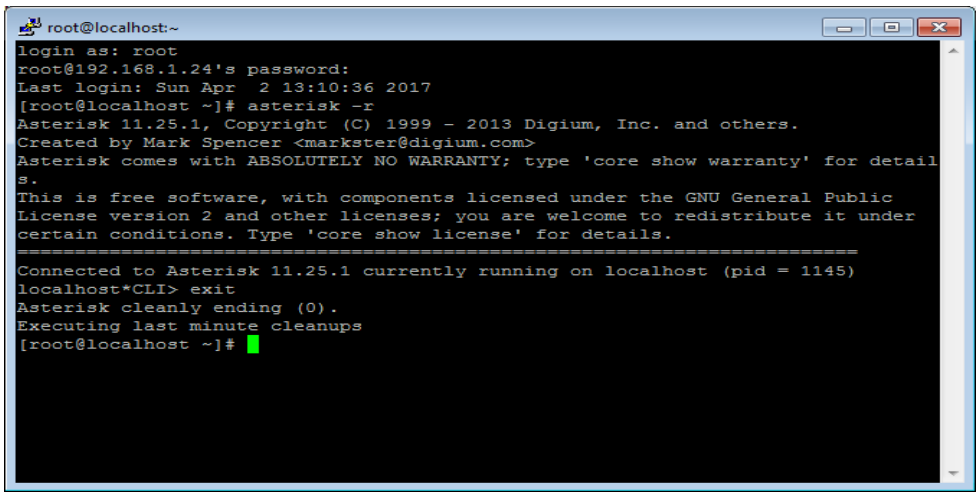


Рисунок 4.18 – Результат выхода из Asterisk.

Asterisk не прекращает своей работы, он работает все время при включении сервера. Для того, чтобы настроить клиентов (абонентов) необходимо прописать их настройки в соответствующем файле Asterisk. Открыть файл sip.conf для редактирования можно командой (рисунок 4.19):

nano /etc/asterisk/sip.conf

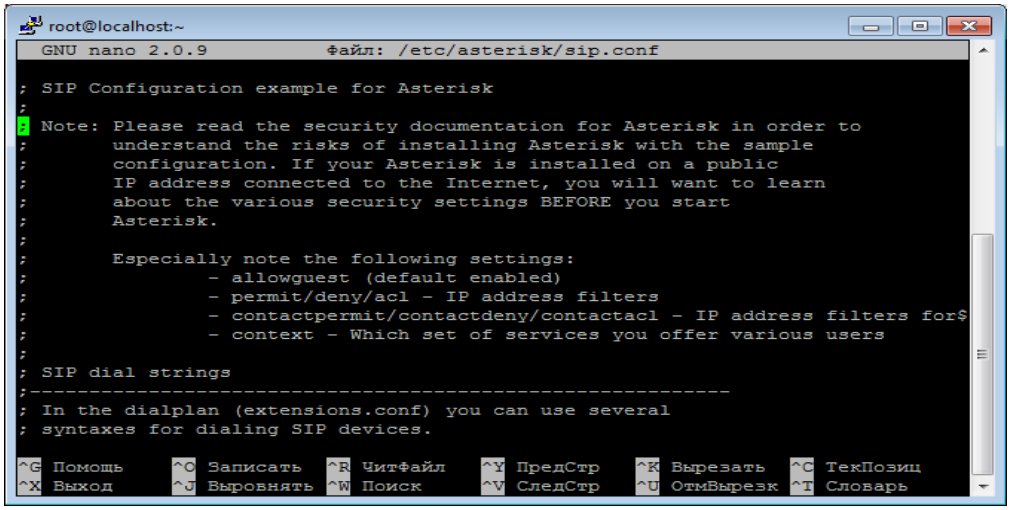


Рисунок 4.19 – Файл sip, открытый для редактирования.

В файл нужно прописать абонентов в соответствии с топологией (рисунок 4.20).

