А.М. Голиков

ЗАЩИТА ИНФОРМАЦИИ В ИНФОКОММУНИКАЦИОННЫХ СИСТЕМАХ И СЕТЯХ

Сборник лабораторных работ

Томск

Голиков А.М. Защита информации в инфокоммуникационных системах и сетях: Сборник лабораторных работ /Второе переработанное издание. – Томск: Томск. гос. ун-т систем управления и радиоэлектроники, 2015. – 374 с.

Сборник содержит описания лабораторных работ по курсу «Защита информации в инфокоммуникационных системах и сетях» специальности 21065-2.65 – Радиоэлектронные системы и комплексы передачи информации. Представлены описания аппаратно-программных комплексов и методики выполнения лабораторных работ. В разработке аппаратно-программных комплексов принимали участие студенты ТУСУР.

ОГЛАВЛЕНИЕ

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

1. Обзор программных продуктов в области анализа рисков и проверки организационных мер обеспечения информационной безопасности
2. Описание системы
3. Интерфейс системы

Лабораторная работа 2. Исследование защищенности беспроводных сетей передачи данных

1. Цель работ
2. Краткие теоретические сведения
3. Порядок выполнения работы
4. Рекомендуемая литература

Лабораторная работа 3. Исследование и администрирование средств обеспечения информационной безопасности Web-сервера Microsoft IIS Server.

1. Цель работы
2. Краткие теоретические сведения
3. Порядок выполнения работы
4. Рекомендуемая литература

Лабораторная работа 4. Исследование и администрирование средств обеспечения информационной безопасности Microsoft ISA Security Server. Установка и конфигурирование брандмауэра ISA. Построение VPN-сети на базе ISA

1. Цель работы
2. Краткие теоретические сведения
3. Порядок выполнения работы
4. Рекомендуемая литература

Лабораторная работа 5. Исследование и развертывание сетевой инфраструктуры Microsoft Windows Exchange Server

1. Цель работы
2. Краткие теоретические сведения
3. Порядок выполнения работы

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.

1. 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.

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

Для проведения полного анализа информационных рисков 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].

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

1.2. 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.

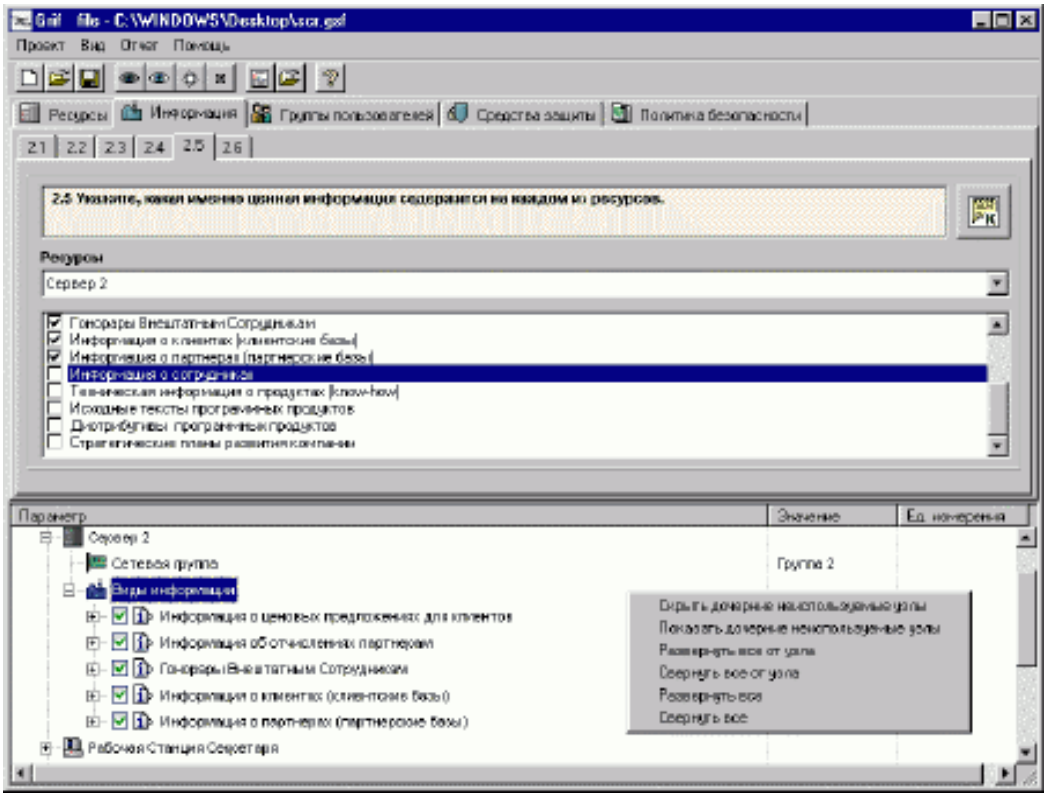


Рис.1. Интерфейс программного комплекса Гриф. Вкладка «Информация».

1.3. 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.

1.4. 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.

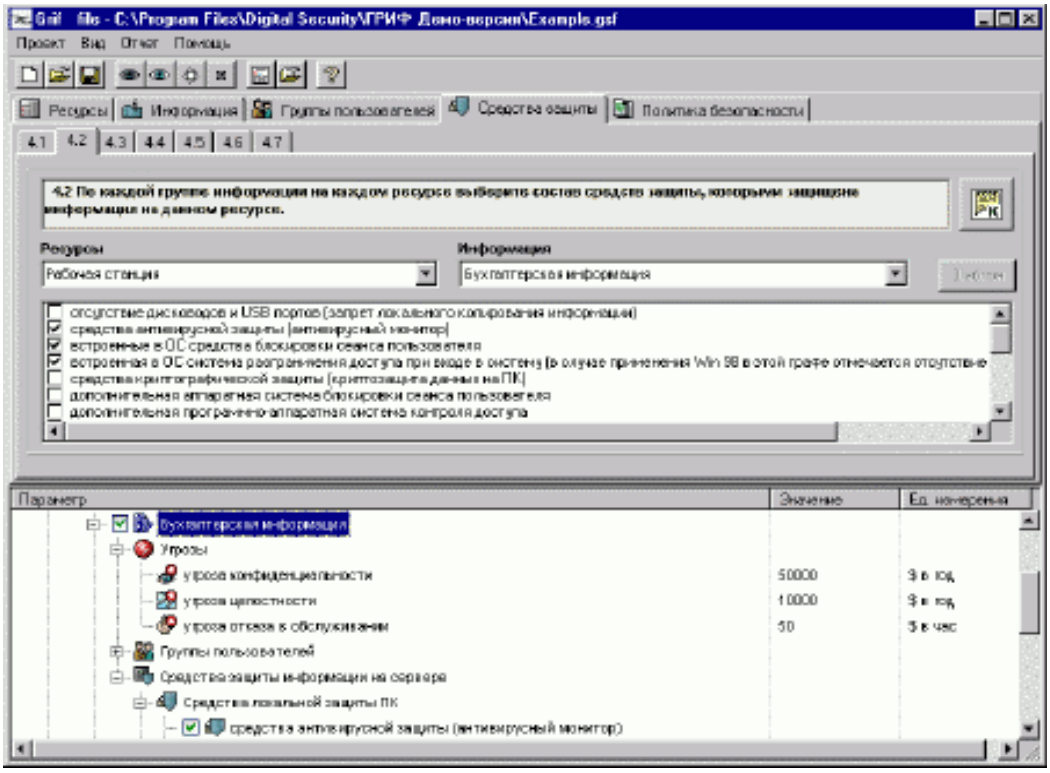


Рис. 2. Интерфейс программного комплекса Гриф. Вкладка «Средства защиты».

1.5. 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.

1.6. Отчет по системе представляет собой подробный, дающий полную картину

возможного ущерба от инцидентов документ, готовый для представления руководству компании.

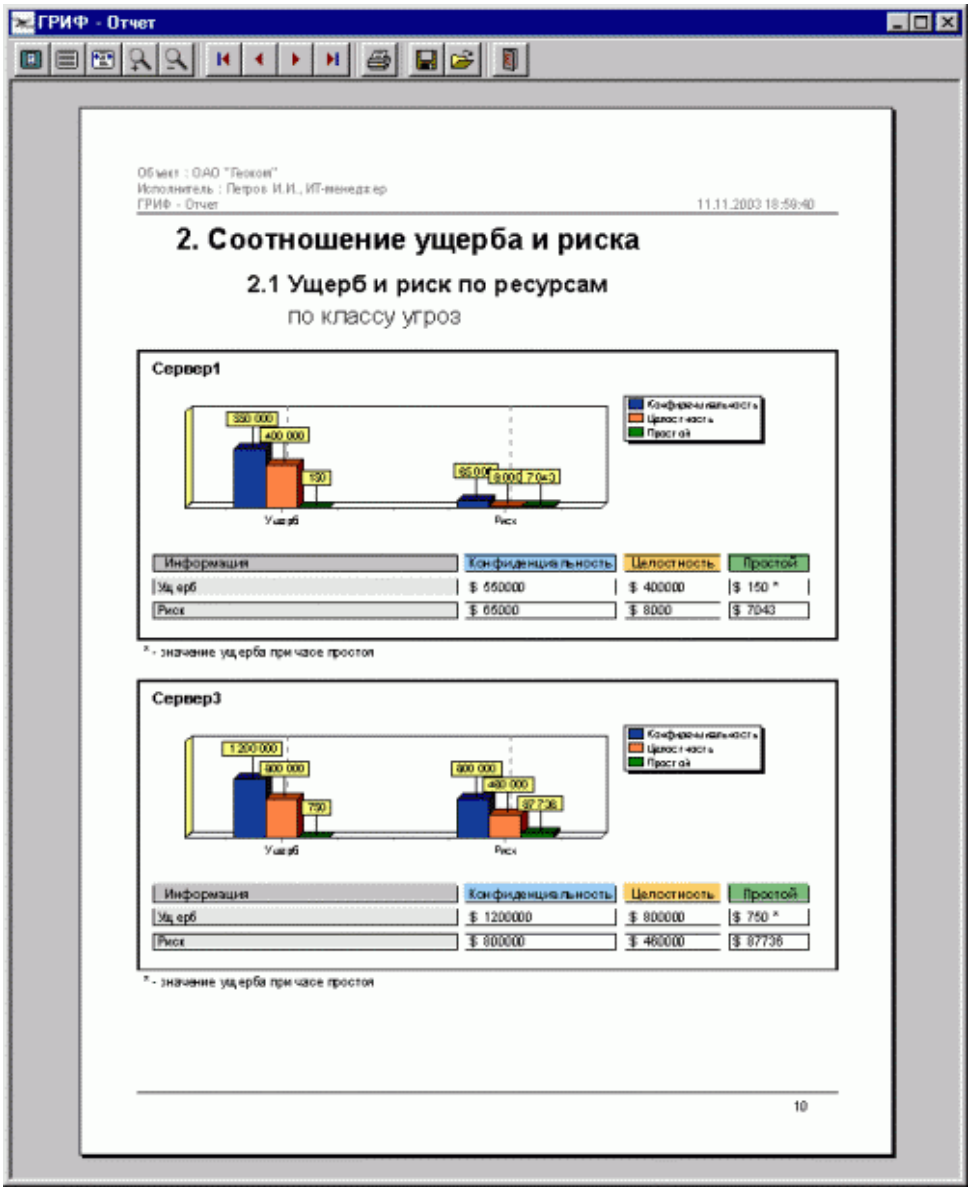


Рис.3. Интерфейс программного комплекса Гриф. Реализация отчета.

1.7. 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.

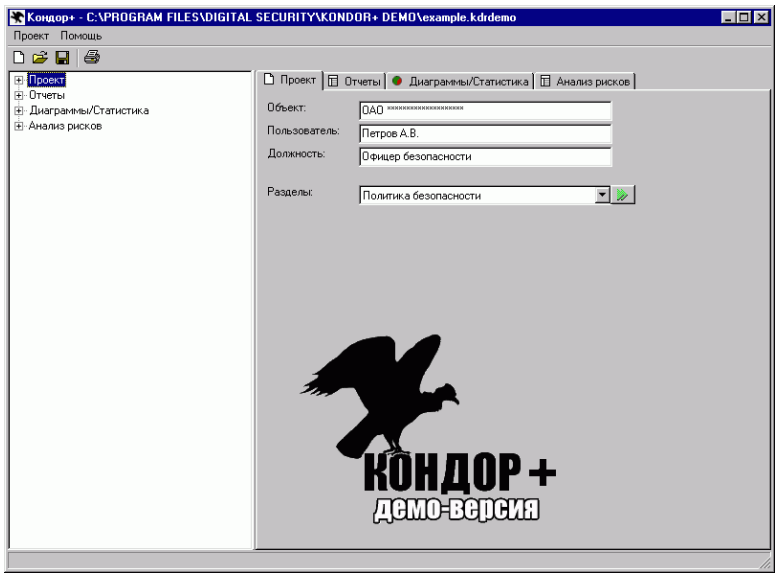


Рис.4. Интерфейс программного комплекса Кондор. Вкладка проект.

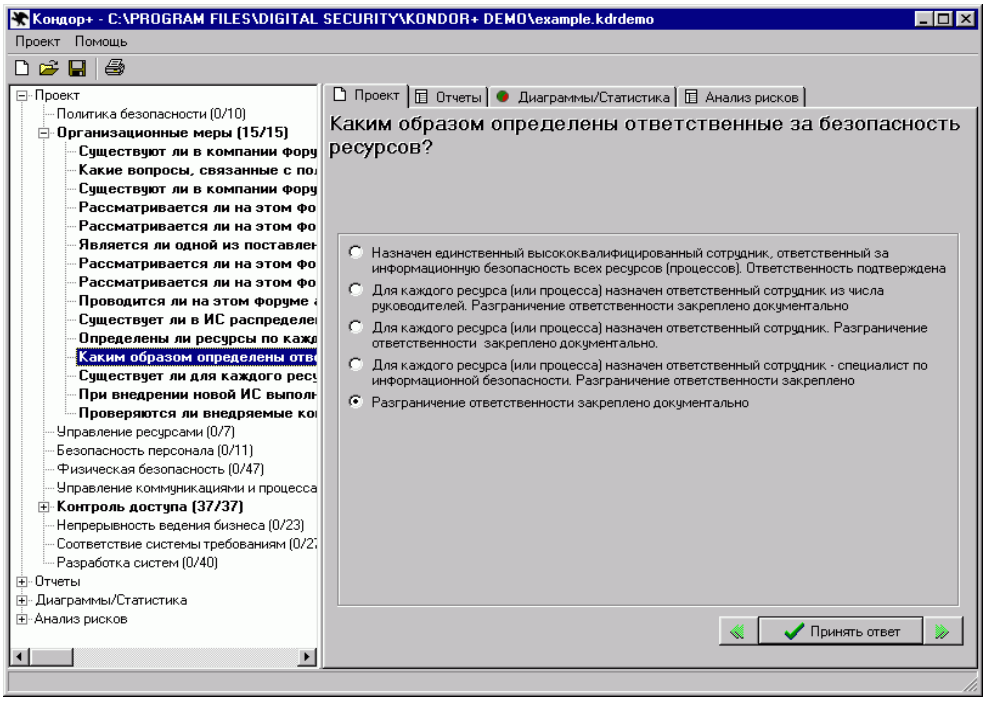


Рис.5. Интерфейс программного комплекса Кондор. Выбор раздела стандарта.

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

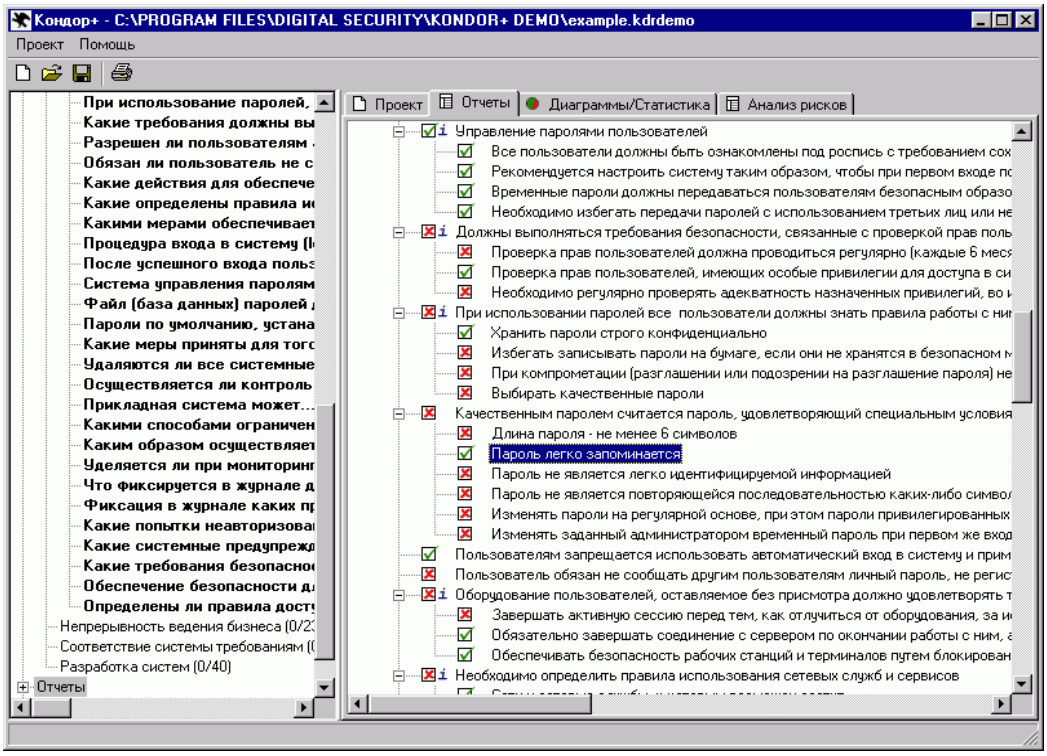


Рисунок.1.6. Интерфейс программного комплекса Кондор. Реализация отчета.

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

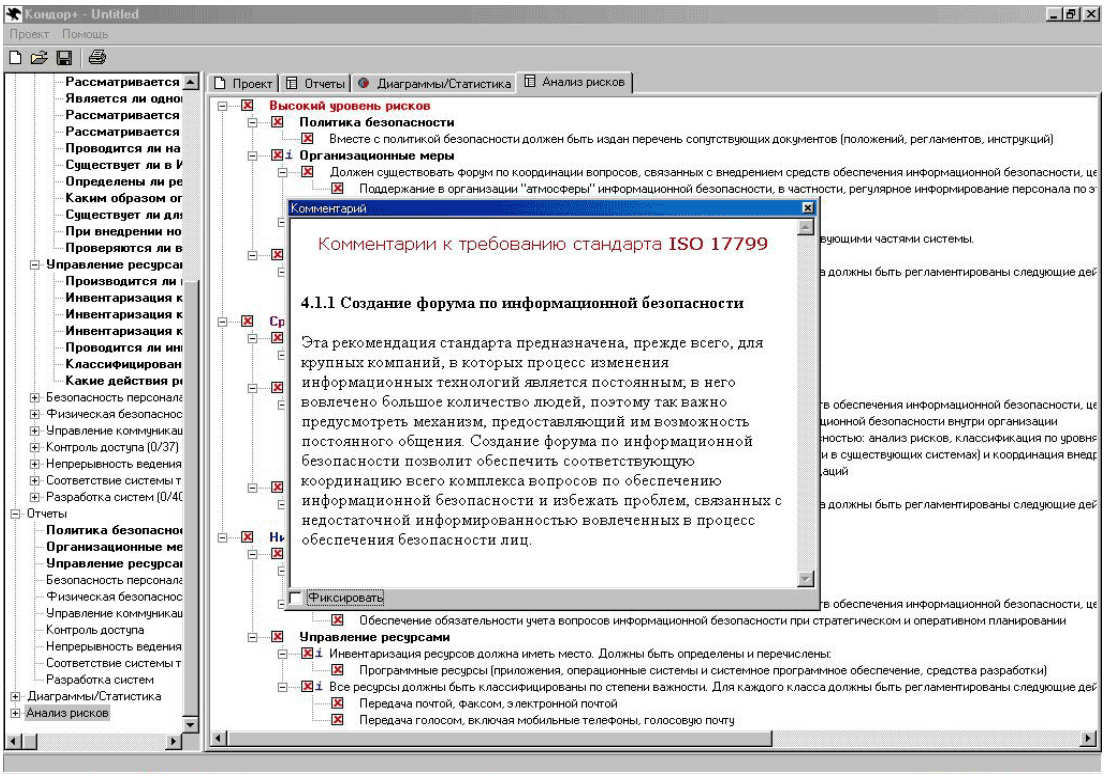


Рис.8. Интерфейс программного комплекса Кондор. Комментарии.

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.

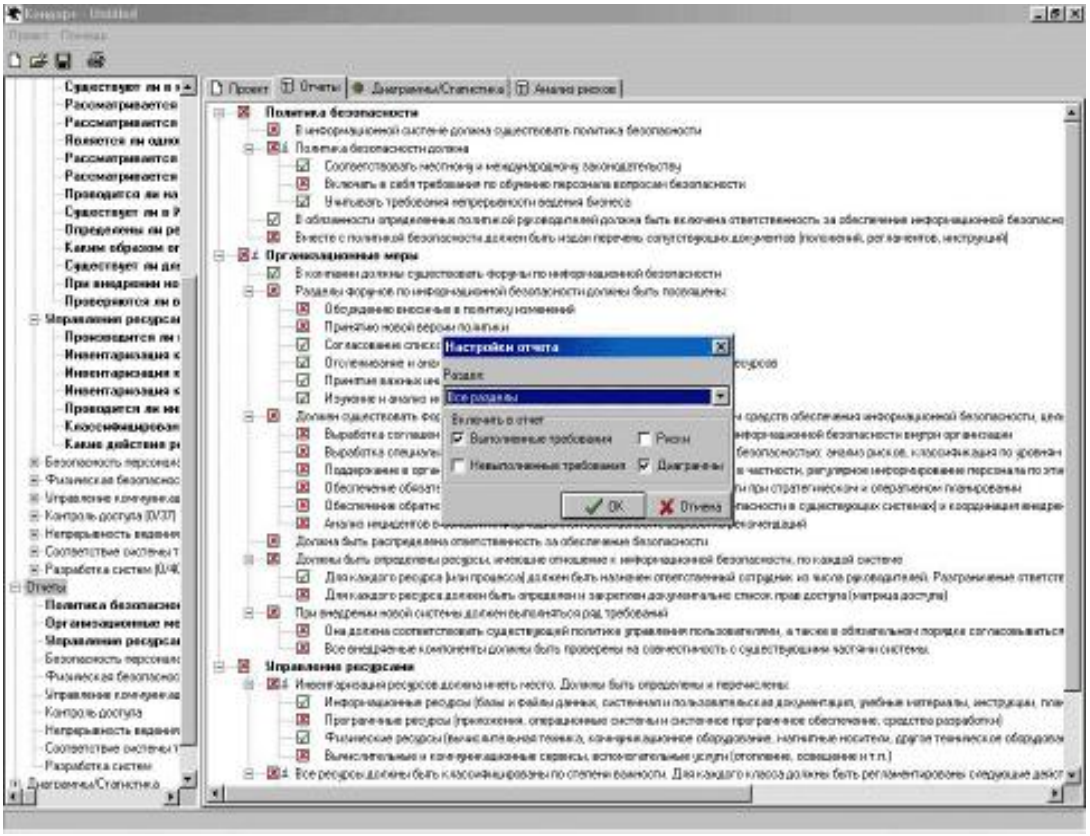


Рис.9. Интерфейс программного комплекса Кондор. Настройка отчета.

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).

2. 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 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.

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.

2. 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, эффективная 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 акустических 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 необходимости противодействовать такой угрозе.

Видеоразведка может вестись с использованием технических средств, таких как

оптические 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» по-

давляющее 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 или

отказов 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 сигналов 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 выделен 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 аварийной 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 предпри-

нимать 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 идея

может 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
A	Низкий риск	Низкий риск	Низкий риск	Средний риск	Средний риск
B	Низкий риск	Низкий риск	Средний риск	Средний риск	Высокий риск
C	Низкий риск	Средний риск	Средний риск	Средний риск	Высокий риск
D	Средний риск	Средний риск	Средний риск	Средний риск	Высокий риск
E	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)

Соответственно, риск определяется следующим образом:

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:

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

2) 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.

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

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.

Таблица.3. Определение риска в зависимости от трех факторов

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.

2.3. 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.

2.4. 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.

2.5. 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.

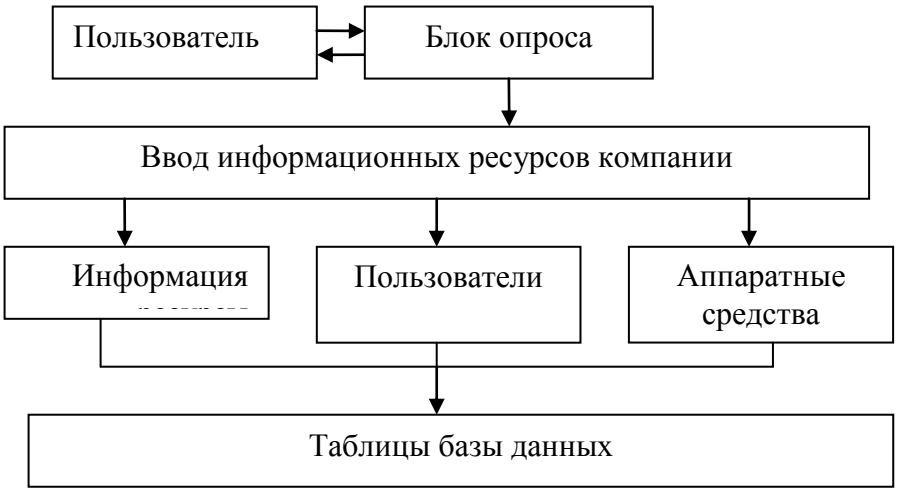


Рис. 11. Схема функционирования блока опроса по выявлению ресурсов компании.

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).

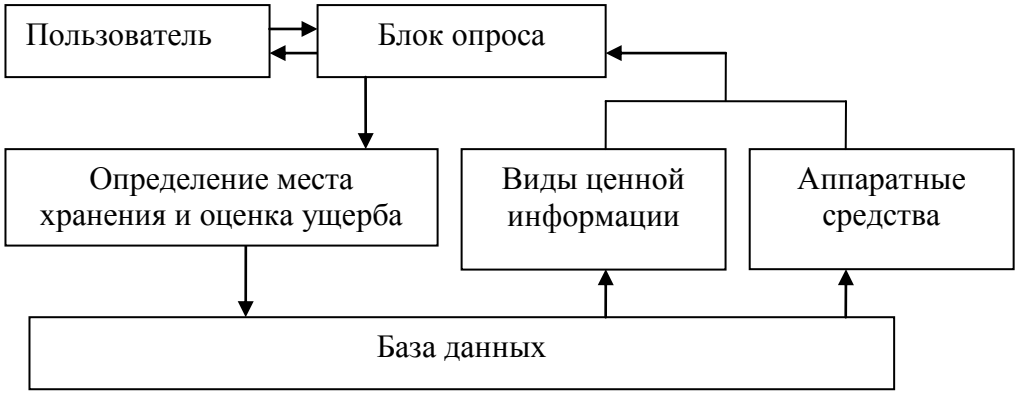


Рис. 12. Схема функционирования блока опроса по привязке данных и оценки ущерба.

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.

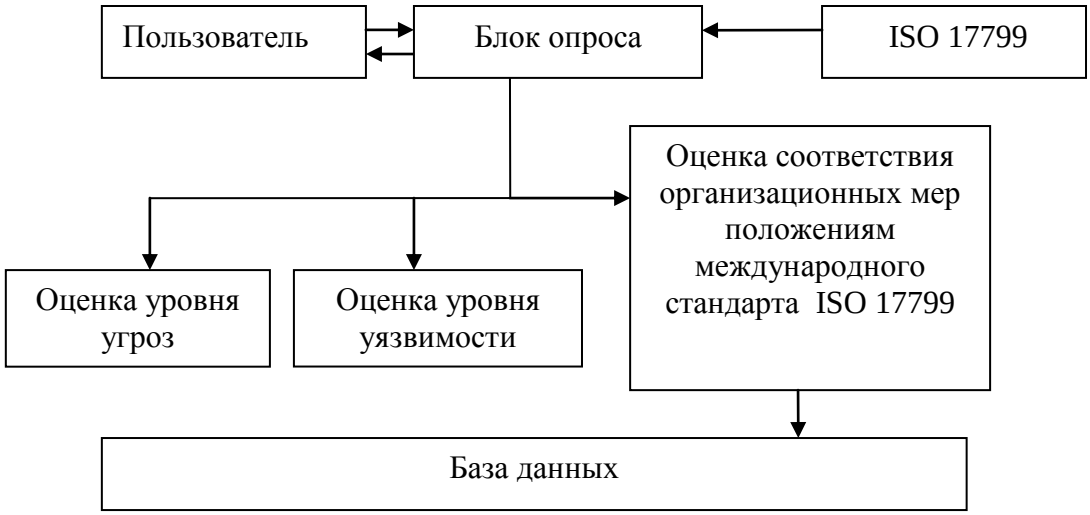


Рис. 13. Схема функционирования блока опроса по оценкам уровня уязвимости, угроз и существующей политики безопасности.

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.

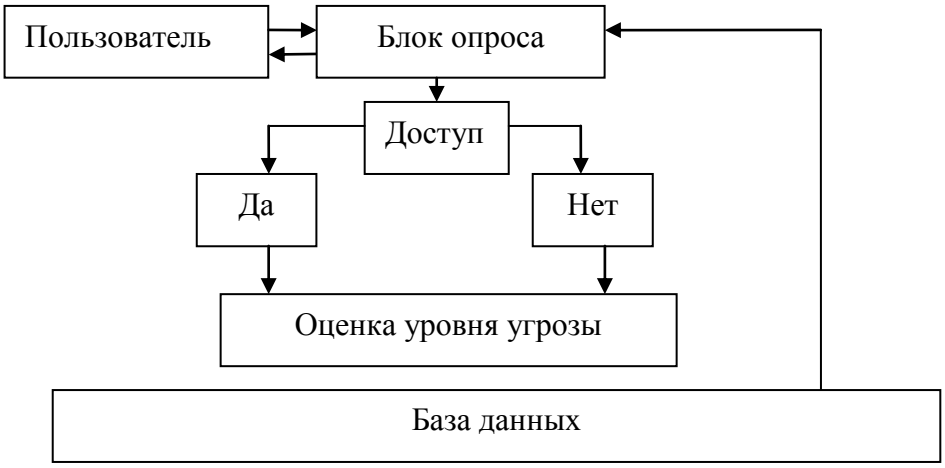


Рис. 14. Схема функционирования блока опроса по выявлению доступа субъектов системы к объектам

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.

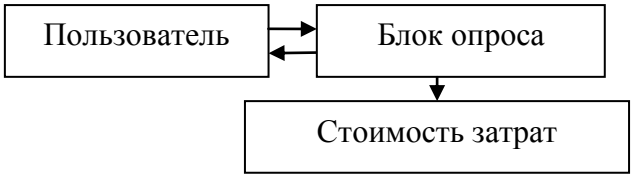


Рис. 15. Схема функционирования блока опроса по выявлению эффективности системы защиты информации.

Следующий этап работы системы происходит анализ рисков.

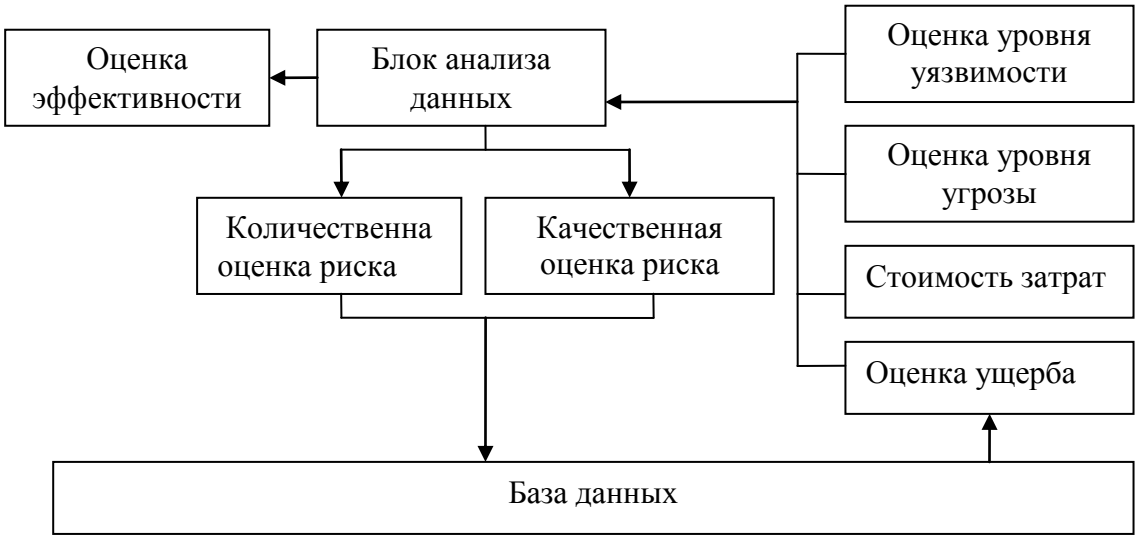


Рис. 16. Схема функционирования блока анализа рисков

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.

2.5. 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 схем

в 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.

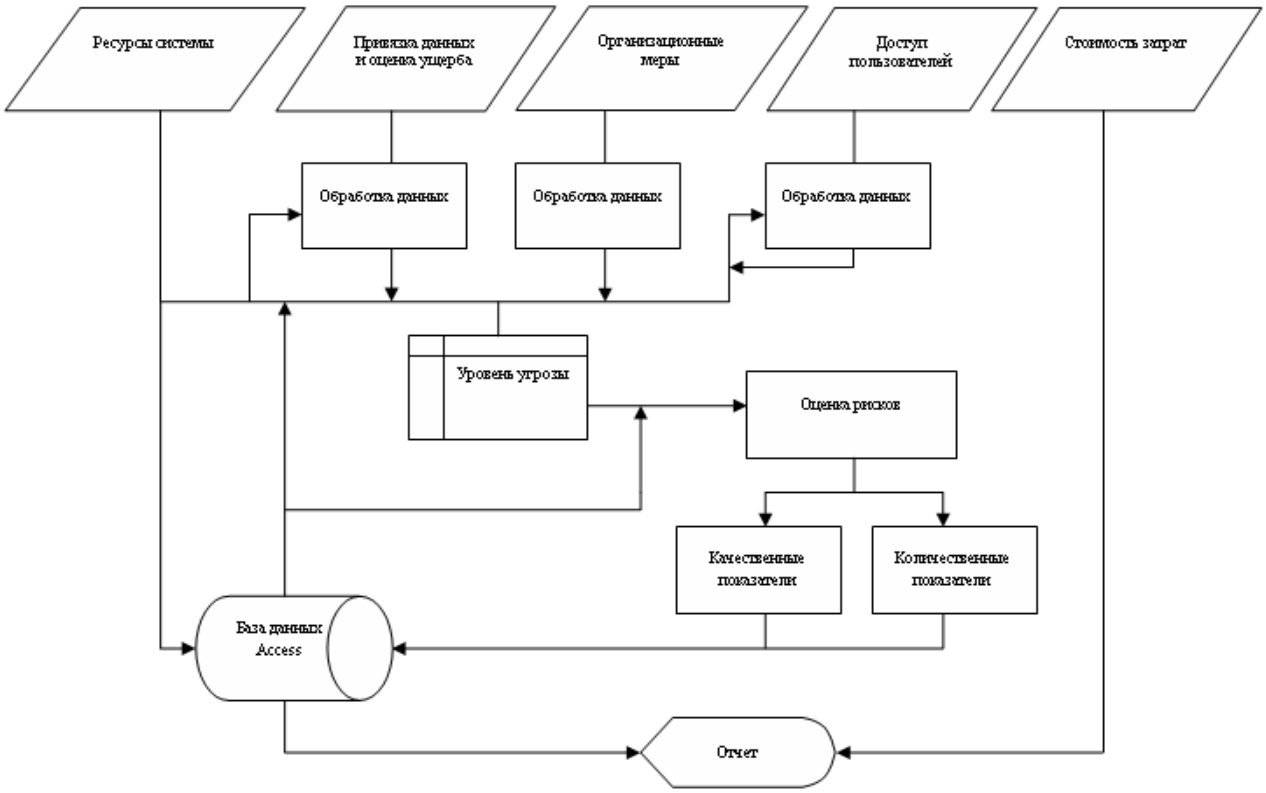


Рис. 17. Алгоритм интерфейса программы анализа информационных рисков.

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 ресурсов

организации.

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.

3. Интерфейс системы.

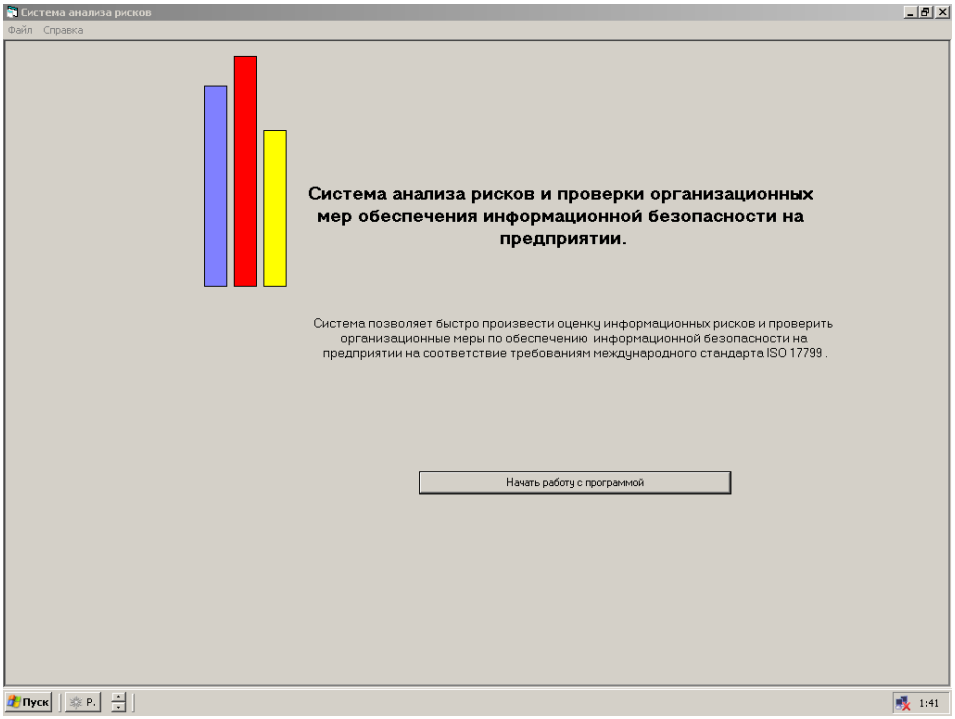


Рис.18. Главное окно программы

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

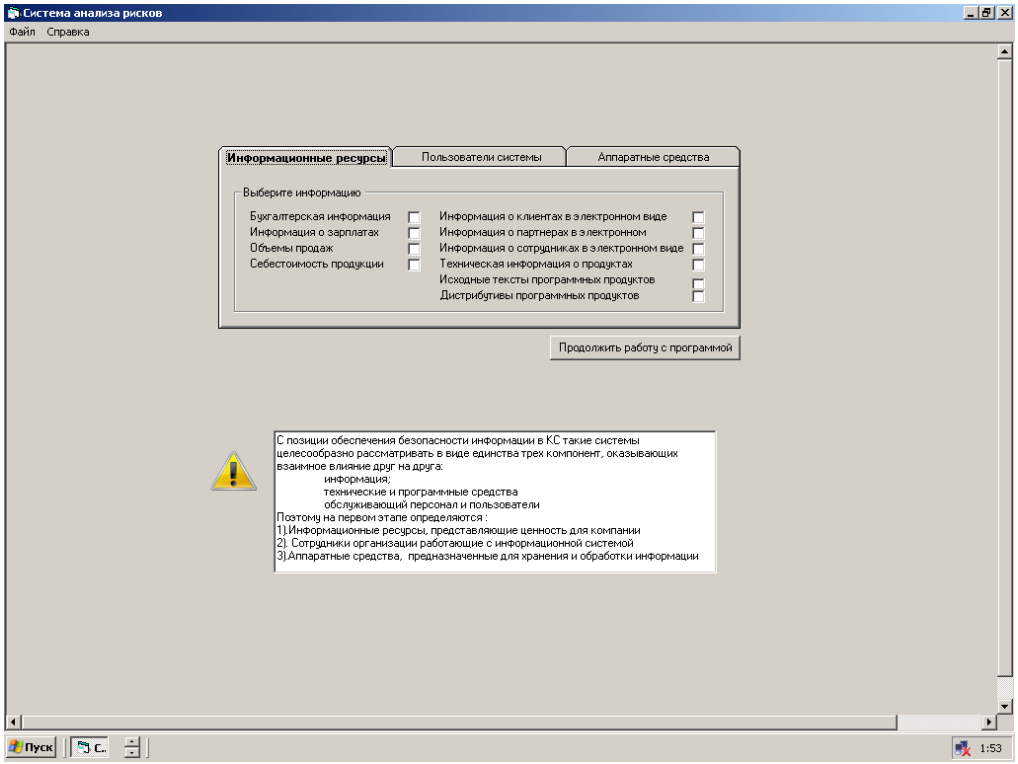


Рис. 19. Интерфейс программы. Вкладка «Информационные ресурсы».

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

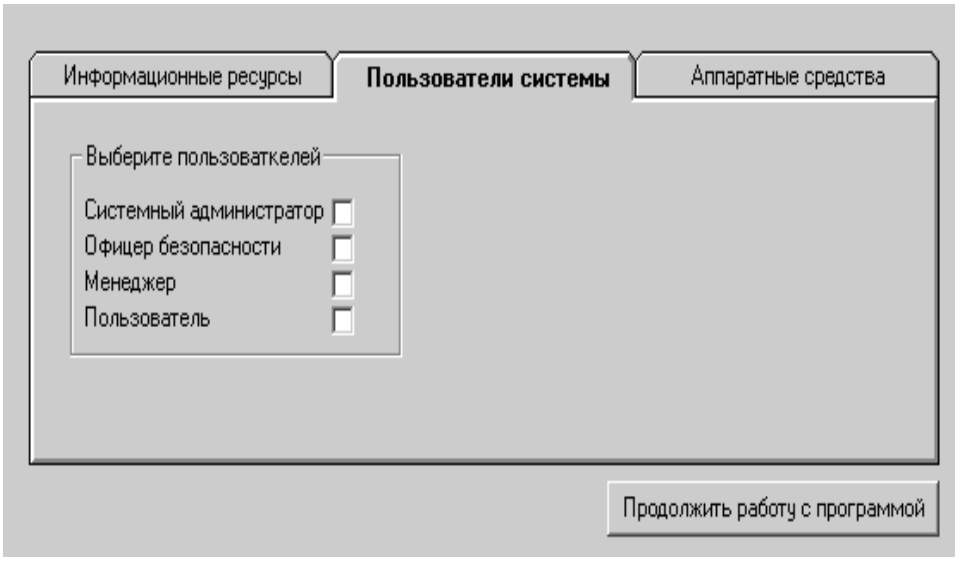


Рис. 20. Интерфейс программы. Вкладка «Пользователи системы»

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

Это могут быть:

Сервера

Рабочие станции

Твердые копии

Рис. 21. 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.

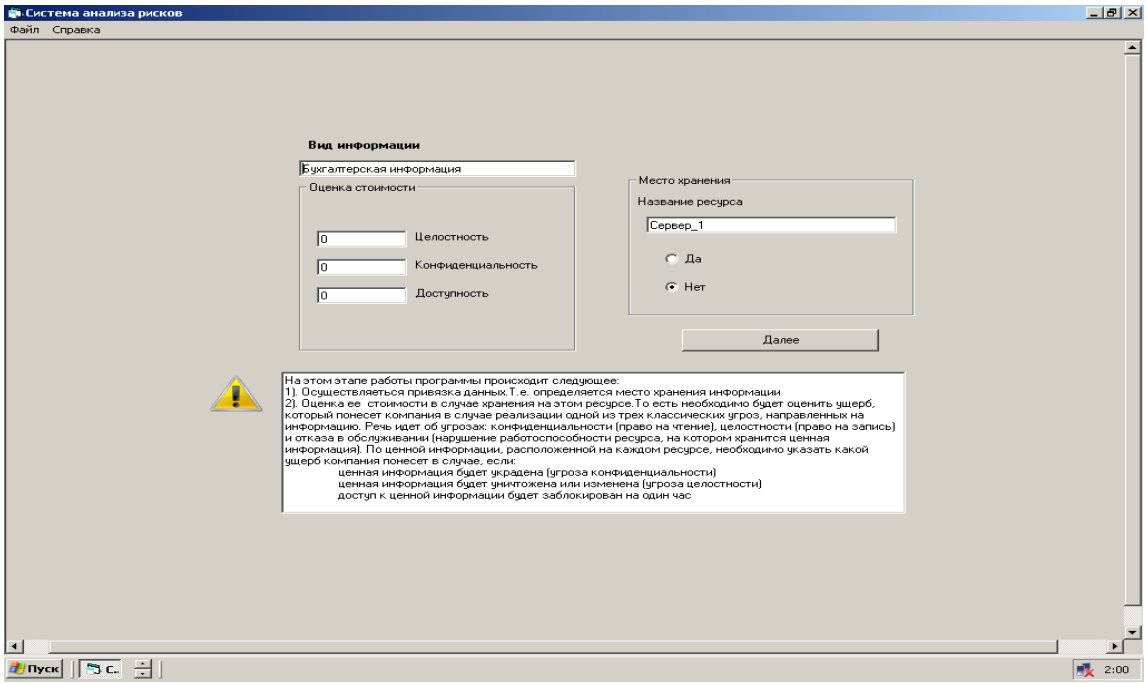


Рис. 22. Интерфейс программы. Вкладка «Привязка данных».

Кроме этого на этом этапе работы необходимо еще определить 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».

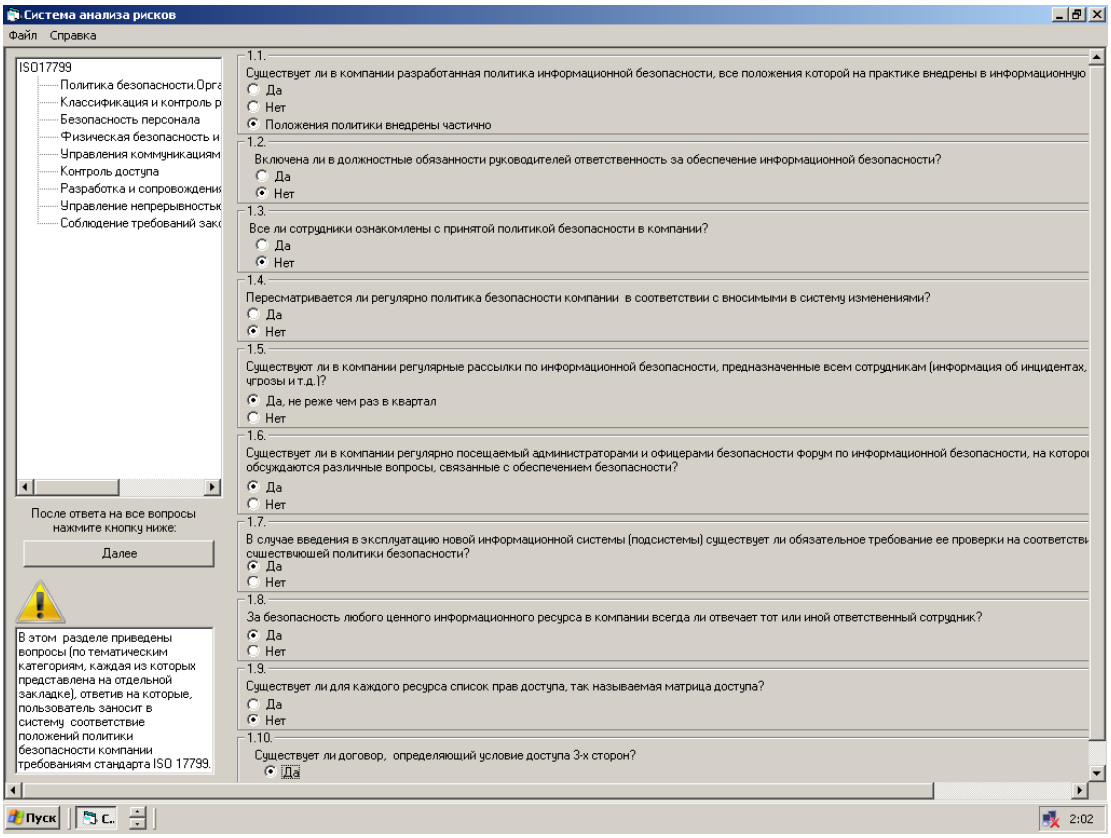


Рис. 23. Интерфейс программы. Вкладка «Организационные меры».

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.

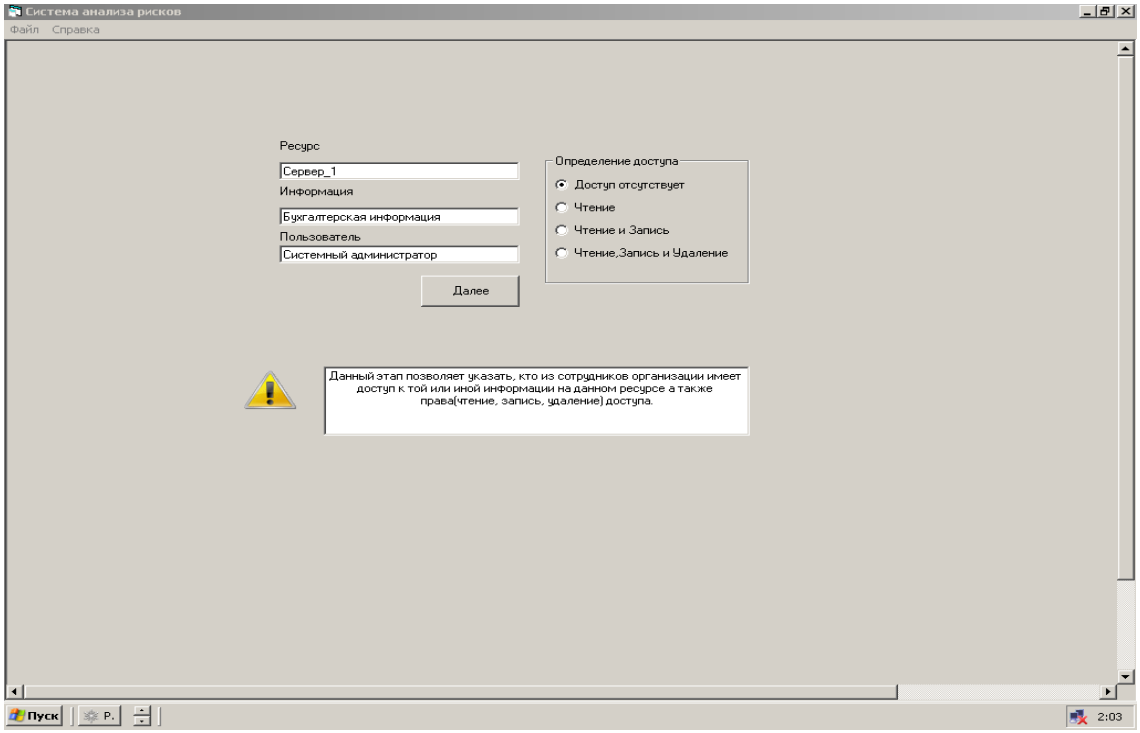


Рис. 24. Интерфейс программы. Вкладка «Доступ».

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

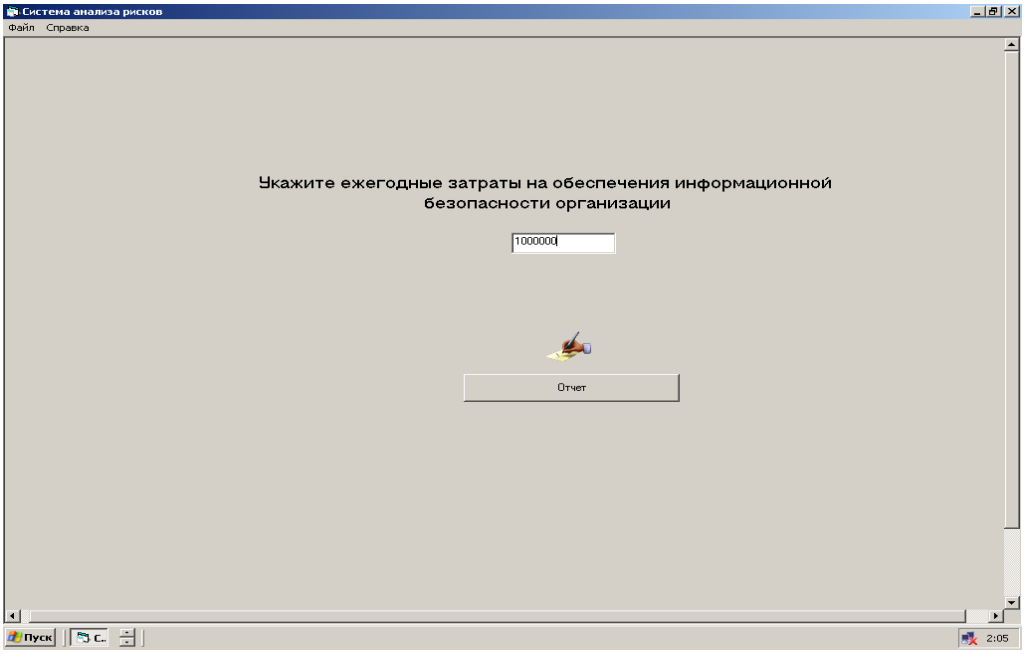


Рис. 25. Интерфейс программы. Оценка затрат на поддержание

системы 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.

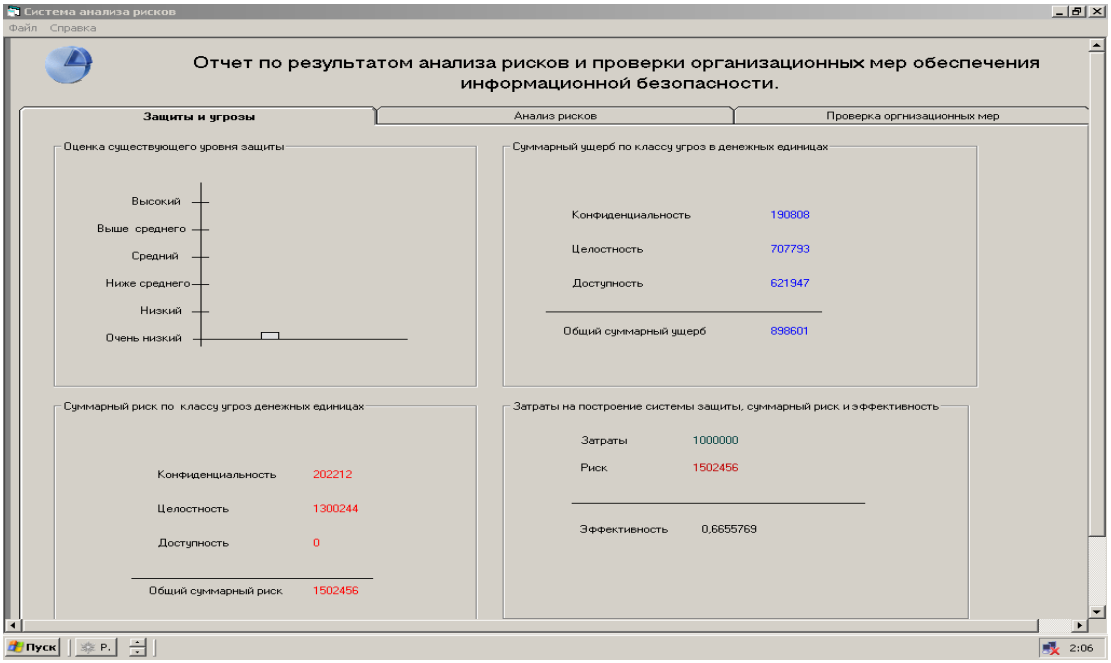


Рис. 26. Интерфейс программы. Вкладка «Защита и угрозы».

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

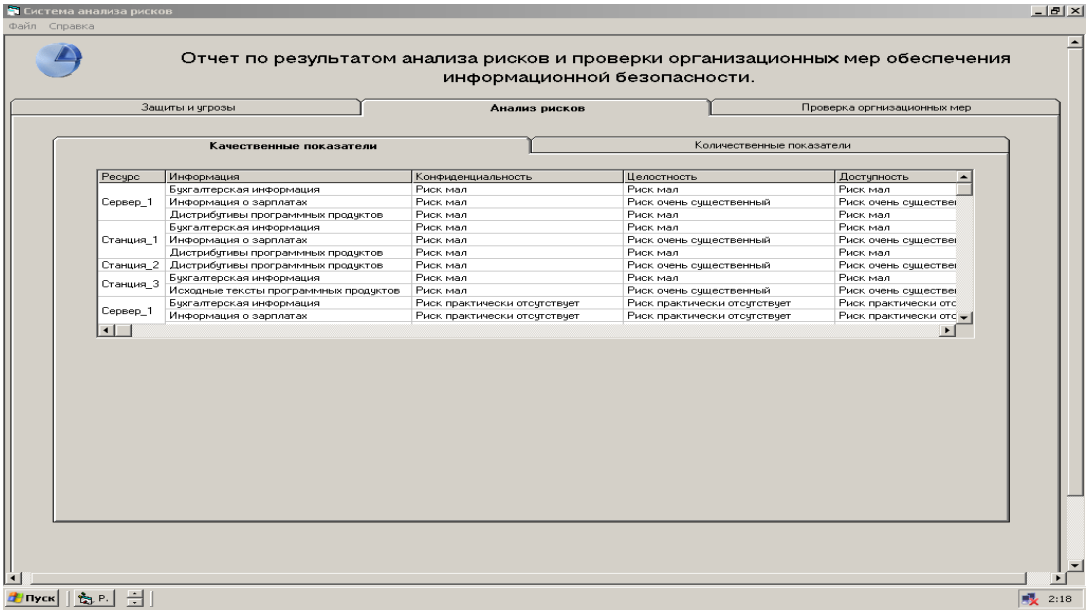
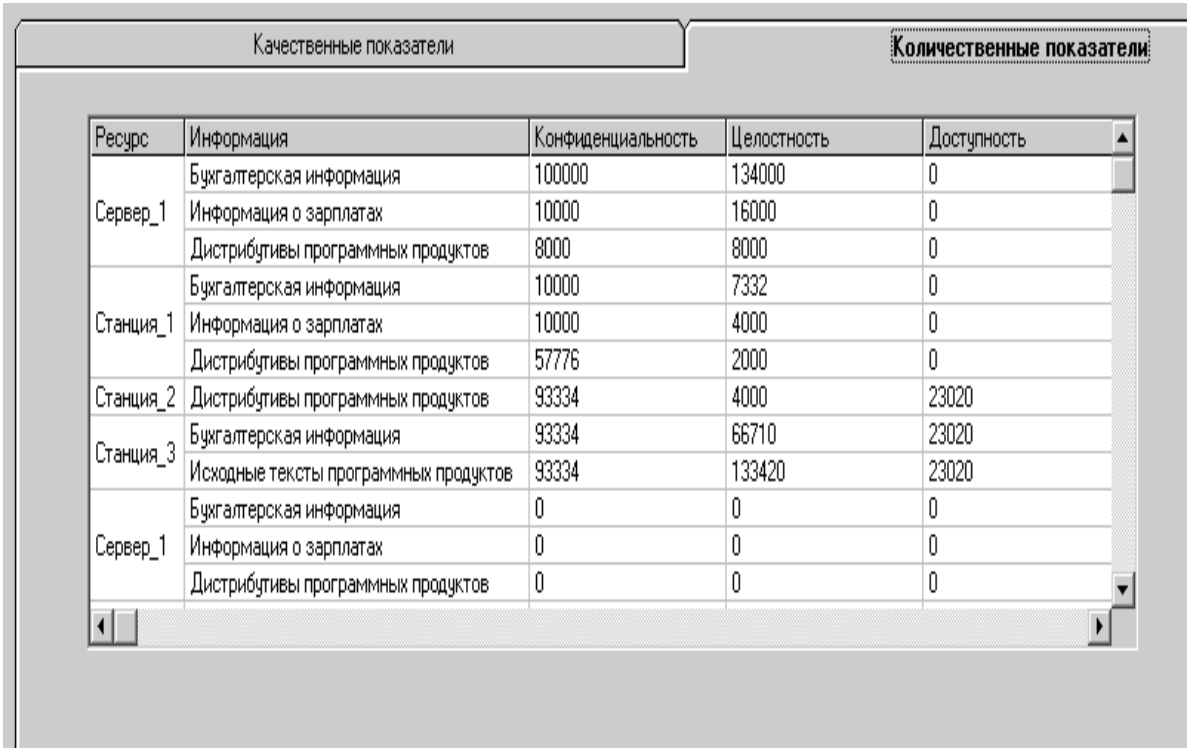


Рис. 27. Интерфейс программы. Вкладка «Анализ рисков. Качественные показатели».



Ресурс	Информация	Конфиденциальность	Целостность	Доступность
Сервер_1	Бухгалтерская информация	100000	134000	0
	Информация о зарплатах	10000	16000	0
	Дистрибутивы программных продуктов	8000	8000	0
Станция_1	Бухгалтерская информация	10000	7332	0
	Информация о зарплатах	10000	4000	0
	Дистрибутивы программных продуктов	57776	2000	0
Станция_2	Дистрибутивы программных продуктов	93334	4000	23020
Станция_3	Бухгалтерская информация	93334	66710	23020
	Исходные тексты программных продуктов	93334	133420	23020
Сервер_1	Бухгалтерская информация	0	0	0
	Информация о зарплатах	0	0	0
	Дистрибутивы программных продуктов	0	0	0

Рис. 28. Интерфейс программы. Вкладка «Анализ рисков. Количественные показатели».

Последняя вкладка “Проверка организационных мер ” демонстрирует

пользователю , количество не соответствующих организационных мер положениям МБО и выводит пояснение.

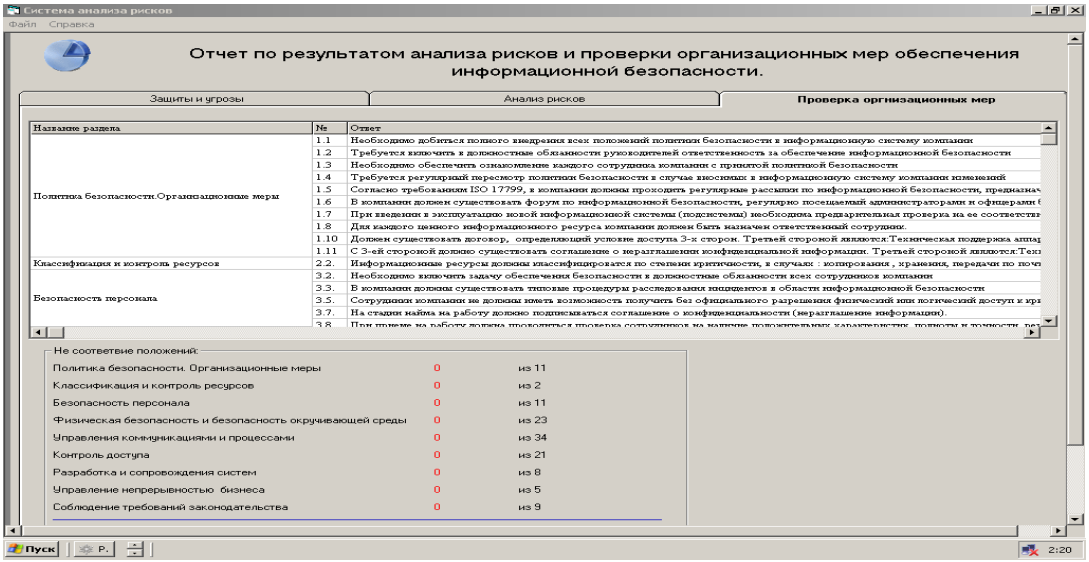


Рис. 29. Интерфейс программы. Вкладка « Проверка организационных мер» ”.

4. 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.

Таблица 6. Привязка данных

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

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.

Таблица 8.Определение прав доступа пользователей на рабочей станции два

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

	Информация о зарплатах	Чтение

3) 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 рисков

Ресурс	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.

Таблица 13.Результат расчета количественной характеристики рисков

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 о зарплатах	260000	520000	200000
Рабочая станция два	Бухгалтерская информация	10000	420000	240000
	Информация о зарплатах	260000	780000	200000
Рабочая станция три	Информация о клиентах в электронном виде	300000	340000	500000
	Информация о партнерах в электронном виде	320000	290000	600000

Таблица 14. Результат расчета качественной характеристики рисков

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

			целостности	доступности
Сервер	Исходные тексты программных продуктов	Риск мал	Риск мал	Риск мал
	Дистрибутивы программных продуктов	Риск мал	Риск существенный	Риск существенный
Рабочая станция один	Бухгалтерская информация	Риск мал	Риск мал	Риск мал
	Информация о зарплатах	Риск мал	Риск мал	Риск мал
Рабочая станция два	Бухгалтерская информация	Риск мал	Риск существенный	Риск существенный
	Информация о зарплатах	Риск мал	Риск существенный	Риск существенный
Рабочая станция три	Информация о клиентах в электронном виде	Риск мал	Риск мал	Риск мал
	Информация о партнерах в электронном виде	Риск мал	Риск мал	Риск мал

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.

5. 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.

Таблица 15. Вариант 1.

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

Таблица 16. Вариант 2.

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

Таблица 17. Вариант 3.

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
Описание	Компания занимается страхованием всех видов деятельности. Расположена в отдельном здании. На входе сидит охранник.
Затраты на информационную безопасность в год	200 000

Таблица 18. Вариант 4.

Название организации	Филиал нефтяной компании в Томске “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.

Таблица 19. Вариант 5.

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

2. 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

3. Выберите те виды информационных ресурсов которые представлены в вашем варианте. Теперь перейдите к вкладке “Пользователи системы”, где надо будет

отметить пользователей информационной системы. На вкладке “Аппаратные средства” определите количество серверов и рабочих станций из вашего варианта. Нажмите кнопку ”Продолжить работу с программой”.

4. 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.

5. 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”.

6. 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.

7. Теперь на экране должно появиться окно для ввода затрат на информационную

безопасность. Затраты можно определить из вашего варианта. Это заключительный этап сбора информации о вашей организации. Далее программа генерирует отчет по результатам анализа.

8. 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.

9. 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.

10. 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.

6. 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).

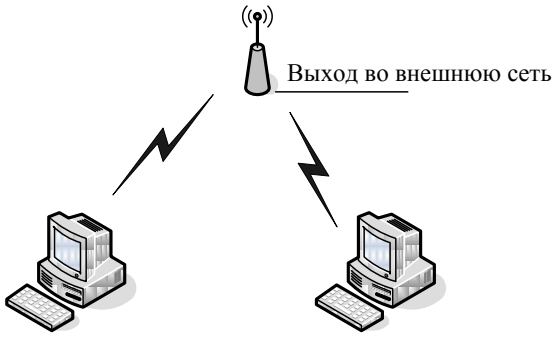


Рис. 2. Структура BSS

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.

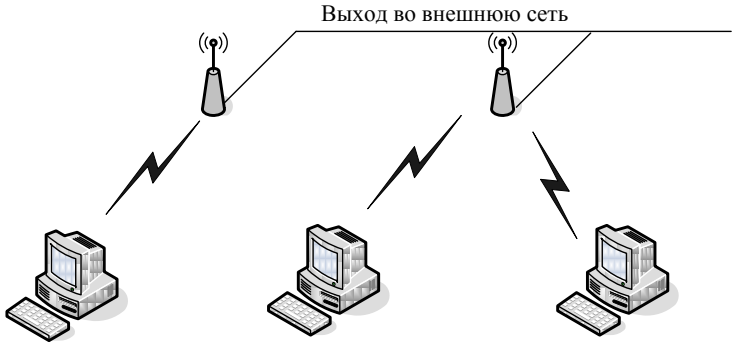


Рис. 3. Структура ESS

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).

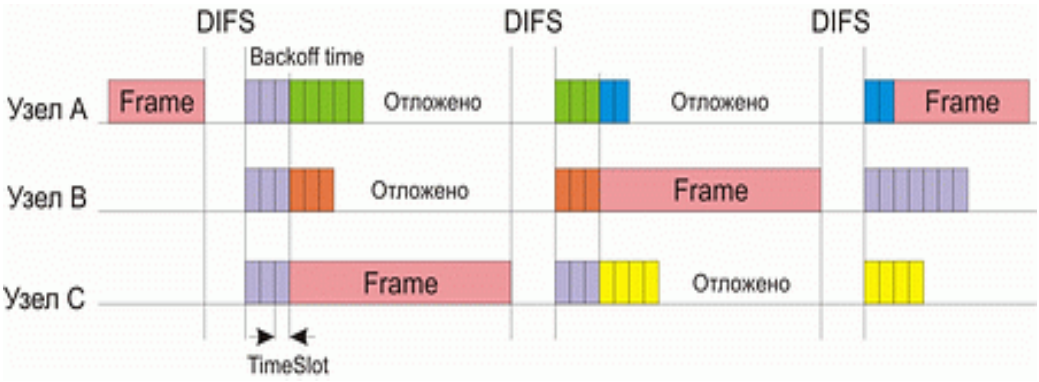


Рис. 4. Реализация равноправного доступа к среде передачи данных в методе DCF

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.

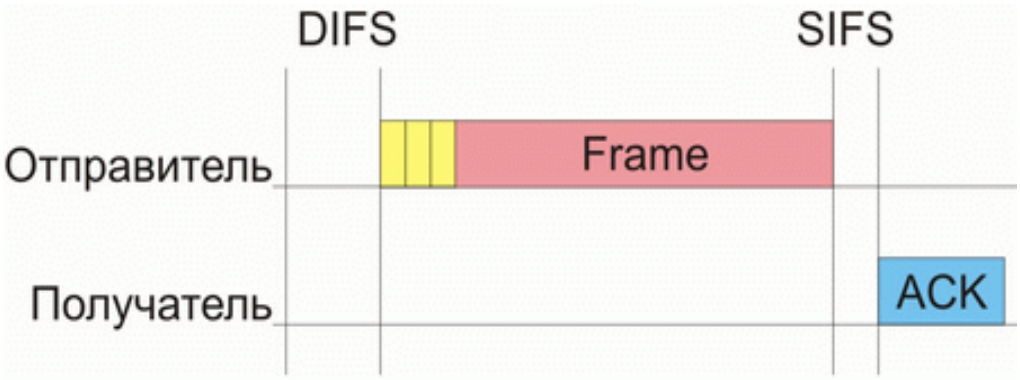


Рис. 5. Кадры квитанции, отсылаемые в случае успешной передачи данных

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.

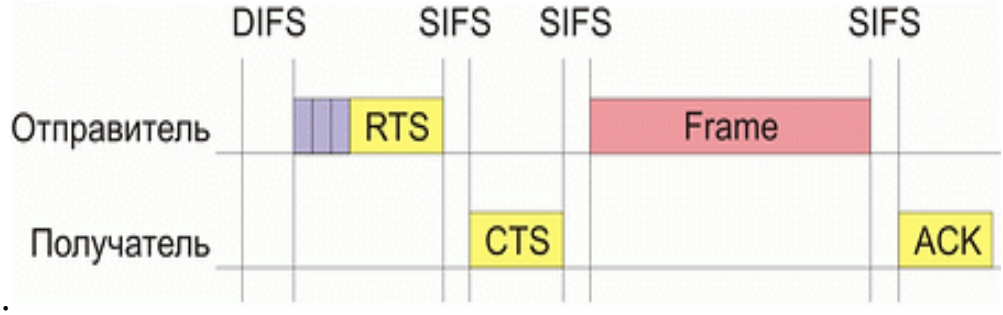


Рис. 6. Взаимодействие между двумя узлами сети в соответствии с алгоритмом RTS/CTS

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.

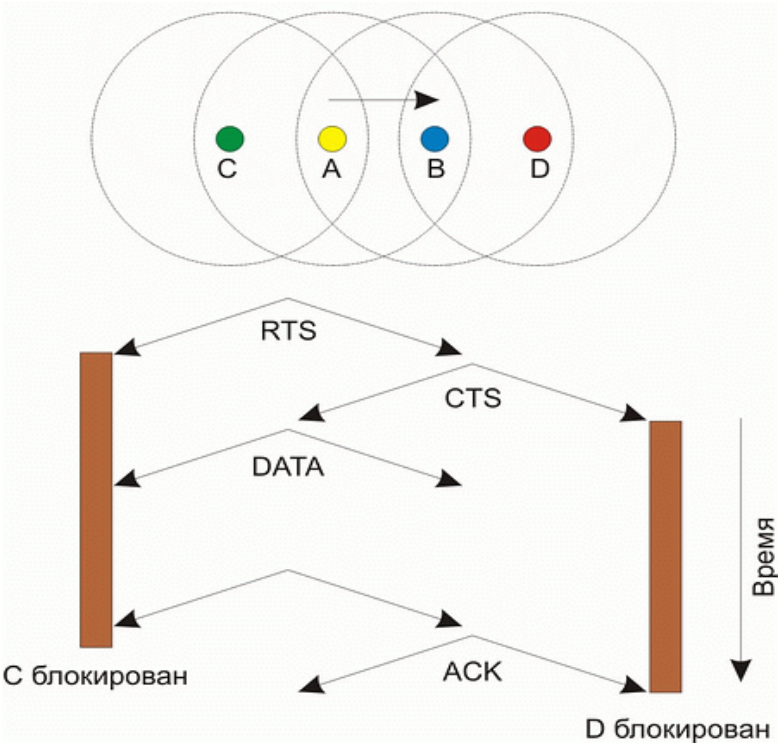


Рис.7. Решение проблемы скрытых узлов в алгоритме RTS/CTS

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 кадр

RTS, то он ложно заблокирует узел G.

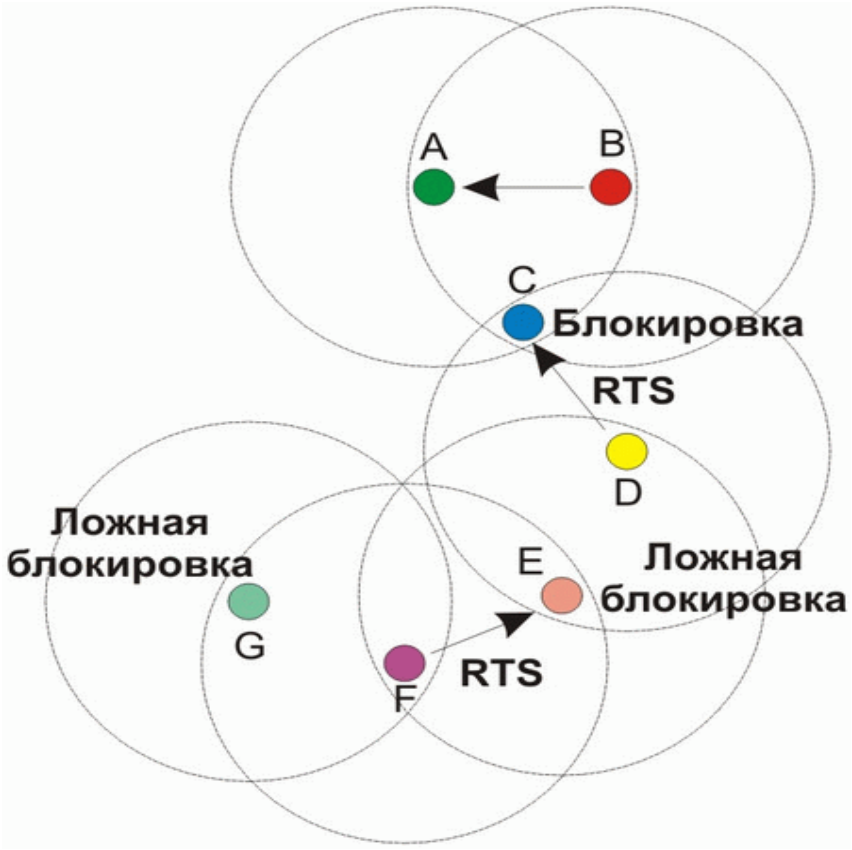


Рис. 7. Возникновение ложных блокировок узлов сети

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

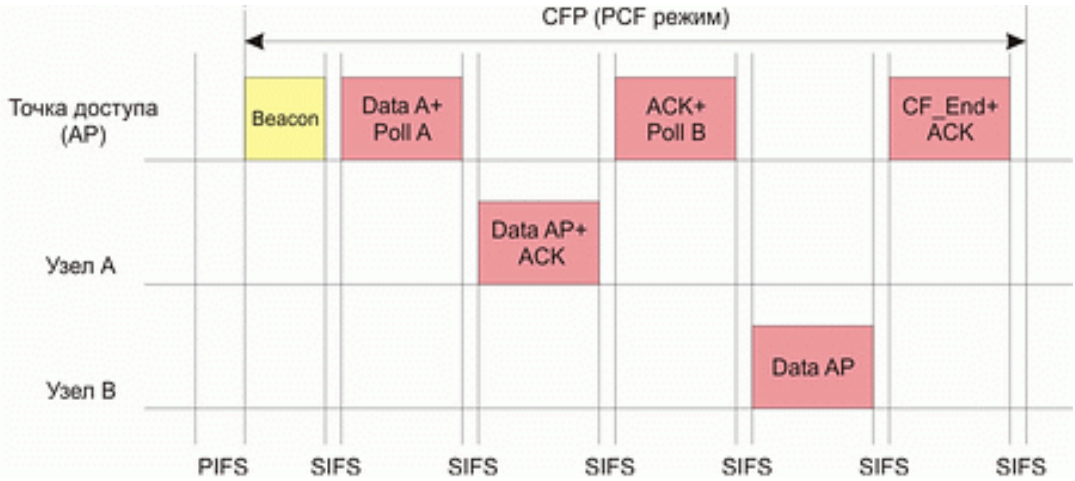


Рис. 9. Организация передачи данных между узлами сети в режиме PCF

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.

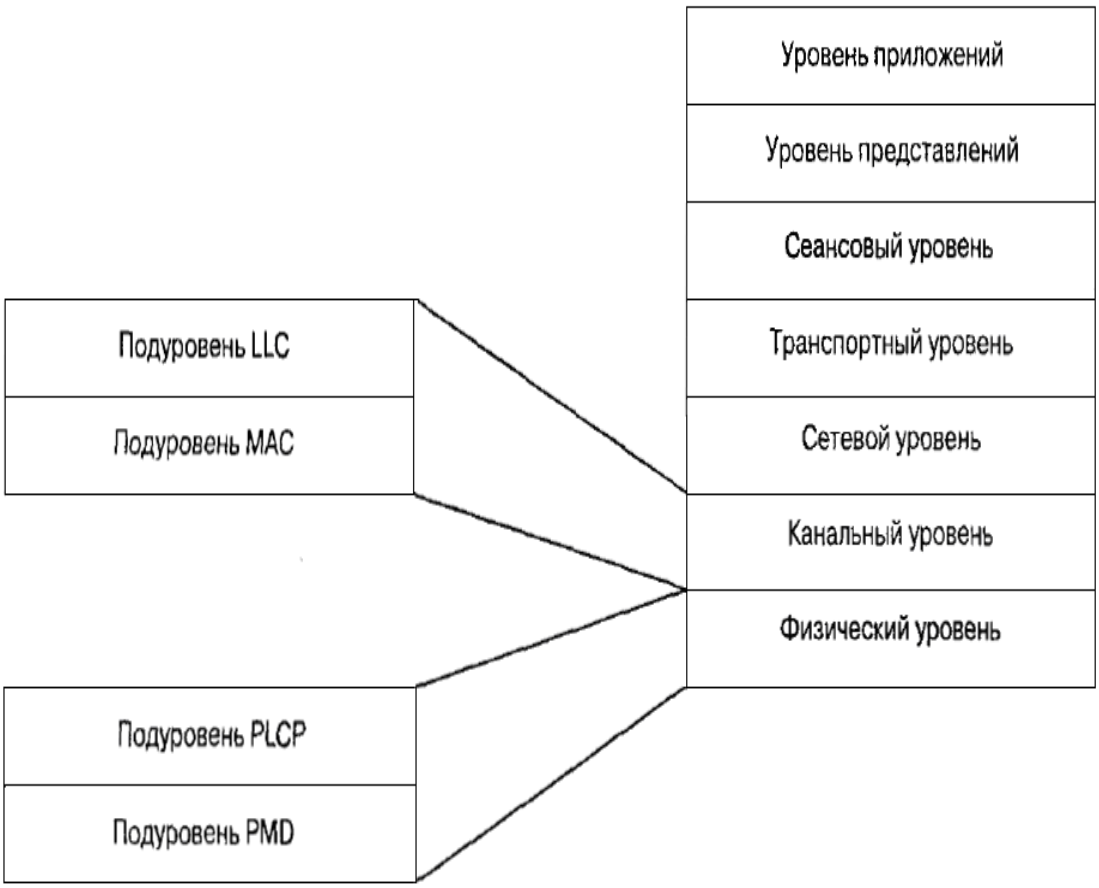


Рис. 10. Подуровни уровня PHY модели взаимодействия открытых систем (OSI)

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 прямой 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.

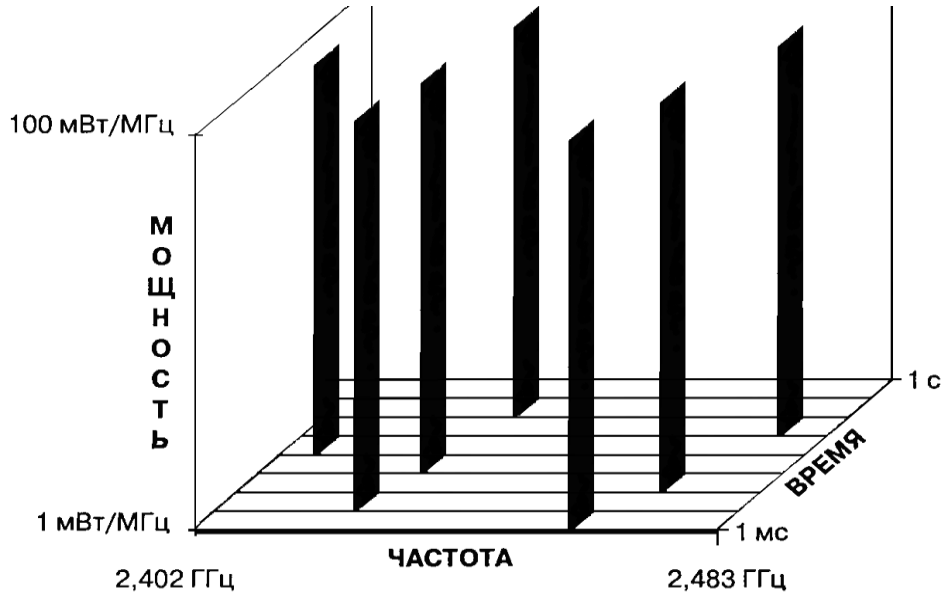


Рис. 11. Пример скачкообразной перестройки частоты

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.

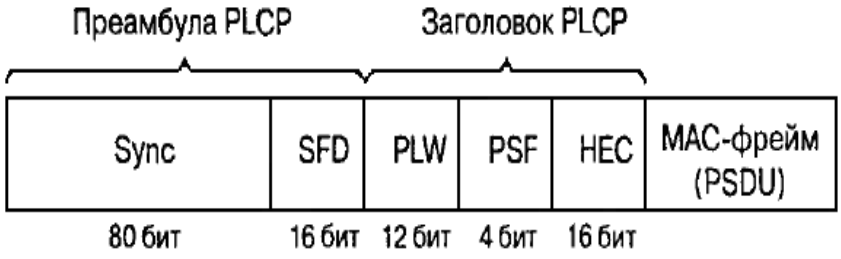


Рис. 12. Формат фрейма FHSS подуровня PLCP

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.

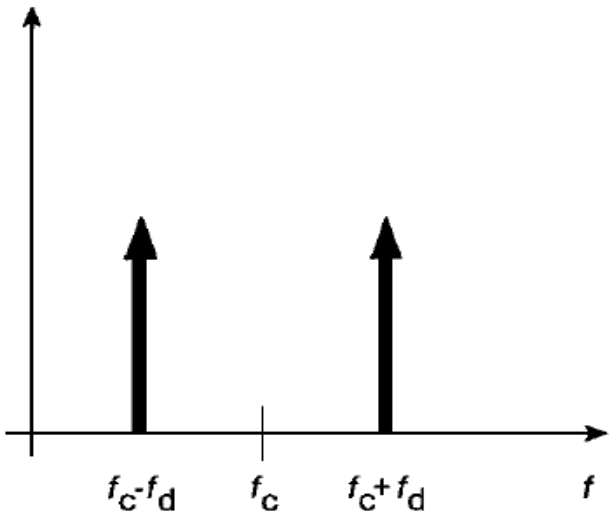


Рис. 13. Модуляция GFSK

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 802.11 добавляет два поля во фрейм MAC, чтобы сформировать PPDU: преамбулу PLCP и заголовок PLCP. Формат фрейма представлен на рис. 14.

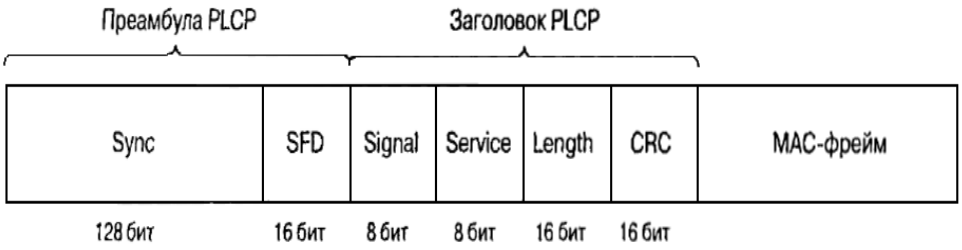


Рис. 14. Формат фрейма DSSS PPDU стандарта 802.11

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.

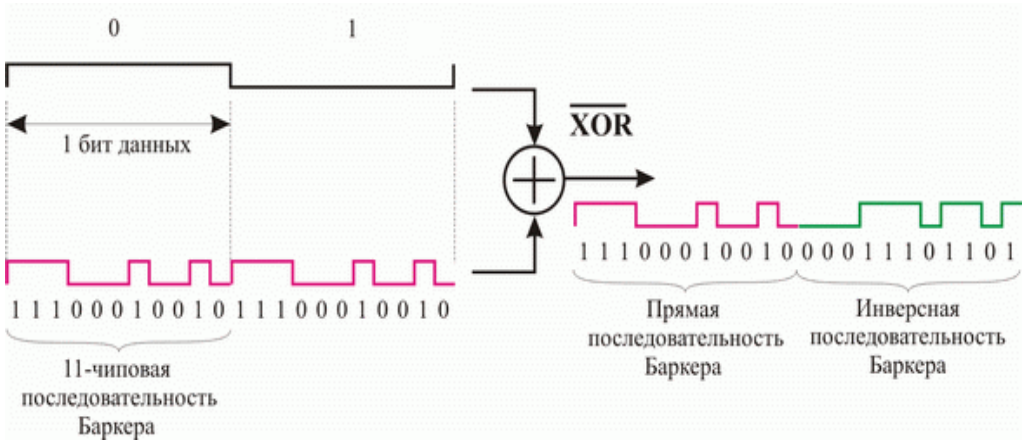


Рис. 15 Расширение спектра по технологии DSSS

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 сигнала при 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, $\pi/2$, π и $3\pi/2$. 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 $\pi/2$; дибиту 11 — сдвиг фазы, равный π; дибиту 10 — сдвиг фазы, равный $3\pi/2$.

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)

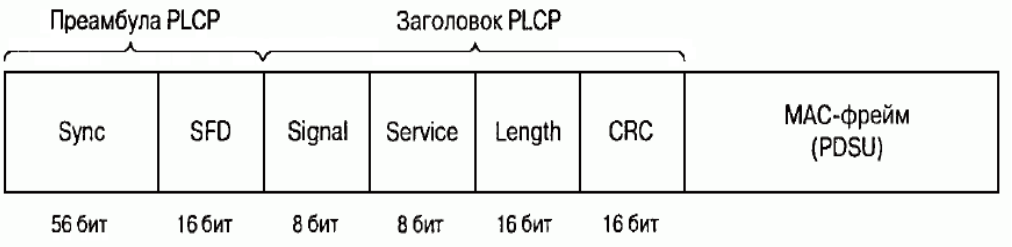


Рис. 16 Короткий PPDU технологии HR-DSSS

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	C1	C2	C3	C4	C5	C6	C7	C8
00	J	1	j	-1	J	1	-1	1
01	-J	-1	-j	1	**J**	1	-j	1
10	-j	1	-j	-1	**-j**	1	j	1
11	j	-1	j	1	-i	1	j	1

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.

Таблица 5. Поворот фазы при CCK модуляции

00	0 градусов
01	90 градусов
11	180 градусов
10	90 градусов

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 три

выходящих. 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 в одном символе
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
11	(обязательно)	CCK	DQPSK	-	1,375	8
	(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).

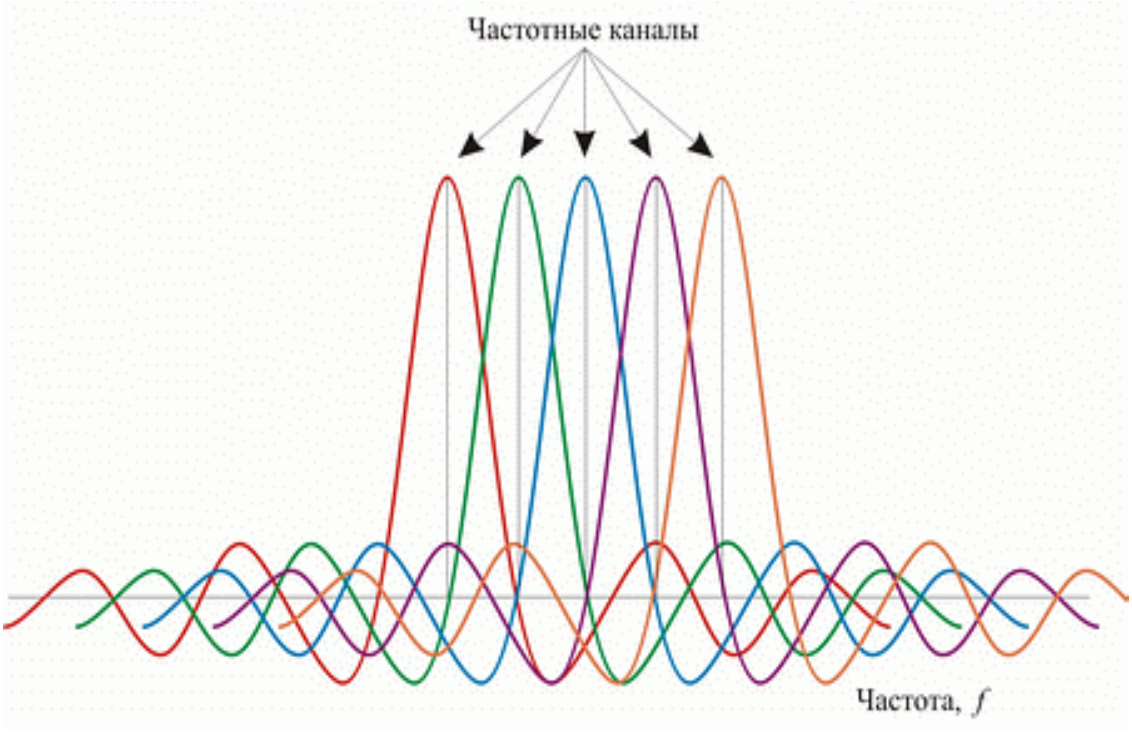


Рис. 17. Пример перекрывающихся частотных каналов с ортогональными несущими

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 многолучевому распространению. Если говорить точнее, то сама по себе технология OFDM не устраняет многолучевого распространения, но создает предпосылки для устранения эффекта межсимвольной интерференции. Неотъемлемой частью технологии OFDM является охранный интервал (Guard Interval, GI) — циклическое повторение окончания символа, пристраиваемое в

начале символа (рис. 18).

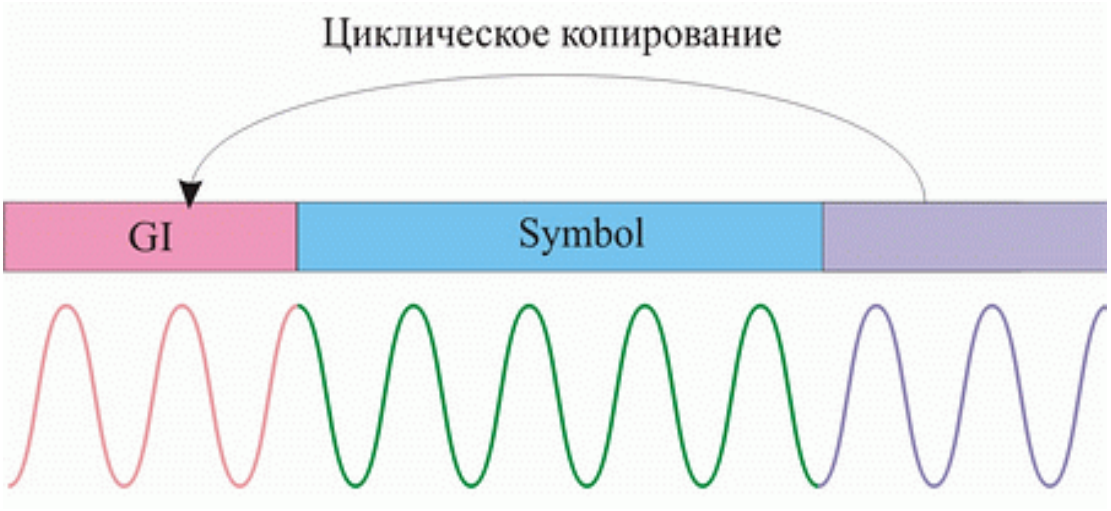


Рис. 18. Охранный интервал GI

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).