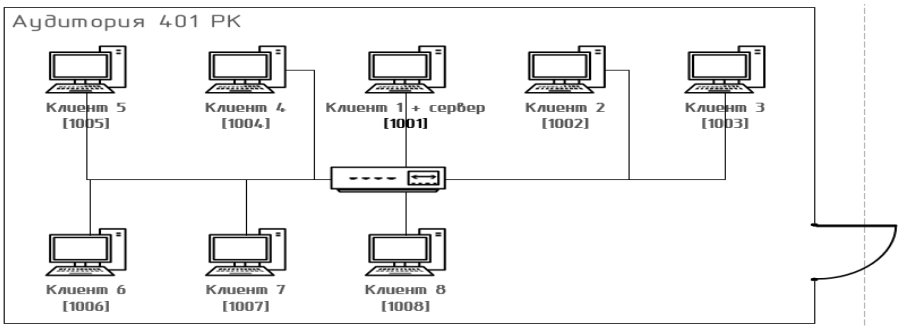


Рисунок 4.20– Топология сети аудитории 401 РК.

Настройка для одного абонента содержит много полей. Самые важные из них:

[1001] – Название абонента

type=friend

regexten=1001 – Номер телефона абонента

secret=1234 – Пароль абонента

context=outcoling

host=dynamic

callerid="1001" <1001> - Идентификатор абонента

disallow=all

allow=alaw

allow=ulaw

language=ru

callgroup=1

pickupgroup=1

qualify=yes

canreinvite=yes

call-limit=4

nat=no

Для того, чтобы прописать первого абонента в Asterisk, в начало файла **sip.conf нужно скопировать и вставить:**

[1001]

type=friend

regexten=1001

secret=1234

context=outcoling

host=dynamic

callerid="1001" <1001>

disallow=all

allow=alaw

allow=ulaw

language=ru

callgroup=1

pickupgroup=1

qualify=yes

canreinvite=yes

call-limit=4

nat=no

Остальным абонентам достаточно минимального набора полей. Их можно прописать после первого абонента:

[1002]

type=friend

host=dynamic

insecure=invite

username=1002

secret=45678

context=outcoling

disallow=all

allow=alaw

[1003]

type=friend

host=dynamic

insecure=invite

username=1003

secret=45678

context=outcoling

disallow=all

allow=alaw

…

[XXXX]

type=friend

host=dynamic

insecure=invite

username=XXXX

secret=45678

context=outcoling

disallow=all

allow=alaw

Вместо X можно указать любой номер абонента. В соответствии с топологией, абоненты в аудитории 401 РК имеют номера 1001-1008. Пример настройки файла sip.conf для 2 абонентов представлен на рисунке 4.21. По окончании редактирования нужно выйти с сохранением (*Ctrl+X > y > Enter*).

По окончании редактирования списка абонентов нужно прописать диал-план (план набора телефонного номера) в файле extensions.conf. Открыть файл для редактирования в консоли командой:

nano /etc/asterisk/extensions.conf

В начале файла extensions.conf прописать (рисунок 4.22):

[outcoling]

exten => _XXXX,1,Dial(SIP/${EXTEN},,m)

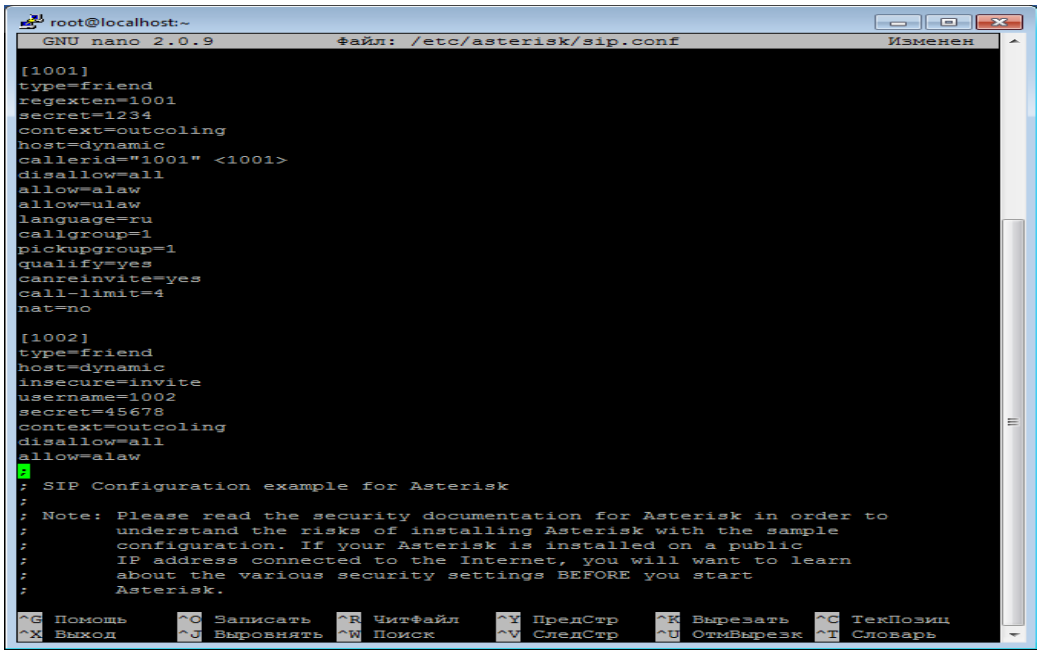


Рисунок 4.21 – Пример настройки sip.conf для 2 абонентов – 1001 и 1002.

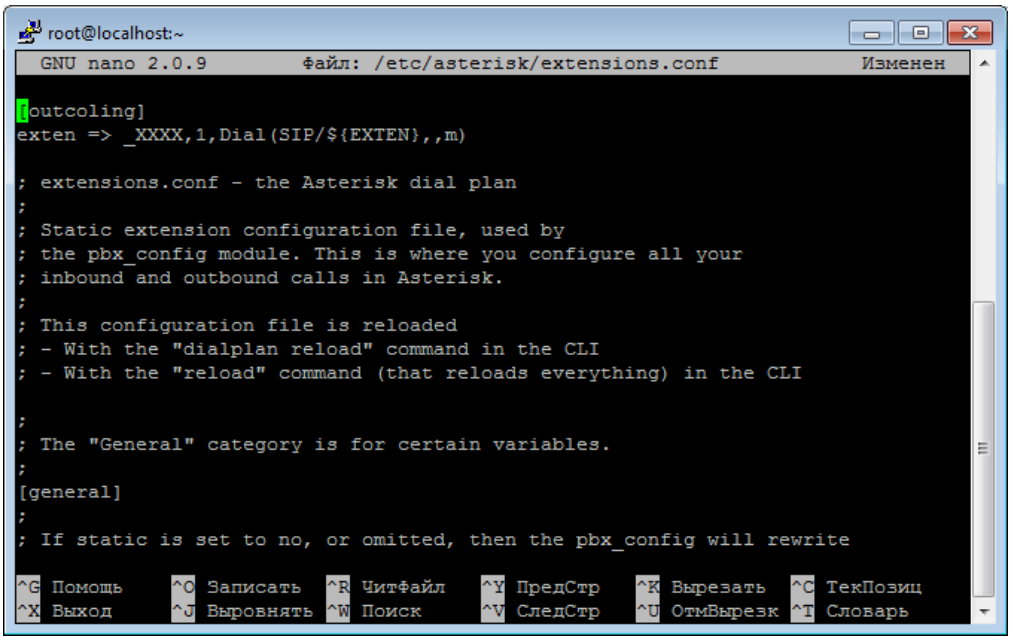


Рисунок 4.22 – Прописанный в **extensions.conf диал-план**.

По окончании редактирования нужно выйти с сохранением (*Ctrl+X > y > Enter*).

Теперь нужно перезагрузить Asterisk, чтобы изменения подействовали (рисунок 4.23). Вход в Asterisk:

asterisk –r

Перезагрузка конфигурации Asterisk:

core reload

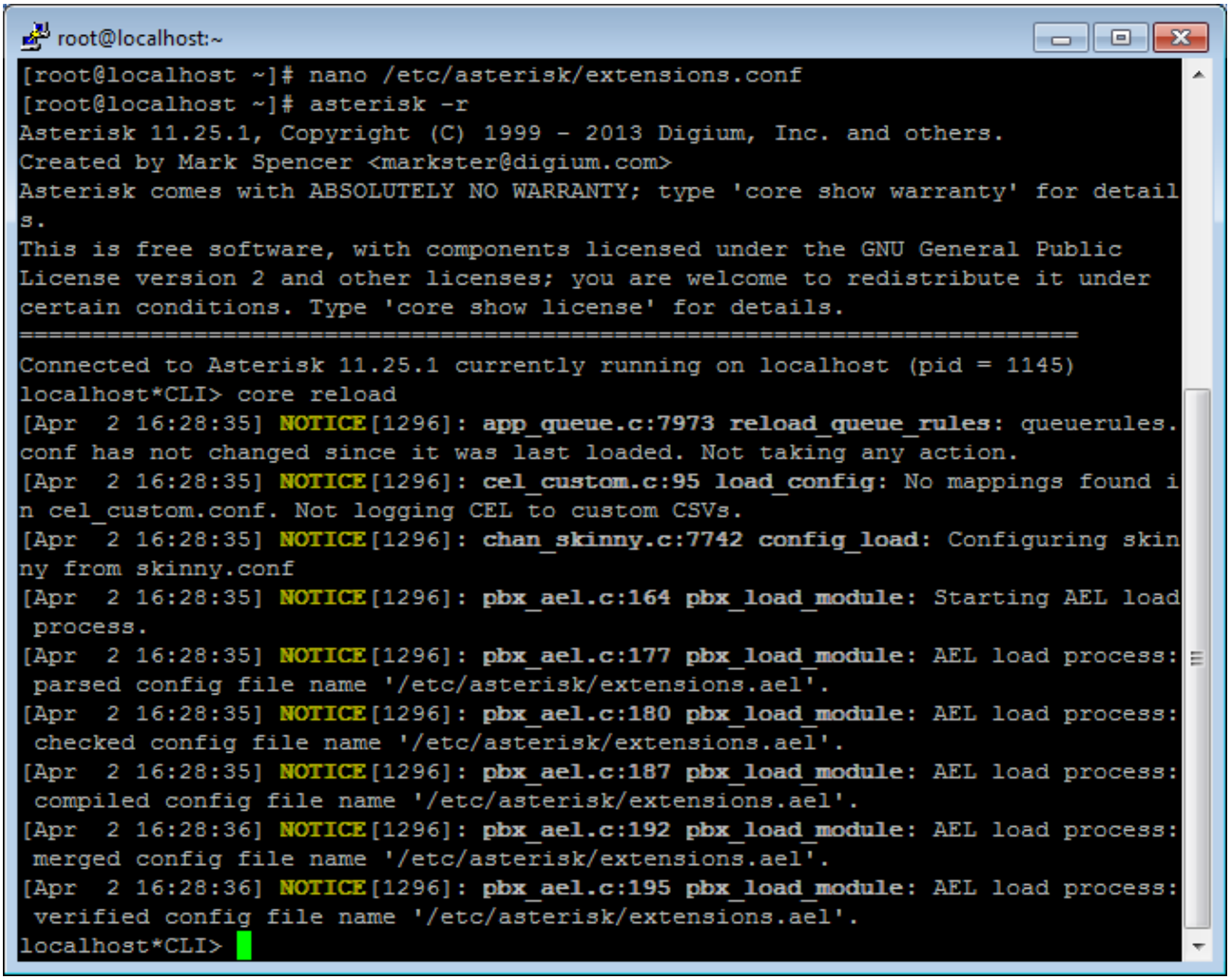


Рисунок 4.23 – Результат перезагрузки конфигурации Asterisk.

На этом настройка Asterisk завершена. Выход из Asterisk:

exit

Выход из putty:

exit

Работа с клиентами. Настройка софтофонов

Виртуальная машина остается работать в фоновом режиме, значит сервер продолжает работу. Теперь к нему нужно подключить абонентов.

На каждом клиентском ПК необходимо установить софтофон. В папке с сопутствующими программами есть пакет установщика софтофона 3CXPhone. Его установка не отличается от установки любой другой программы Windows. После установки можно

запустить софтофон. При первом запуске программа предлагает создать профиль (рисунок 4.24), нажимаем Create Profile > New.

Рисунок 4.24 – Предложение создать профиль абонента 3CXPhone.