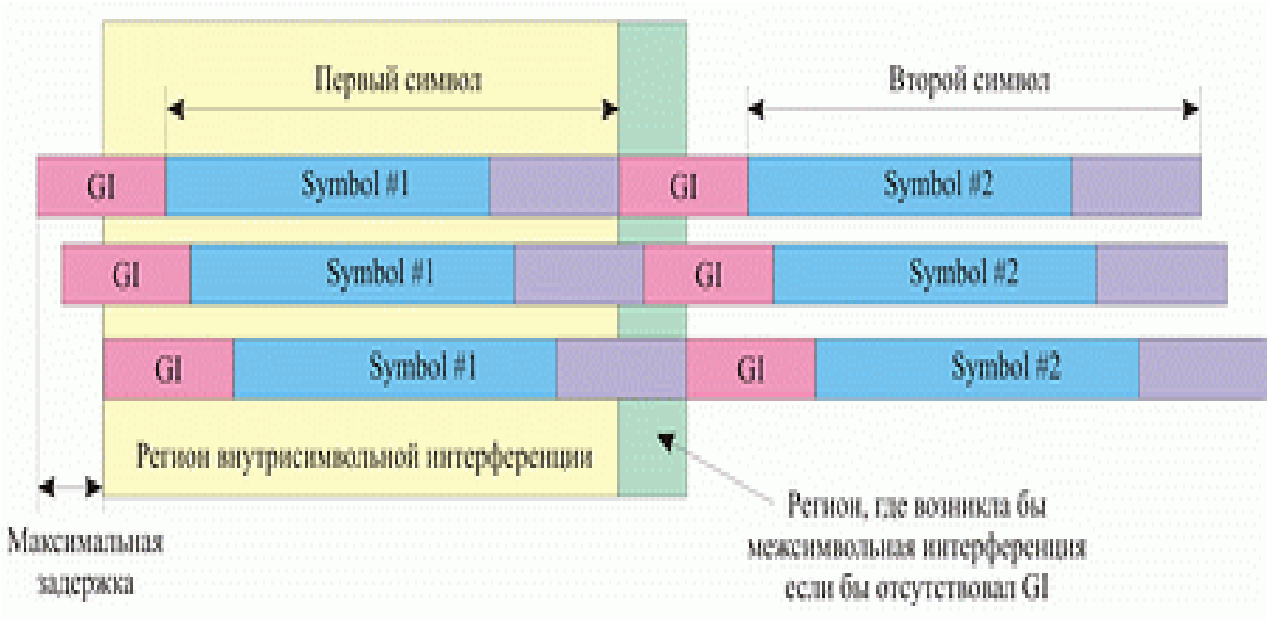


Рис. 19. Избежание межсимвольной интерференции за счет использования охранных интервалов

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.

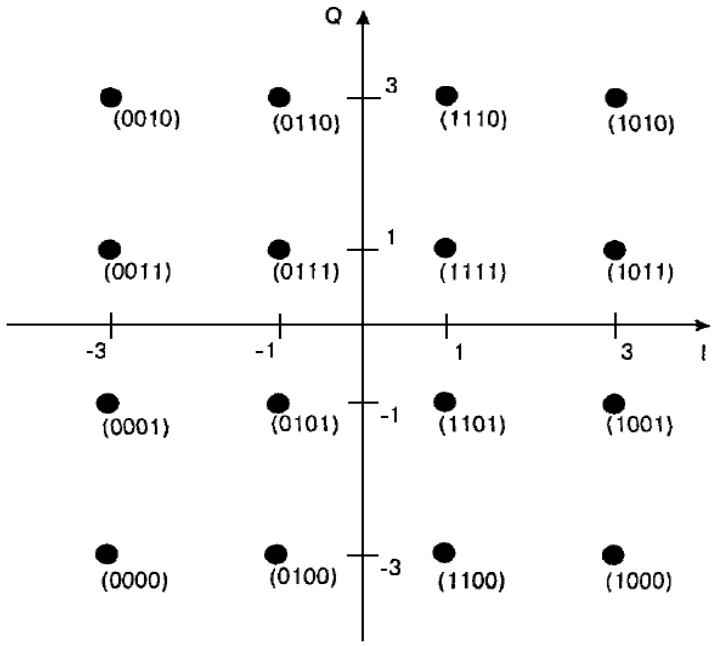


Рис. 20. Представление сигнала при QAM-16

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	Q SK
	(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

Характе истики	**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.

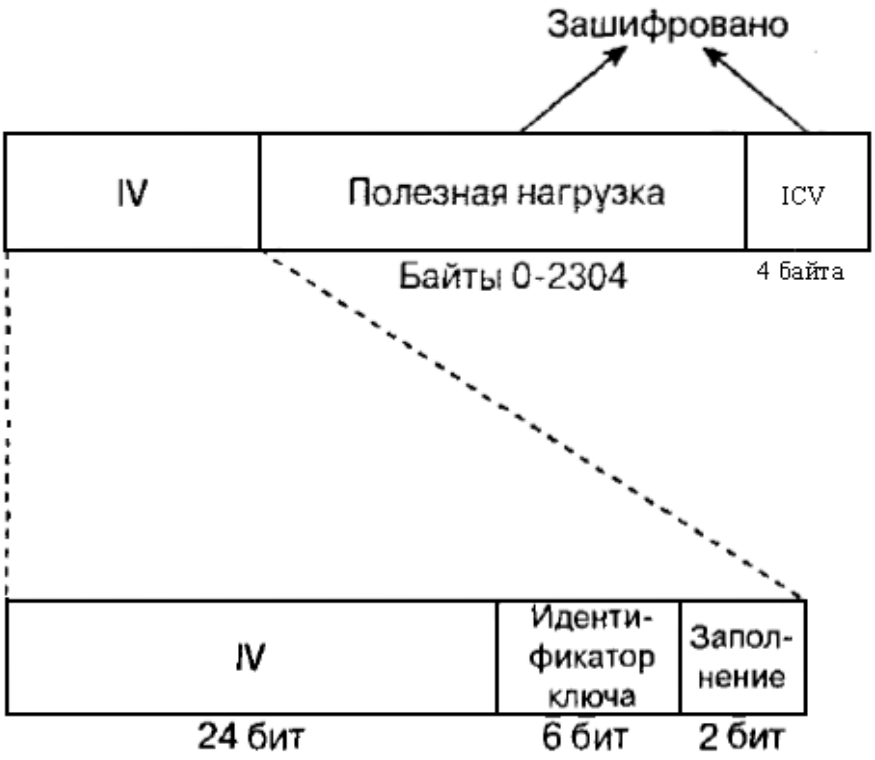


Рис. 21. Фрейм, зашифрованный алгоритмом WEP

Спецификация стандарта 802.11 требует, чтобы одинаковые WEP-ключи были сконфигурированы как на клиентах, так и на устройствах, образующих инфраструктуру сети. Можно определять до четырех ключей на одно устройство, но одновременно 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 корректной расшифровки 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.

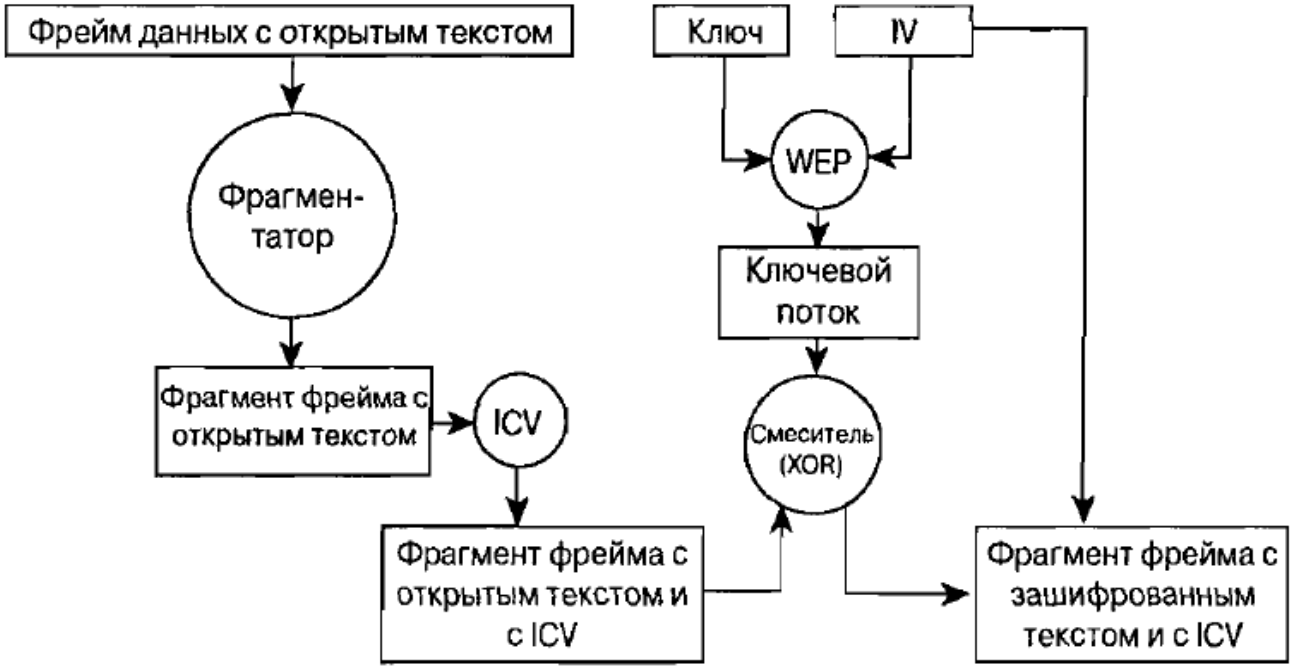


Рис. 22. Шифрование по алгоритму WEP

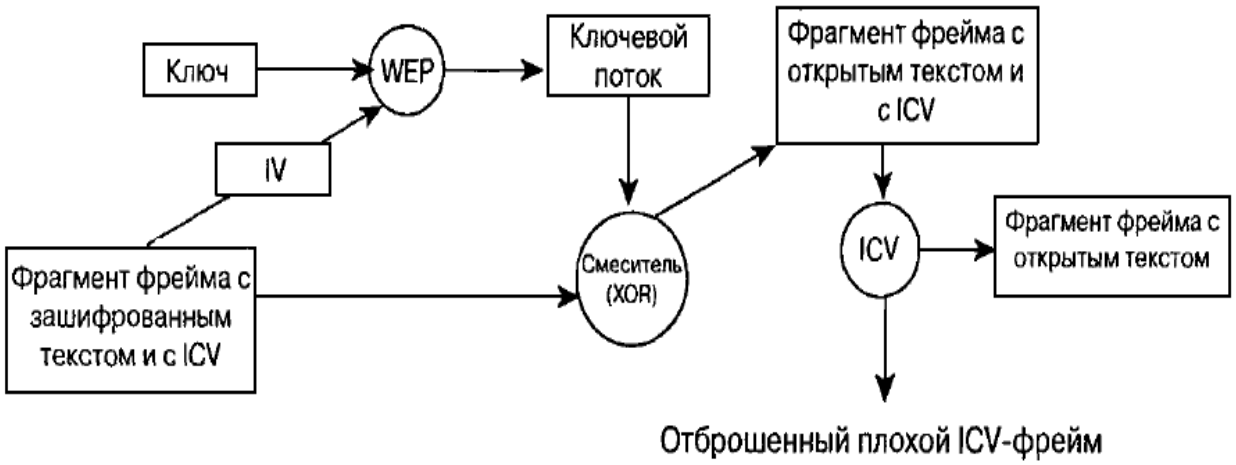


Рис. 23. Дешифрование по алгоритму WEP

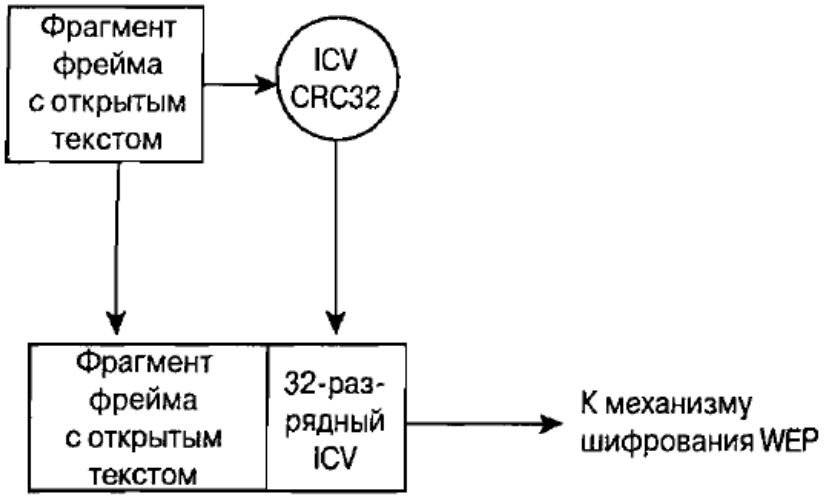


Рис. 24. Диаграмма функционирования механизма ICV

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.

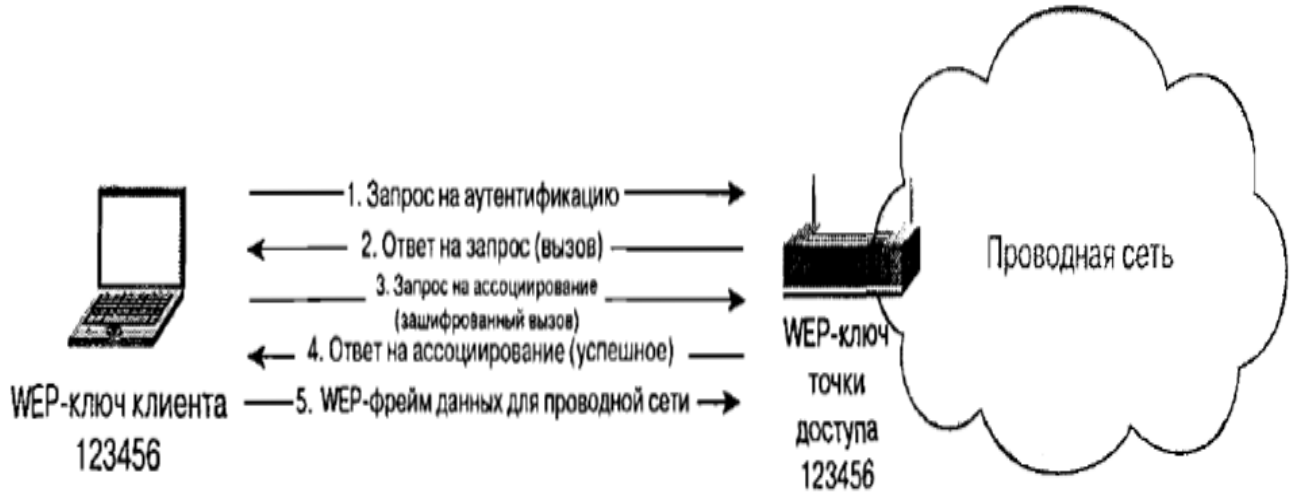


Рис. 25. Процесс аутентификации с совместно используемым ключом

Предпосылки, на которых основана аутентификация с совместно используемым ключом, точно такие же, как и те, которые предполагались при открытой аутентификации, использующей WEP-ключи в качестве средства контроля доступа. Разница между этими двумя схемами состоит в том, что клиент не может ассоциировать 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.

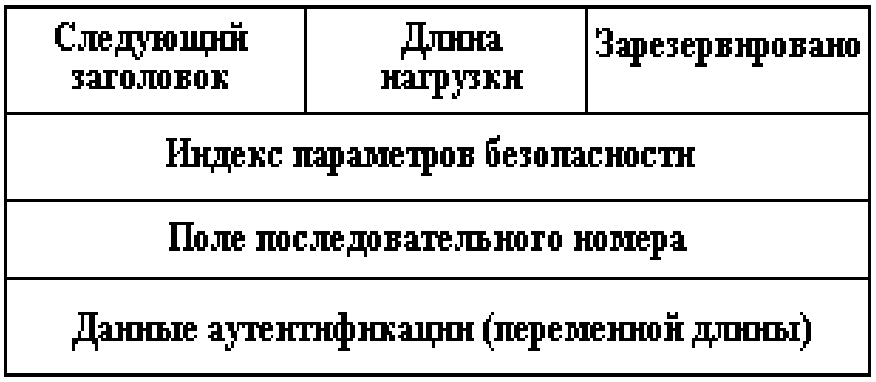


Рис. ***26. Формат заголовка AH***

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 передаётся 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 трёх 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”.

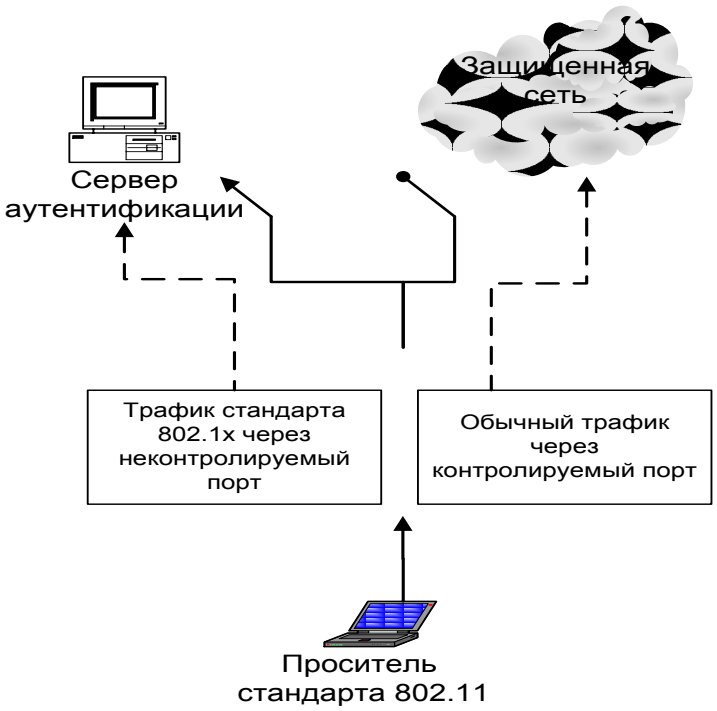


Рис. 28. Логические порты аутентификатора стандарта 802.1X

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 этом

случае 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)

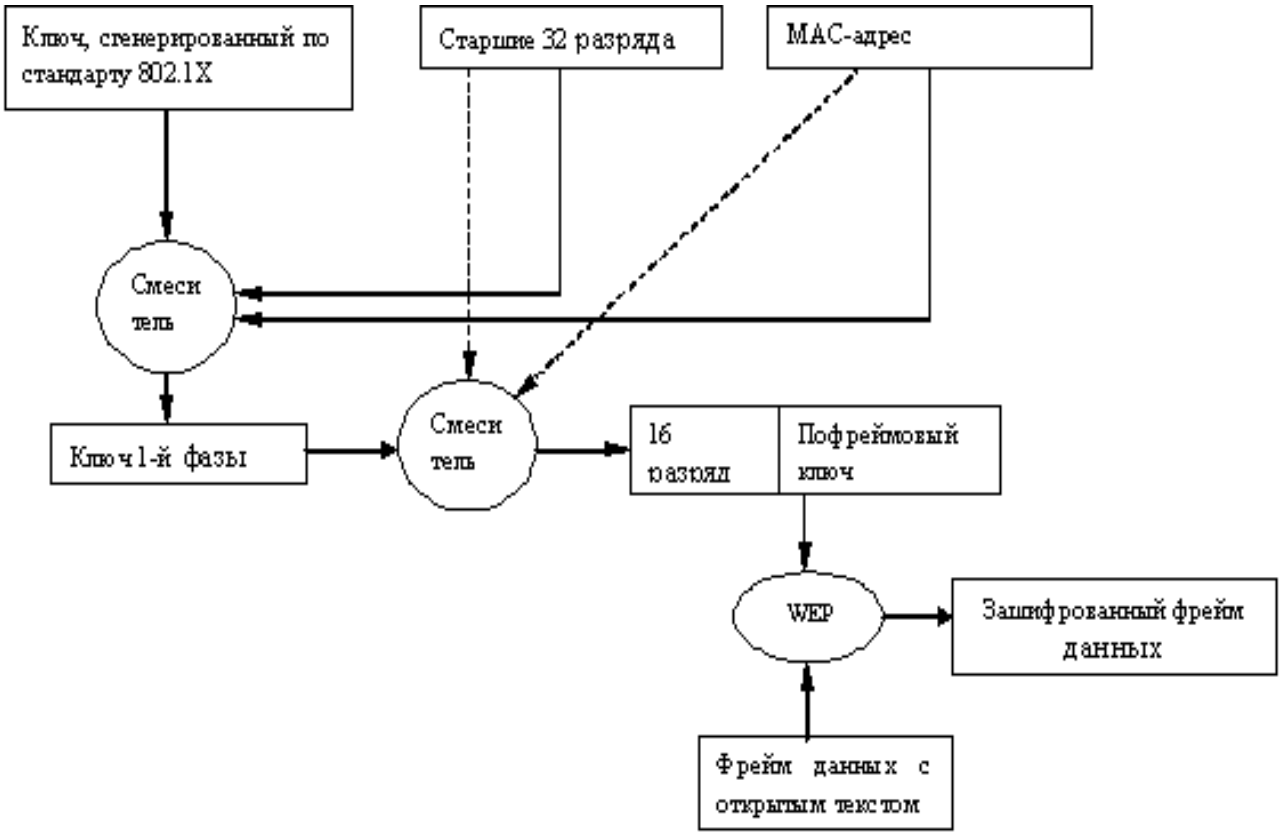


Рис. 29. Пофреймовое изменение ключей

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.

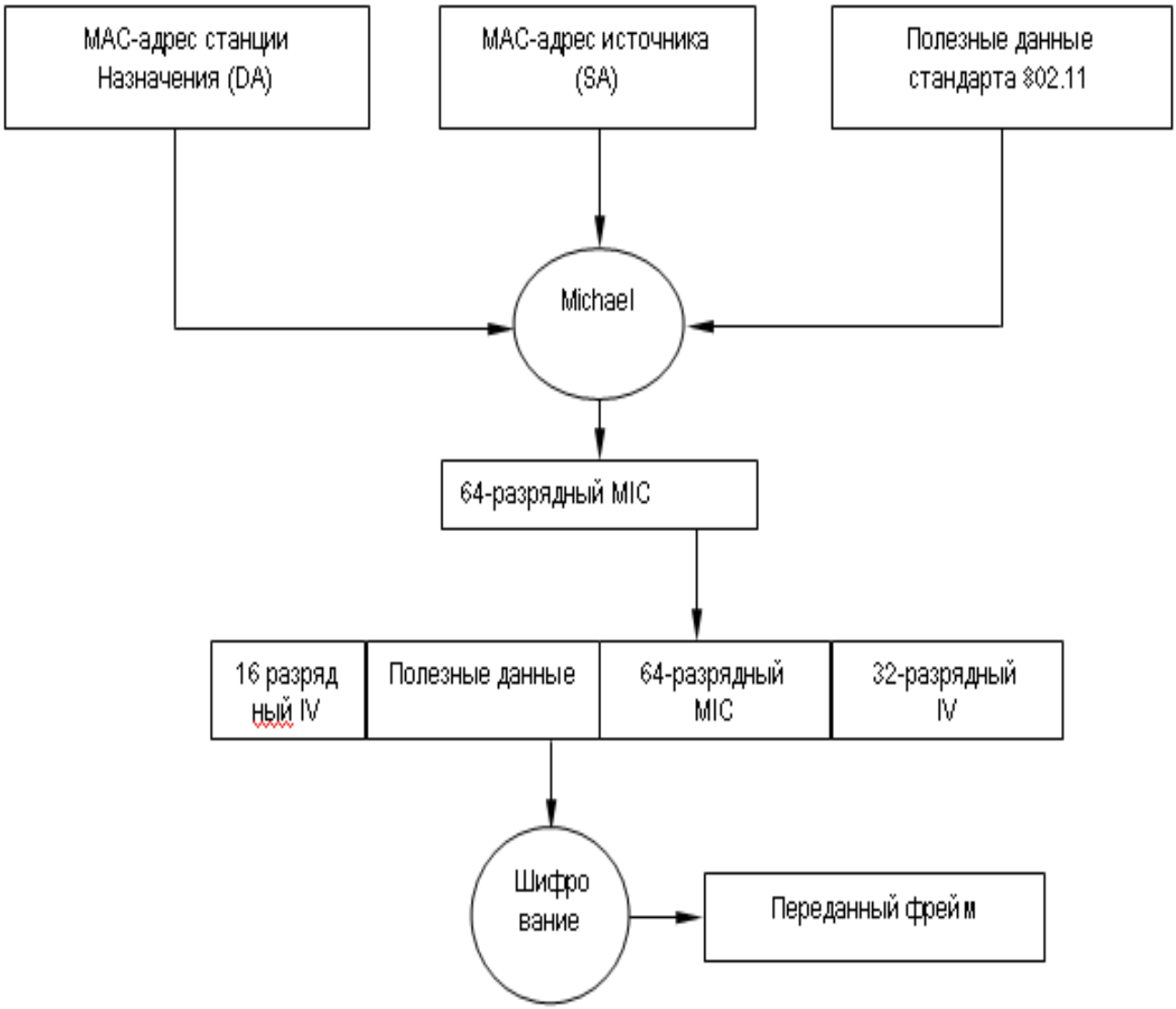


Рис. 30. Работа алгоритма MIC

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.

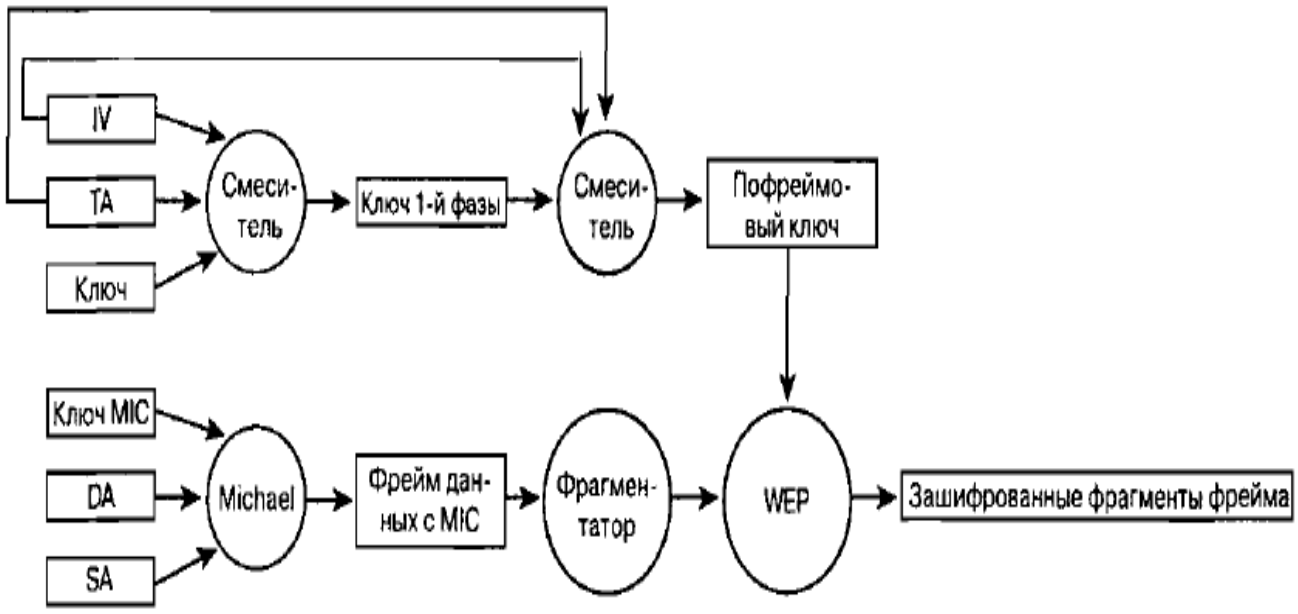


Рис. 31 – Алгоритм шифрования TKIP

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

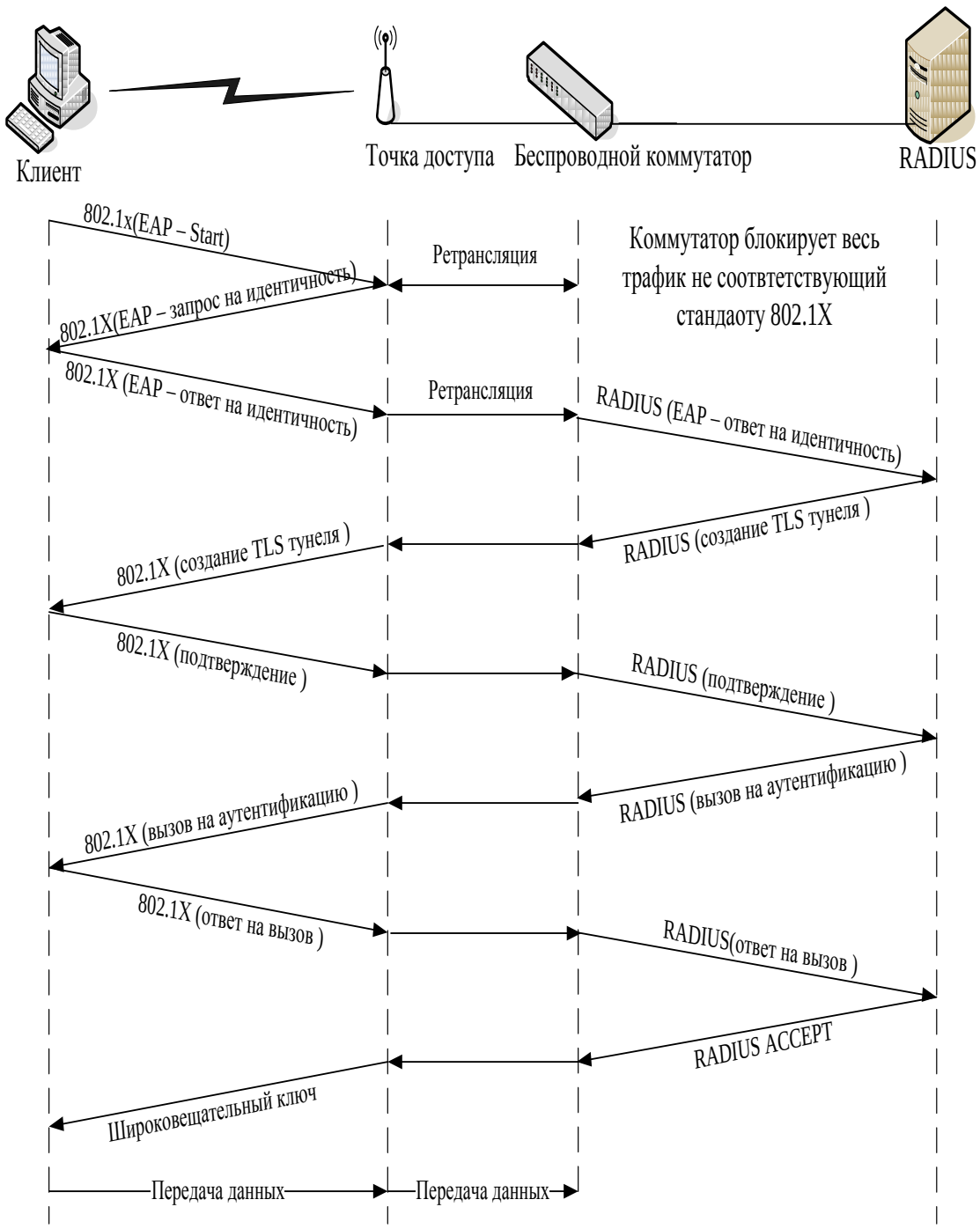


Рис. 37. Процедура прохождения аутентификации EAP-PEAP-MSCHAP V2

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.

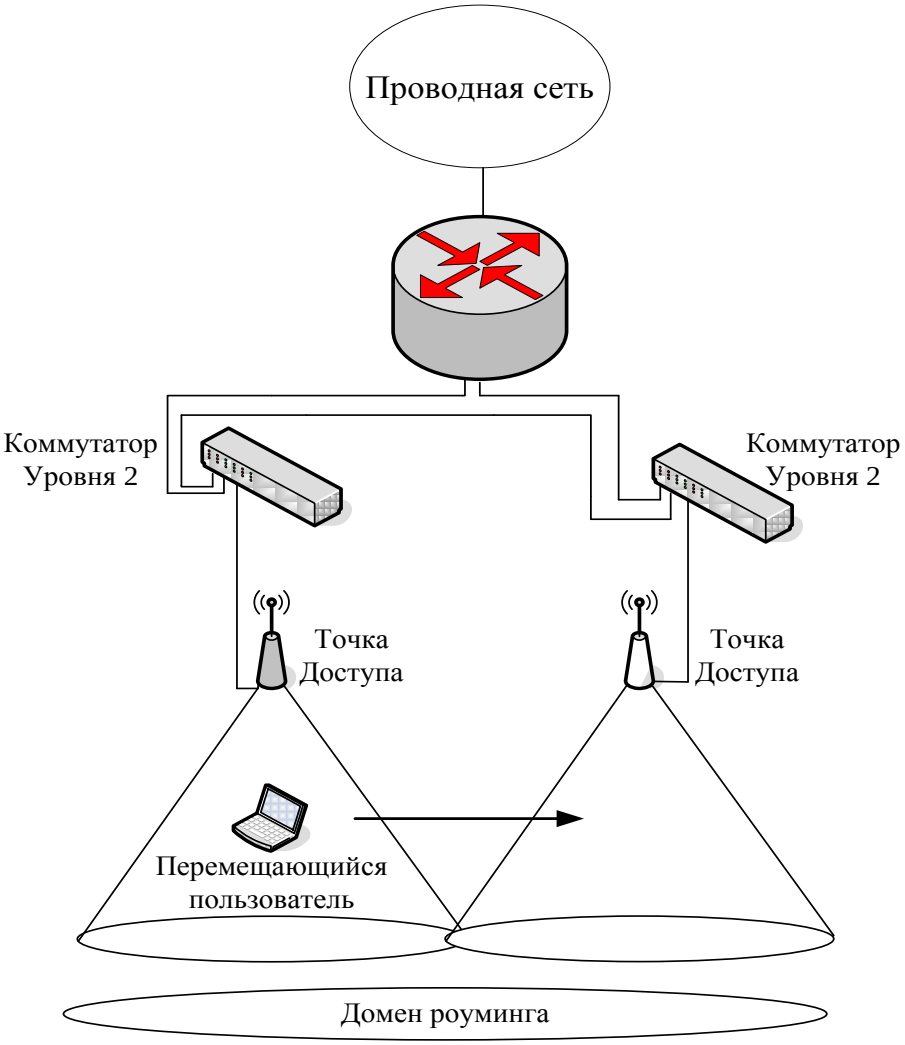


Рис. 38. Домен роуминга уровня два

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, как аутентификация 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 помощью мобильного брандмауэра выполняет также 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 вокруг уровня управления радиотрафиком.

Алгоритм работы

Беспроводной клиент получает доступ к сети, пытаясь подключиться для этого к точке доступа с наиболее сильным сигналом. Запрос на соединение может исходить от нового пользователя, регистрирующегося в сети, или от активного, изменившего свое местонахождение. Запрос на соединение направляется к беспроводному коммутатору, который пытается восстановить состояние клиента из

БД активных пользователей. Если пославший запрос не был ранее активен, то коммутатор начнет процесс регистрации с помощью протокола 802.11x и базовых механизмов аутентификации, например RADIUS, Active Directory. Процесс аутентификации завершается добавлением нового клиента в БД со всей необходимой информацией о его статусе. Затем между пользователем и беспроводным коммутатором устанавливается VPN-сессия.

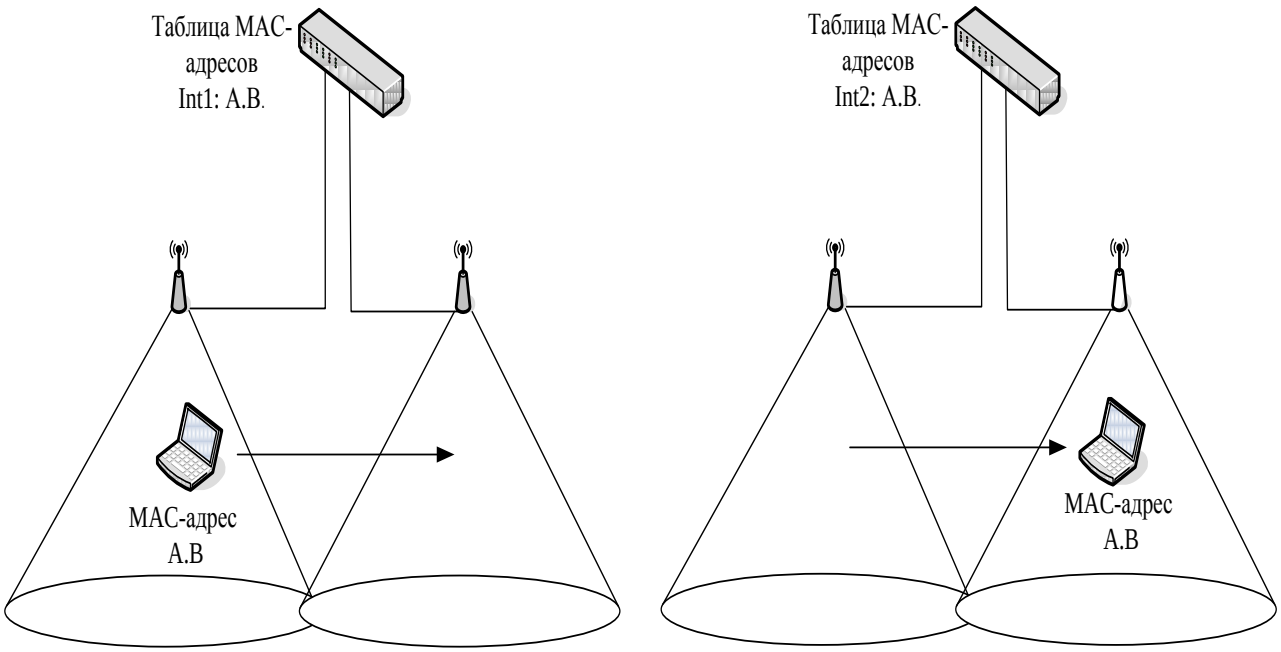


Рис. 39. Процесс роуминга с использованием беспроводного коммутатора

Описание аппаратно-программного комплекса

Критерии оптимальности системы

Для проектирования беспроводной сети, необходимо задаться некоторыми качественными требованиями к системе. Это позволит, в дальнейшем, определить технологию, наилучшим образом подходящую для решения поставленной задачи.

Итак, сформулируем и поясним основные требования, предъявляемые к

выбираемому стандарту, а, следовательно, и к программно-аппаратному комплексу:

Диапазон рабочих частот. Данный параметр является особенно важным, поскольку развертываемая беспроводная сеть передачи данных должна использовать аппаратуру, работающую в частотном диапазоне, разрешенном ГКРЧ РФ (Государственная комиссия по радиочастотам). На сегодняшний день в России, для внутриофисных систем передачи данных, разрешено использование полосы частот 2400 - 2483,5 МГц (решение № 04-03-04-003 от 6.12.2004г.). По этому применение стандарта 802.11a, расчитаного на работу в диапазоне 5 ГГц, не представляется возможным.

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 поддерживает

спецификацию 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, которое

может 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.

Централизованный аудит и учет использования. Поддержка стандарта RADIUS позволяет службе IAS централизованно собирать записи об использовании

(записи учета), отправленные всеми серверами доступа. Служба IAS хранит сведения аудита (например, успехи проверки подлинности и отказы) и использования (например, подключения и отключения) в файлах журналов. Служба IAS поддерживает формат файла журнала, допускающий непосредственный импорт в базу данных. Последующий анализ данных может быть выполнен с помощью любого обычного пакета анализа.

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.

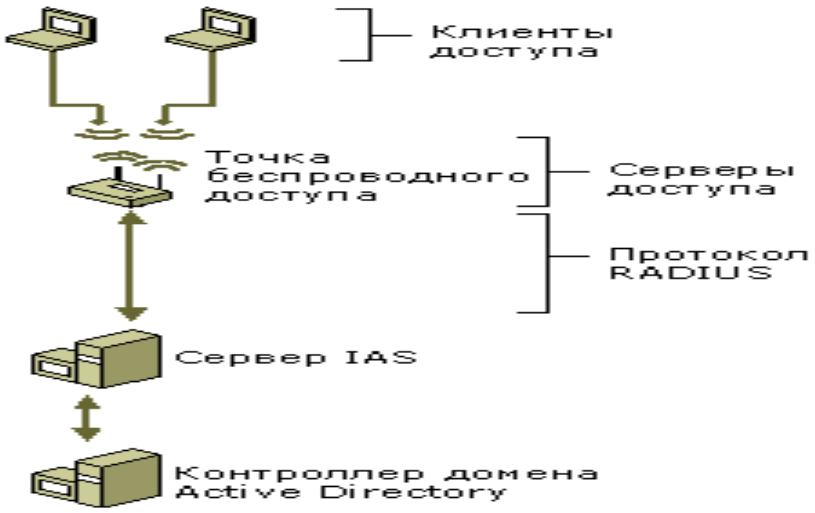


Рис. 39. Использование IAS в качестве RADIUS-сервера

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.

3. 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”.

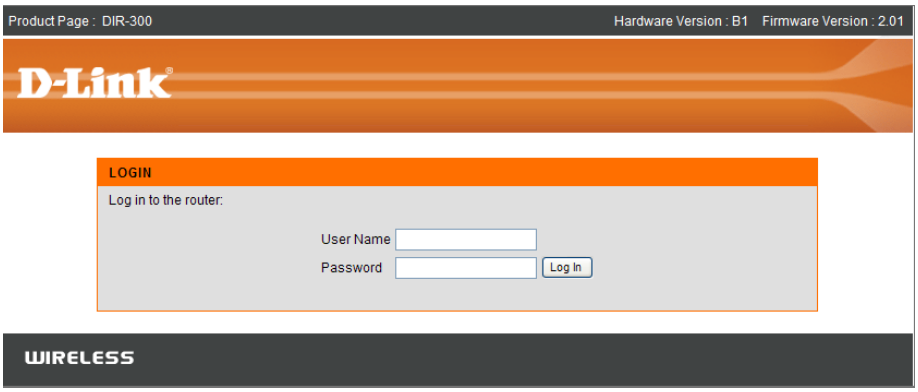


Рис. 40. Начало настройки маршрутизатора

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

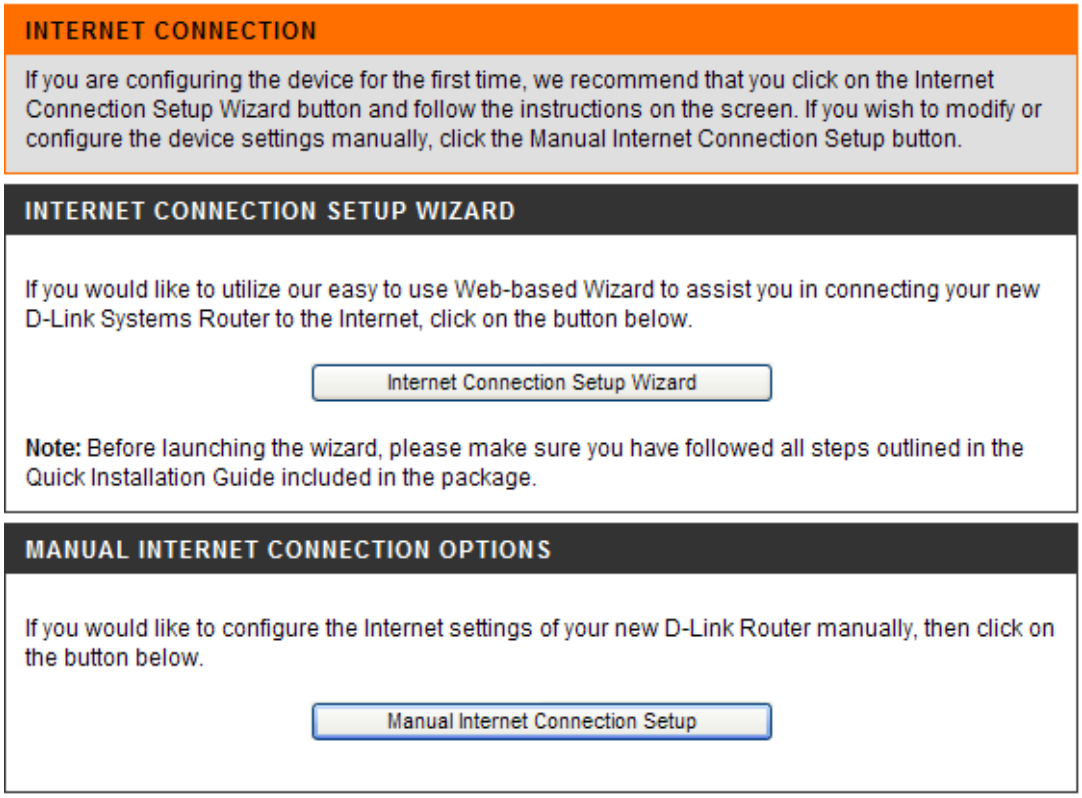


Рис. 41. Настройка Internet.

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.

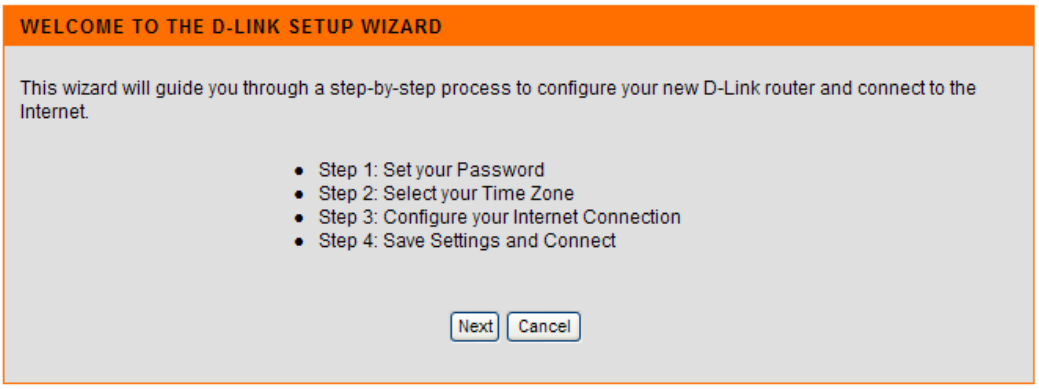


Рис. 42. Первый шаг

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

Рис. 43. Второй шаг

Необходимо ввести пароль.

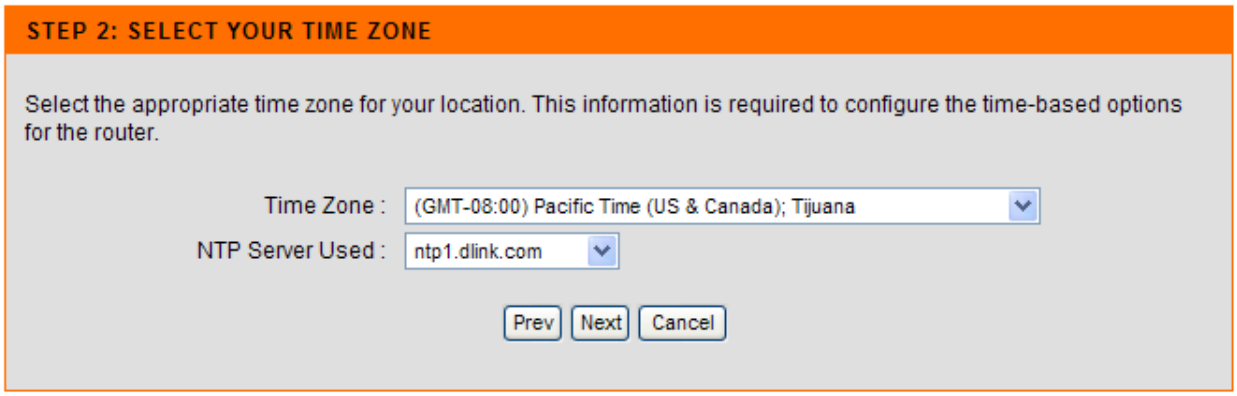


Рис. 44. Третий шаг

Затем выбрать соответствующий часовой пояс.