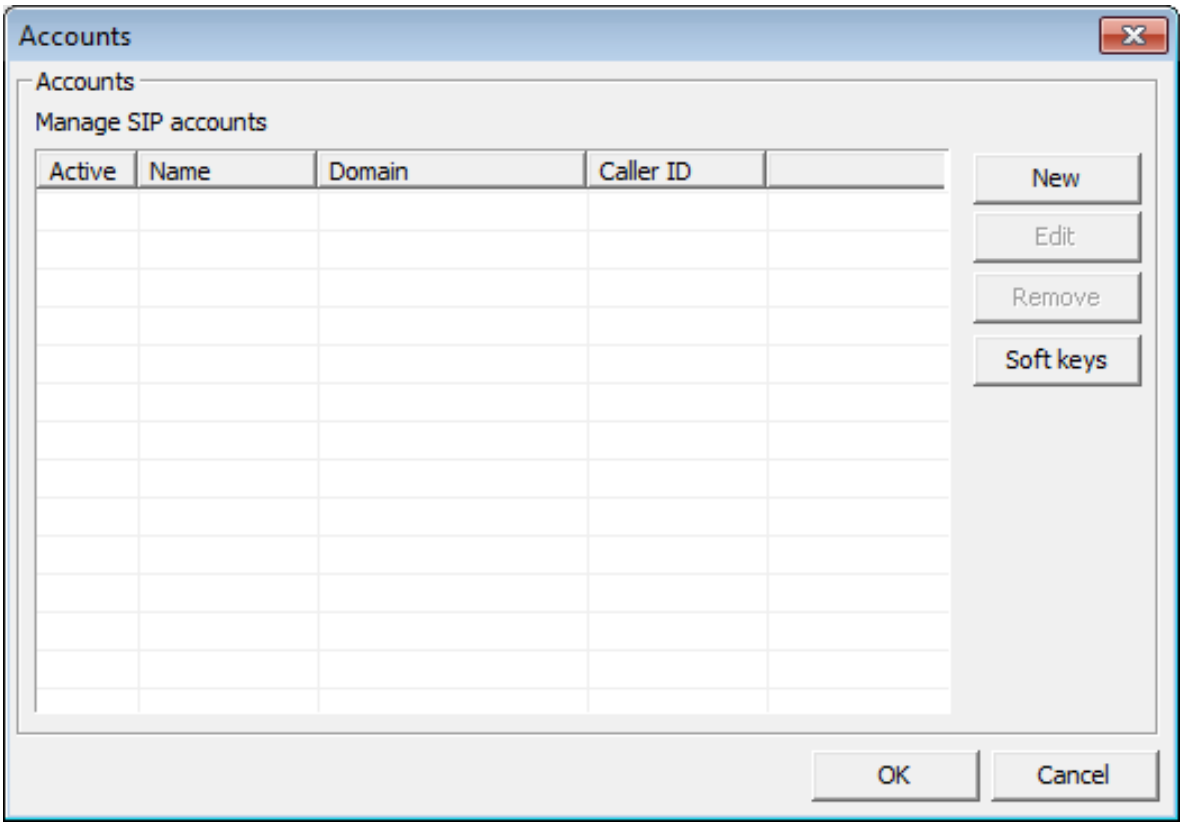


Рисунок 4.25 – Список профилей абонентов 3CXPhone до создания профиля.

Заполнение профиля абонента представлено на рисунке 4.26. В строке IP адреса нужно прописать адрес сервера Asterisk. При корректном заполнении софтофон свяжется с сервером (рисунок 4.27).

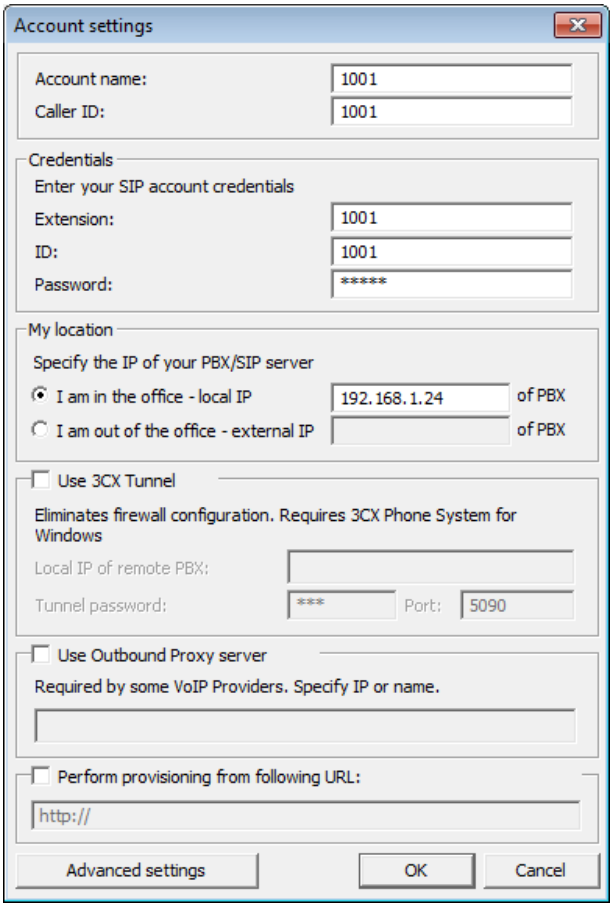


Рисунок 4.26 – Пример заполнения профиля абонента 1001.