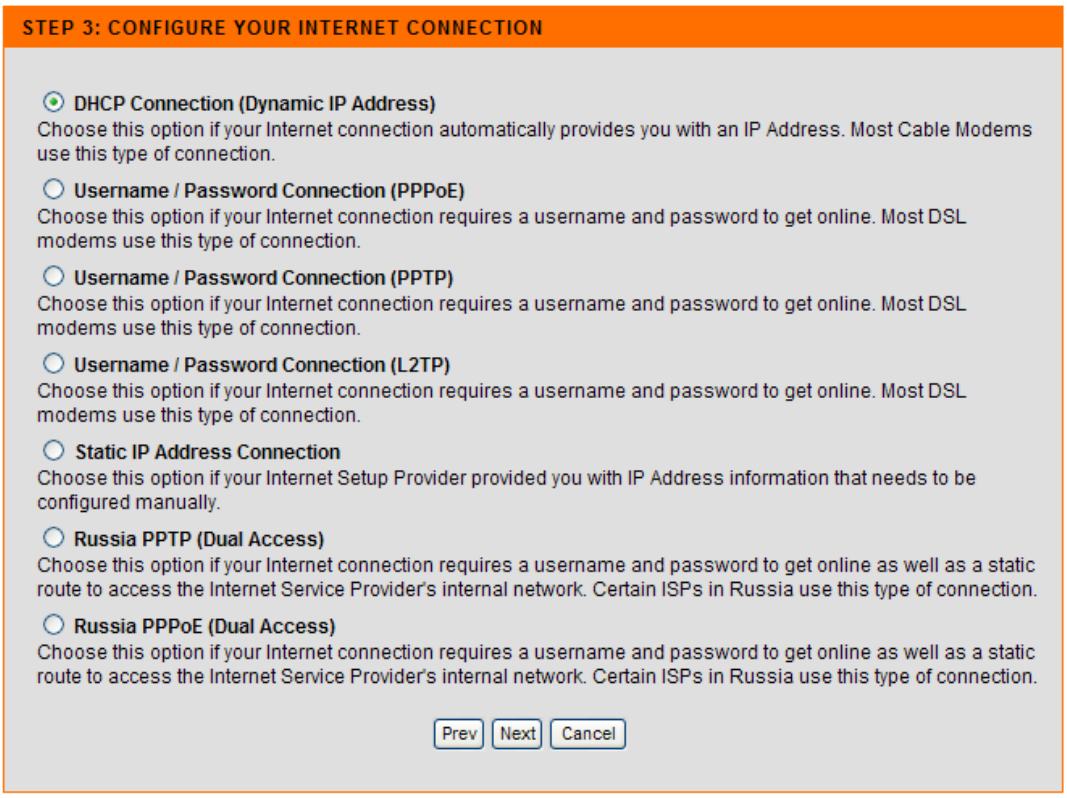


Рис. 45. Четвертый шаг

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

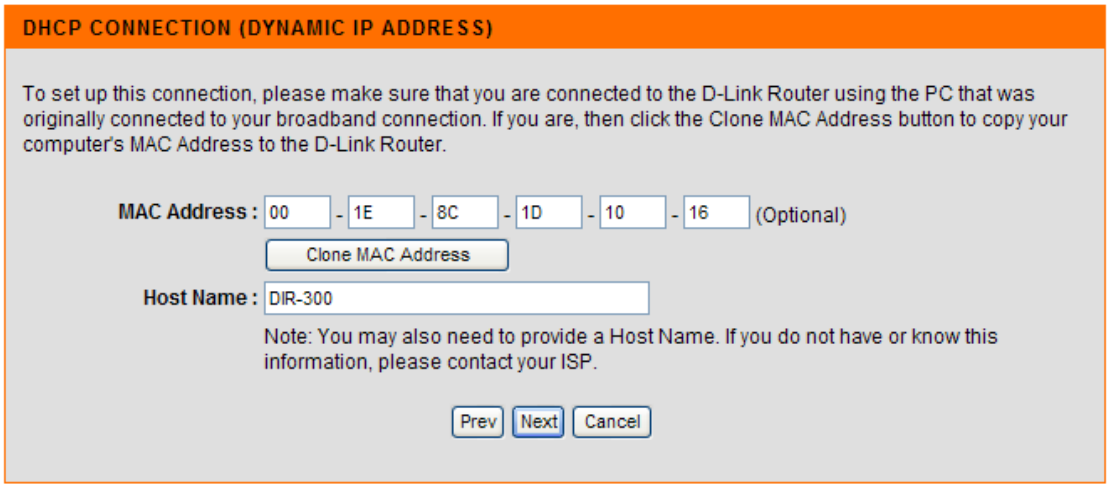


Рис. 46. Проверка MAC адреса

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

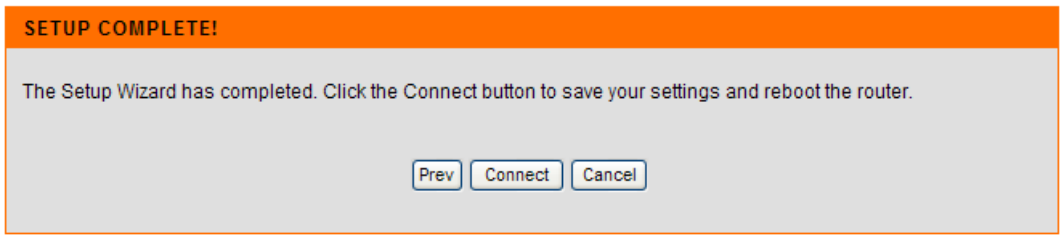


Рис. 47. Завершение настройки

Поле нажатия Connect будет установлено соединения.

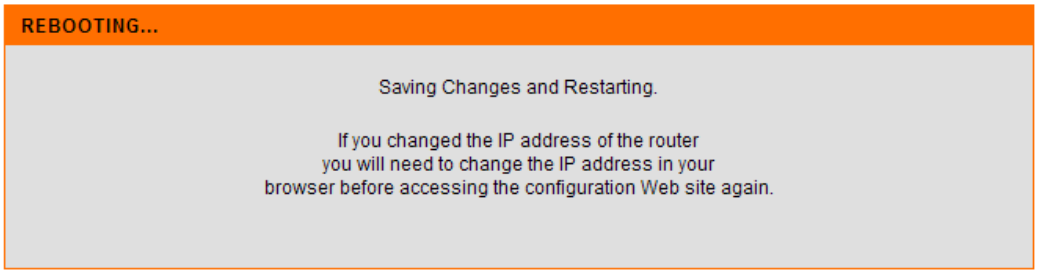


Рис. 48. Сохранение и перезапуск маршрутизатора

Далее необходимо сохранить изменения и перезапустить точку доступа.

Далее необходимо настроить беспроводное соединение. Для этого надо зайти на вкладку Setup – Wireless Setup.

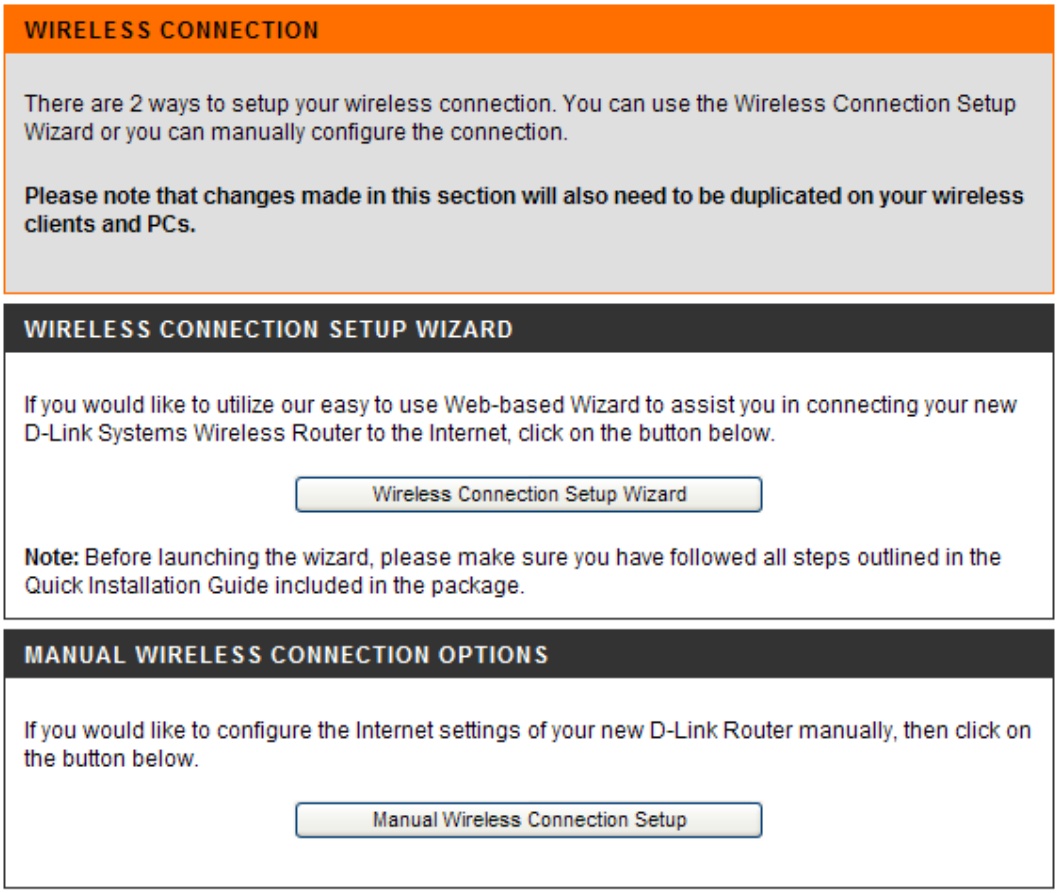


Рис. 49. Настройка беспроводной сети

Здесь также предлагается два типа настройки Internet connection Setup Wizard или Manual Internet Connection Setup. В этот раз выберем Manual Internet Connection Setup .

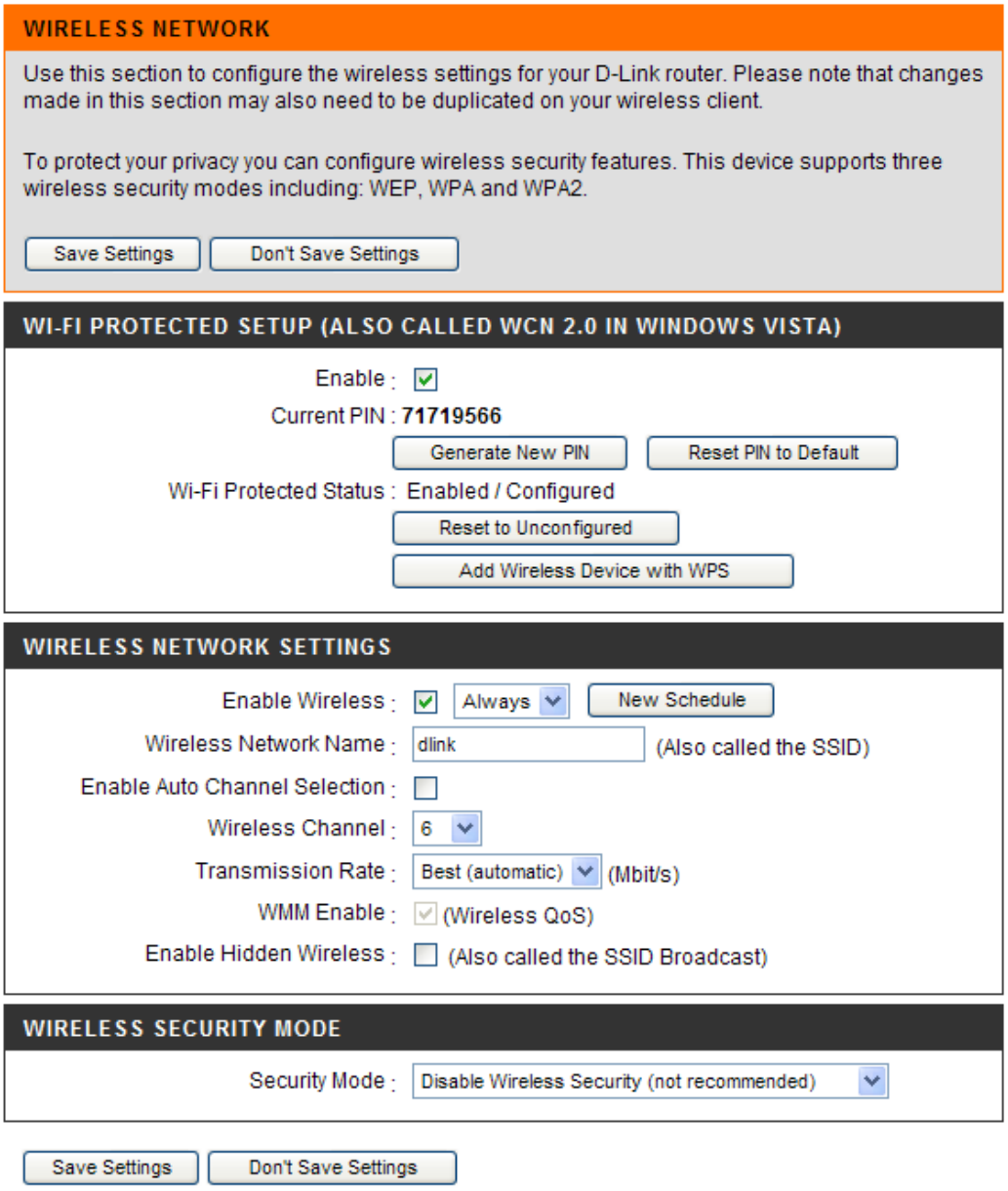


Рис. 50. Вкладка настроек

В строке Wireless Network Name вводим имя создаваемой беспроводной сети. В строке Wireless Channel предлагается выбрать канал, используемый для передачи данных. По умолчания выбран 6 канал, но при необходимости можно выбрать любой из предложенных (если только на таком этом канале не работает другая точка доступа).

В пункте Wireless security mode выбирается метод шифрования данных. По умолчанию эта функция отключена. В ходе проведения лабораторной работы придется меня метод шифрования. Это делается следующим образом.

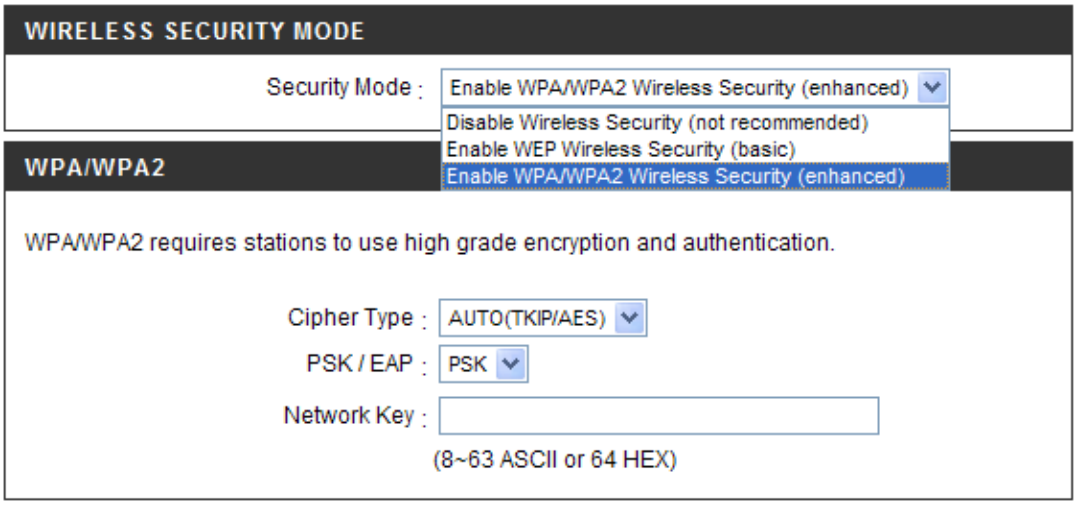


Рис. 51. Настройка режима шифрования

Из выпадающего списка выбирается необходимый метод шифрования. Затем в строке Network Key вводится ключ шифрования. При установки соединения с адаптером вводится этот ключ.

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.

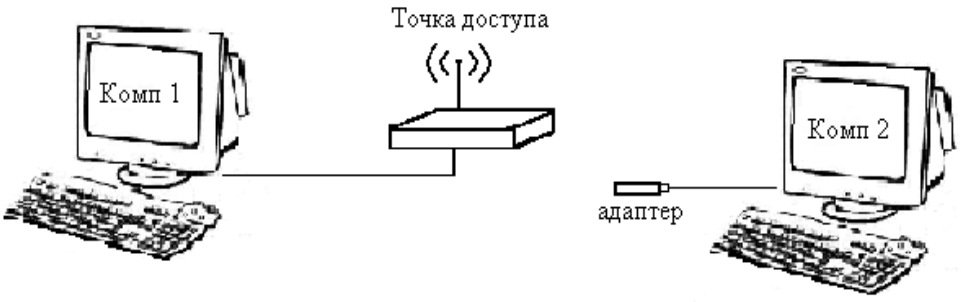


Рис. 52. Тестовый стенд для определения максимальной пропускной способности.

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;

c. Пакеты размера 64 байта;

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

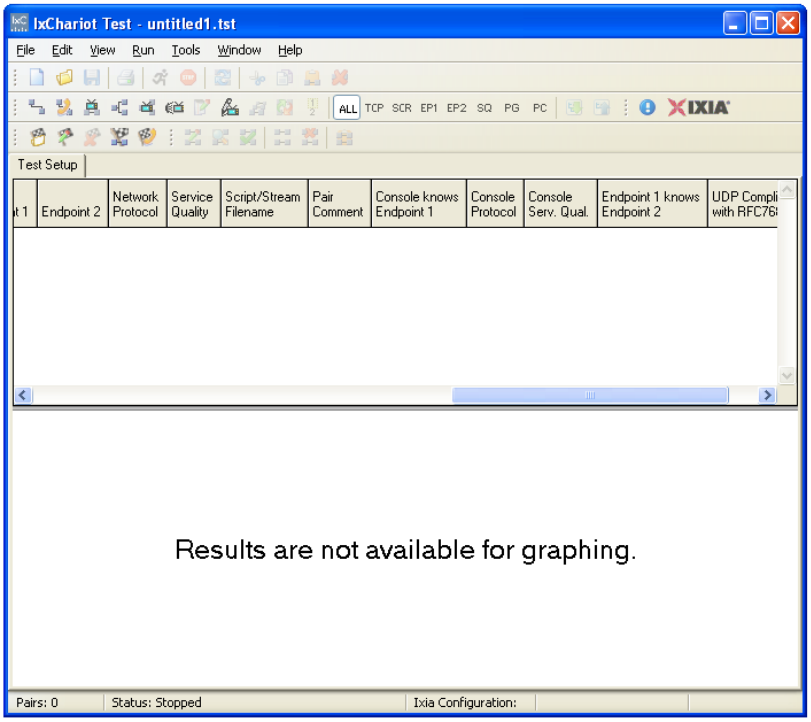


Рис. 53. Интерфейс IXChariot

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.

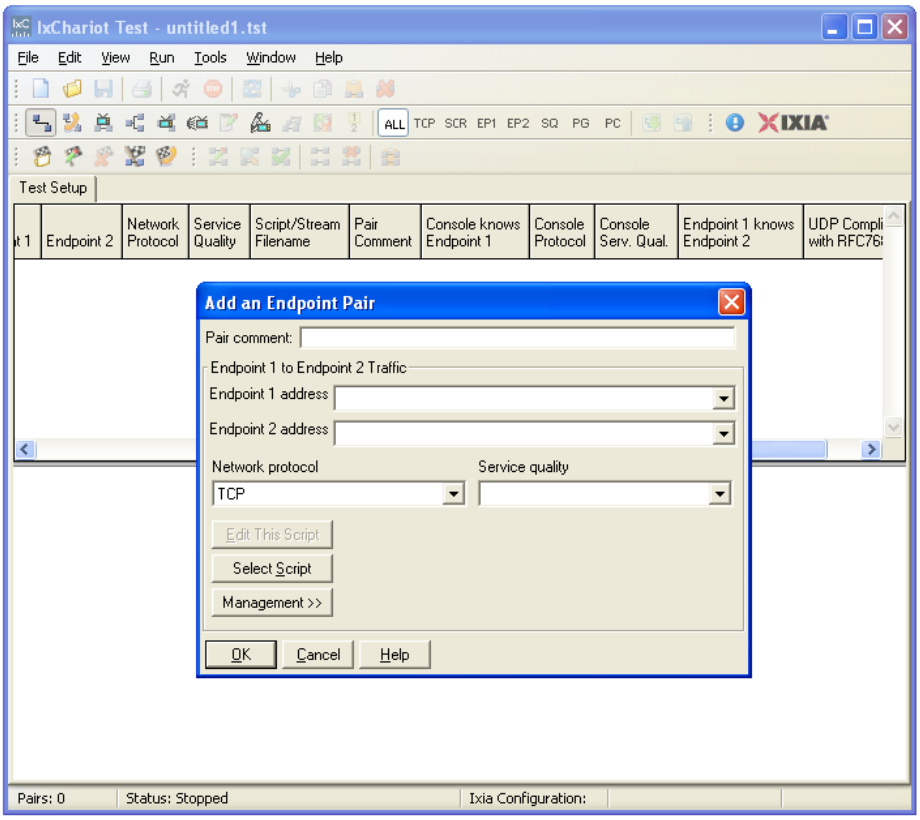


Рис. 54. Окно Add an Endpoint Pair

В строке Endpoint 1 вводим IP адрес копьютера с которого буду проводиться измерения, в строке Endpoint 2 вводится IP адрес Комп 2.

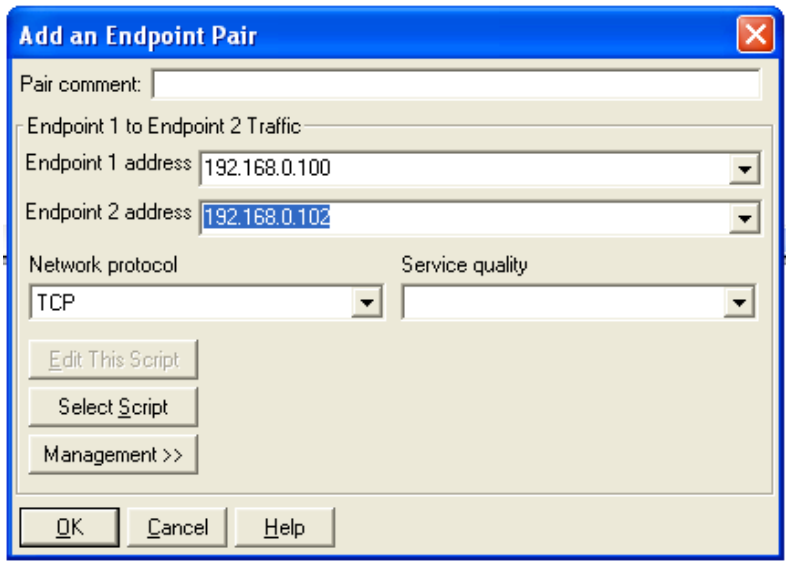


Рис. 55. – Ввод IP адресов тестируемых устройств

Далее выбираем Select Script и выбираем throughput.

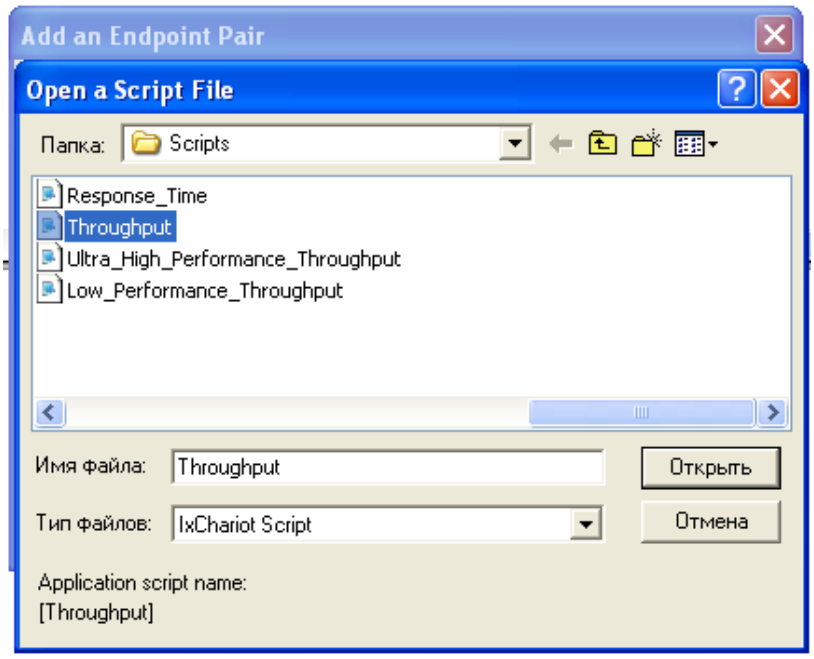


Рис. 56. Выбор скрипта

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

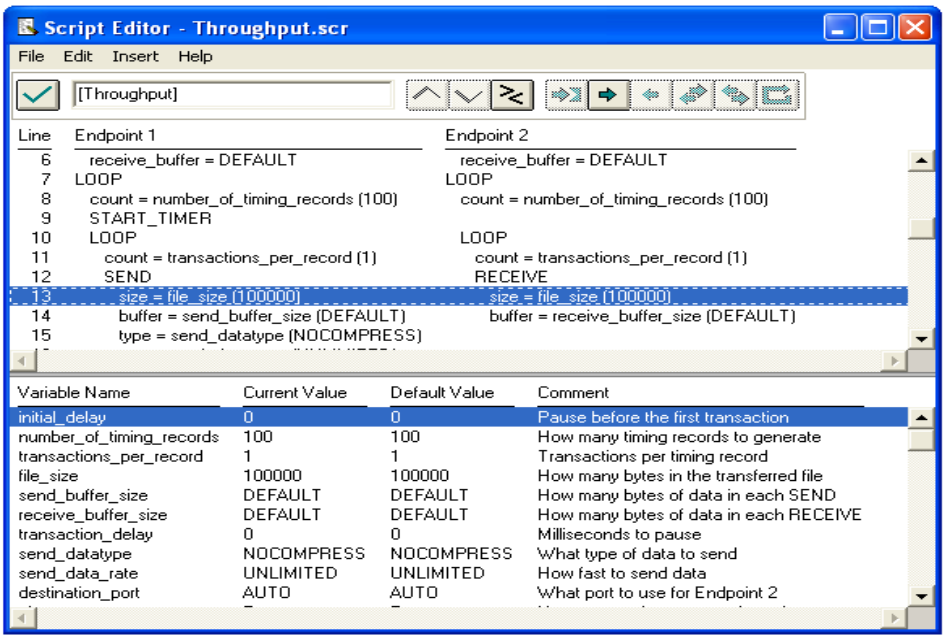


Рис. 57. Настройка скрипта

Результаты измерений.

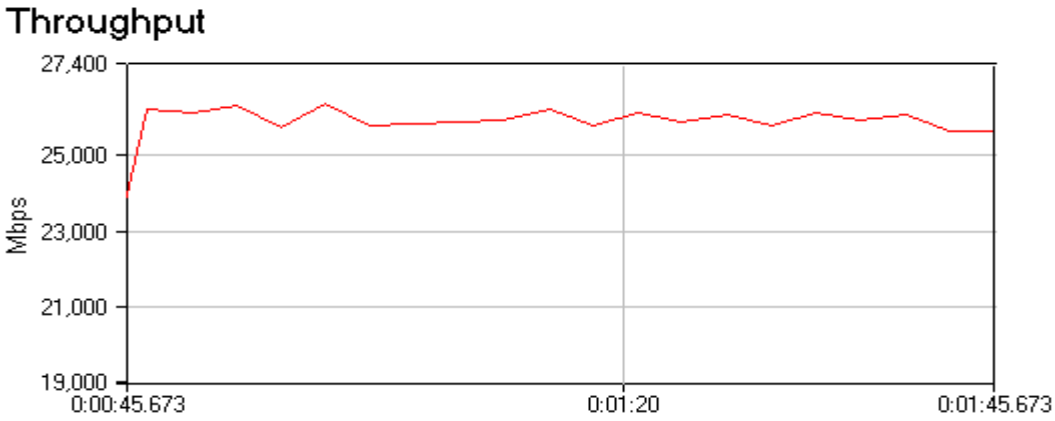


Рис. 58. Размер пакета 1500 байт.

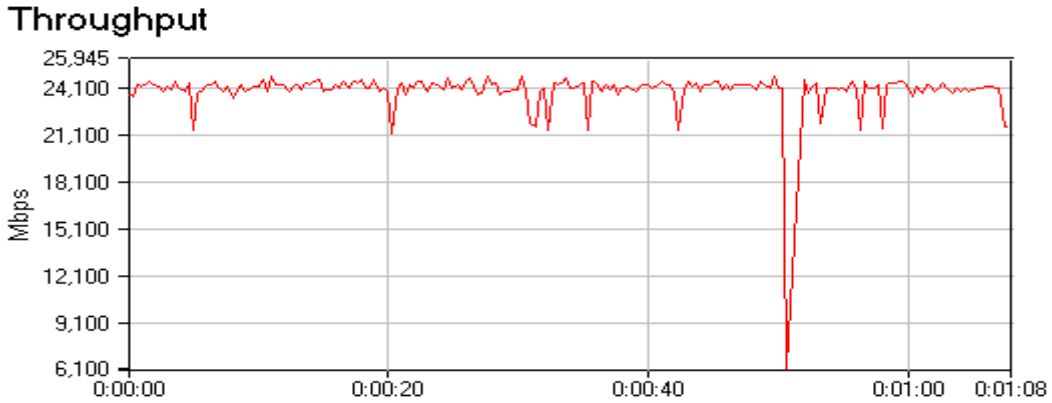


Рис. 59. Размер пакета 512 байт.

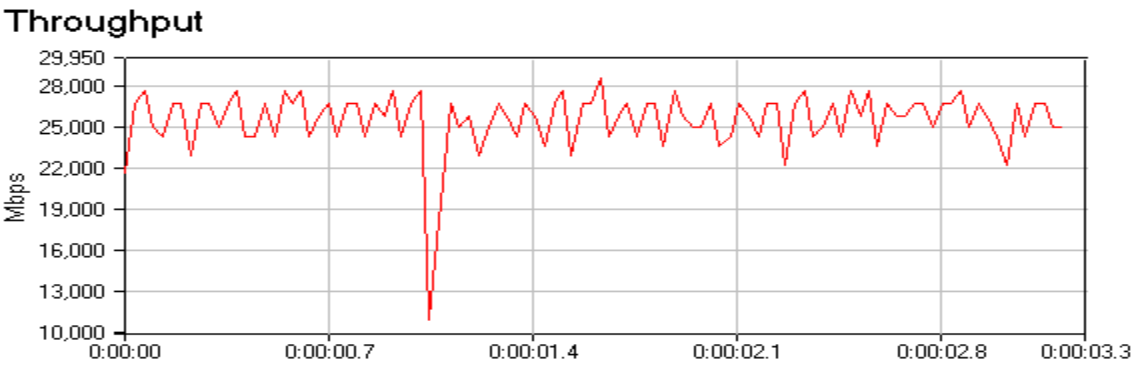


Рис. 60. Размер пакета 64 байта.

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

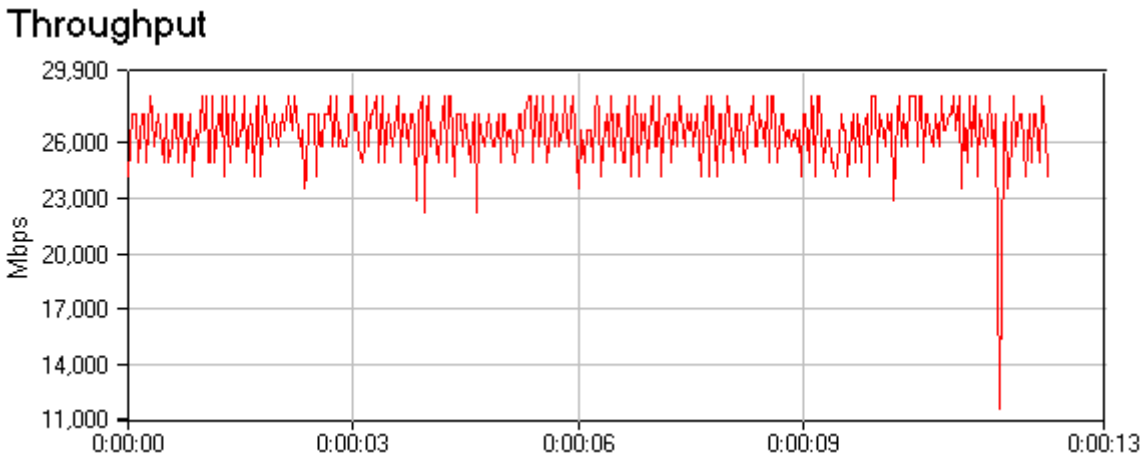


Рис. 62. Результаты измерений в режиме без шифрования

WPA/WPA 2 PSK

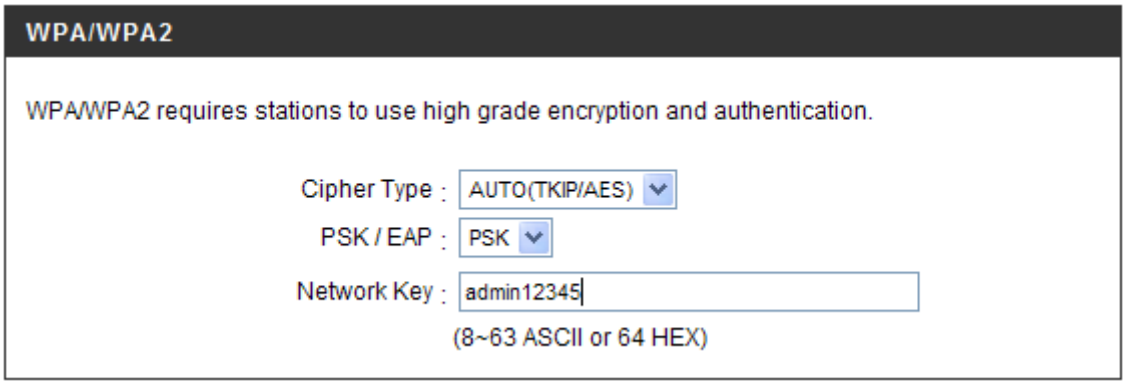


Рис. 63. Настройка маршрутизатора для режима шифрования WPA/WPA 2 PSK

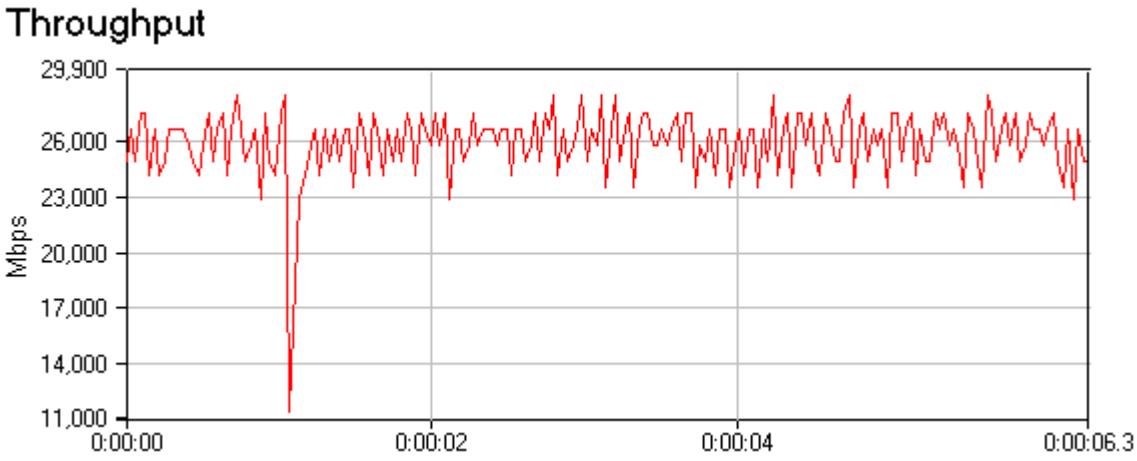


Рис. 64. Результаты измерений режима WPA/WPA 2 PSK

AES

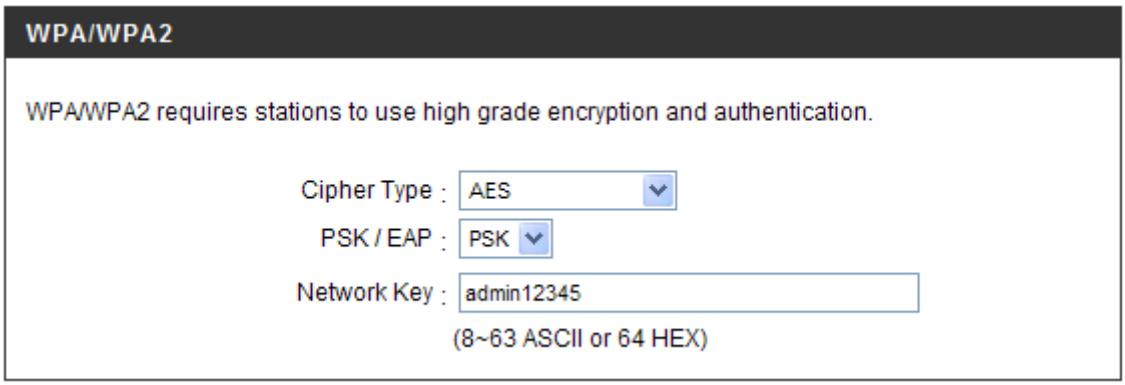


Рис. 65. Настройка маршрутизатора для режима шифрования AES

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.

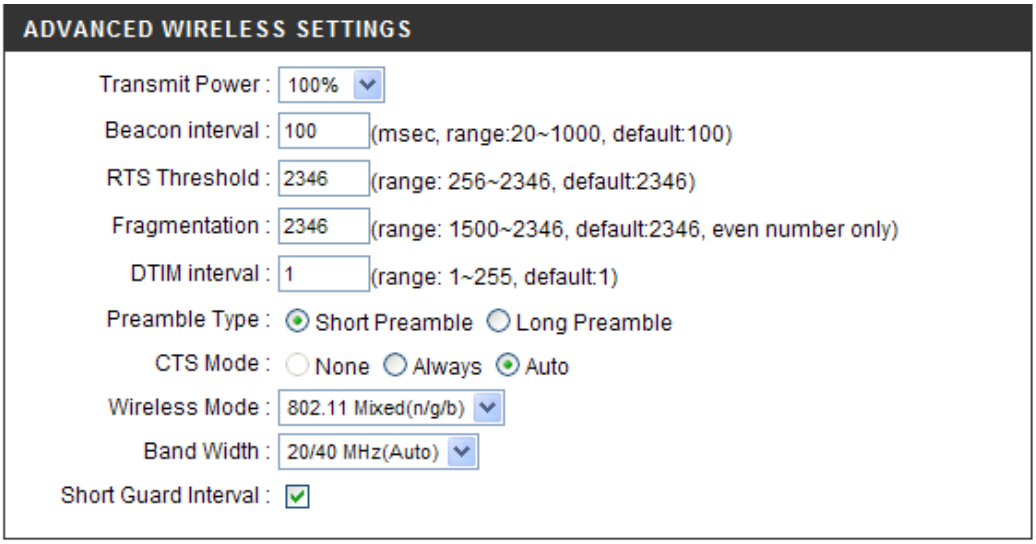


Рис. 67. Настройка длины поля данных передаваемого фрейма

Результаты тестирования

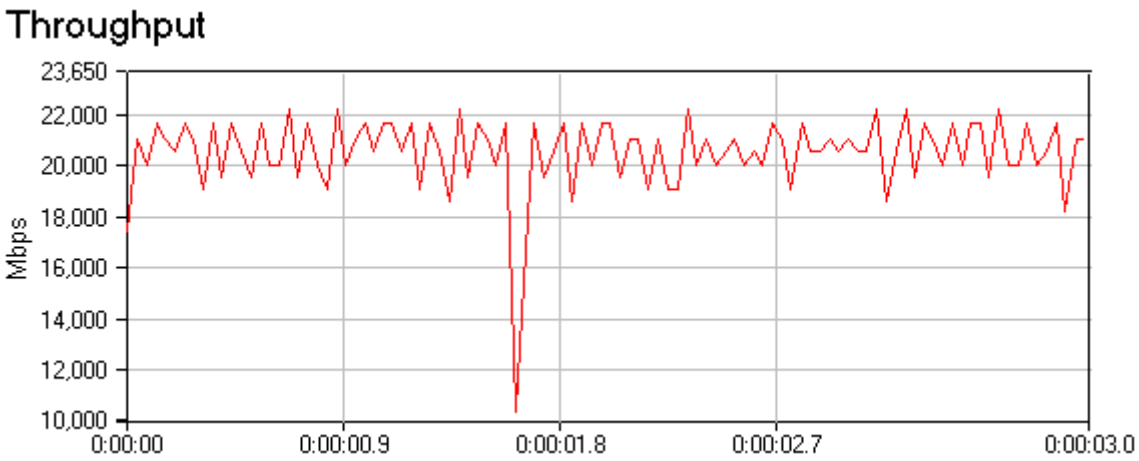


Рис. 68. Длина поля данных 1500 бит

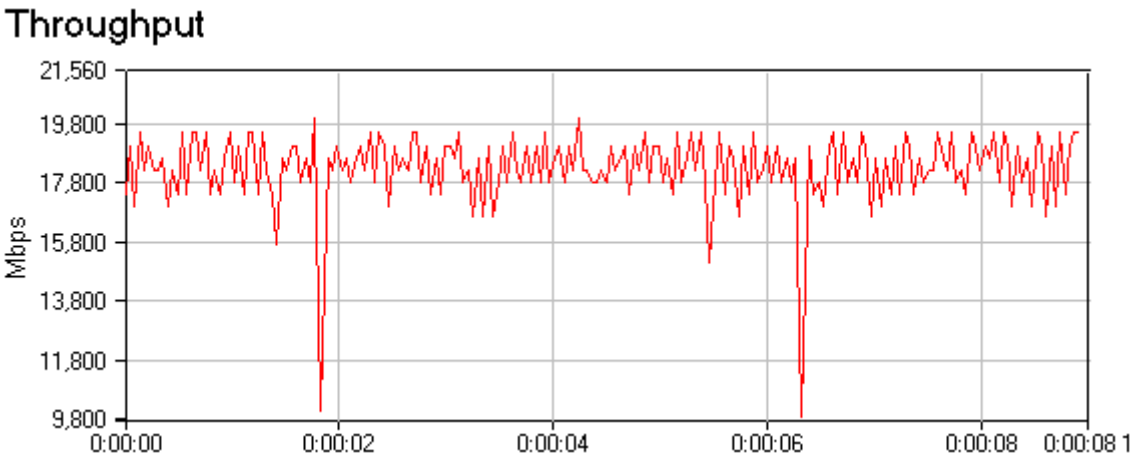


Рис. 69. длина поля данных 2000 бит

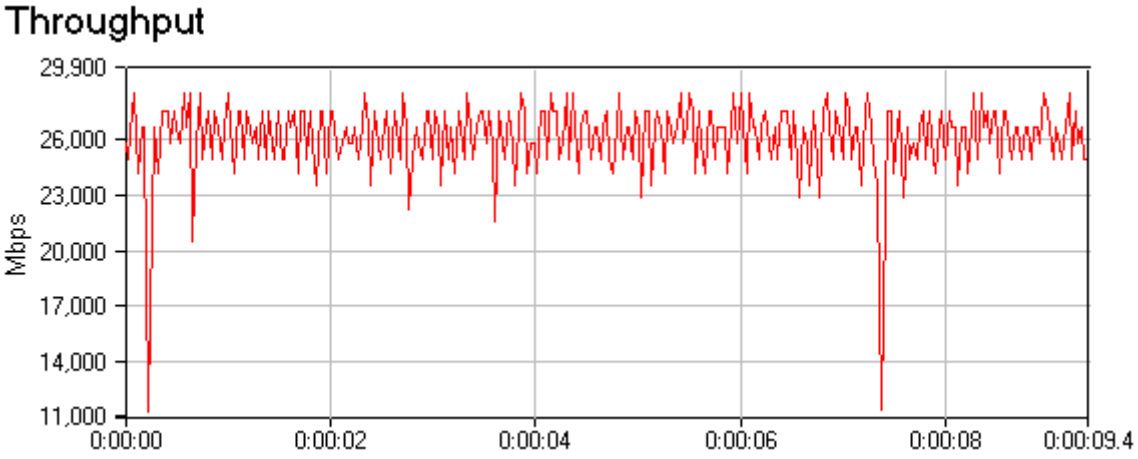


Рис. 70. длина поля данных 2346 бит

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.

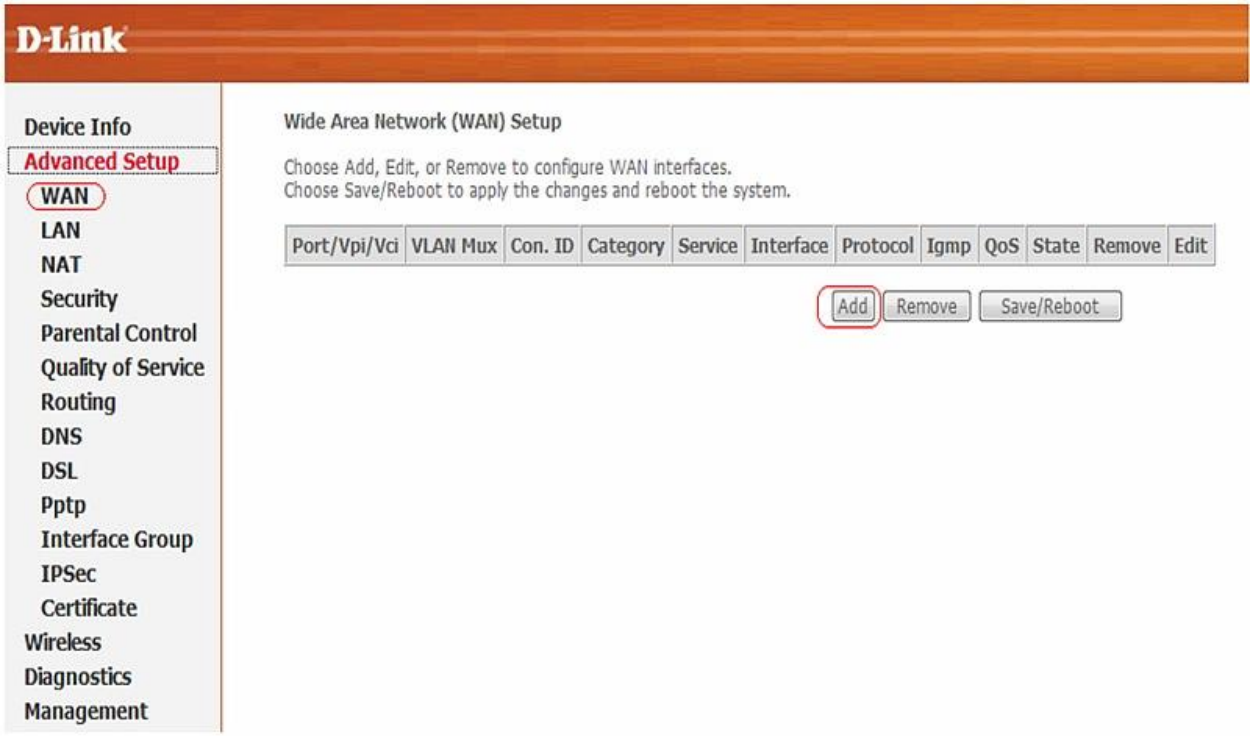


Рис. 71. Создание нового соединения

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

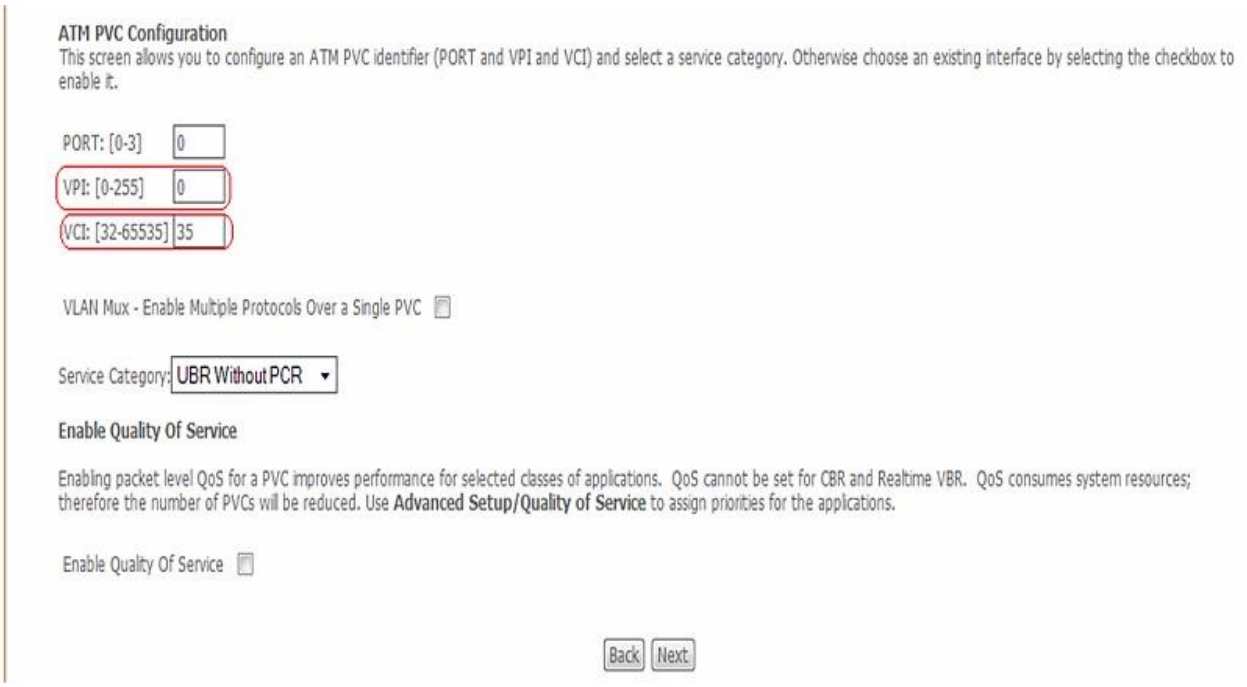


Рис. 72. Значение VPI и VCI

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

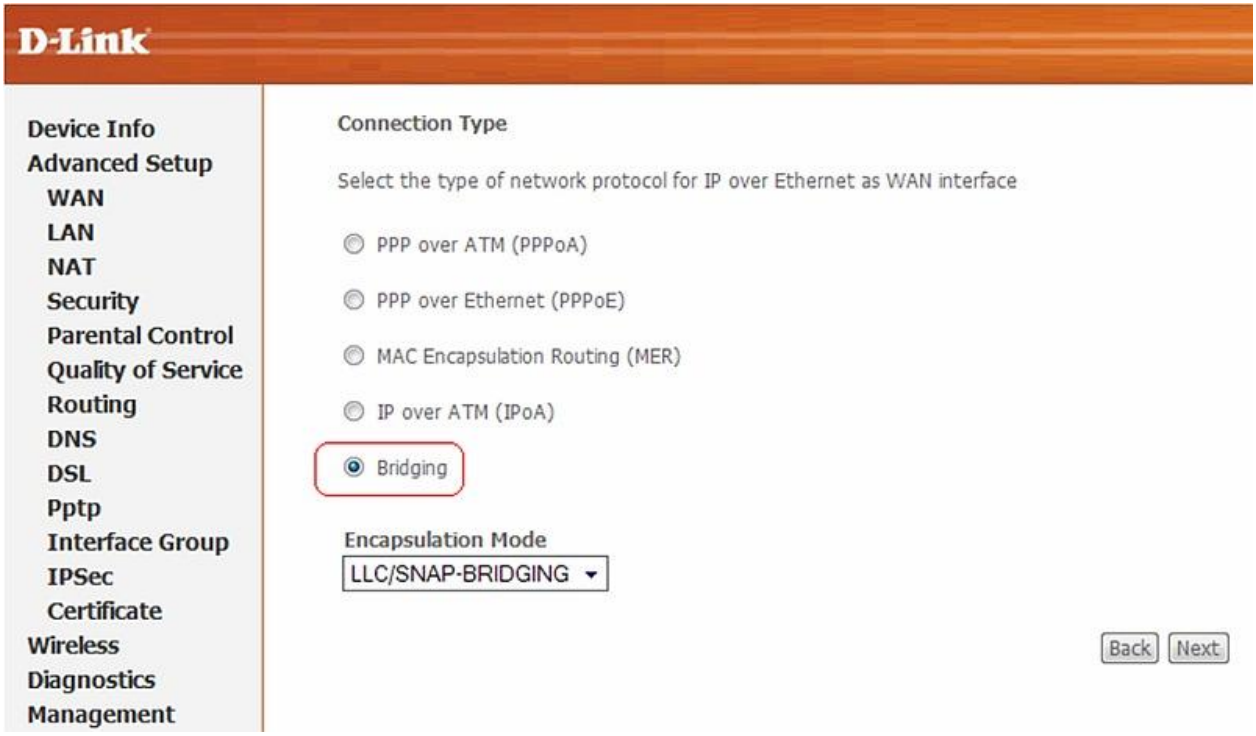


Рис. 73. Установка режим моста.

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

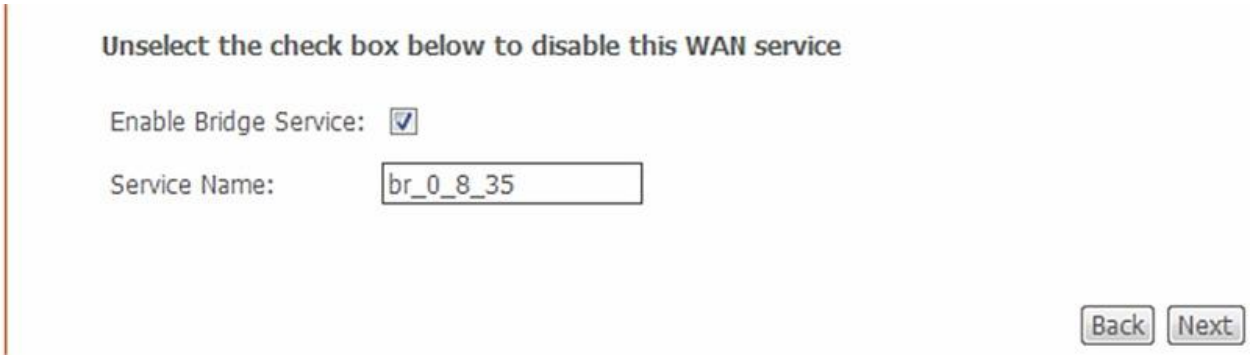


Рис. 74. Создаем имя моста

5. На следующей странице нажмите кнопку «Save».

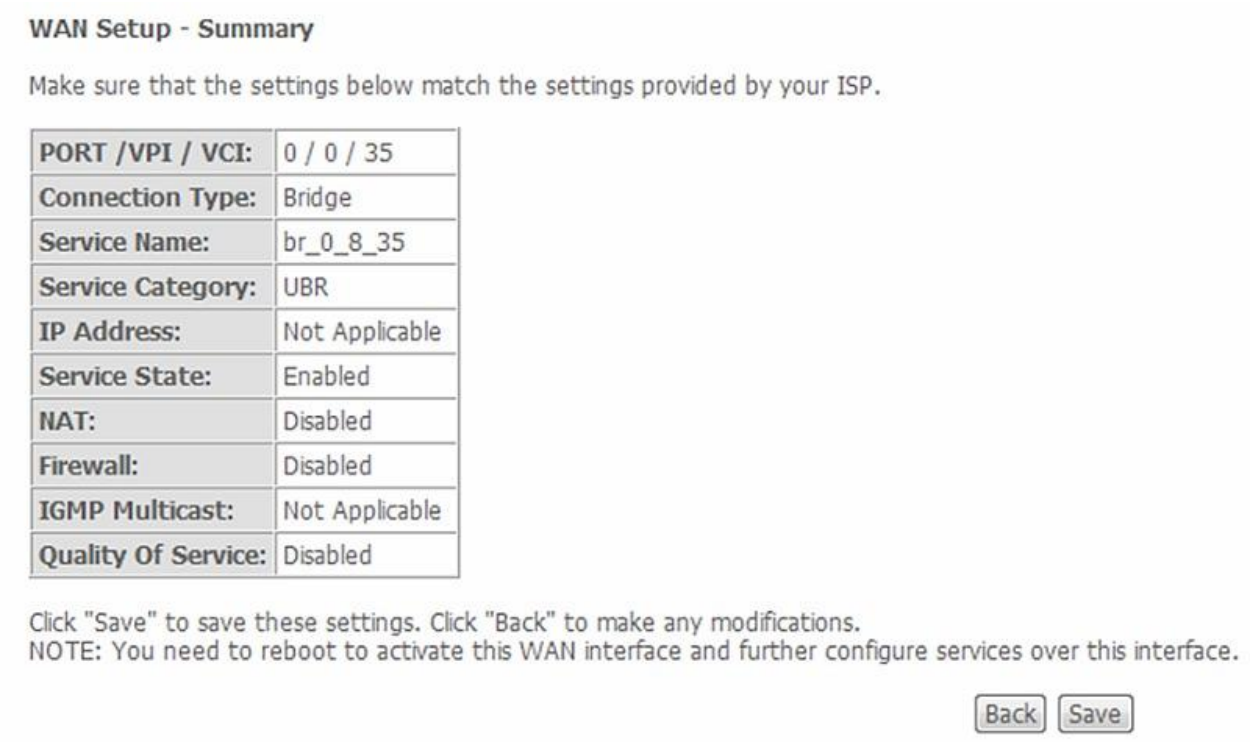


Рис. 75. Проверка настроек

6. 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.

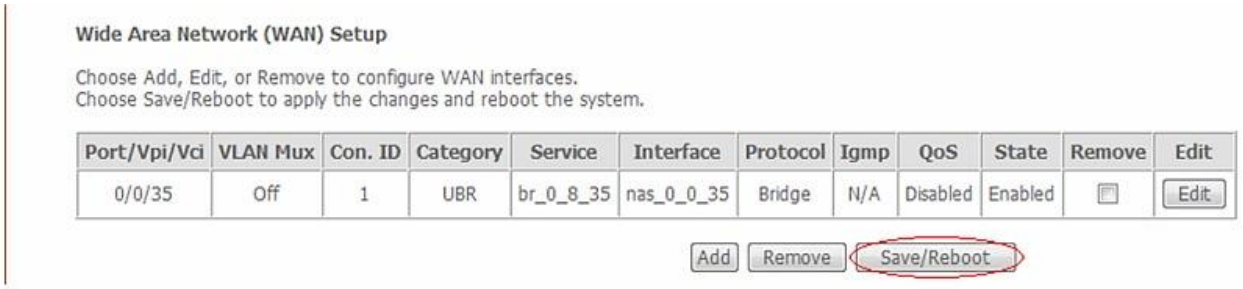


Рис. 76. Перезагрузка устройства

7. 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.

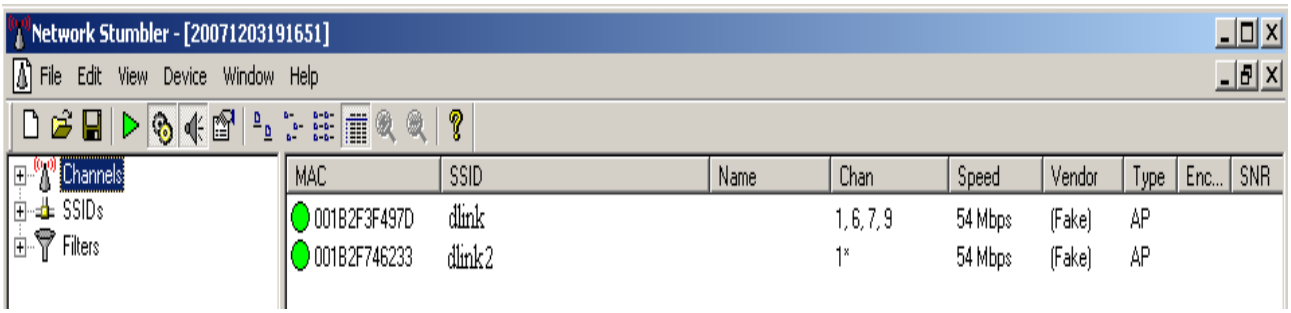


Рис. 78. Влияние точек доступа

Взлом ключей шифрования для стандарта IEEE 802.11

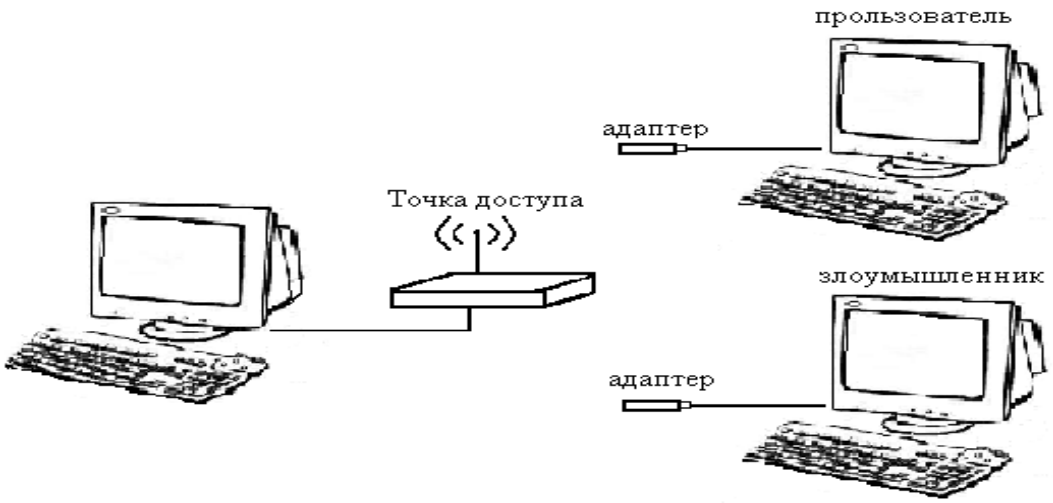


Рис. 79. Тестовый стенд для проверки методов шифрования

Настроим точку доступа на режим шифрования как показано в пункте 7. Затем произведем подключение адаптера к нашему компьютеру.

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

a. Перевести адаптер в режим мониторинга

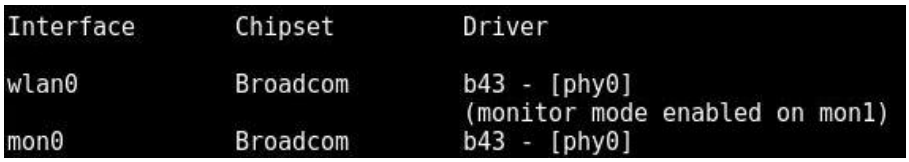


Рис. 80. Перевод адаптера в режим мониторинга

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

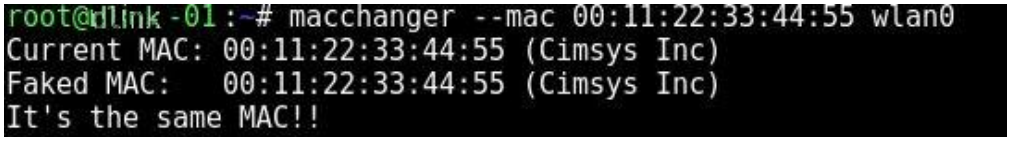


Рис. 81. Замена MAC адреса

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.

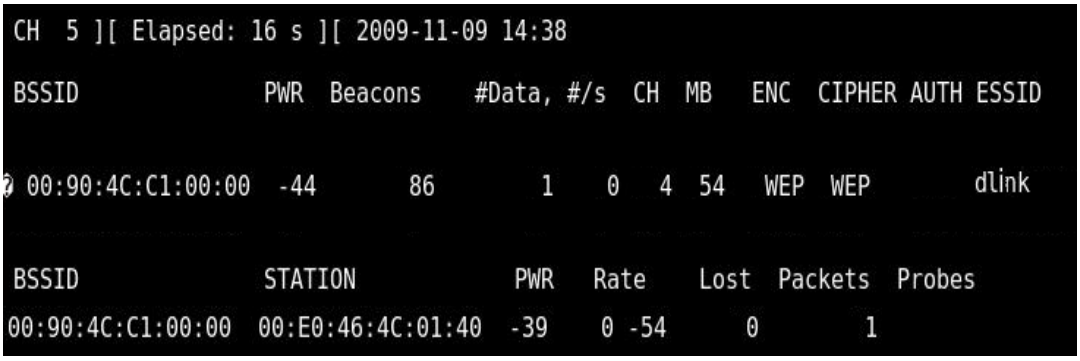


Рис. 82. Поиск сети

d. 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

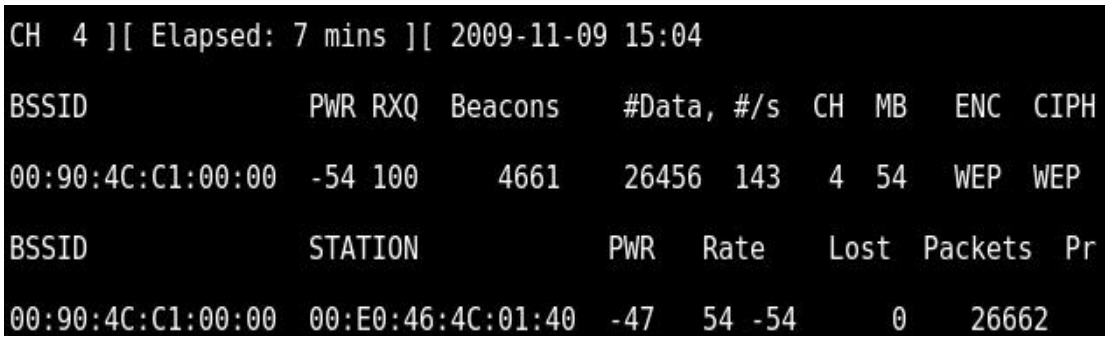


Рис. 83. Сбор пакетов

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.

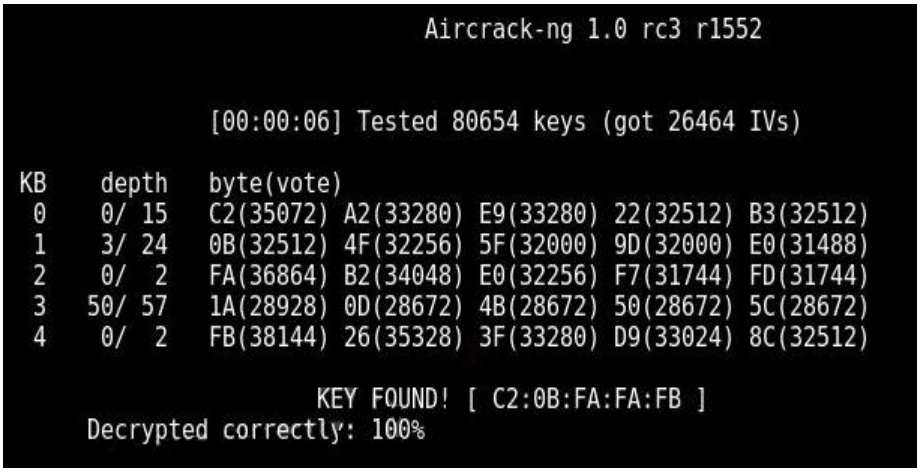


Рис. 84. Нахождение ключа

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

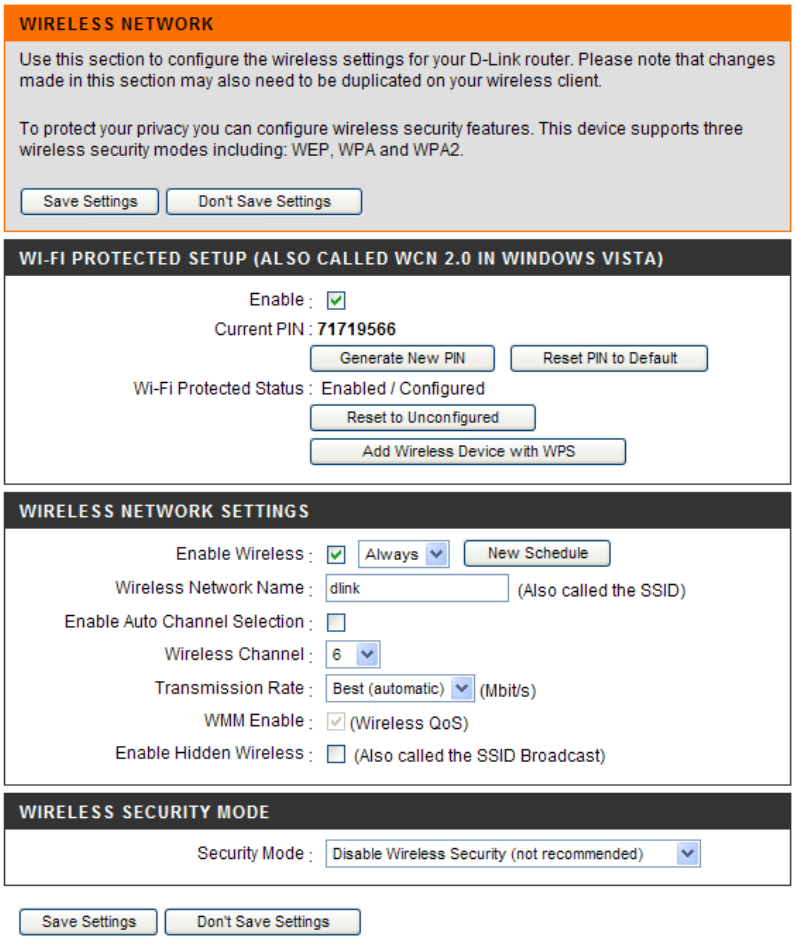


Рис. 85. Настройка точки доступа

b. Перевести адаптер в режим мониторинга

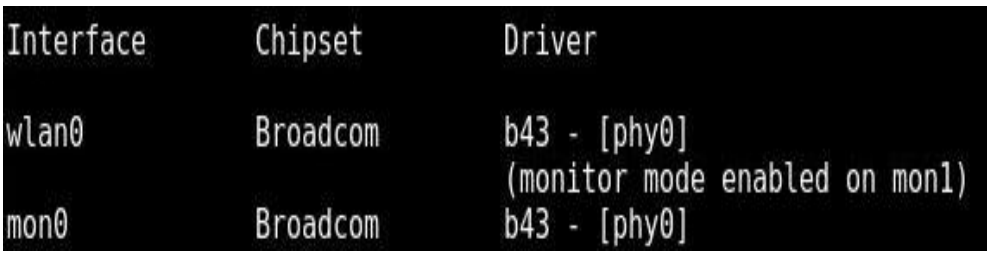


Рис. 86. Перевод адаптера в режим мониторинга

c. Выбрать пользователя для атаки и посылать покаты к точке доступа под MAC – адреса пользователя (это необходимо чтобы точка доступа отключила пользователя и он начал авторизоваться снова)

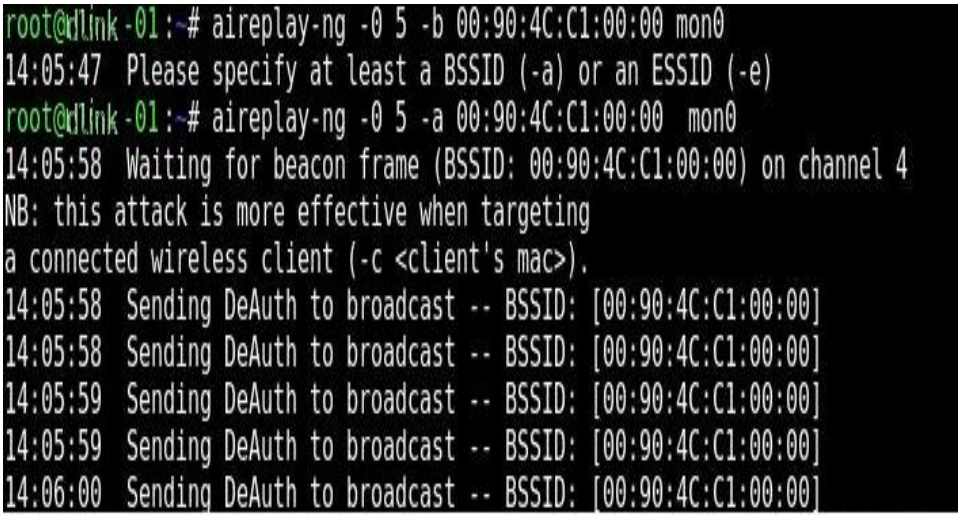


Рис. 87. Деавторизация пользователя

Рис. 88. Отключение пользователя от точки доступа

Пользователь которого мы усиленно отключим от точки доступа будет переключатся заново, то есть проходить авторизацию еще раз. Пакеты авторизации нам и нужны. Поймав эти пакеты, мы начнем перебор. Если пароль легкий то времени займет от 5 минут до 1 дня.

d. Перехватить пакеты авторизации

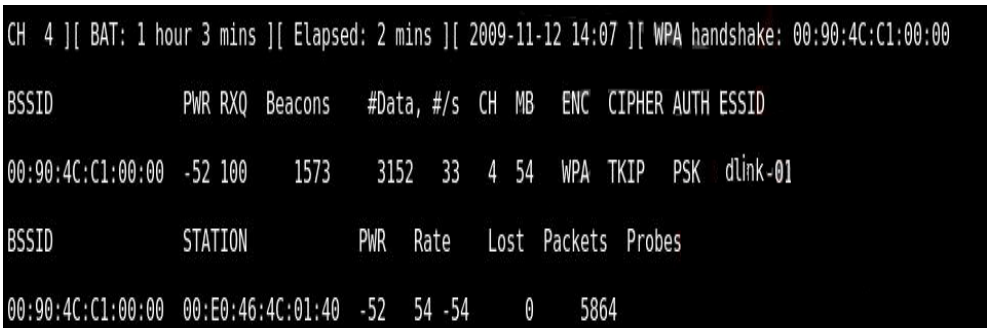


Рис. 89. перехват пакетов

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

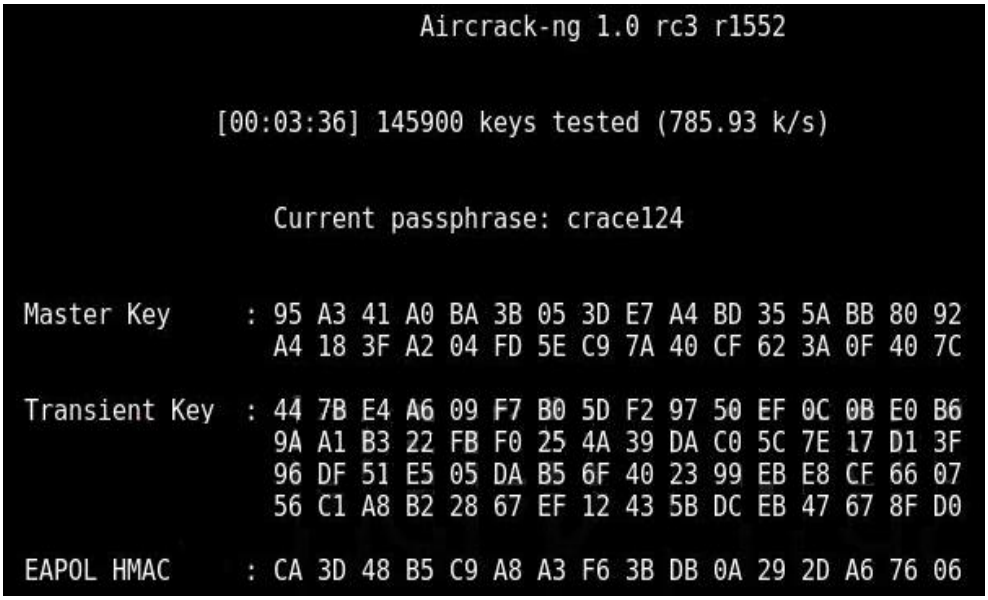


Рис. 90. Нахождение ключа

Для демонстрации устойчивости шифра к перебору, мы взяли простой пароль. Но заметно, что на эксперимент потребовалось 22 часа. Что позволяет сказать о том, что пароль будет сильнее и дольше перебираться, если его содержимое будет составлять Буквы нижних и верхних регистров, чисел и спецзнаков.

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 снизить

вероятность подключения «с улицы». Используйте направленные антенны, не используйте радиоканал по умолчанию.

8. 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)).
9. 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 четырёх заранее заданных ключей — сообщите клиентам о том, в какой день недели какой ключ используется).
10. 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.
11. Если вы используете статические ключи и пароли, позаботьтесь об их частой смене. Делать это лучше одному человеку — администратору.
12. Обязательно используйте сложный пароль для доступа к настройкам точки доступа.
13. 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.

14. По возможности не используйте в беспроводной сети DHCP — вручную распределить статические IP-адреса между легитимными клиентами безопаснее.
15. 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.
16. 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.

4.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.

5.5 Сделать выводы.

6. Взлом ключа шифрования WEP:

6.1. Ввести в настройках точки доступа ключ шифрования.

6.2. Открыть программу aircrack-ng.

6.3. 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 и администрирование средств обеспечения информационной безопасности Web-сервера Microsoft IIS Server

1. Цель работы

Изучение, установка, настройка и администрирование Web-сервера IIS 7.0 на Windows Server 2008 R2, создание на основе IIS 7.0 хостинга, специально оптимизированного для размещения сайтов в Интернете.

2. Краткие теоретические сведения

Веб-сервером (от англ. Web-Server) называют как программное обеспечение, выполняющее функции веб-сервера, так и компьютер, на котором это программное обеспечение работает. Таким образом, веб-сервер – это компьютер, специально оптимизированный для размещения сайтов в Интернете (со специальным программным обеспечением), и сервер, принимающий HTTP - запросы от клиентов, обычно веб-браузеров, и выдающий им HTTP-ответы, обычно вместе с HTML-страницей, изображением, файлом, медиапотоком или другими данными. Веб-серверы — основа Всемирной паутины. Клиенты получают доступ к веб-серверу по URL адресу нужной им веб-страницы или другого ресурса.

У веб-сервера одна задача: получить по сети запрос и послать на него ответ. Формально, запрос – это указание веб-серверу, какой ресурс вы бы хотели получить. Под ресурсом подразумевается документ HTML. Итак, набирая в адресной строке браузера какой-либо адрес на самом деле формируете запрос веб-серверу. Веб-сервер должен принять запрос. Понять его и обработать. Обработка означает передачу запрошенного ресурса или объяснение, почему ресурс не может быть предоставлен. Если вы не ошиблись в запросе и таковой ресурс имеются вналичии и вы его можете получить, тогда веб-сервер выбирает нужный документ HTML и передает его по сети вам. Причем, передает он его

без каких-либо модификаций.

Internet Information Services 7.0

Internet Information Services 7.0 (IIS 7.0) – это последняя версия веб-сервера компании Microsoft. IIS был включен в состав семейства операционных систем Windows Server начиная с операционной системы Windows 2000 Server в качестве компонента Windows Component, а также для Windows NT в качестве дополнения. IIS 7.0 входит в состав операционных систем Windows Vista и Windows Server 2008, которые были выпущены в первой четверти 2008. IIS 7.0 претерпел множество изменений и новый дизайн был написан с нуля. Это было сделано для того, чтобы сделать его самой гибкой и безопасной платформой для размещения веб-приложений.

IIS 7.0 был спроектирован, чтобы быть самой безопасной и гибкой платформой для веб-приложений от компании Microsoft. Microsoft полностью переделала дизайн IIS, и во время этого процесса команда разработчиков IIS сфокусировалась на 5 основных областях:

- Безопасность
- Расширяемость
- Конфигурация и установка
- Администрирование и диагностика
- Производительность

Компания Microsoft сфокусировалась на модульности при создании IIS 7.0, что означает, что для установки необходимы лишь бинарные файлы, что минимизирует пространство для атак на веб-сервер. Операционная система Windows Server 2008 включает в себя все возможности IIS, необходимые для поддержки и размещения веб содержимого в промышленных средах.

Роль веб-сервера (IIS)

Основные характеристики служб IIS 7.0:

- гибкая модель расширения для эффективной настройки;
- эффективные средства диагностики, а также поиска и устранения неполадок;
- делегированное администрирование;
- улучшенная защита и ограничение уязвимости для атак путем настройки;
- реальное развертывание приложений с помощью команды xcopy;
- интегрированные средства управления приложениями и работоспособностью для служб Windows Communication Foundation (WCF);
- усовершенствованные средства администрирования.

Благодаря этим преимуществам службы IIS 7.0 обеспечивают единую согласованную модель разработки и администрирования интернет решений.

Гибкая модель расширения для эффективной настройки

Службы IIS 7.0 поддерживают новые более эффективные способы расширения функциональности в соответствии с конкретными требованиями. Модель расширения IIS 7.0 включает новые прикладные программные интерфейсы основных компонентов сервера, позволяющие разрабатывать функциональные модули как в машинном коде (C/C++), так и в управляемом коде (языки, использующие .NET Framework, такие как C# и Visual Basic 2005).

IIS 7.0 также поддерживают наборы расширений настройки, сценариев, регистрации событий и средств администрирования, предоставляя разработчикам программного обеспечения полную серверную платформу для

создания расширений веб-сервера.

Эффективные средства диагностики, а также поиска и устранения неполадок

Службы IIS 7.0 облегчают поиск и устранение неполадок в работе веб-узлов и приложений. Они обеспечивают ясное представление внутренних диагностических сведений о работе IIS, а также собирает и позволяет изучать события диагностики, помогая устранять неполадки в работе проблемных серверов.

Делегированное администрирование

Службы IIS 7.0 позволяют при размещении или администрировании веб-узлов или служб WCF делегировать администрирование разработчикам или владельцам содержимого, что сокращает стоимость владения системой и снижает нагрузку на администратора. Для использования этих функций делегирования предоставляются новые средства администрирования.

Улучшенная защита и ограничение уязвимости для атак путем настройки

Компоненты, устанавливаемые и выполняемые на веб-сервере, можно выбирать. Службы IIS 7.0 включают более 40 отдельных функциональных модулей. Каждый из них можно установить на сервере независимо от других для уменьшения числа возможных направлений атаки на сервер и сокращения нагрузки на администратора.

Развертывание приложений с помощью команды xcopy

Службы IIS 7.0 позволяют хранить параметры конфигурации IIS в файлах web.config, что значительно облегчает использование команды xcopy для копирования приложений между интерфейсными веб-серверами, позволяя обходиться без дорогостоящих и подверженных ошибкам процедур репликации

и избегать проблем, возникающих при синхронизации вручную.

Управление приложениями и работоспособностью для служб WCF

Для повышения эффективности разработки и размещения служб WCF с использованием различных протоколов в Windows Server 2008 включена служба активации Windows (WAS), поддерживающая модульную активацию произвольных прослушивателей протоколов. Служба WAS предоставляет доступ к различным приложениям, активируемым сообщениями, с интеллектуальным управлением ресурсами, активацией процессов по запросу, наблюдением за работоспособностью, а также автоматическим обнаружением сбоев и перезапуском процессов. Служба WAS основана на модели обработки запросов IIS 6.0.

Усовершенствованные средства администрирования

В IIS 7.0 реализован новый пользовательский интерфейс, ориентированный на выполнение задач, и новое средство командной строки для администрирования веб-серверов, веб-узлов и веб-приложений. Дополнительные сведения см. ниже, в подразделе "Средства администрирования" раздела.

Архитектура

В основе использовался модульный дизайн. Модульный дизайн обеспечивает больше гибкости и безопасности для IIS 7.0, по сравнению с предыдущими версиями IIS.

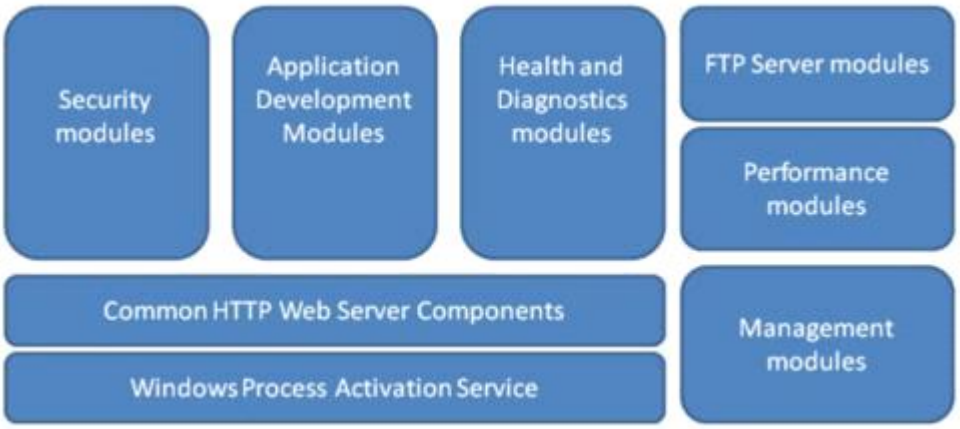


Рис. 1. Обзор основных модулей и компонентов IIS 7.0

Основное преимущество нового модульного дизайна заключается в том, что он помогает снизить опорную поверхность, что обеспечивает большую безопасность платформы для веб-сервера, т.к. в этом случае минимизируется поверхность для атак.

IIS 7.0 снабжен новым собственным корневым API, который заменил фильтр ISAPI filter, используемый в предыдущих версиях IIS. Благодаря новому API появилась возможность для расширения IIS с помощью новых модулей, или даже замены любых встроенных модулей собственными модулями.

Администрирование

Существует несколько способов для администрирования IIS 7.0.

- Графический интерфейс GUI с помощью менеджера IIS Manager
- Инструмент командной строки APPCMD
- Удаленное администрирование (Remote administration) с помощью IIS Manager
- Написание сценариев с помощью Windows PowerShell
- Интерфейс Microsoft.Web.Administration API interface

Графический интерфейс для управления GUI Management был также изменен,

новый менеджер IIS Manager теперь более ориентирован на выполнение задач.

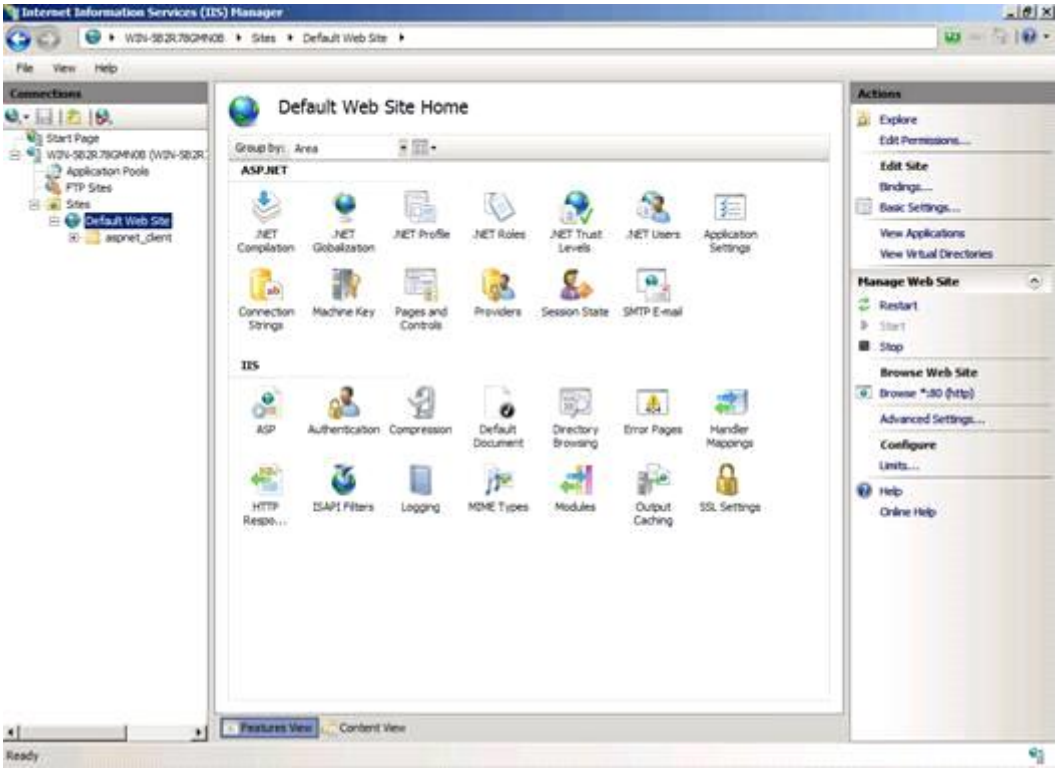


Рис. 2. Окно менеджера IIS Manager

Менеджер IIS Manager можно использовать для настройки параметров IIS и ASP.NET, конфигурационные параметры записываются в конфигурационные файлы в формате xml. Информация о состоянии и диагностика теперь доступна напрямую из менеджера IIS Manager, и теперь является частью IIS 7.0.

APPCMD – это новый инструмент общего назначения для IIS 7.0, работающий из командной строки, который используется для администрирования и настройки IIS. APPCMD – это новая улучшенная версия старого модуля adsutil.vbs.

Удаленное администрирование (Remote Administration) было также улучшено, и теперь появилась возможность использование менеджера IIS Manager, при безопасном взаимодействии по https с веб-сервером.

Существует также возможность написания сценариев для управления IIS.

Это делается с помощью Windows PowerShell, который является новым языком для написания сценариев от компании Microsoft. Это простой и эффективный способ для администрирования IIS на вашем веб-сервере, которое особенно полезно, если вы управляете несколькими веб-серверами или большими веб фермами. Windows PowerShell может напрямую использоваться для интерфейса WMI IIS или использоваться для чтения или записи в конфигурационные файлы IIS 7.0 XML.

IIS 7.0 обладает обратной совместимостью с метабазой IIS 6.0 metabase и ADSI, а также интерфейсом для написания сценариев WMI scripting interface, известный с версии IIS 6.0, что означает, что все ваши сценарии, написанные для версии IIS 6.0 будут работать и для версии IIS 7.0.

Microsoft.Web.Administration API – это интерфейс для разработчиков, которые хотят писать свои собственные программы или сценарии для управления IIS 7.0.

В IIS 7.0 существует возможность передачи управления над IIS и веб-сайтами. Вы можете передать полный административный доступ владельцам веб-сайта. Владельцы веб-сайта могут контролировать и управлять всеми настройками веб-сайта с помощью менеджера IIS Manager, при этом безопасность сервера не будет страдать. Все настройки, которые меняют владельцы сайтов, записываются в файл в формате xml под названием web.config на их веб сайте.

Конфигурация

Конфигурация значительно упростилась, и теперь она основана на распределенных XML файлах, которые содержат конфигурационные параметры для всего IIS и ASP.NET.

Конфигурационные параметры могут быть настроены глобально для всего веб-сервера или для определенных веб-сайтов, с помощью XML файлов, или с помощью графического интерфейса управления (GUI Management interface). Графический интерфейс лишь записывает конфигурационные параметры в то те же самые XML файлы. Основные конфигурационные файлы xml в IIS 7.0 это:

- Applicationhost.config
- Global web.config
- Machine.config
- Site web.config
- App web.config

Благодаря использованию конфигурационных файлов в формате xml, установка и масштабирование в больших средах значительно оптимизировалась. Теперь достаточно просто скопировать конфигурацию IIS на новый сервер и просто запустить его.

Выполнение репликации конфигурации веб-сервера также значительно упростилось для IIS 7.0 по сравнению с IIS 6.0, благодаря использованию конфигурационных файлов в формате xml. Благодаря этому очень просто скопировать и установить конфигурацию в крупных средах.

Общая конфигурация (Shared Configuration) – это новая возможность в IIS 7.0, которая была разработана для веб ферм (web farm). С помощью общей конфигурации (Shared Configuration) теперь появилась возможность для нескольких веб-серверов использовать один конфигурационный файл (applicationhost.config). Главный файл размещается по общему пути UNC. Возможность использования общей конфигурации (Shared Configuration) – это великолепная альтернатива перспективе копирования настроек IIS.

Файл в формате xml под названием Applicationhost.config является

основным конфигурационным файлом IIS 7.0, этот конфигурационный файл содержит всю информацию о сайтах, виртуальных директориях, приложениях, пулах приложений и глобальных настройках для веб-сервера.

Репликация содержимого может быть легко выполнена с помощью команды x-copy или robocopy, точно также как и особые настройки веб-сайта, которые хранятся в файле web.config в формате xml внутри сайта.