Рисунок 4.27 – Настроенный абонент 1001.

В результате курсовой работы был настроен и запущен сервер IP-телефонии Asterisk в аудитории 401 РК на виртуальной машине CentOS 6.4.

Для безопасного использования IP-АТС в дальнейшем планируется:

1. Изменить логины и пароли для доступа к сетевым устройствам.
2. Изменить стандартные порты на любые незадействованные.

3. Запретить пользователю root доступ к Asterisk.
4. Настроить белый список IP-адресов.
5. Установить лимит одновременных звонков.
6. Отключить ответ о неверном пароле.

Полный процесс установки сервера Asterisk

Устанавливаем ОС Linux сборки CentOS

В нашем случае это была Linux сборка CentOS 6.4. Использовать будем дистрибутив minimal - он без графической оболочки Gnome. То есть работать будем полностью через интерфейс CLI, то есть через командную строку

a) Скачиваем дистрибутив отсюда: http://vault.centos.org/

b) Устанавливаем Linux

c) Сразу после установки пишем команду:

ifconfig –a

(показывает сетевые адаптеры)

Если ОС видит сетевой адаптер, то он отобразится. У меня он назывался eth0. Но беда - нет ip адреса. Для того, чтобы ОС прицепила ip адрес к сетевой карте пишем команду:

ifup eth0

(определяет ip интерфейса eth0)

Снова пишем команду

ifconfig -a

и видим свой ip адрес для интерфейса eth0.

Внимание – после перезагрузки придется снова определять ip адрес!

Для того, чтобы ip адрес цеплялся автоматически при старте CentOS, мы выполняем следующие действия:

a) устанавливаем текстовый редактор nano (на подобии блокнота в Windows)

yum install nano

б) Затем пишем следующую команду:

nano /etc/sysconfig/network-scripts/ifcfg-eth0

и в появившемся файле переменную ***ONBOOT=”no”*** меняем на ***ONBOOT=”yes”***

Как пользоваться редактором nano: http://habrahabr.ru/post/106554/

Установка Putty

Итак, мы установили операционную систему, определили ip адрес, теперь нужно поставить саму систему. Удобнее будет работать через putty, ибо приятнее шрифт и можно

работать с буфером обмена. Скачиваем, запускаем putty и цепляем его к нашей centOS. Скачать можно здесь: http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html

Установка Asterisk

Полная статья по установке Asterisk здесь:

http://www.voip-info.org/wiki/view/Asterisk+11+Installation+on+CentOS+6

Устанавливать будем Asterisk 11.0.0.Кратко:

a) Отключаем улучшенную систему безопасности SELinux:

sed -i s/SELINUX=enforcing/SELINUX=disabled/g /etc/selinux/config

b) Установка необходимых компонентов для установки Asterisk:

yum install -y make wget openssl-devel ncurses-devel newt-devel libxml2-devel kernel-devel gcc gcc-c++ sqlite-devel

c) Загружаем исходный код Asterisk. Для этого переходим в папку:

cd /usr/src/

и загружаем с помощью команды wget:

wget http://downloads.asterisk.org/pub/telephony/dahdi-linux-complete/dahdi-linux-complete-current.tar.gz

wget http://downloads.asterisk.org/pub/telephony/libpri/libpri-1.4-current.tar.gz

wget http://downloads.asterisk.org/pub/telephony/asterisk/asterisk-11-current.tar.gz

d) Распаковываем скаченные архивы:

tar zxvf dahdi-linux-complete*

tar zxvf libpri*

tar zxvf asterisk*

e) Устанавливаем LibPRI

cd /usr/src/libpri*

make && make install

f) Переходим в директорию, в которую распаковался Aterisk:

cd /usr/src/asterisk*

Кстати, находясь в /usr/src/ можно набрать ls и посмотреть как конкретно называется директория, в которую распаковался asterisk

g) Запускаем конфигурационные скрипты для Asterisk. Для этого, сначала узнаем какой битности наш Asterisk. Набираем:

uname –a

Если ответ: 2.6.18-238.12.1.el5 #1 SMP Tue May 31 13:23:01 EDT 2011 i686 i686 i386 GNU/Linux то значит 32 бита

Если ответ: 2.6.18-238.19.1.el5 #1 SMP Fri Jul 15 07:31:24 EDT 2011 x86_64 x86_64 x86_64 GNU/Linux то значит 64 бита.