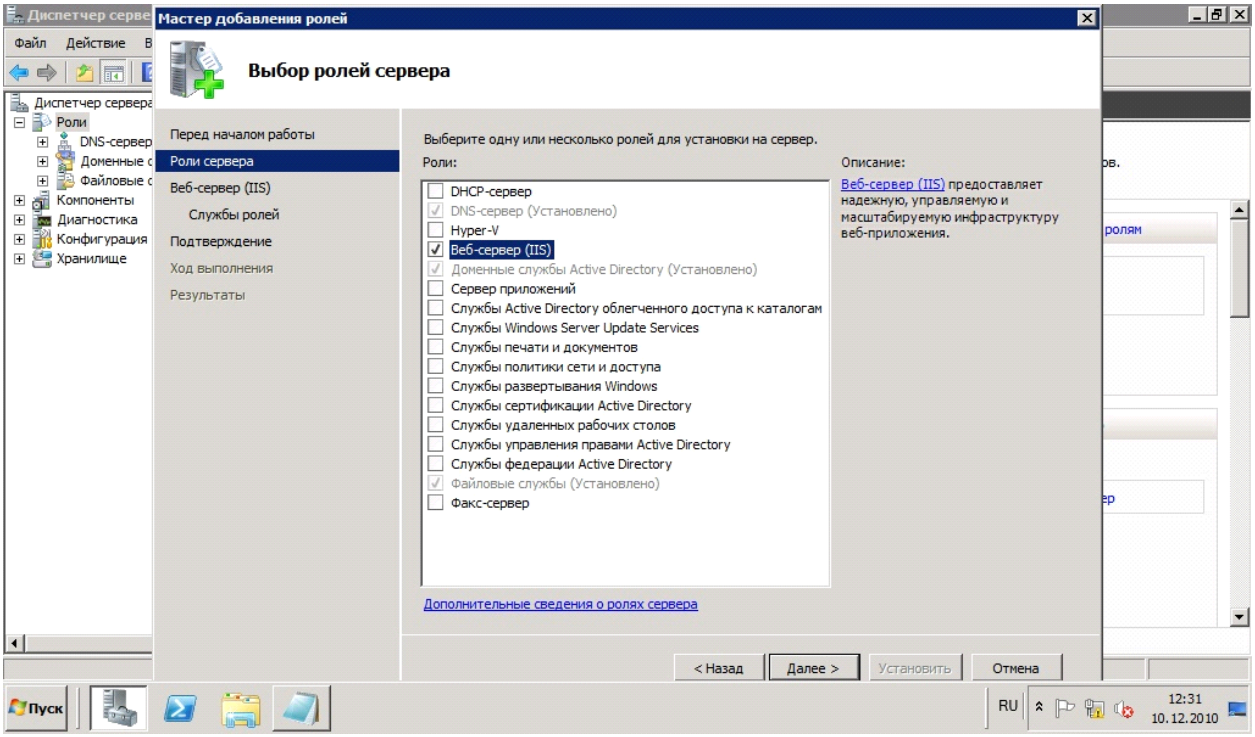
Благодаря изменению дизайна IIS, компания Microsoft сделала IIS 7.0 лучшим веб-сервером для всех, начиная со специалистов по информационным технологиям IT и разработчиков до Web Hosters. IIS 7.0 является очень мощным продуктом:

- Продукт стал более безопасным – можно устанавливать только бинарные файлы
- Он расширяем и гибок благодаря использованию новой модульной архитектуры
- Он стал более масштабируемым благодаря упрощению настройки, для которой теперь используются файлы в формате xml
- Улучшение производительности благодаря улучшениям в ядре IIS (http.sys)

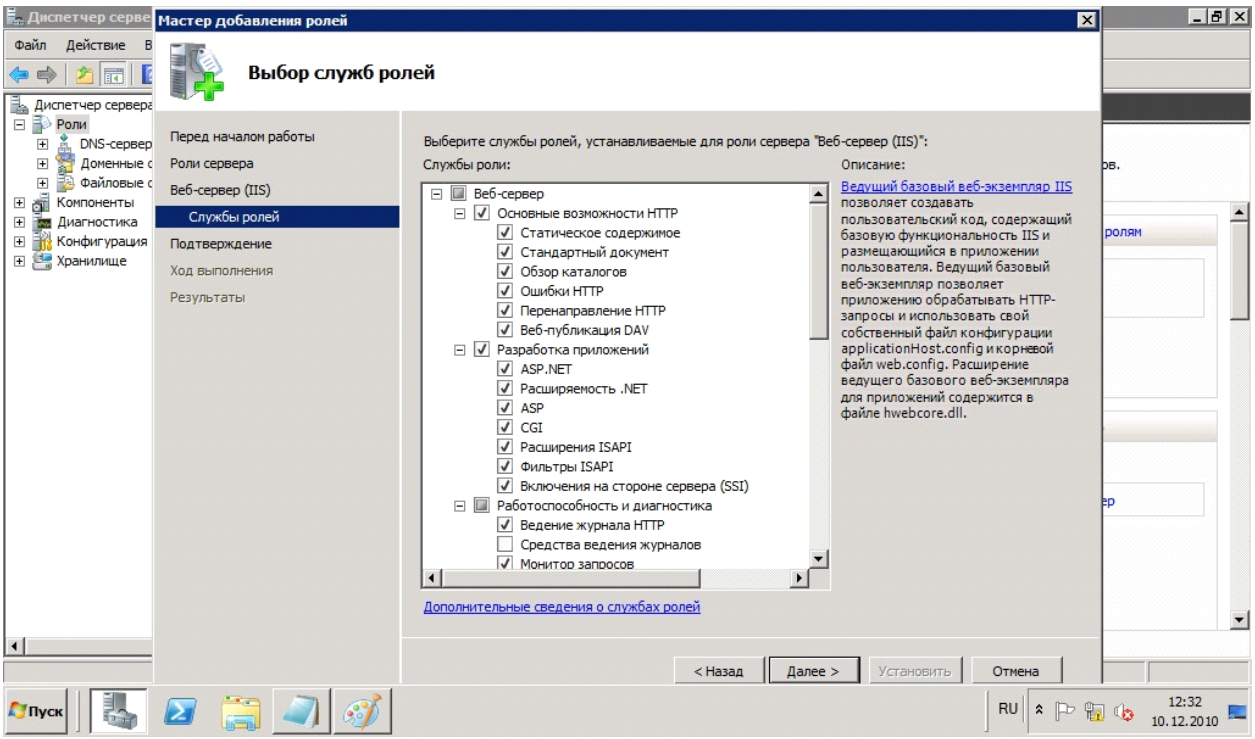
3. Порядок выполнения работы

Установка и настройка IIS на Windows Server 2008 R2, а так же установка различных cms (на конкретном примере - drupal)

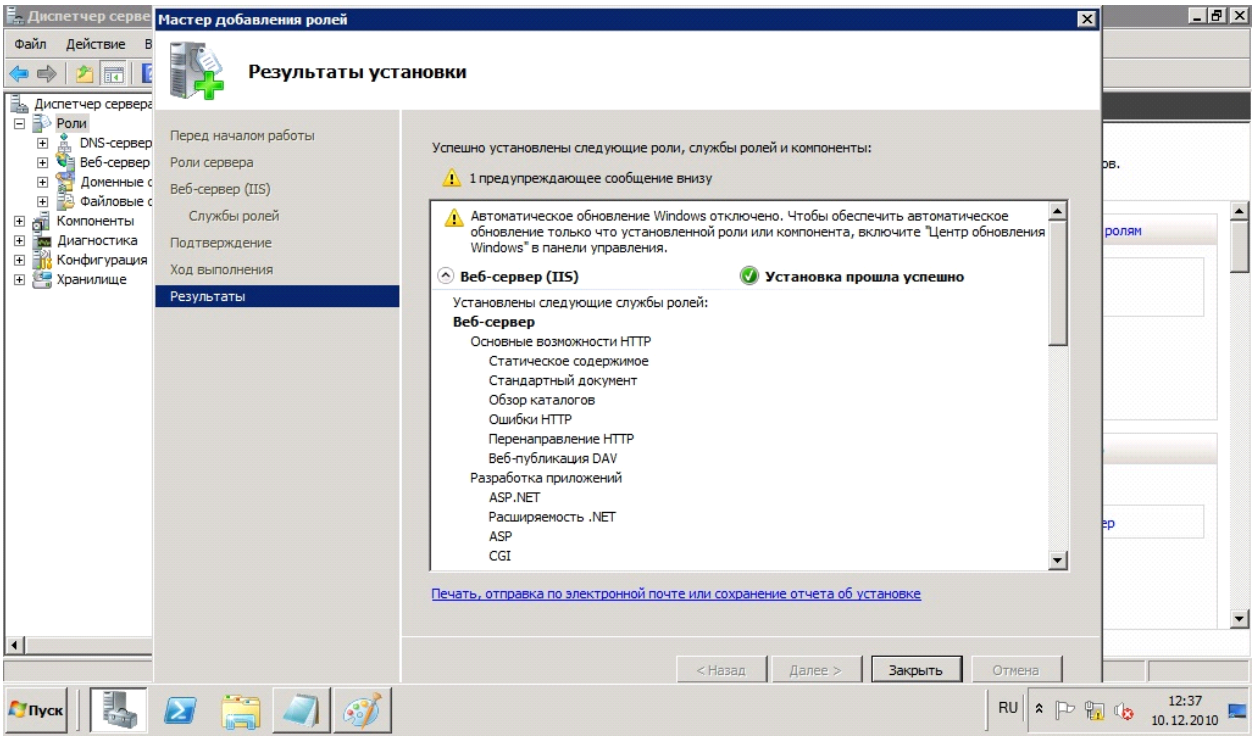
1) Включаем роль IIS. Для этого заходим в пуск - администрирование - диспетчер сервера - вкладка роли. Кликаем - добавить роли и в ролях отмечаем веб-сервер iis для установки.



Выбираем службы ролей, которые потребуются в дальнейшем использовании



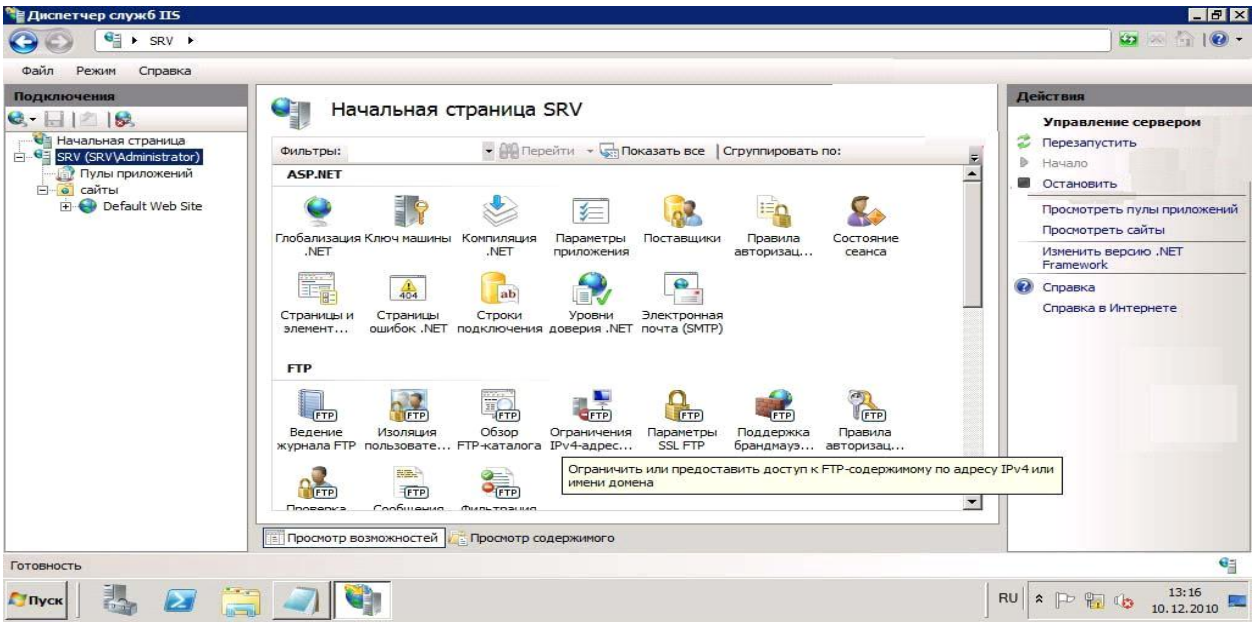
Затем выводятся результаты об установке



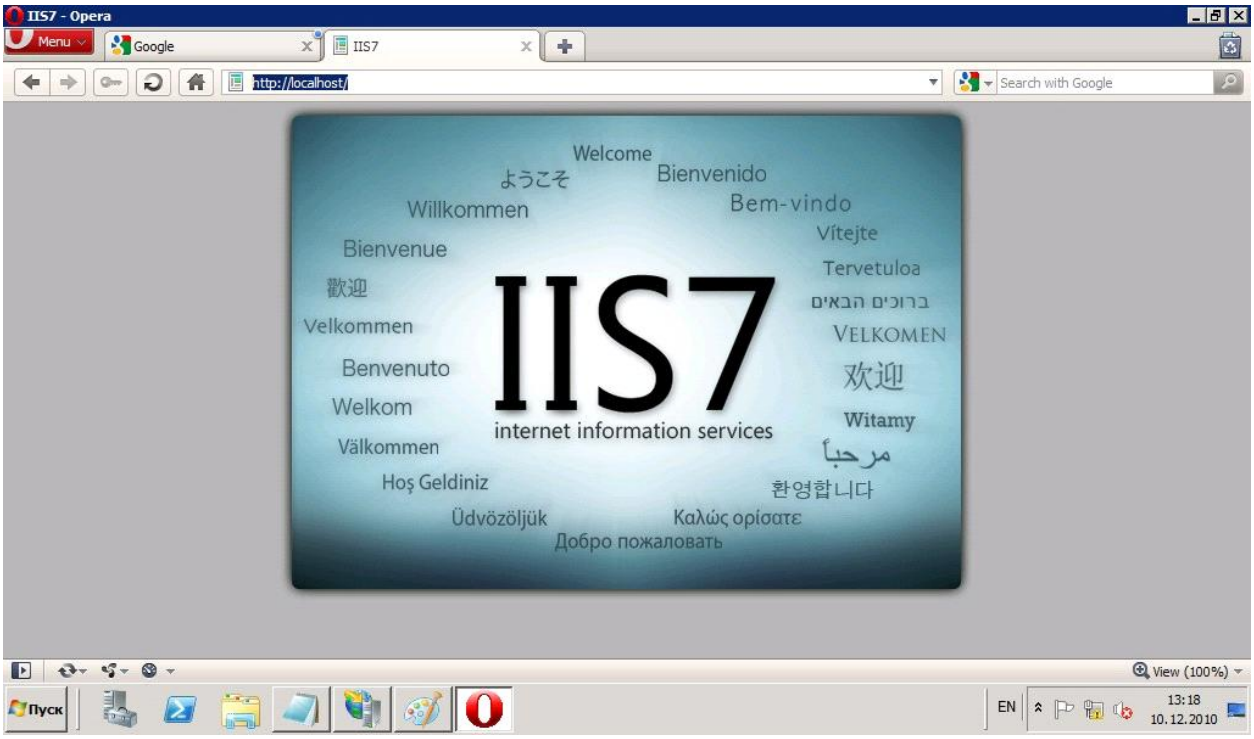
На этом этапе установка заканчивается.

2) Настройка IIS сервера

Идем по адресу пуск - администрирование - диспетчер служб iis. Жмем кнопку начало, тем самым запускаем сервер.



для теста идем на localhost. (в браузере вводим строку http://localhost/) Если приветствие отобразилось, значит все действия выполнены верно и можно продолжать работу.



Далее возможны два варианта развития событий:

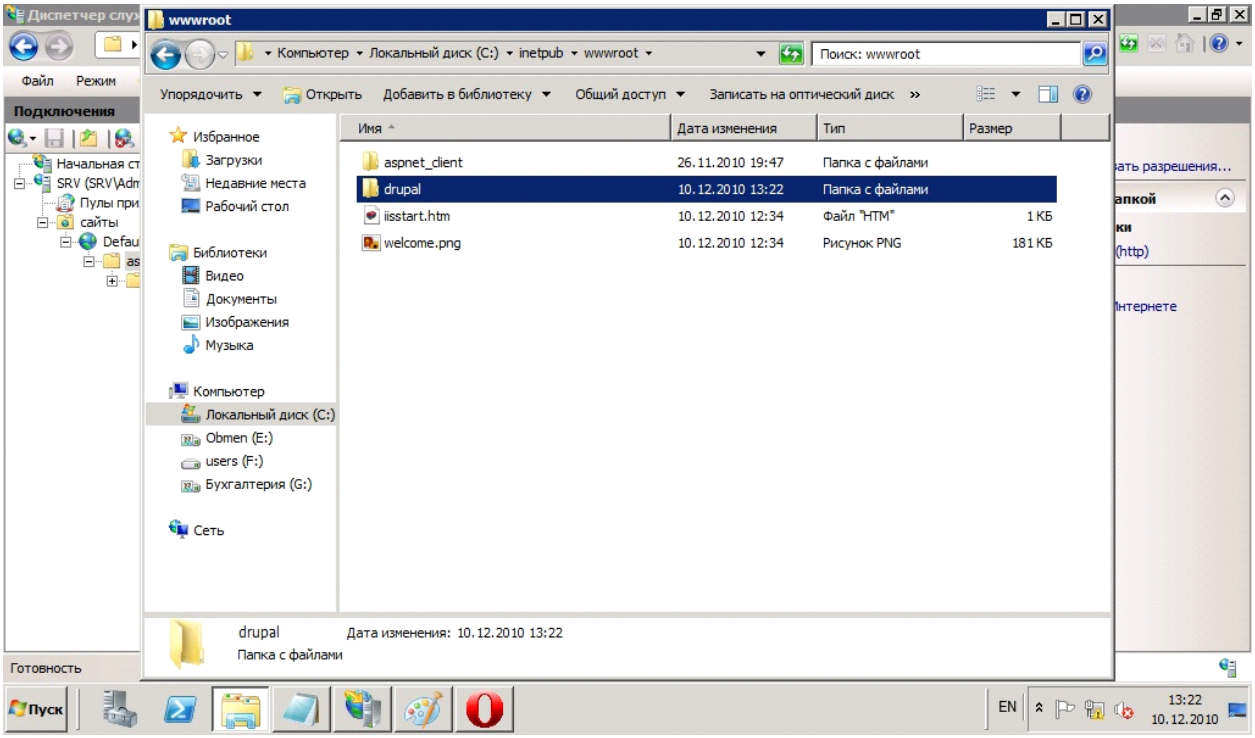
1) Ручная установка всех элементов IIS и ручная установка всех элементов cms. Этот вариант не рациональный, ведь нам нужно все сделать качественно, но в максимально сжатые сроки.

2) Мы можем воспользоваться автоматической установкой всех элементов. Как IIS, так и cms. Но все же рассмотрим оба метода.

Ручная установка всех элементов.

Готовим drupal для установки. качаем архив с официального сайта. Распаковываем. Создаем в папке iis каталог с названием вашего сайта, то есть

путь будет выглядеть так: C:\inetpub\wwwroot и переносим все директории из распакованного архива в папку C:\inetpub\wwwroot\drupal



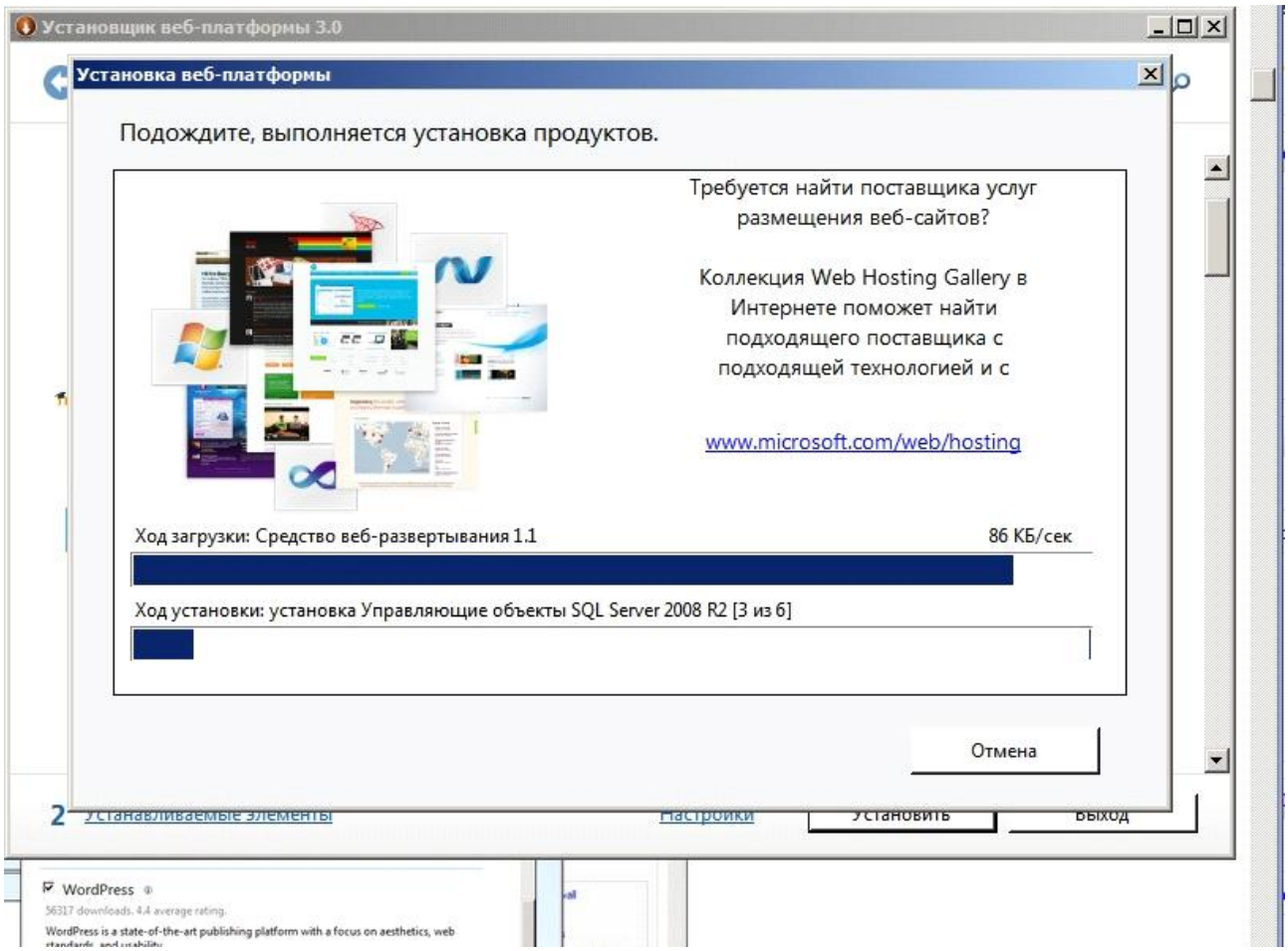
Установим php и mysql:

Заходим на сайт http://dev.mysql.com/downloads/mysql/ и качаем нужный для нашего сервера архив. В нашем случае для windows server 2008 r2 x64. Запускаем инсталлятор и следуем его действиям. Установка php. Для этого качаем инсталлятор по адресу http://windows.php.net/download/ и производим установку.

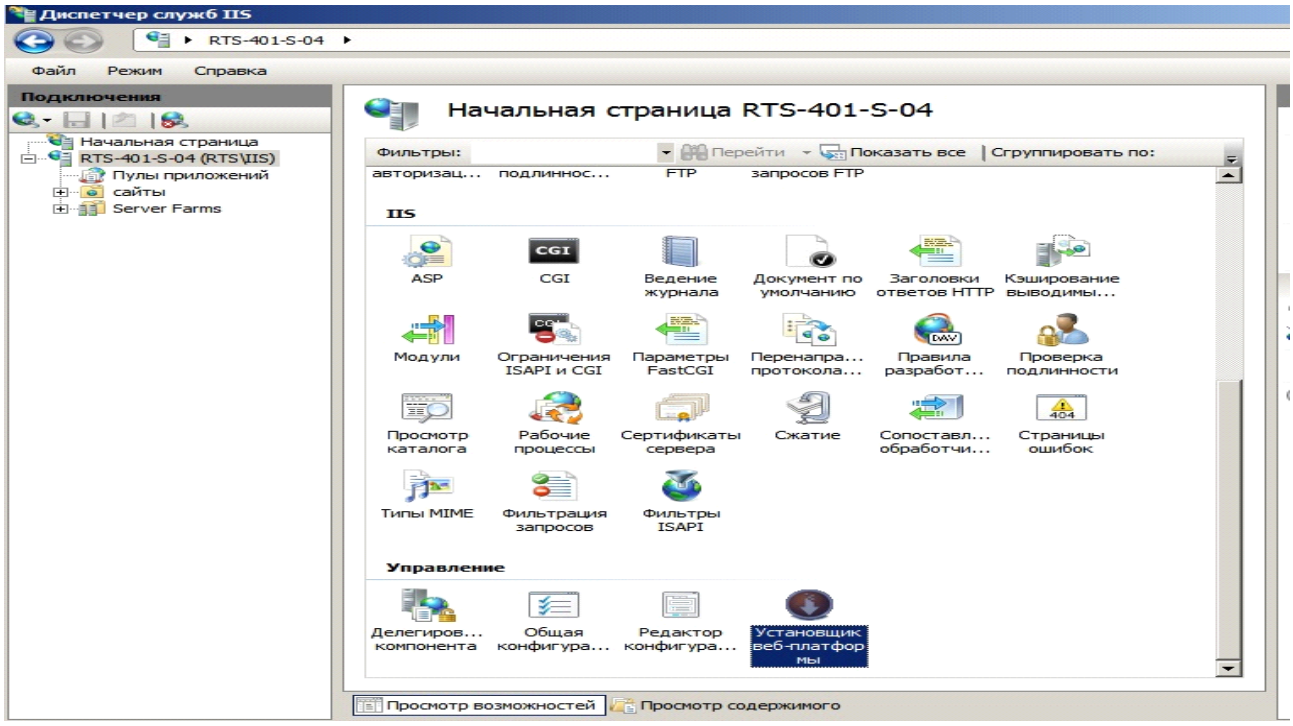
После этого мы идем по адресув браузере: http://localhost/drupal и видим, что нас перекинуло на экран установки cms!

Автоматическая установка (рекомендуемый)

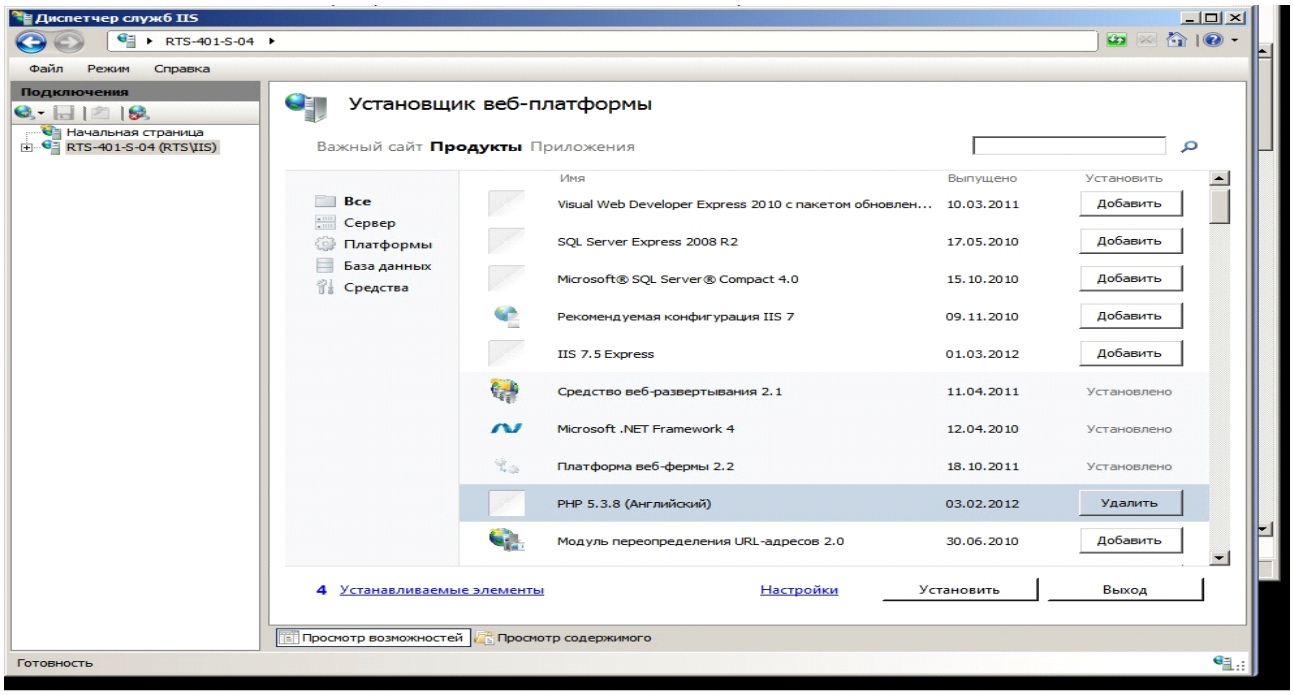
Для выполнения этой установки заходим в диспетчер служб iis и устанавливаем установщик веб-платформ.



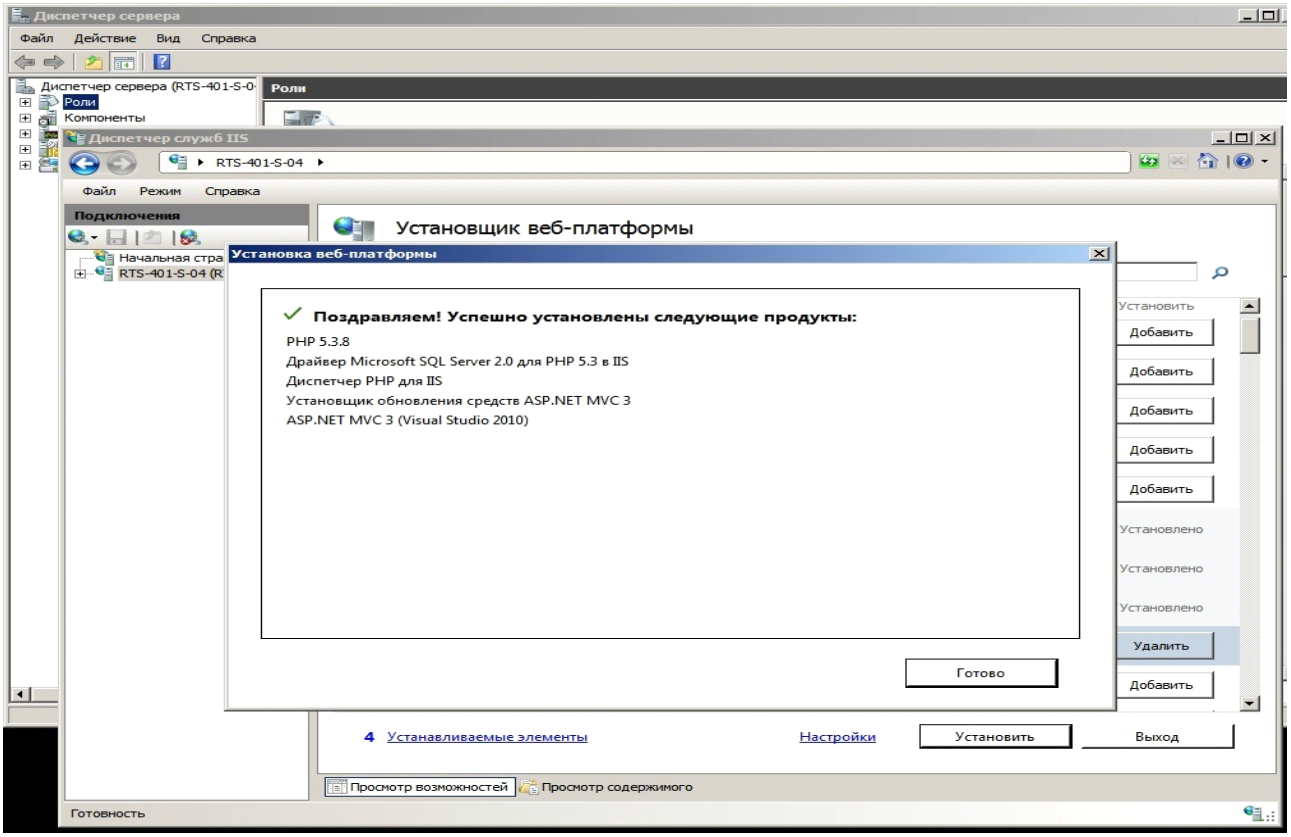
Выбираем закладку веб-платформа.



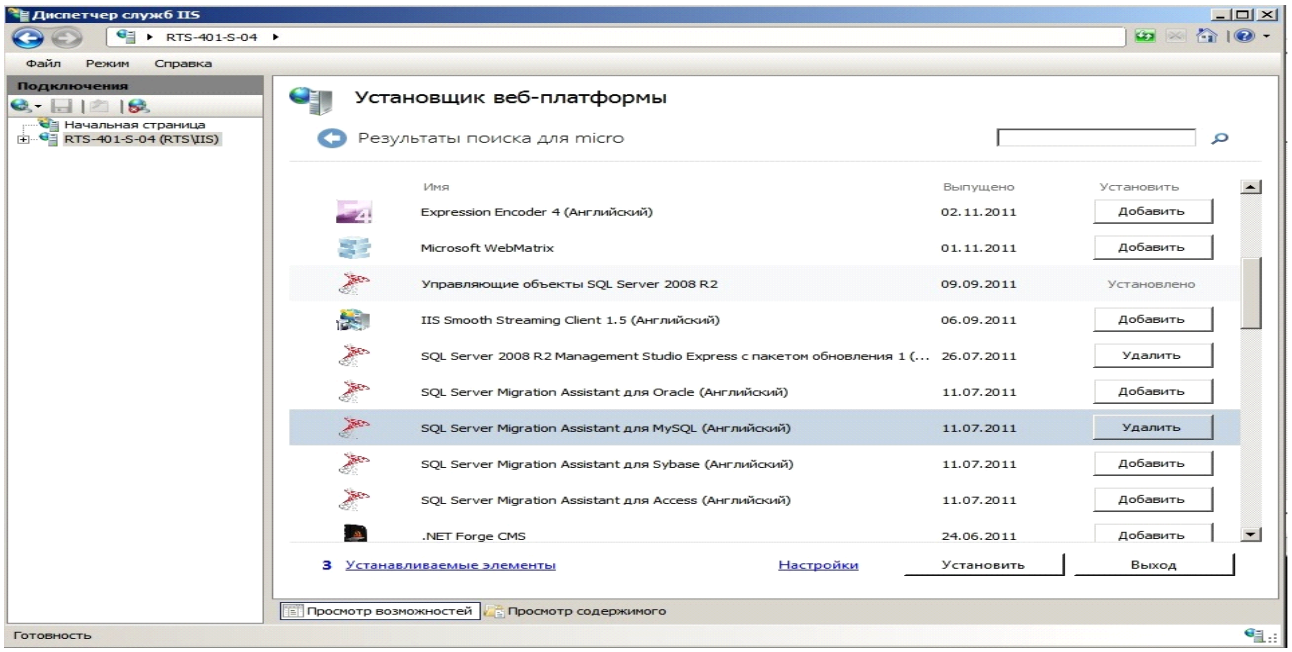
Отмечаем для установки продуктов ASP.NET, NET Framework 3.5, Microsoft.NET Framework 4, Windows Powershell 2.0, диспетчер PHP для IIS, PHP 5.2.13.



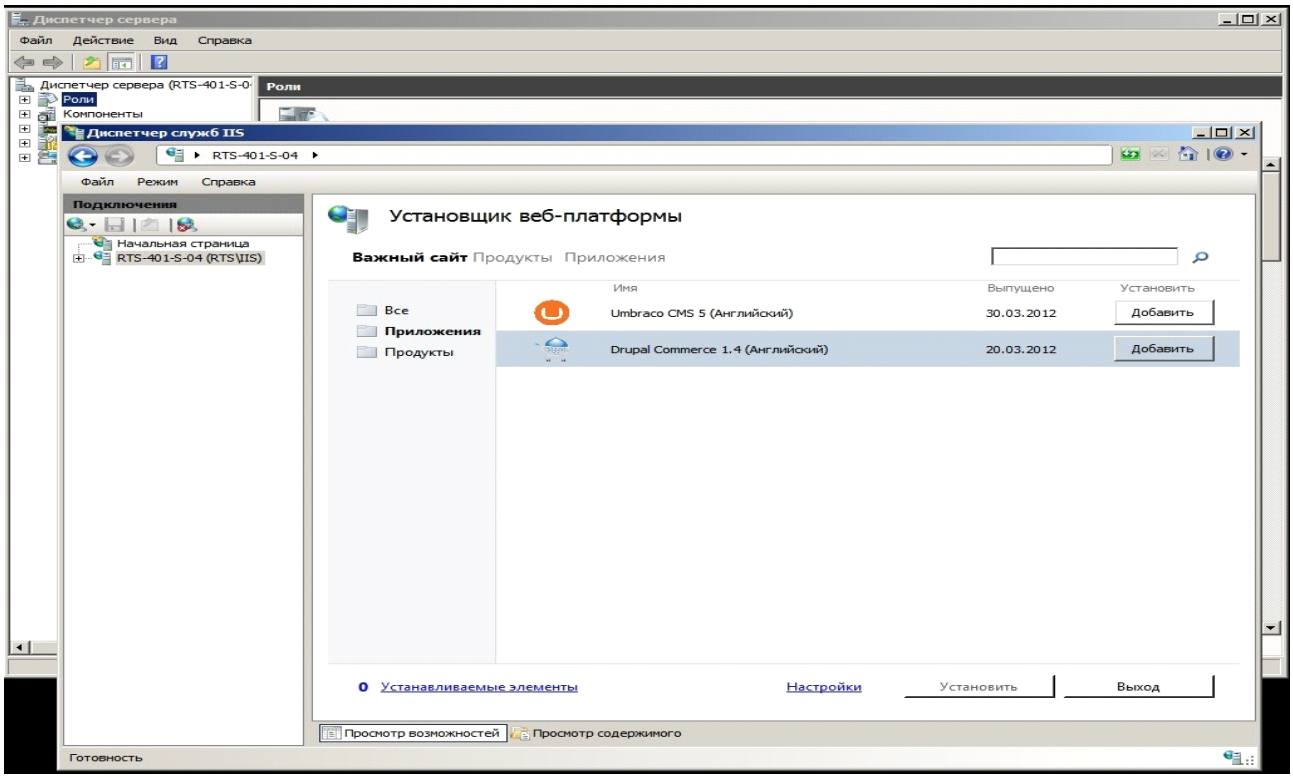
Жмем установить. Дожидаемся окончания установки.



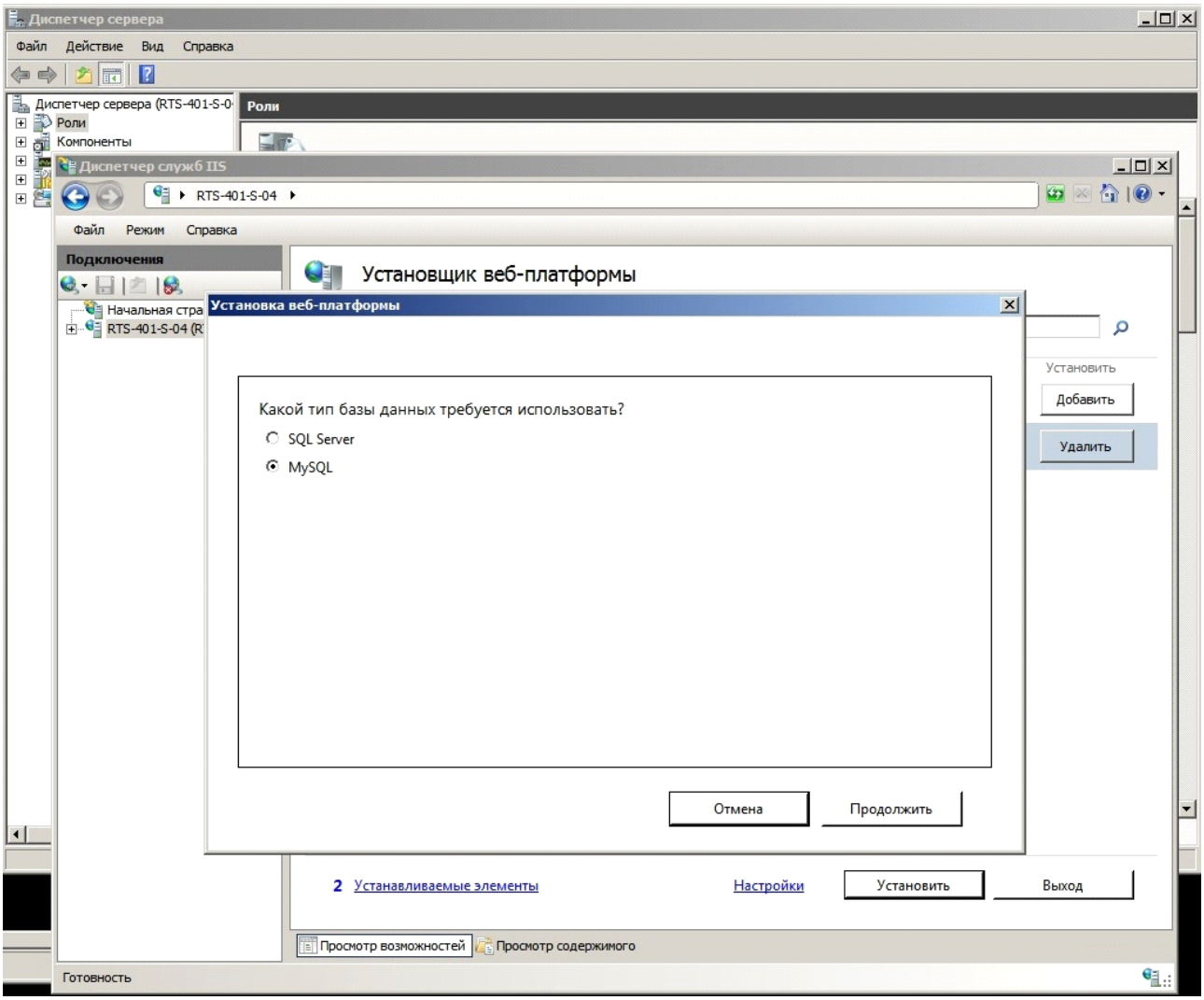
Заходим в установщик веб-приложений, выбираем драйвер SQL Server для PHP 2.0, SQL Server Express 2008 R2, SQL Server 2008 R2 Management Studio Express.



Теперь заходим снова ы установщик веб-платформ и выбираемпункт веб-приложения. Выбираем drupal и жмем установить.

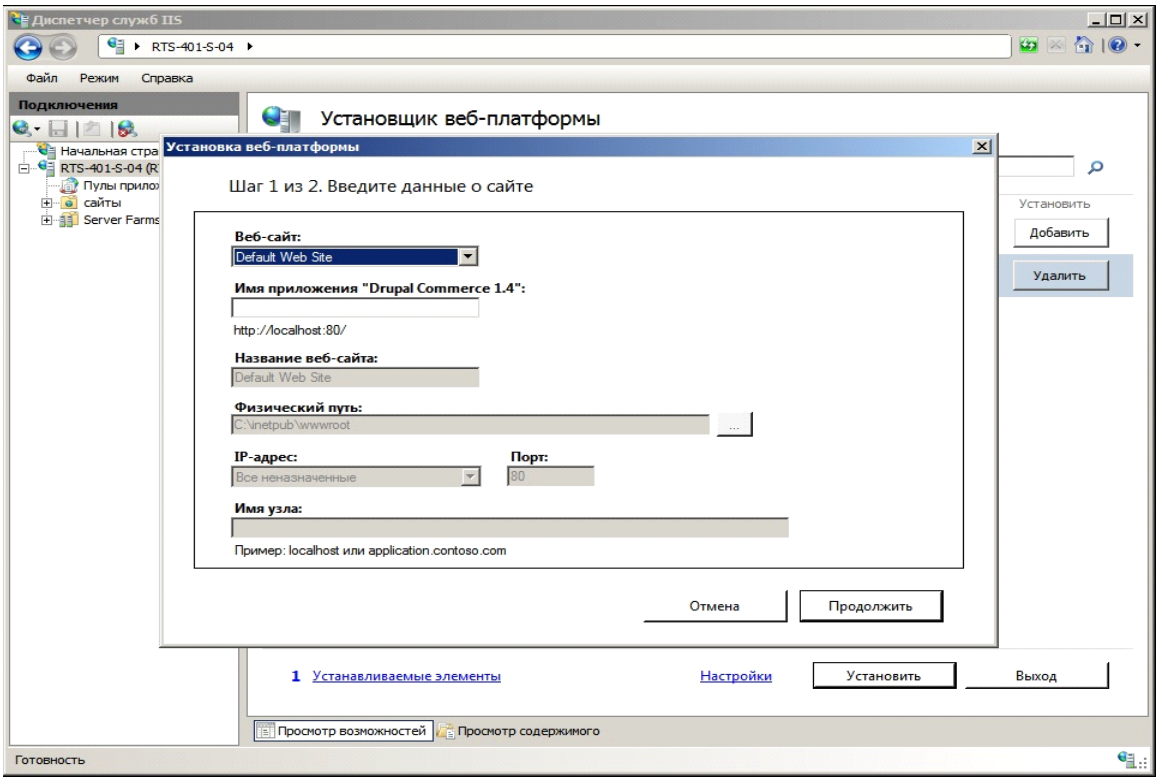


Видим запуск установки компонентов mySQL. Нам необходимо ввести пароль для администратора (пользователь root), используем пароль 12345.

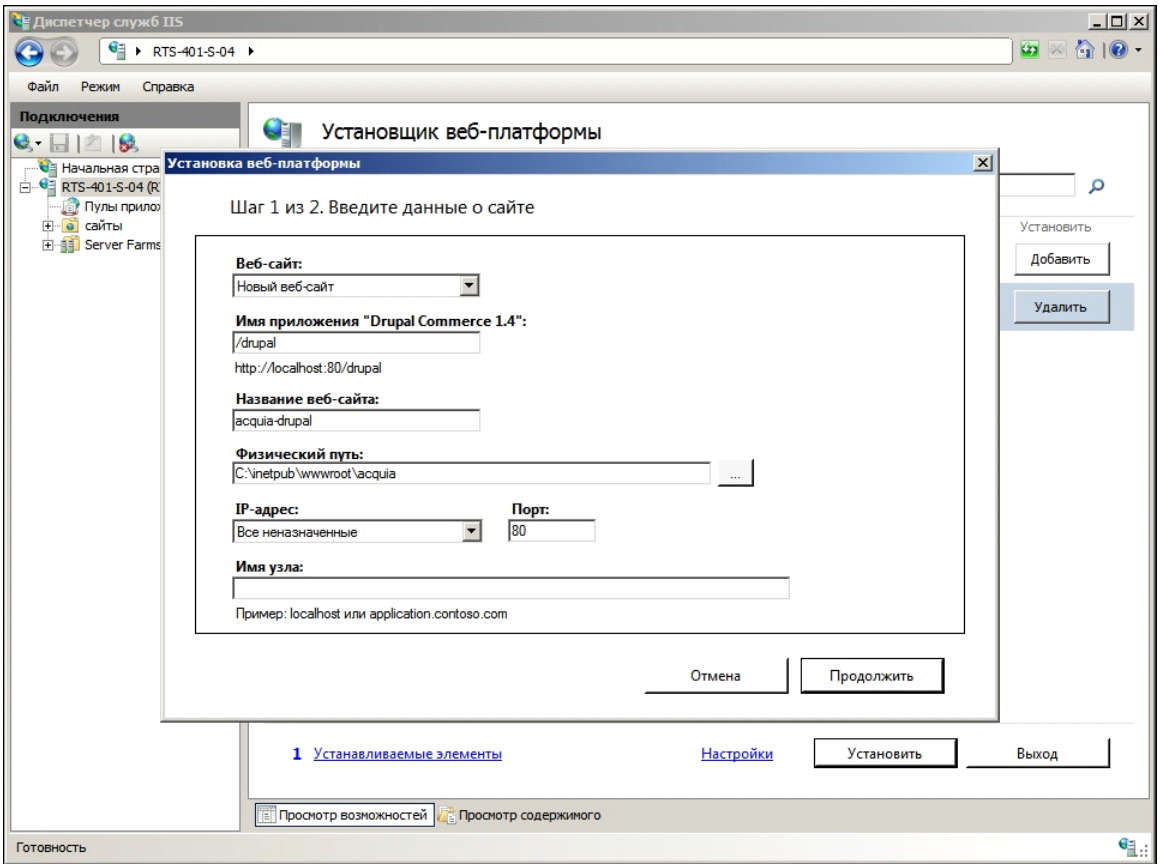


Окно для ввода данных о сайте.

Заполняем:

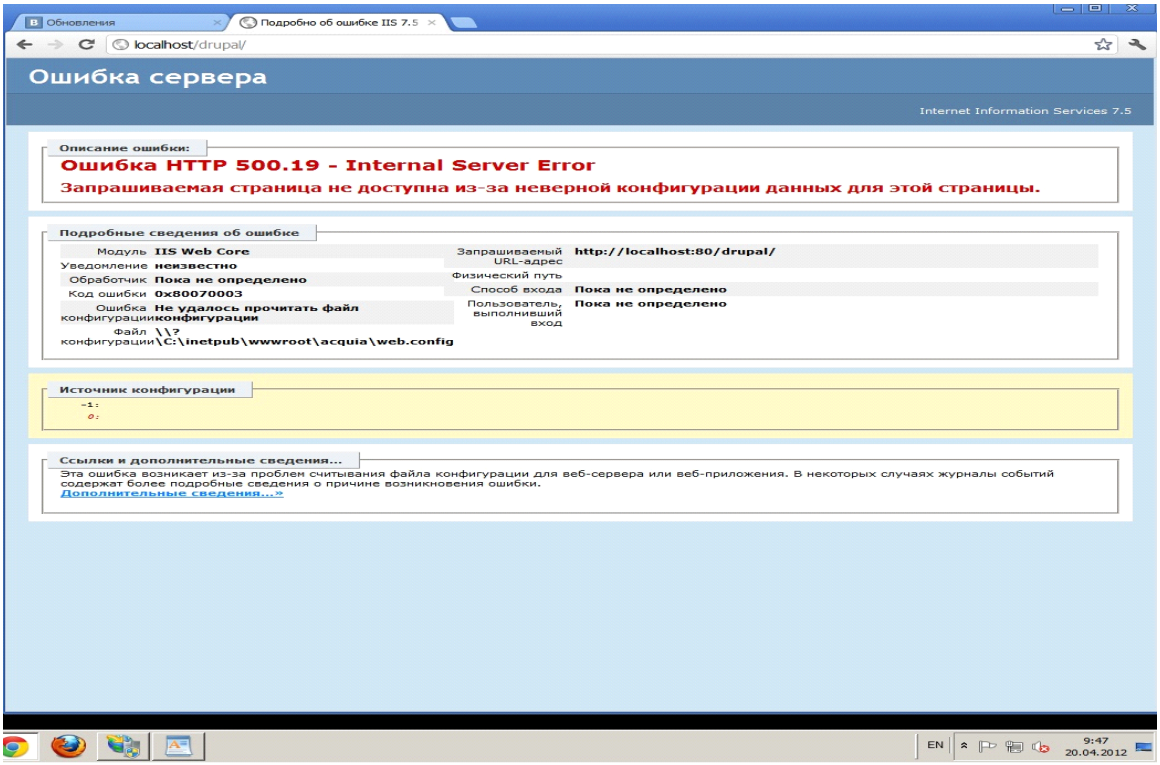


Приступаем ко второму шагу ввода данных о приложении (данные о базе данных):



Жмем далее и ждем завершения установки. Выводится на экран о не возможности завершения установки.

Запускается браузер, где видны частично установленные элементы.



Сайт доступен по адресу: http://localhost/drupal/

4.Рекомендуемая литература

1. IIS 7.0. Resource kit / M. Volodarsky, O. Londer, B. Cheah, B. Hill, S. Schofield, C.A. Mares. – Washington: Microsoft Press, 2008. – 753 p.

2. Хенриксон Х., Хофманн С. IIS 6. Полное руководство. Справочник профессионала. /Пер. с англ., - М.: Изд-во «СП ЭКОМ», 2004. – 672 с.

3. http://habrahabr.ru/post/78946/

Лабораторная работа 4. Исследование и администрирование средств обеспечения информационной безопасности Microsoft ISA Security Server. Установка и конфигурирование брандмауэра ISA. Построение VPN-сети на базе ISA

1. Цель работы

1) Разработать политику межсетевого экрана для безопасной работы пользователей в сети Internet. Политику направить на фильтрацию нежелательного трафика, способного нанести вред пользователям локальной сети, а также на обнаружение и предотвращение типовых сетевых атак.
2) Построение VPN, позволяющей получить доступ к ресурсам локальной сети из дома или другого удаленного места, не имеющего непосредственного подключения к локальной сети.

2. Краткие теоретические сведения

В данной работе рассматривается широко известный продукт корпорации Майкрософт - Microsoft® Internet Security and Acceleration (ISA) Server 2006. Это решение, объединяющее в себе последние достижения в области обеспечения безопасности сетей и реализующее функциональные возможности мощного многоуровнего межсетевого экрана, средства управления частными виртуальными сетями (VPN) и службы веб-кэширования.

Общие сведения о Microsoft ISA Server 2006

Сервер Microsoft ISA (Internet Security and Acceleration) Server 2006 – это решение, объединяющее в себе усовершенствованный межсетевой экран уровня приложений, средства организации и управления виртуальной частной сетью и службу кэширования веб-данных, использование которого позволяет повысить

эффективность вложений в информационные технологии путем повышения безопасности и производительности локальной сети.

Таблица 1. Основные возможности ISA Server 2006

Защита важных корпоративных приложений и данных	
Многоуровневая проверка содержимого	Включает межсетевой экран уровня приложения, обеспечивающий защиту от хакеров и вирусов, запрещение нежелательного потока данных, и одновременно позволяющий осуществлять передачу данных приложений через интернет.
Интеграция с различными приложениями	Обеспечивает пользователям более безопасный и быстрый доступ к приложениям и службам, включая сервер Microsoft Exchange Server и службы Internet Information Services.
Встроенная поддержка виртуальных частных сетей (VPN)	Обеспечивает безопасность потока данных входящих сообщений и защиту сети от внутренних атак. Встроенная поддержка туннельного режима IPSec позволяет без труда осуществить соединение между узлами и удаленное подключение через виртуальные частные сети.
Улучшенные механизмы проверки подлинности	Проверка подлинности пользователей сети во встроенных пространствах имен Windows или RADIUS с помощью разнообразных механизмов проверки учетных данных, включая RSA SecurID.
Простое управление политиками безопасности сети и конфигурацией	

межсетевого экрана	
Возможности поддержки нескольких сетей и сетевые шаблоны	Позволяет быстро развертывать ISA Server 2006 в существующей среде ИТ в качестве граничного межсетевого экрана или межсетевого экрана отдела или филиала – без изменения топологии сети.
Единый интерфейс управления межсетевым экраном и VPN	Обеспечивает простые в использовании средства управления, включая визуальное средство редактирования политик, позволяющие сократить время обучения и минимизировать бреши в защите из-за неправильной настройки.
Усовершенствованное устранение неполадок	Включает новую панель наблюдения с возможностью просмотра журнала в режиме реального времени, позволяющую просматривать сводную информацию о состоянии межсетевого экрана с подробными сведениями.
Более высокая скорость доступа и повышение производительности	
Расширенная архитектура межсетевого экрана	Обеспечивает более быстрое прохождение разрешенного потока данных через межсетевой экран, тем самым повышая производительность сети. Фильтрация на уровне приложений и возможность централизованной настройки политик кэширования объектов позволяет повысить производительность.

Более высокая скорость доступа в интернет с меньшими затратами	Вэб-кэш сервера ISA позволяет повысить эффективность работы пользователей и сократить затраты на передачу данных за счет хранения веб-содержимого на локальном сервере.

Создание и применение политики доступа в межсетевом экране ISA Server 2006

Политика доступа межсетевого экрана ISA (известная так же как политика брандмауэра) включает правила публикации Web-сервера (Web Publishing Rules), правила публикации сервера (Server Publishing Rules) и правила доступа (Access Rules). Правила публикации Web-сервера и обычного сервера используются для предоставления входящего доступа (inbound access), а правила доступа применяются для управления исходящим доступом (outbound access).

Главная задача брандмауэра ISA – контроль трафика между сетью-источником информации и сетью-адресатом. Политика доступа (Access Policy) брандмауэра ISA позволяет клиентам сети-источника получить доступ к хостам сети-адресата информации, а правила доступа можно сконфигурировать для блокировки соединений хостов исходной сети с хостами сети-адресата. Политика доступа определяет способ доступа хостов к хостам других сетей.

Когда брандмауэр ISA перехватывает запрос на исходящее соединение, он проверяет как сетевые правила, так и правила политики брандмауэра для того, чтобы определить, разрешен ли доступ. Первыми проверяются сетевые правила. Если нет сетевого правила, определяющего преобразование сетевых адресов (NAT) или маршрут между сетью-источником и сетью-адресатом, попытка соединения окажется безуспешной. Это обычная причина неудавшихся соединений, и именно ее следует искать, когда политика доступа приводит к неожиданным результатам.

Правила доступа можно сконфигурировать для определенного исходного или конечного хостов. Клиенты могут быть заданы IP-адресом (например, используя сетевые объекты компьютера или набора компьютеров) или именем пользователя. Брандмауэр ISA обрабатывает запросы по-разному, в зависимости от типа клиента, запрашивающего объект, и варианта настройки правил доступа.

Когда брандмауэр ISA получает запрос на соединение, он, прежде всего, проверяет наличие сетевого правила, определяющего маршрут между сетью-источником информации и сетью-адресатом. Если такого сетевого правила нет, брандмауэр ISA предполагает, что сеть-источник и сеть-адресат не соединены. При наличии правила, определяющего маршрут между ними, брандмауэр ISA обрабатывает правила политики доступа.

После того, как брандмауэр ISA подтвердил соединение сети-источника и сети-адресата, рассматривается политика доступа. Брандмауэр ISA обрабатывает правила доступа в политике доступа сверху вниз (системная политика реализуется до выполнения политики доступа, определенной пользователем).

Если с запросом исходящего соединения связано разрешающее правило (Allow rule), брандмауэр ISA разрешит выполнение запроса. Для выполнения разрешающего правила необходимо, чтобы характеристики соединения в запросе соответствовали характеристикам, определенным в правиле доступа.

Элементы правил доступа межсетевого экрана ISA

В брандмауэр ISA включены следующие элементы политики:

- протоколы;
- наборы пользователей;
- типы содержимого;
- расписания или часы работы;
- сетевые объекты.

Протоколы

В состав брандмауэра ISA входит ряд встроенных протоколов, которые можно использовать для создания правил доступа, правил публикации Web-серверов и правил публикации серверов.

Помимо встроенных протоколов можно создать собственные протоколы, используя мастер создания новых протоколов (New Protocol Wizard) брандмауэра ISA. Заготовленные заранее, встроенные протоколы нельзя модифицировать или удалить. Но можно редактировать и удалять созданные протоколы. Существует несколько протоколов, которые устанавливаются вместе с прикладными фильтрами, их нельзя модифицировать, но можно удалить. Существует возможность устранить связь прикладных фильтров с этими протоколами.

Наборы пользователей

Для управления исходящим доступом можно создать правила доступа и применить их к конкретным IP-адресам (Internet Protocol addresses) или определенным пользователям или группам пользователей. Когда правила доступа применяются к пользователям или группам, пользователи должны подтвердить подлинность с помощью протокола аутентификации (authentication protocol). Клиент брандмауэра всегда использует интегрированную аутентификацию и всегда отправляет незаметно для пользователя его верительные данные – имя и пароль (credentials). Клиент Web-прокси может применять ряд разных методов подтверждения подлинности или аутентификации.

Брандмауэр ISA позволяет группировать пользователей и группы пользователей в наборы пользователей (User Set), которые, лучше называть «группами брандмауэра». Наборы пользователей включают один или несколько пользователей или группы пользователей с любой схемой аутентификации, поддерживаемой брандмауэром ISA.

Брандмауэр ISA поставляется со следующими заранее сконфигурированными наборами пользователей:

- **Все подтвердившие свою подлинность пользователи (All Authenticated Users)**

Этот предопределенный набор содержит все подтвердившие подлинность пользователи, независимо от избранного метода аутентификации. Правило доступа, использующее этот набор, применяется ко всем подтвердившим подлинность пользователям.

- **Все пользователи (All Users)**

Этот предопределенный набор пользователей представляет всех пользователей, как подтвердивших подлинность, так и не сделавших этого, и никаких имен и паролей не требуется для доступа к правилу, использующему этот набор пользователей.

- **Системный и сетевой сервис (System and Network Service)**

Этот заранее подготовленный пользовательский набор представляет локальный системный и сетевой сервисы на машине брандмауэра ISA. Он применяется в некоторых правилах системной политики.

Типы содержимого

Типы содержимого задают типы MIME (Multipurpose Internet Mail Extensions, многоцелевые расширения электронной почты в сети Интернет) электронной корреспонденции и расширения файлов. При создании правила доступа для протокола HTTP можно ограничить типы содержимого, к которым оно будет применяться. Контроль типа содержимого позволяет очень детально конфигурировать политику доступа, поскольку можно управлять доступом, основываясь не только на протоколах и адресатах, но и на конкретном содержимом.

Управление типом содержимого возможно только для HTTP-трафика и туннельного (tunneled) FTP-трафика.

Когда хост сети, защищенной брандмауэром ISA, создает исходящий HTTP-запрос, брандмауэр ISA посылает запрос на Web-сервер через фильтр Web-прокси (по умолчанию). При возврате Web-сервером запрошенного Web-объекта брандмауэр ISA проверяет MIME-тип объекта (который находится в данных заголовка HTTP) или его расширение файла (в зависимости от информации в заголовке, который возвращается Web-сервером). Брандмауэр ISA определяет, применяется ли правило к заданному типу содержимого, включая расширение файла, и обрабатывает правило соответствующим образом.

Брандмауэр ISA поставляется с предопределенным встроенным списком типов содержимого, которые можно использовать. Можно также создать собственные типы содержимого, задавая как MIME-тип, так и расширение файла.

Часы работы или расписание

Можно задать расписание (Schedule), управляющее временем применения правила. Имеются три встроенных расписания:

- **Work Hours (Рабочие часы)**

Разрешает доступ в период с 09:00 утра до 17:00, начиная с понедельника и заканчивая пятницей (для данного правила);

- **Weekends (Выходные дни)**

Разрешает доступ в любое время в субботу и воскресенье (для данного правила);

- **Always (Всегда)**

Разрешает доступ в любое время (для данного правила).

Обратите внимание на то, что правила могут быть разрешающими и запрещающими. Расписания применяются ко всем правилам доступа, а не только к разрешающим правилам.

Сетевые объекты

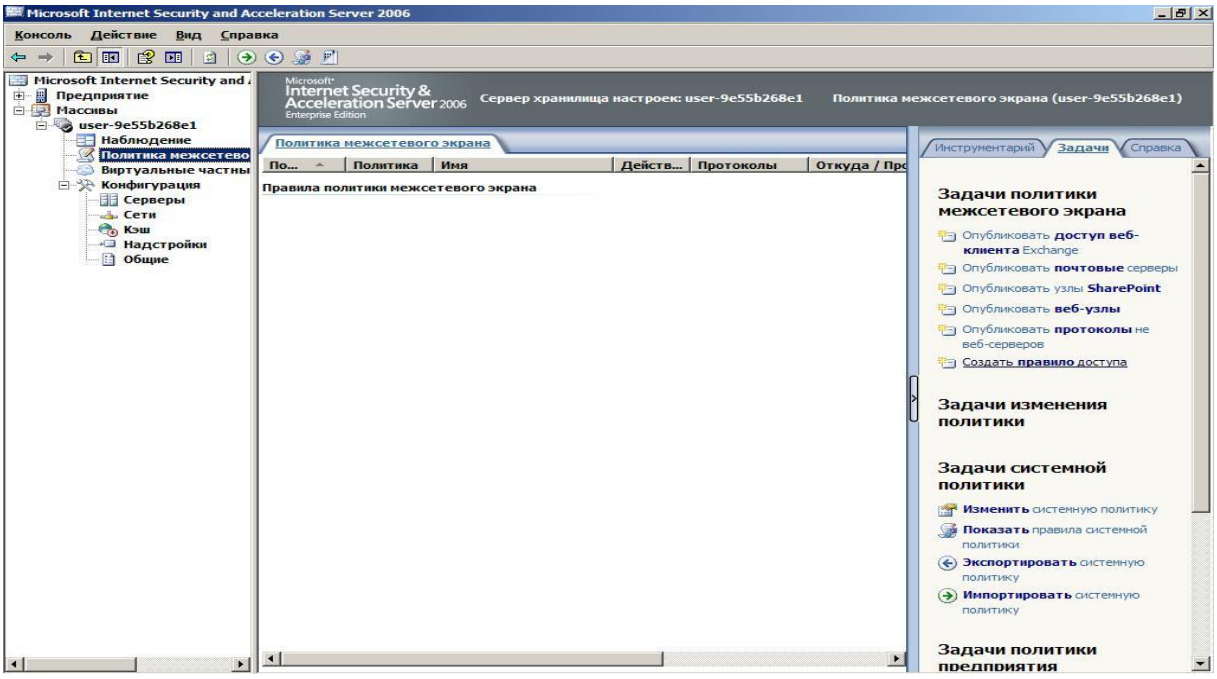
Сетевые объекты применяются для контроля над источниками и адресатами соединений, проходящих через брандмауэр ISA.

Конфигурирование правил доступа для исходящих соединений через межсетевой экран ISA

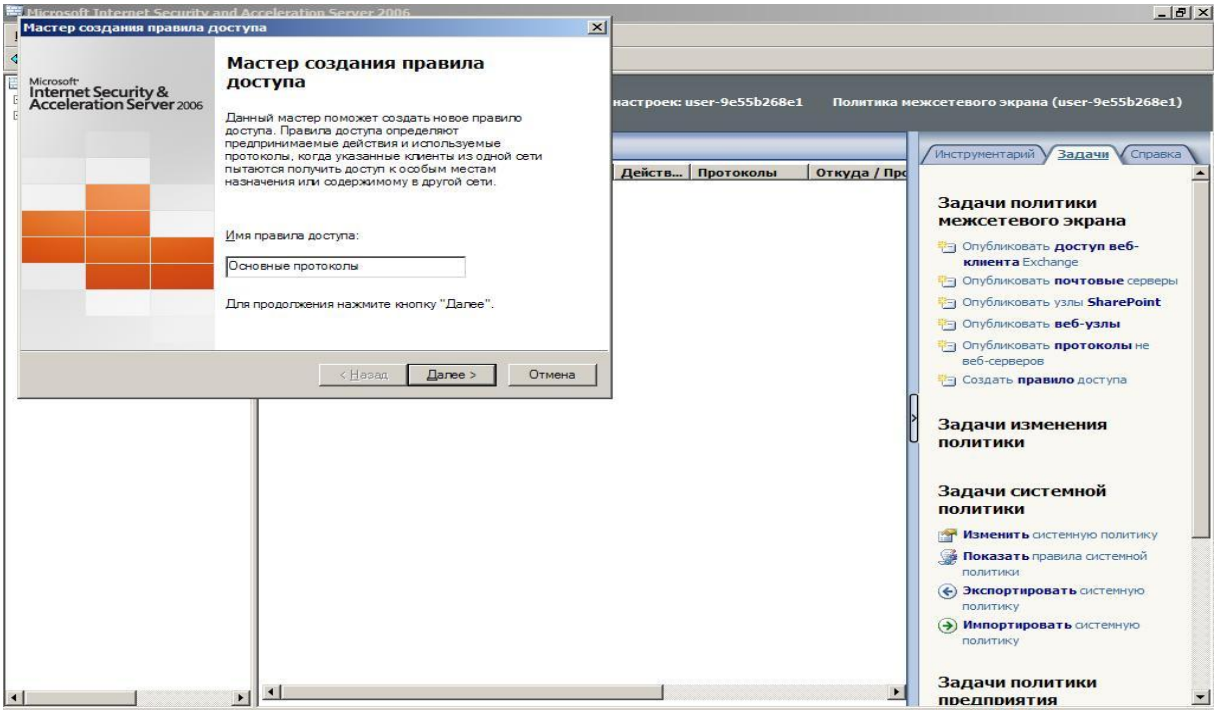
К исходящим соединениям всегда применяются правила доступа. Только протоколы с первичным соединением в исходящем направлении или направлении отправки можно использовать в правилах доступа. Правила доступа управляют доступом от источника к адресату с помощью исходящих протоколов.

В этом разделе мы подробно рассмотрим процесс создания правила доступа и каждый из его параметров, доступных в мастере создания нового правила (New Access Rule Wizard).

Для начала откройте консоль управления Microsoft Internet Security and Acceleration Server 2006, раскройте окно, связанное с именем сервера, и щелкните кнопкой мыши узел «Политика межсетевого экрана».



Щелкните кнопкой мыши вкладку «Задачи» на панели задач и ссылку «Создать правило доступа». На экране появится страница с заголовком «Мастер создания правила доступа».

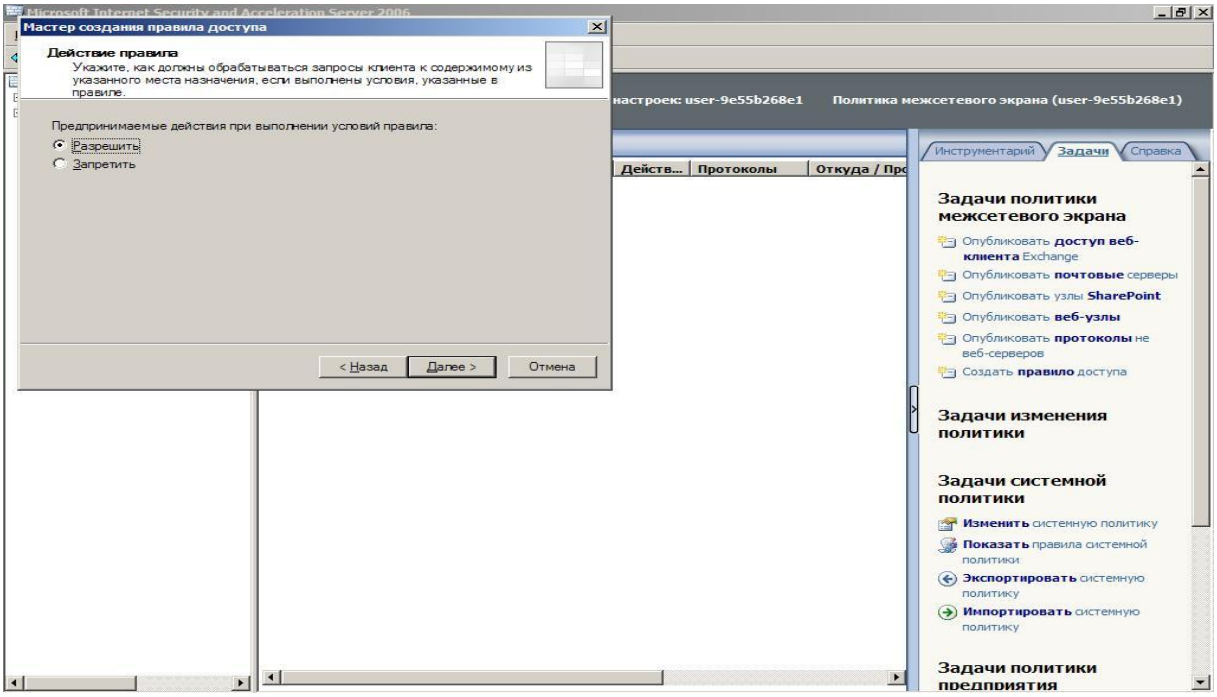


Введите имя правила в текстовое поле ввода «Имя правила доступа». В этом примере мы создадим правило доступа «Основные протоколы», пропускающее весь трафик по выбранным протоколам от локального компьютера и из внутренней сети во внешнюю сеть.

Щелкните мышью по кнопке Next (Далее).

Страница «Действие правила»

На странице «Действие правила» есть два варианта: «Разрешить» или «Запретить». В нашем примере мы выберем вариант «Разрешить» и щелкнем мышью кнопку «Далее».



Страница «Протоколы»

На странице «Протоколы» выбираются протоколы, которые следует разрешить для исходящего соединения сети-источника с адресатом. В списке «Данное правило применяется к» есть три возможных варианта:

- **«Весь исходящий трафик»**

Этот вариант разрешает использовать все протоколы для исходящего доступа.

- **«Выбранные протоколы»**

Этот вариант позволит выбрать конкретные протоколы, к которым применяется данное правило. Можно выбрать из списка протоколов по умолчанию, включенного в брандмауэр ISA

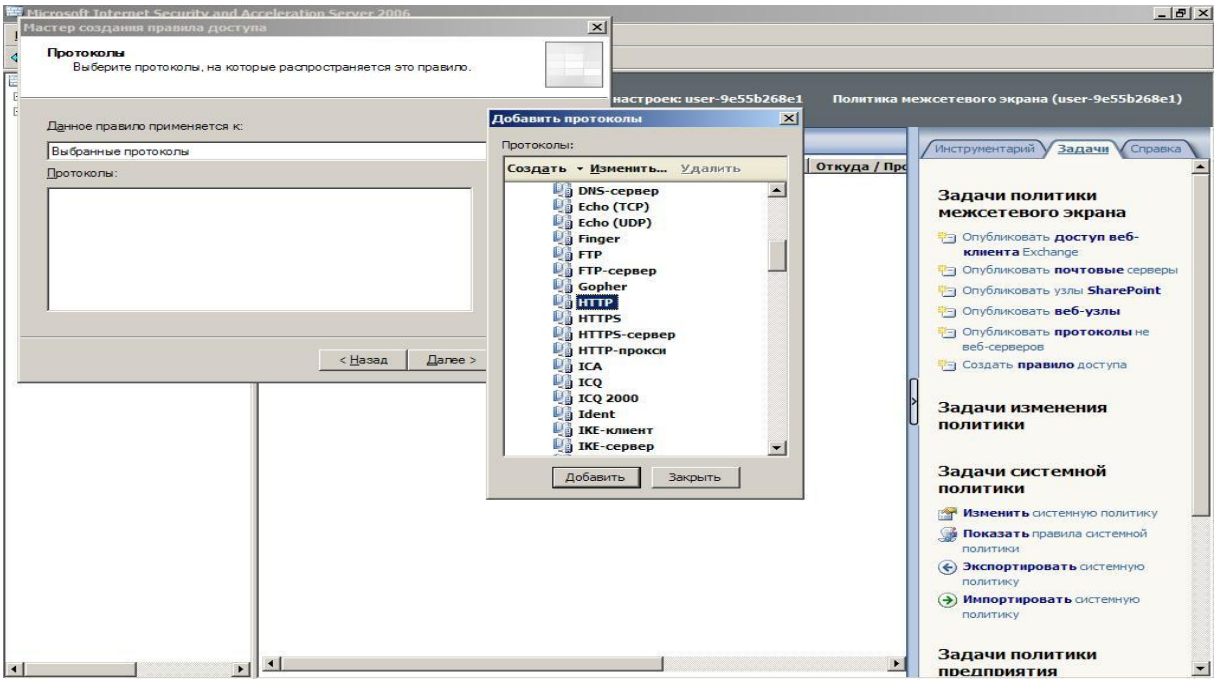
- **«Весь исходящий трафик кроме выбранного»**

Этот вариант позволит сделать все протоколы доступными для исходящего доступа, за исключением определенных протоколов для исходящего доступа.

Выделите строку «Выбранные протоколы» и щелкните мышью кнопку «Добавить». На экране появится диалоговое окно «Добавить протоколы». В

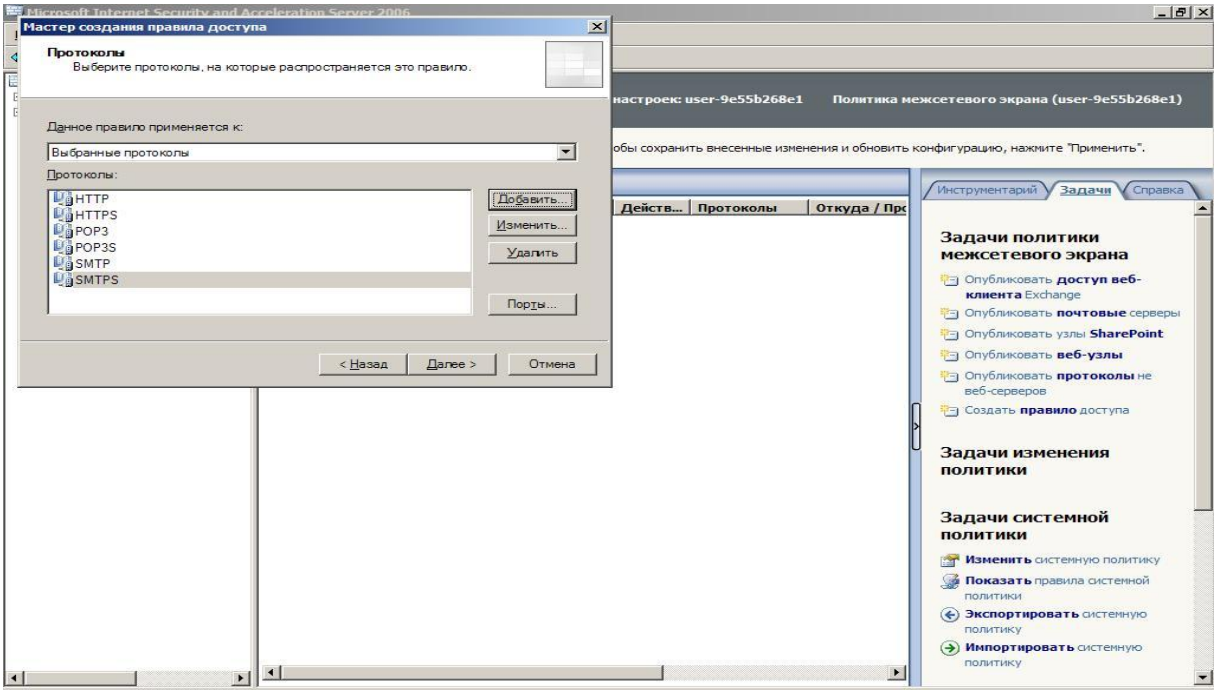
этом диалоговом окне вы увидите список папок, в которых сгруппированы протоколы в зависимости от основной сферы их применения. Например, папка «Общие протоколы» содержит протоколы, которые обычно применяются для подключения к Интернету, а в папке «Почтовые протоколы» собраны протоколы, которые, как правило, используются для доступа через брандмауэр ISA к сервисам электронной почты. Папка «Все протоколы» содержит все протоколы, как встроенные, так и определенные пользователем, включенные в конфигурацию брандмауэра ISA.

После щелчка кнопкой мыши папки «Все протоколы» появятся все протоколы, сконфигурированные в брандмауэре ISA. Брандмауэр ISA поставляется с определениями ста протоколов, которые можно использовать в правилах доступа.



После определения протокола, который необходимо включить в правило, дважды щелкните его кнопкой мыши. Повторите это действие для других протоколов, которые необходимо включить в правило, и затем щелкните мышью кнопку «Закрыть» диалогового окна «Добавить протоколы». В нашем

примере мы хотим разрешить доступ для протоколов HTTP, HTTPS, POP3, POP3S, SMTP, SMTPS.

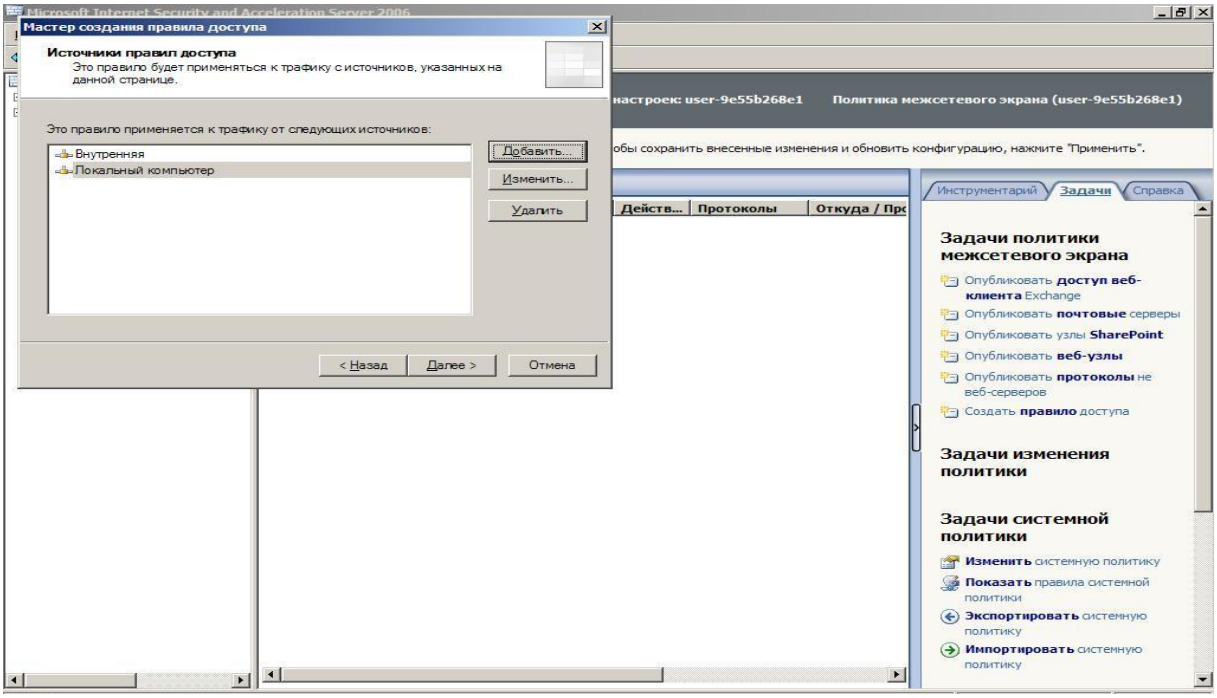


Страница «Источники правил доступа»

На странице «Источники правил доступа» выберите местонахождение источника информации, к которому следует применить правило доступа. Щелкните мышью кнопку «Добавить», чтобы вставить источник связи, к которому будет применяться данное правило.

В диалоговом окне «Добавление сетевых сущностей» можно выбрать местонахождение источника информации для данного правила. Дважды щелкните кнопкой мыши источник, к которому нужно применить правило.

В нашем примере щелкните кнопкой мыши папку «Сети», чтобы раскрыть ее, и дважды щелкните мышью строку «Внутренняя» и строку «Локальный компьютер». Нажмите кнопку «Закрыть» для закрытия диалогового окна.

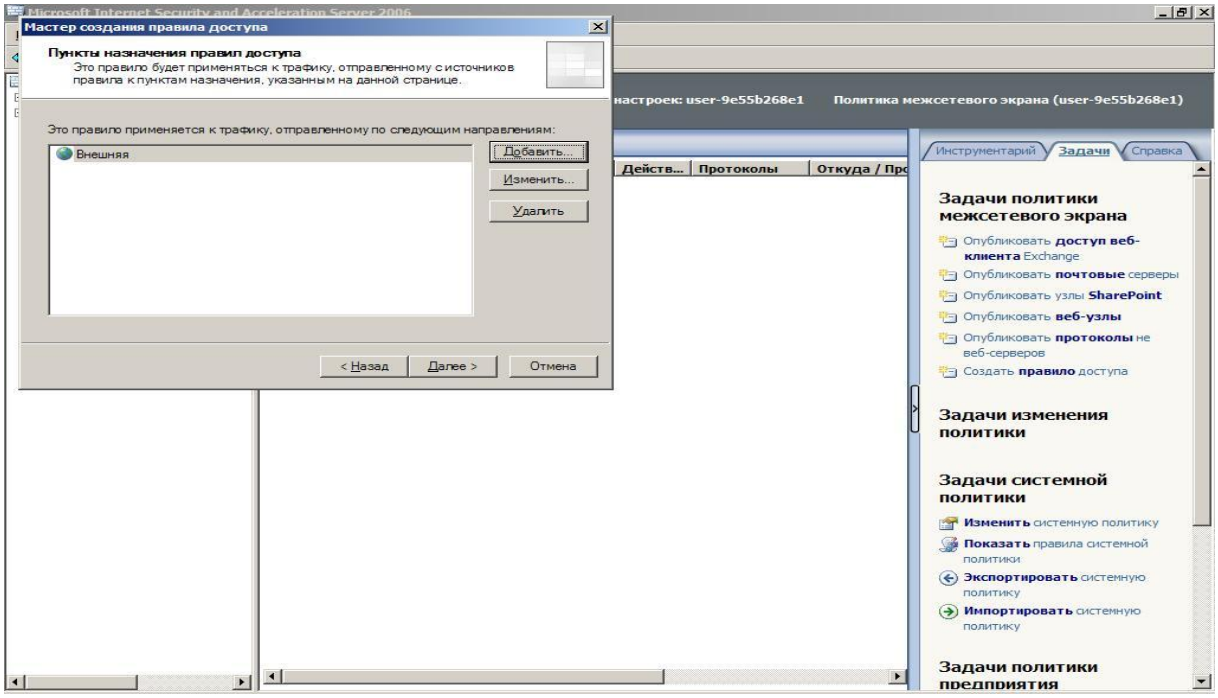


Щелкните мышью кнопку «Далее» на странице «Источники правил доступа».

Страница «Пункты назначения правил доступа»

На странице «Пункты назначения правил доступа» выберите адресат информации, к которому нужно применить данное правило. Щелкните мышью кнопку «Добавить», чтобы добавить местонахождение адресата. На экране появится диалоговое окно «Добавление сетевых сущностей», в нем можно выбрать сетевой объект в качестве адресата информации, к которому будет применяться данное правило доступа.

В нашем примере мы щелкнем кнопкой мыши папку «Сети», а далее двойным щелчком кнопки мыши выберем строку «Внешняя». Щелкните мышью кнопку «Закрыть», чтобы закрыть диалоговое окно. Затем щелкните мышью кнопку «Далее»

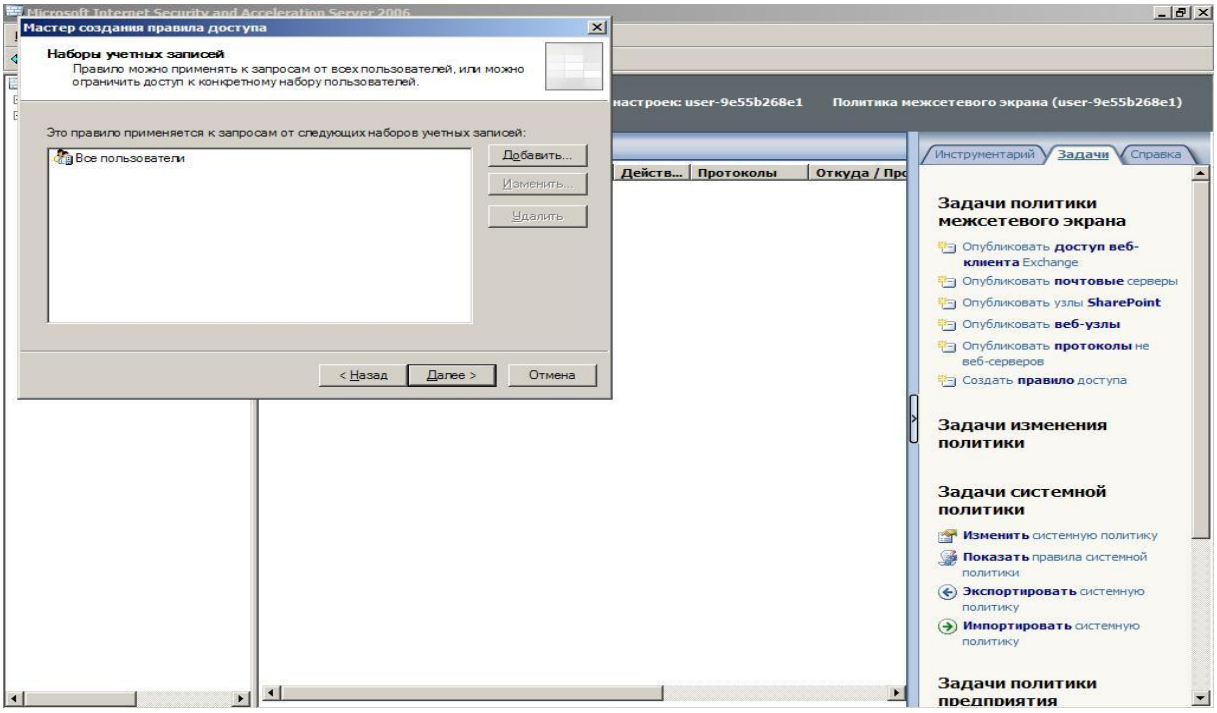


Страница «Наборы учетных записей»

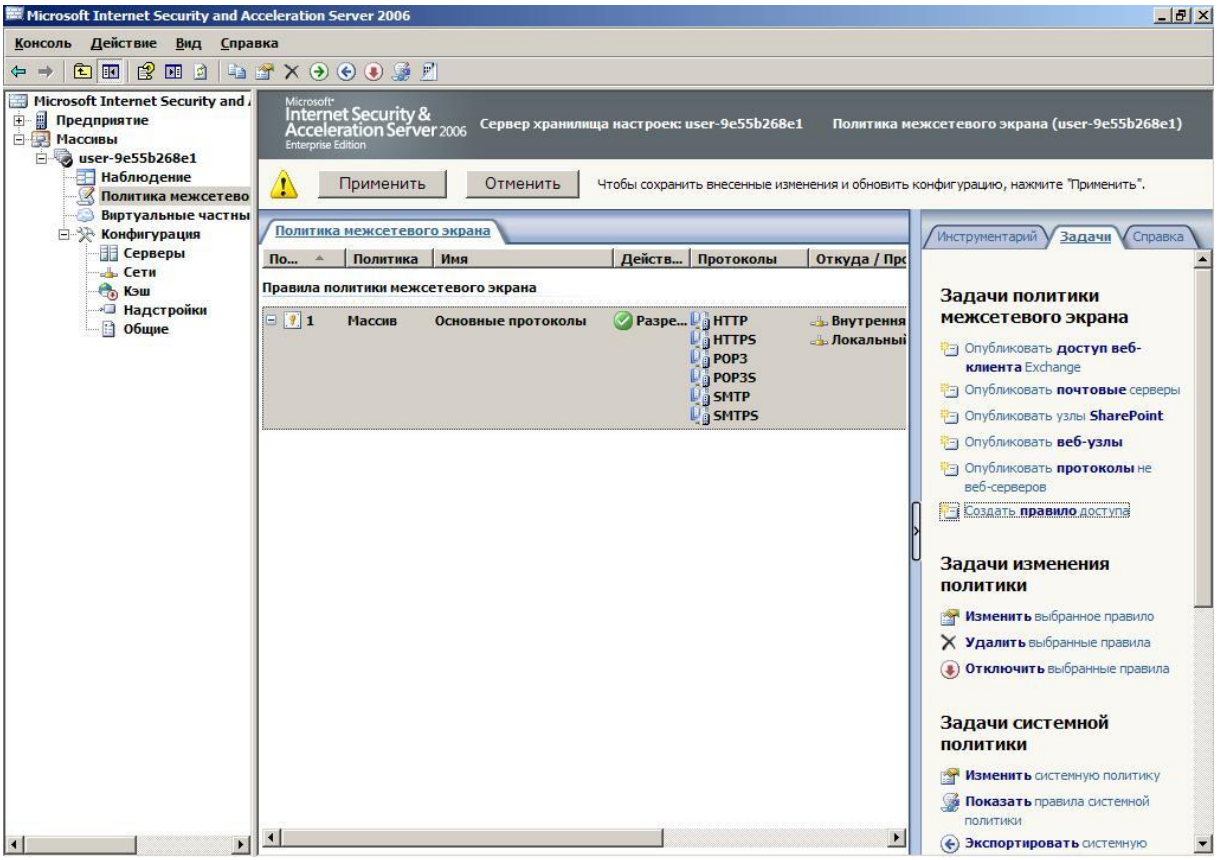
На странице «Наборы учетных записей» можно задать пользователей, к которым применяется данное правило. Установка по умолчанию – «Все пользователи». Если нужно удалить этот набор пользователей или любой другой из списка пользователей, к которым применяется данное правило, выберите набор пользователей и щелкните мышью кнопку «Удалить». Можно также отредактировать набор пользователей, приведенный в списке, щелкнув мышью кнопку «Редактировать».

Добавить набор пользователей можно, щелкнув мышью кнопку «Добавить». Можно также создать новые группы брандмауэра, щелкнув кнопкой мыши пункт меню «Новая».

В нашем примере мы воспользуемся установкой по умолчанию «Все пользователи». Щелкните мышью кнопку «Закрыть», чтобы закрыть диалоговое окно «Добавить пользователей». Затем щелкните мышью кнопку «Далее».



Далее появляется страница «Завершение мастера создания правила доступа». Проверьте сделанные установки и щелкните мышью кнопку «Готово».



После этого нажмите кнопку «Применить» для применения созданных правил доступа.

HTTP-фильтр

HTTP-фильтр (HTTPS-фильтр) брандмауэра ISA – одно из ключевых средств фильтрации и проверки на прикладном уровне, включенных в состав брандмауэра ISA. Этот фильтр позволяет брандмауэру ISA выполнять проверку на уровне приложений всех HTTP-коммуникаций, проходящих через брандмауэр ISA, и блокировать соединения, не отвечающие требованиям вашей защиты протокола HTTP.

Применение HTTP-фильтра основано на правилах, можно использовать различные параметры HTTP-фильтрации в каждом правиле, разрешающем исходящие HTTP-коммуникации. Такой подход обеспечивает тщательный, хорошо настраиваемый контроль над типами соединений, которые могут проходить по HTTP-каналу.

В текущий раздел включены следующие темы:

- обзор установочных параметров HTTP-фильтра защиты;
- пример политик HTTP-фильтра защиты;

Обзор установочных параметров HTTP-фильтра защиты

HTTP-фильтр защиты содержит ряд вкладок, позволяющих, основываясь на правилах, установить строгий контроль над типами HTTP-сообщений, которым разрешен проход через брандмауэр ISA. Конфигурирование HTTP-фильтра защиты выполняется на следующих вкладках:

- General (Общие);
- Methods (Методы);
- Extensions (Расширения);

- Headers (Заголовки);
- Signatures (Подписи).

Вкладка General

На вкладке General (Общие) можно настроить следующие параметры:

- максимальную длину заголовков;
- размер полезных данных;
- максимальную длину URL-адреса;
- проверку нормализации;
- удаление символов, использующих старшие биты;
- блокирование ответов, содержащих исполняемые файлы ОС Windows.

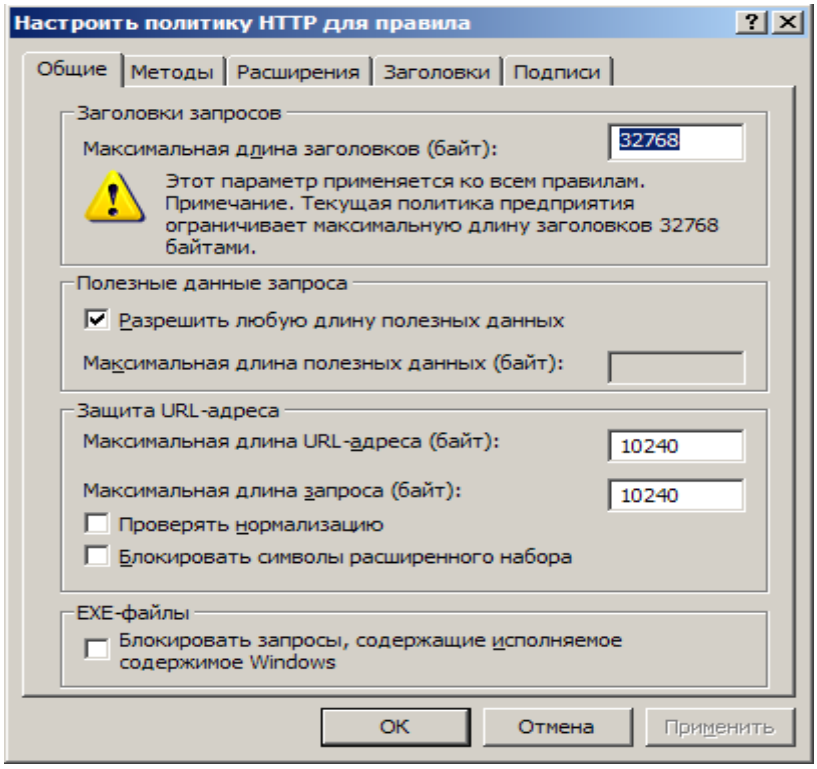


Рис. 1. Вкладка «Общие (General)»

Параметр **Maximum headers length (bytes) (Максимальная длина заголовков, в байтах)** позволяет задать максимальную длину всех заголовков, включенных в запрос соединения по HTTP-протоколу. Он применяется ко всем

правилам, использующим HTTP-фильтр защиты. Этот установочный параметр защищает от атак, пытающихся создать переполнение буферов Web-сайта за счет отправки на Web-сервер избыточно длинных заголовков.

В области **Request Pay load (Полезные данные запроса)** можно разрешить любой размер полезных данных или задать конкретную максимальную длину для них. Полезные данные – это часть HTTP-сообщения, не относящаяся к HTTP-заголовку или структуре команды. Например, если разрешить пользователям посылать данные на Web-сайт (бланк заказа или обсуждение для форума), то можно установить предельную длину для этих отправлений, сбросив флажок Allow any payload length (Разрешена любая длина полезных данных) и введя настраиваемое значение в текстовое поле Maximum payload length (bytes) (Максимальная длина полезных данных, в байтах).