В зависимости от того, какова битность Asterisk, запускаем конфигурационный скрипт:

Для 32 бита:

./configure && make menuselect && make && make install

Для 64 бита:

./configure --libdir=/usr/lib64 && make menuselect && make && make install

Внимание! Может возникнуть проблема, при которой после выполнения последней команды возникнет ошибка. Будет ругаться на .xml файл. Тогда необходимо добавить строчку к этой команде, после чего для 64-бита будет выглядеть так:

./configure --(команда, которую предлагает астериск) --libdir=/usr/lib64 && make menuselect && make && make install

Об успешной установке свидетельствует синее окно

h) Добавляем поддержку звонков. Дело в том, что при такой конфигурации Asterisk вроде бы как работает, но звонки совершаться не будут. Будет возникать ошибка

[Apr 27 21:35:51] ERROR[1225][C-00000009]: rtp_engine.c:259 ast_rtp_instance_new: No RTP engine was found. Do you have one loaded?

Поэтому, делаем следующее:

yum install uuid uuid-devel libuuid libuuid-devel uuid-c++

после этого:

./configure

make menuselect

и потом

make

make install

(полная статья про это дело здесь: http://forums.asterisk.org/viewtopic.php?f=1&t=86518i)

Далее устанавливаем образцы. Без установки этих образцов у нас не появятся конфигурационные файлы sip.conf и extensions.conf

make samples

make config

j) пишем

cd

и затем пишем

reboot

k) После перезагрузки пишем

asterisk

В результате Asterisk должен запуститься. Поздравляю! Мы запустили asterisk.

Конфигурация Asterisk для совершения звонков между внутренними абонентами

a) Теперь необходимо отключить фаерволл в самой CentOS. Без этого софтовый телефон X-Lite не хочет цепляться к серверу Asterisk.

Полная статья по этому делу: http://www.sl-s.ru/kak-otklyuchit-firewall-v-centos-redhat/

Для этого пишем следующие команды:

service iptables save

service iptables stop

chkconfig iptables off

b) Переходим непосредственно к редактированию sip.conf:

nano /etc/asterisk/sip.conf

У нас открывается файл. Пишем свои конфиги в самое начало файла. В моем случае это определение двух sip клиентов (телефонов):

[1001]
type=friend
regexten=1001
secret=1234
context=outcoling
host=dynamic
callerid="1001" <1001>
disallow=all
allow=alaw
allow=ulaw
language=ru
callgroup=1
pickupgroup=1
qualify=yes

canreinvite=yes
call-limit=4
nat=no
[1002]

type=friend

host=dynamic

insecure=invite

username=1002

secret=45678

context=outcoling

disallow=all

allow=alaw

После этого находим секцию [general] и удаляем её. Так же удаляем надпись «context=public» после надписи [general].

Обращаем внимание на контексты.

Для телефонов (sip клиентов) [1001] и [1002] это outcoling.

Что такое контекст и зачем он нужен? Контекст связывает файл sip.conf с файлом extensions.conf. Тоесть если у [1001] прописан контекст outcoling, то [1001] будет искать правило в extensions.conf под названием outcoling.

Нажимаем ctrl+x, нажимаем y и нажимаем enter. Файл сохранен.

Подробная статья по этому делу:

http://wiki.zadarma.com/index.php/Asterisk (настройка транка для задармы)

http://habrahabr.ru/post/122898/ простая настройка sip клиентов

c) Переходим к редактированию extensions.conf

nano /etc/asterisk/extensions.conf

Подробнее в видеоуроках Астериск с нуля на канале YouTube «Learning»:

https://www.youtube.com/watch?v=y3MRe-L8TxE&list=PL1LeoQF_fJbwBLeP3qXoq1jcsw7gF1_aD