В области URL Protection (Защита URL-адреса) есть несколько параметров. Вариант **Maximum URL length (bytes) (Максимальная длина URL-адреса, в байтах)** позволяет задать максимальную длину URL-адреса, который пользователь может переслать через брандмауэр, выполняя запрос к Web-сайту через брандмауэр. Злонамеренные программы могут посылать избыточно длинные URL-адреса, пытаясь создать переполнение буфера или другой тип атаки на Web-сервере. Значение по умолчанию – 10240, но его можно изменить в соответствии с требованиями сайтов. Параметр **Maximum query length (bytes) (Максимальная длина запроса, в байтах)** позволяет задать максимальную длину доли запроса в URL-адресе. Эта часть URL-адреса появляется после вопросительного знака (?) в URL-запросе. Значение, установленное по умолчанию, – 10240, но его можно изменить в соответствии с определенными требованиями. Имейте в виду, что Maximum URL length (Максимальная длина URL-адреса) должна быть больше Maximum query length (Максимальная длина запроса), поскольку запрос – это только часть URL-адреса.

Параметр **Verify normalization (Проверка нормализации)** также включен в область URL Protection. Нормализация – процесс декодирования так называемых «управляющих» («escaped») символов. Web-серверы могут получать запросы, закодированные с помощью таких символов. Один из наиболее распространенных примеров – наличие пробела в URL-адресе, таком как http://msfirewall.org/Dir%20One/default%20file.htm. Символьная комбинация %20 – это escape-символ, представляющий пробел. Проблема заключается в том, что злоумышленники могут закодировать символ «%» и выполнить так называемые дважды кодированные (double encoded) запросы. Двойное кодирование может применяться в атаках на Web-серверы. Когда выбран параметр Verify normalization, HTTP-фильтр защиты нормализует или декодирует запрос дважды. Если запрос после первого и второго декодирования не один и тот же, HTTP-фильтр защиты отбросит его. Это действие защищает от атак «двойного кодирования». Вариант **Block high bit characters (Блокировать символы расширенного набора)** позволяет удалять HTTP-запросы, включающие URL-адреса с символами, использующими старшие биты. Символы, для представления которых используются старшие биты, применяются во многих языках, использующих расширенные наборы символов, поэтому, если выяснится, что невозможно получить доступ к Web-сайтам, применяющим такие расширенные наборы символов в своих URL-адресах, следует сбросить этот флажок.

Параметр **Block responses containing Windows executable content (Блокировать запросы, содержащие исполняемые файлы Windows)** позволяет помешать пользователям пересылать исполняемые файлы Windows (такие как файлы с расширением .exe, но для обозначения исполняемых файлов Windows может быть использовано любое расширение файла). HTTP-фильтр защиты способен определить, является ли файл исполняемым файлом Windows, поскольку ответ будет начинаться с комбинации MZ. Это свойство может

оказаться очень полезным, если необходимо помешать пользователям загружать исполняемые файлы через брандмауэр ISA.

Вкладка Methods

Используя установочные параметры на вкладке Methods (Методы) можно управлять HTTP-методами (способами), применяемыми в правиле доступа. Предлагаются три варианта:

- разрешить все способы;
- разрешить только указанные способы;
- блокировать указанные способы (разрешить все остальные).

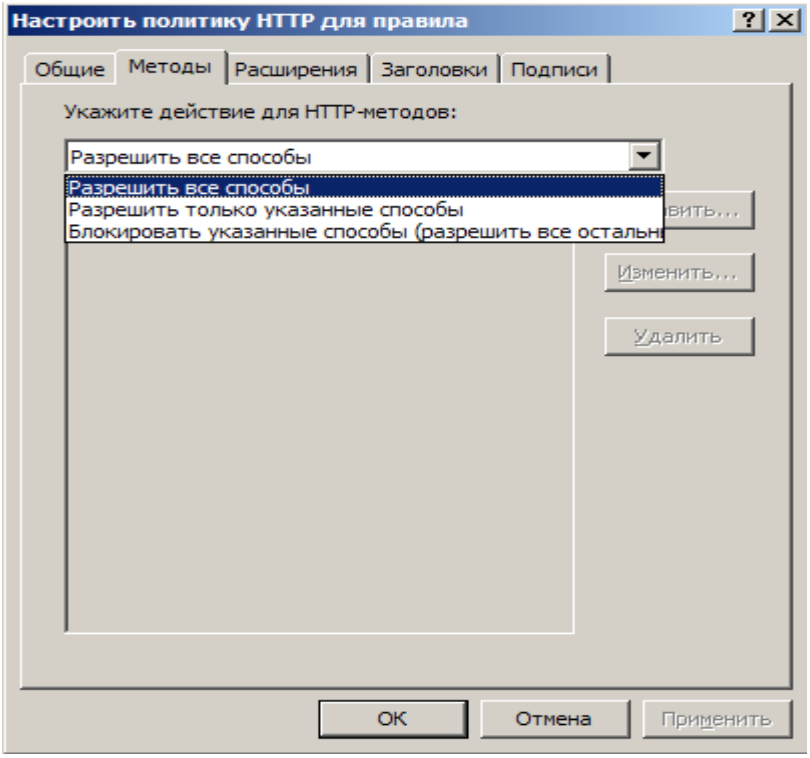


Рис. 2. Вкладка «Методы (Methods)»

HTTP-методы – это HTTP-команды, которые хосты могут посылать на Web-сервер для выполнения определенных действий, такие как GET, PUT и POST. Существуют и другие команды, с которыми вы можете быть незнакомы как администратор сети и брандмауэра, к ним можно отнести HEAD, SEARCH и CHECKOUT. Есть и узкоспециализированные методы, применяемые конкретными Web-приложениями, такие как Outlook Web Access. Вариант Allow

all methods (Разрешить все методы) позволит разрешить использование HTTP-методов в HTTP-соединении, устанавливаемом через брандмауэр ISA.

Вариант **Allow only specified methods (Разрешить все способы)** позволяет указать, какие именно методы разрешается пересылать через брандмауэр ISA.

Параметр **Block specified methods (allow all others) (блокировать указанные способы, разрешить все остальные)** позволяет разрешить применение всех методов за исключением заданных, которые следует запретить. Этот вариант наделяет пользователя несколько большими возможностями, даже если он не знает всех методов, которые могут потребоваться сайту, но может знать некоторые из тех, что определенно не нужны. Одним из примеров может быть метод POST. Если пользователям не разрешается посылать данные на Web-сайт, нет смысла разрешать метод POST, и его можно блокировать явным образом.

Если выбран параметр Allow only specified methods (Разрешить только указанные способы) или вариант Block specified methods (allow all others) (блокировать указанные способы, разрешить все остальные), необходимо щелкнуть мышью кнопку Add (Добавить) и ввести метод, который нужно разрешить или запретить. После нажатия кнопки Add (Добавить) на экране появляется диалоговое окно Method (Метод).

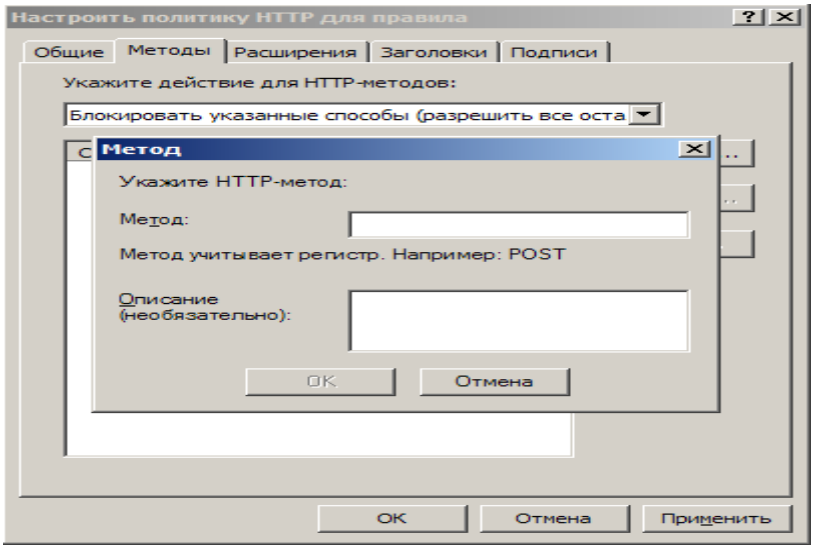


Рис. 3. Диалоговое окно «Метод»

В диалоговом окне Method (Метод) вводится имя метода в одноименное текстовое поле. Можно также добавить описание метода в текстовое поле Description (Описание). Оно поможет запомнить, что делает метод, а также окажет помощь пришедшему вам на смену специалисту, столкнувшемуся с необходимостью управления брандмауэром ISA и не знающему внутренней структуры набора команд HTTP-протокола.

Вкладка Extensions

На вкладке Extensions (Расширения) представлены следующие варианты:

- Allow all extensions (Разрешить все расширения);
- Allow only specified extensions (Разрешить только указанные расширения);
- Block specified extensions (allow all others) (Блокировать все указанные расширения, разрешить все остальные);
- Block requests containing ambiguous extensions (Блокировать запросы, содержащие неоднозначные расширения)

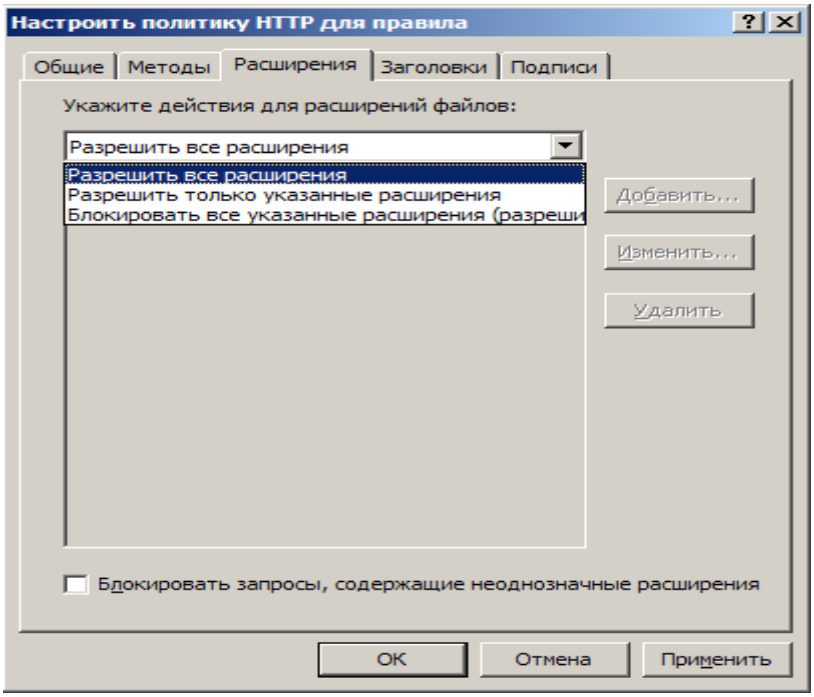


Рис. 4. Вкладка «Расширения (Extensions)»

Предоставляется возможность управлять расширениями файлов, которые можно запрашивать через брандмауэр ISA. Это крайне полезно, если нужно

запретить пользователям запросы файлов определенных типов через брандмауэр. Например, можно запретить пользователям доступ через брандмауэр ISA к файлам с расширениями .exe, .com, .zip и любыми другими.

Вариант **Allow all extensions (Разрешить все расширения)** позволяет настроить правило доступа или правило публикации Web-сервера для разрешения доступа пользователей, основанного на расширении файла, к файлам любого типа через брандмауэр ISA. Выбрав вариант **Allow only specified extensions (Разрешить только указанные расширения)**, можно задать определенные расширения файлов, к которым возможен доступ пользователей через брандмауэр ISA. Вариант **Block specified extensions (allow all others) (Блокировать все указанные расширения, разрешить все остальные)** предоставляет возможность запретить заданные расширения файлов, которые вы считаете опасными.

Если выбран вариант Allow only specified extensions (Запретить указанные расширения, разрешить все остальные) или Block specified extensions (allow all others) (Блокировать все указанные расширения, разрешить все остальные), необходимо щелкнуть мышью кнопку Add (Добавить) и ввести расширения, которые вы хотите разрешить или запретить.

После нажатия мышью кнопки Add (Добавить) на экране появится диалоговое окно Extension (Расширение). Введите расширение в текстовое поле Extension (Расширение). Например, если следует запретить доступ к файлам с расширением .exe, введите .exe. Есть возможность ввести описание в необязательное текстовое поле Description (optional) (Описание, необязательно). Щелкните мышью кнопку ОК для сохранения добавленного расширения.

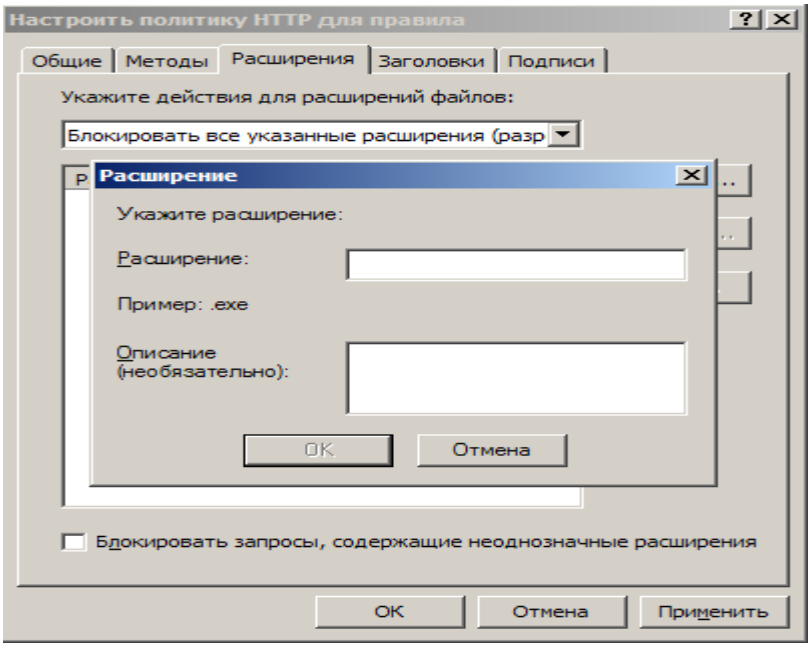


Рис. 5. Диалоговое окно «Расширение (Extension)»

Вкладка Headers

На вкладке Headers (Заголовки) представлены следующие параметры:

- Allow all headers except the following (Разрешить все заголовки, кроме следующих);
- Server header (Заголовок сервера);
- Via header (Заголовок VIA).

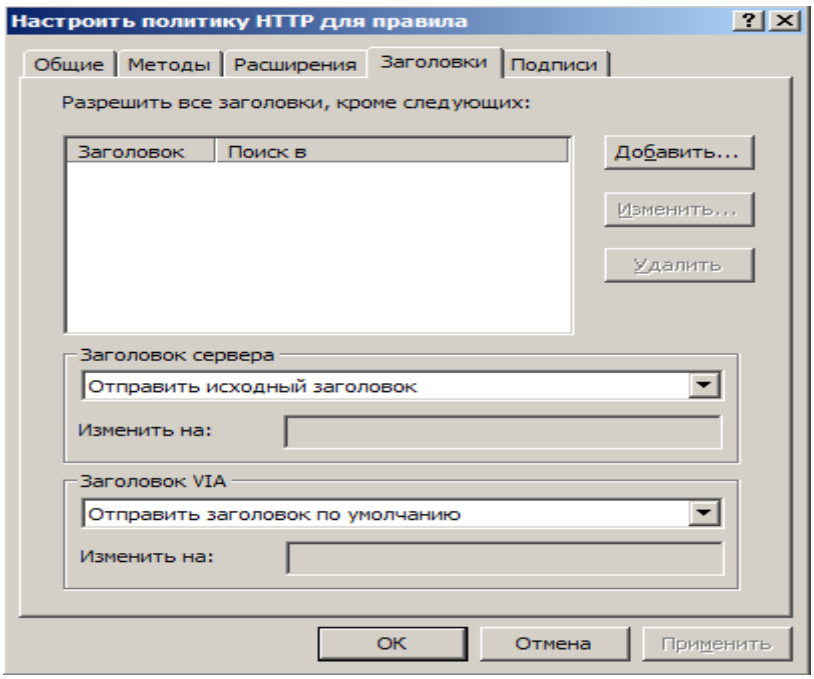


Рис. 6. Вкладка «Заголовки (Headers)»

HTTP-заголовок содержит характерную для HTTP-сообщения информацию, которая включается в HTTP-запросы, сделанные Web-клиентом (таким как Web-обозреватель), и HTTP-ответы, посылаемые Web-сервером обратно Web-клиенту. Эти заголовки выполняют многочисленные функции, такие как определение статуса и состояния HTTP-коммуникаций и других характеристик HTTP-сеанса связи.

К общим HTTP-заголовкам относятся следующие:

- размер содержимого (Content-length);
- директива (Pragma);
- пользователь-агент (User-Agent);
- принятое кодирование (Accept-Encoding).

Можно принимать все HTTP-заголовки или запретить конкретные, заданные HTTP-заголовки. Существуют определенные HTTP-заголовки, которые рекомендуется блокировать всегда, например такие, как заголовок P2P-Agent, используемый многими одноранговыми (peer-to-peer) приложениями. Если нужно запретить конкретный HTTP-заголовок, щелкните мышью кнопку Add (Добавить).

В диалоговом окне Header (Заголовок) выберите вариант Request headers (Заголовки запросов) или вариант Response headers (Заголовки ответов) в раскрывающемся списке Search in (Искать в). Введите HTTP-заголовок, который вы хотите запретить, в текстовое поле HTTP header (HTTP-заголовок). Щелкните мышью кнопку ОК.

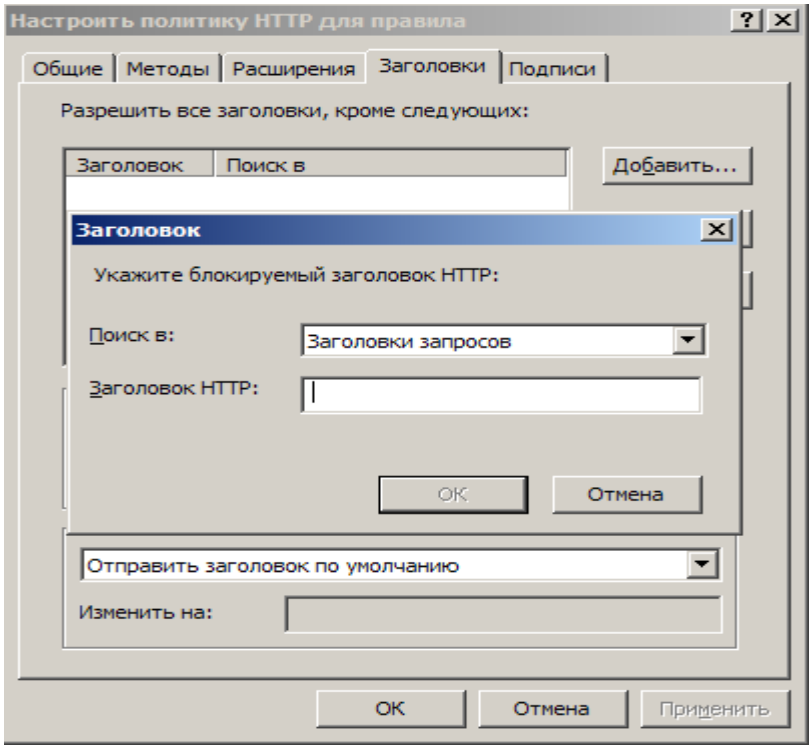


Рис.7. Диалоговое окно «Заголовок»

Можно настроить заголовок сервера, возвращаемый в HTTP-ответах, выбрав вариант Server Header (Заголовок сервера) в раскрывающемся списке. Заголовок сервера – это HTTP-заголовок, посылаемый Web-сервером обратно Web-клиенту и информирующий последнего о типе Web-сервера, с которым соединяется клиент. Злоумышленники могут использовать эту информацию для атаки Web-сервера. Имеются следующие возможности:

- отправить исходный заголовок;
- вырезать заголовок из ответа;
- изменить заголовок в ответе.

Вариант **Send original header (Отправить исходный заголовок)** позволяет передать неизмененным заголовок, посланный Web-сервером. Вариант **Strip header from response (Вырезать заголовок из ответа)** разрешает брандмауэру ISA убрать заголовок сервера, а вариант **Modify header in response (Изменить заголовок в ответе)** позволяет изменить заголовок. Следует изменять заголовок, чтобы запутать злоумышленников. Поскольку Web-клиенты

не требуют этот заголовок, можно изменить его на Private, CompanyName или другое понравившееся вам имя.

Перечисленные варианты помогут помешать злоумышленникам (или, по крайней мере, задержать их). Им придется потратить больше усилий и использовать альтернативные методы для просмотра идентификационной информации («fingerprint») вашего Web-сервера.

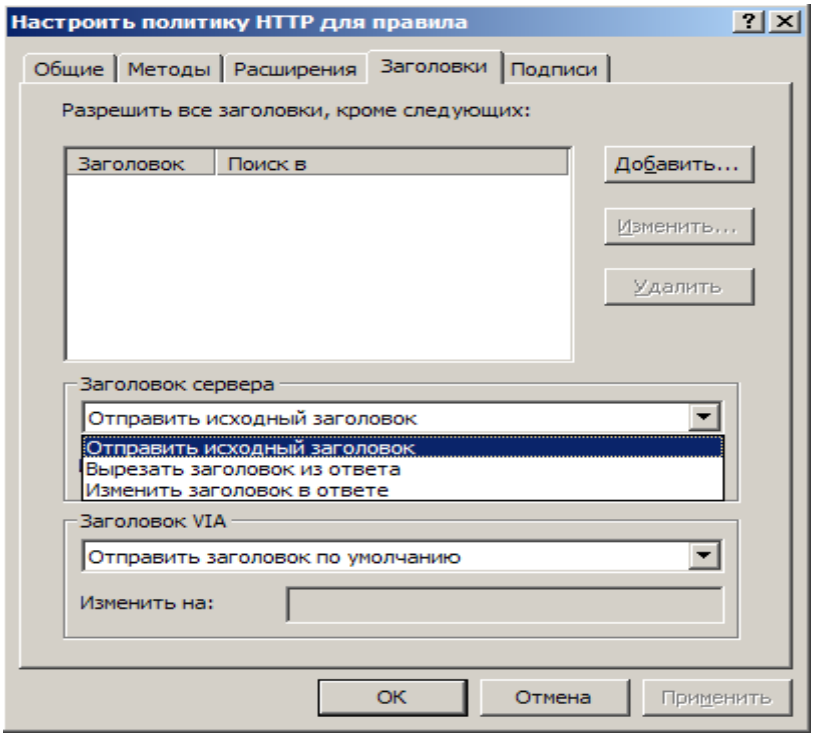


Рис.8. Параметр «Заголовок сервера (Server Header)»

Параметр Via Header (Маршрутный заголовок) позволяет управлять маршрутным заголовком, посылаемым Web-клиенту. Если между клиентом и Web-сервером располагаются серверы Web-прокси, то сервер Web-прокси вставляет маршрутный заголовок в HTTP-сообщение, информирующий клиента о том, что запрос был обработан сервером Web-прокси в процессе передачи. Каждый сервер Web-прокси на пути запроса может добавить свой собственный маршрутный заголовок, и каждый отправитель на пути следования ответа удаляет свой маршрутный заголовок и пересылает ответ на сервер, заданный в следующем маршрутном заголовке, хранящемся в «стеке» маршрутных заголовков. Параметры маршрутного заголовка позволяют изменить имя

брандмауэра ISA, включенное в его собственный маршрутный заголовок, или скрыть это имя. Установка по умолчанию на брандмауэре ISA – включать имя компьютера, на котором размещен брандмауэр, в маршрутный заголовок.

Имеются два возможных варианта:

- послать заголовок, установленный по умолчанию;
- изменить заголовок в запросе и ответе.

Вариант **Send default header (Отправить заголовок, установленный по умолчанию)** оставляет маршрутный заголовок без изменений. Вариант **Modify header in request and response (Изменить заголовок в запросе и ответе)** позволяет изменить имя, включенное в маршрутный заголовок, вставляемый вашим брандмауэром ISA. Советуем изменять его, чтобы скрыть действительное имя вашего брандмауэра ISA и тем самым помешать злоумышленникам определить настоящее имя компьютера вашего брандмауэра ISA.

Введите другой маршрутный заголовок в текстовое поле Change To (Заменить на).

Вкладка Signatures

На вкладке Signatures (Подписи) можно управлять доступом через брандмауэр ISA с помощью HTTP-сигнатур или подписей, созданных вами. Эти сигнатуры представляют собой строки, содержащиеся в следующих компонентах HTTP-сообщения:

- URL-адресе запроса;
- заголовке запроса;
- тексте запроса;
- заголовке ответа;
- тексте ответа.

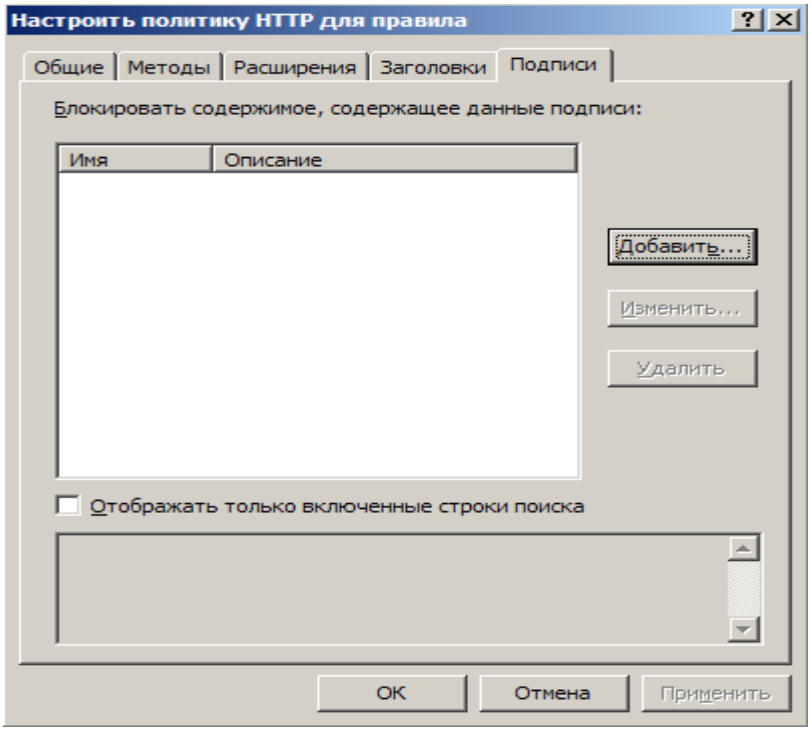


Рис. 9. Вкладка «Подписи (Signatures)»

Получить доступ к диалоговому окну Signatures (Сигнатуры) можно, щелкнув мышью кнопку Add (Добавить).

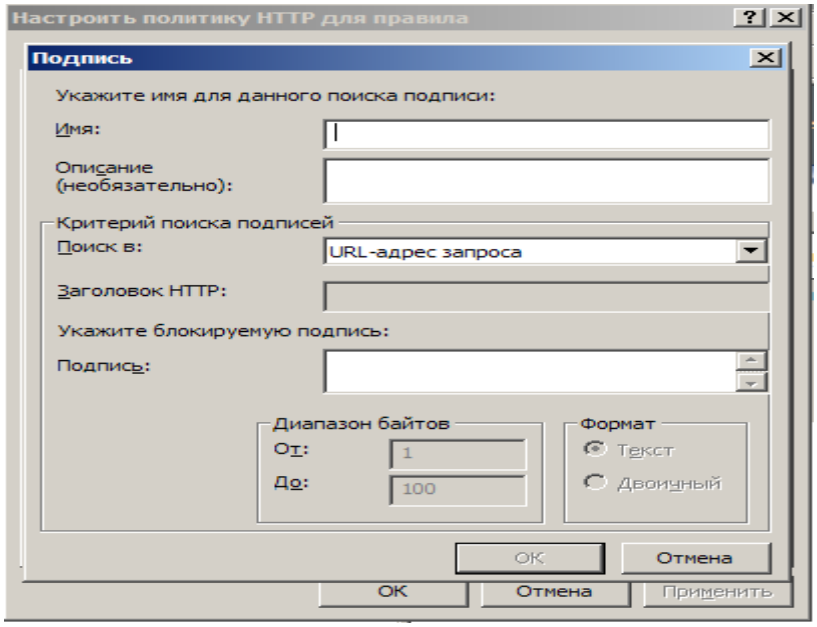


Рис.10. Диалоговое окно «Подпись (Signature)»

В диалоговом окне Signature (Сигнатура) введите имя сигнатуры в текстовое поле Name (Имя) и описание сигнатуры в текстовое поле Description

(Описание). Последнее особенно полезно для того, чтобы знать о назначении и смысле этой сигнатуры.

В раскрывающемся списке Search in (Поиск в) укажите, где брандмауэру ISA искать заданную строку. Возможны следующие варианты:

- Request URL (URL-адрес запроса). Выбор этого варианта позволяет ввести строку, обнаружение которой в URL-адресе запроса Web-клиента вызовет блокирование соединения. Например, если нужно предотвратить любые запросы к сайтам, содержащим строку “Kazaa” в URL-адресе, включенном в запрос Web-клиента, введите “Kazaa” в текстовое поле Signature (Подпись).
- Request headers (Заголовки запроса). При выборе этого варианта введите в текстовое поле HTTP header (Заголовок HTTP) конкретный HTTP-заголовок, который должен проверять брандмауэр ISA, и в текстовое поле Signature – строку в заголовке, которую необходимо блокировать. Например, если необходимо блокировать приложения P2P (одноранговые) файлообменной сети eDonkey, можно выбрать этот вариант, а затем User-Agent (Пользователь-агент) в текстовом поле HTTP header. Далее в текстовое поле Signature (Подпись) введите ed2k. Обратите внимание на то, что этот вариант предоставляет более тонкое управление, чем на вкладке Headers (Заголовки), – простая блокировка заголовков. Если запретить конкретный заголовок на вкладке Headers (Заголовки), то будут блокироваться все HTTP-сообщения, использующие заданный заголовок. Создав сигнатуру, встроенную в указанный заголовок, можно разрешить этот заголовок во всех сообщениях, не содержащих строку, которая введена как сигнатура.
- Request body (Текст запроса). Можно блокировать HTTP-сообщения, основываясь на теле Web-запроса, информации, не входящей ни в

HTTP-команды, ни в заголовки. Несмотря на то, что это очень мощная функциональная возможность, она может потреблять большой объем ресурсов на компьютере брандмауэра ISA. По этой причине следует определить диапазон проверяемых брандмауэром ISA байтов в текстовых полях From (От) и To (До) в области вкладки Byte range (Диапазон, в байтах).

- Response headers (Заголовки ответов). Если выбран этот вариант, то вводится конкретный HTTP-заголовок, который следует блокировать, основываясь на HTTP-ответе, возвращенном Web-сервером. Введите этот заголовок в текстовое поле HTTP header, а строку, включенную в HTTP-заголовок, – в текстовое поле Signature.
- Response body (Текст ответа). Этот вариант функционирует так же, как вариант Request body (Текст запроса), за исключением того, что он применяется к содержимому, возвращаемому Web-клиенту с Web-сервера. Например, если нужно блокировать Web-страницы, содержащие конкретные строки, которые определяются как опасные или неподходящие, можно создать сигнатуру для блокирования этих строк. Вспомните об этом, узнав о новейшей Web-ориентированной атаке, и создайте сигнатуру, блокирующую соединения, организующие подобные атаки.

Таблица 2. Пример политики HTTPS-фильтра

Вкладка	Параметр
General (Общие)	• Максимальная длина заголовка – 32768 • Установлен флажок «Разрешать любую длину полезных даных» • Максимальная длина URL-

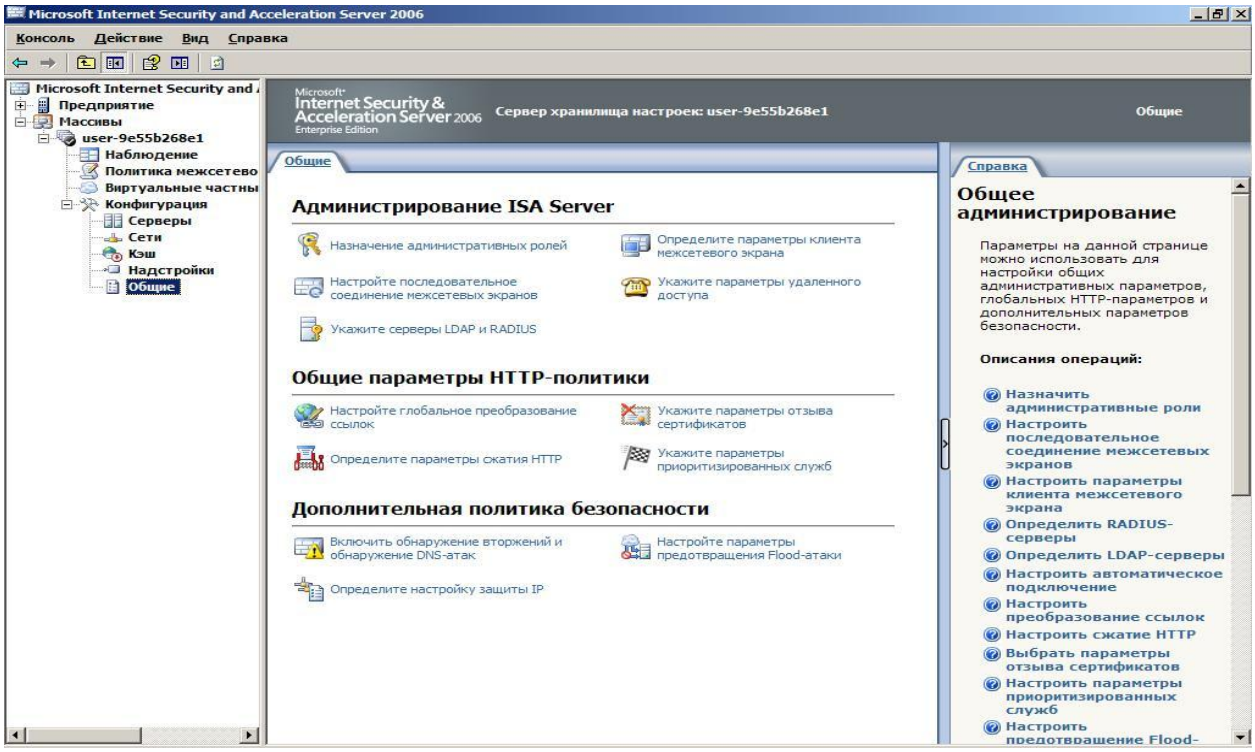
	адреса – 260 • Максимальная длина запроса – 4096 • Установлен флажок «Проверять нормализацию» • Сброшен флажок «Блокировать символы расширенного набора»
Methods (Методы)	• Разрешить только указанные способы GET HEAD POST
Extensions (Расширения)	• Блокировать все указанные расширения, разрешить остальные .exe, .bat, .cmd, .com, .htw, .ida, .idq, .htr, .idc, .shtm, .shtml, .stm, .printer, .ini, .log, .pol, .dat
Headers (Заголовки)	Никаких изменений по сравнению с установками по умолчанию
Signatures (Подписи) (Request URL, URL-адрес запроса)	Блокировать содержимое, содержащее эти сигнатуры: ./

	\ % $

Дополнительная политика безопасности

Обнаружение и предотвращение типовых атак

Получить доступ к диалоговому окну «Обнаружение вторжений» можно, открыв консоль управления Microsoft Internet Security and Acceleration Server 2006, раскрыв окно, связанное с именем сервера, а затем раскрыв узел «Конфигурация». Щелкните кнопкой узел «Общие».



В узле «Общие» щелкните кнопкой мыши ссылку «Включить обнаружение вторжений и обнаружение DNS-атак». На экране появится вкладка «Распространенные атаки».

На вкладке «Распространенные атаки» установите флажок «Включить обнаружение вторжений». Установите флажки, расположенные слева от тех типов атак, которые необходимо предотвращать. Если включается атака типа

«Сканирование портов», введите значения в поля «Стандартные порты» и «Все порты»

Можно отключить регистрацию пакетов, отвергнутых фильтром обнаружения вторжения, сбросив флажок «Регистрировать отброшенные пакеты».

Атаки отказов от обслуживания

Атаки отказов от обслуживания (Denial-of-service, DoS-атака) особенно популярны у интернет-хакеров, стремящихся нарушить сетевые операции. Хотя эти атаки не разрушают и не крадут данные, как делают некоторые атаки других типов, цель злоумышленника, запускающего атаку DoS, вывести сеть из строя и вызвать отказ от обслуживания ее законных пользователей. Атаки отказов от обслуживания легко инициировать, программное обеспечение готово и доступно на Web-сайтах хакеров и в группах новостей краденого программного обеспечения (warez newsgroups), что позволяет любому человеку, имеющему небольшой технический навык или вообще не имеющему таковых, запустить DoS-атаку.

В феврале 2000 г. массовые DoS-атаки парализовали работу самых крупных сайтов, включая Yahoo.com и Buy.com.

Цель DoS-атаки – сделать сеть недоступной за счет типа или объема сетевого трафика, который приведет к аварийному сбою серверов, переполнению маршрутизаторов или в противном случае нарушит нормальную работу сетевых устройств. Отказ от обслуживания достигается связыванием сетевых ресурсов, например за счет переполнения CPU (центрального процессора) или объема памяти. В других случаях определенный пользователь/компьютер может стать объектом DoS-атак, «подвешивающих» компьютер и требующих его перезагрузки.

ПРИМЕЧАНИЕ

В сообществе компьютерной безопасности DoS-атаки иногда называют атаками «nuke» (ядерными).

Распределенная атака отказа от обслуживания

Распределенные атаки отказов от обслуживания (DDoS) используют промежуточные компьютеры, называемые агентами, на которых предварительно тайно установлены программы, именуемые зомби. Злоумышленник удаленно активизирует программы-зомби, вызывая на промежуточных компьютерах (которых может быть сотни и даже тысячи) одновременный запуск действительной атаки. Поскольку атака приходит с компьютеров, выполняющих программы-зомби и расположенных в сетях по всему миру, хакер способен скрыть истинный источник атаки.

К средствам распределенных атак отказов от обслуживания относятся TFN (Tribe FloodNet), TFN2K, Trinoo и Stacheldraht (German for «barbed wire» – «колючая проволока»). В то время как ранние версии этих средств поражали операционные системы UNIX и Solaris, программа TFN2K уже может выполняться как в ОС UNIX, так и в Windows.

Важно отметить, что распределенные атаки отказов от обслуживания можно трактовать двояко. Сеть может быть целью DoS-атаки, вызывающей сбои в работе серверов и нарушающей входящий и исходящий трафик, и компьютеры сети могут использоваться как «невинные посредники» (innocent middlemen) для запуска DoS-атаки, направленной против другой сети или сайта.

SYN-атака/LAND-атака

SYN-атаки используют «трехстороннее квитирование» («three-way handshake») по TCP-протоколу – процесс, с помощью которого сеанс связи устанавливается между двумя компьютерами. Поскольку TCP-протокол (в отличие от UDP-протокола) ориентирован на соединение, сеанс или прямой канал связи один-к-одному устанавливается прежде, чем посылаются данные. Компьютер клиента инициирует соединение с сервером (компьютер, к ресурсам которого он хочет получить доступ).

Квитирование включает следующие шаги

Компьютер клиента посылает сегмент SYN (запрос синхронизации). Сервер отправляет сообщение ACK (acknowledge, подтверждение), подтверждающее получение запроса с машины клиента, отправленного на шаге 1, и SYN, свой собственный запрос синхронизации. Компьютеры клиента и сервера должны синхронизировать номера последовательности друг друга. Клиент отправляет сообщение ACK обратно серверу, подтверждая получение запроса сервера на синхронизацию. Когда оба компьютера подтвердили запросы друг друга, рукопожатие успешно завершается и между ними устанавливается соединение.

Было приведено описание нормального течения процесса. SYN-атака использует его для лавинной загрузки выбранной в качестве жертвы атаки системы многочисленными пакетами синхронизации, имеющими неверные IP-адреса источников, которые заставляют систему отвечать с помощью сообщений SYN/ACK. Проблема возникает, когда система, ожидающая сообщение ACK от клиента, обычно приходящее в ответ на ее сообщение SYN/ACK, помещает ожидаемые сообщения SYN/ACK в очередь. Дело в том, что очередь может хранить ограниченное число таких сообщений. Когда она заполнена, все последующие приходящие пакеты SYN будут игнорироваться. Для удаления сообщения SYN/ACK из очереди необходимо, чтобы вернулось сообщение ACK от клиента или было превышено допустимое время ожидания и завершился процесс трехстороннего квитирования.

Поскольку исходные IP-адреса пакетов SYN, посланных злоумышленником, неверны, сообщения ACK, ожидаемые сервером, никогда не придут. Очередь остается заполненной, и нет места для обработки корректных запросов синхронизации. Таким образом, законным пользователям, пытающимся установить соединения с сервером, будет отказано в обслуживании.

LAND-атака (атака с обратной адресацией) – это разновидность SYN-атаки. В LAND-атаке вместо отправки пакетов синхронизации с несуществующими IP-адресами вся лавина пакетов посылается на один ложный IP-адрес подтверждения (spoof IP address), совпадающий с адресом атакуемого компьютера.

LAND-атака может быть предотвращена за счет отфильтровывания входящих пакетов, в которых IP-адреса источника совпадают с адресами компьютеров внутренней сети. У брандмауэра ISA Server есть заранее установленная функциональная возможность обнаружения вторжения, позволяющая выявить попытки LAND-атак и настроить сигнальные оповещения (Alerts), уведомляющие об обнаружении такой атаки.

Ping of Death

Другой тип DoS-атаки, на обнаружение которой можно настроить ISA Server, – так называемый «Ping смерти» (также известный как «пингование большими пакетами»). Атака «Ping смерти» проводится созданием IP-пакета, большего чем 65 536 байтов, максимума, разрешенного IP-спецификацией (иногда такой пакет называют «пакетом-убийцей»). Он может вызвать аварийный сбой, зависание или перезагрузку системы.

Брандмауэр ISA позволяет включить специальное обнаружение атак «Ping смерти».

Teardrop

Атака Teardrop действует несколько иначе, чем «Ping смерти», но с теми же результатами. Программа Teardrop создает IP-фрагменты, части IP-пакета, на которые он может делиться, путешествуя по Интернету. Проблема заключается в том, что поля смещения (offset fields) в этих фрагментах, которые должны отображать величину

порции исходного пакета (в байтах), содержащейся в фрагменте, накладываются друг на друга.

Когда компьютер-адресат попытается повторно собрать эти пакеты, он не сможет этого сделать и аварийно завершит работу, зависнет или выполнит перезагрузку.

У этого типа атаки есть следующие варианты:

- NewTear;
- Teardrop2;
- SynDrop;
- Boink.

Все эти программы создают тот или иной сорт наложения фрагментов.

Ping-лавина (ICMP-лавина)

Ping-лавина (ping flood), или ICMP-лавина (ICMP flood) (Internet Control Message Protocol, протокол управляющих сообщений в сети Интернет), – средство «связывания» определенной машины клиента. Оно создается за счет отправки злоумышленником большого количества ping-пакетов (ICMP-пакетов эхо-запросов) программному обеспечению интерфейса Winsock или набора телефонного номера. Эти действия мешают компьютеру-клиенту отвечать серверу на запросы ping-активности и в конечном итоге приводят к разрыву соединения по истечении допустимого времени ожидания ответа. Симптомом Ping-переполнения может служить невероятная активность модема, о чем свидетельствуют его сигнальные лампочки. Иногда этот тип атаки называют ping storm (ping-шторм).

К ping-шторму относится и fraggle-атака («осколочная граната»). Используя ложный IP-адрес подтверждения (spoofed IP address), адрес компьютера-жертвы, злоумышленник посылает ping-пакеты в подсеть, заставляя все компьютеры подсети отвечать по ложному адресу подтверждения, и заваливает его сообщениями эхо-ответов.

Smurf-атака

Smurf-атака – это разновидность атаки «brute force» (атаки грубой силой), использующая тот же метод, что и ping-лавина, но направляющая лавину ICMP-пакетов эхо-запросов на маршрутизатор сети. Адресом назначения ping-пакетов в этом случае служит широковещательный адрес сети, вынуждающий маршрутизатор рассылать пакет всем компьютерам сети или ее сегмента. Это может привести к большому объему сетевого трафика, если имеется много компьютеров-хостов, способных создать перегрузку, вызывающую отказ от обслуживания законных пользователей.

ПРИМЕЧАНИЕ

Широковещательный адрес обычно в идентификаторе хоста представляется всеми единицами. Это означает, что, например, в сети класса C 192.168.1.0 широковещательный адрес будет 192.168.1.255 (255 в десятичной системе счисления и 1111111 — в двоичной), а идентификатор хоста в сети класса C представляется последним или z-октетом. Сообщение, посланное на широковещательный адрес, немедленно отправляется на все хосты сети.

Самая коварная форма – применение Smurf-атакующим ложного IP-адреса подтверждения получения ping-пакетов. В этом случае и сеть, в которую посланы пакеты, и сеть, которой принадлежит IP-адрес ложного источника будут перегружены трафиком. Сеть, к которой относится адрес ложного источника, будет наводнена ответами на команду ping, когда все хосты, которым послана эта команда, ответят на эхо-запрос эхо-ответом.

Smurf-атаки могут нанести гораздо больший ущерб, чем некоторые другие разновидности DoS-атак, такие как SYN-лавины. Последние воздействуют только на способность других компьютеров устанавливать соединения по TCP-протоколу с атакованным сервером, а Smurf-атака может полностью нарушить работу ISP (провайдер интернет-услуг) на несколько минут или часов. Это объясняется тем, что один злоумышленник может легко

отправить 40 или 50 ping-пакетов в секунду даже с помощью медленного модемного соединения. Поскольку каждый запрос пересылается каждому компьютеру в сети-адресате, число ответов в секунду равно от 40 до 50, помноженным на число компьютеров в сети, т. е. может достигать сотен или тысяч. Этих данных достаточно, чтобы перегрузить даже канал T-1.

Один из способов предотвращения Smurf-атаки на сеть как цель широковещательной рассылки – отключение возможности передачи широковещательного трафика на маршрутизатор. Большинство маршрутизаторов позволяют сделать это. Для того чтобы помешать сети стать жертвой, IP-адрес который используется для ложного подтверждения, необходимо конфигурировать брандмауэр для отфильтровывания входящих ping-пакетов.

UDP-бомба, или UDP-шторм

Злоумышленник может применить протокол пользовательских дейтаграмм (User Datagram Protocol, UDP) и один из нескольких сервисов, формирующих эхо-пакеты на адресатах, для создания сетевой перегрузки и отказов от обслуживания за счет генерации лавины UDP-пакетов между двумя системами назначения. Например, генерирующий символы (chargen) UDP-сервис на первом компьютере, служащий тестирующим средством, которое создает последовательность символов для каждого полученного им пакета, посылает пакеты на эхо-сервис UDP другой системы, который формирует эхо-ответ на каждый полученный символ. С помощью этих тестирующих средств бесконечный поток эхо-символов пересылается в обоих направлениях между двумя системами, создавая перегрузку сети. Иногда этот тип атаки называют штормом UDP-пакетов (UDP packet storm).

Помимо эхо-порта 7 злоумышленник может использовать порт 17 сервиса quote of the day (quotd) или порт 13 сервиса daytime. Эти сервисы также создают эхо-ответы на получаемые ими пакеты. Символы, сгенерированные UDP-сервисом, поступают на порт 19.

Отключение ненужных UDP-сервисов на каждом компьютере (особенно упомянутых ранее) или применение брандмауэра для отфильтровывания этих портов/ сервисов защитит от атаки этого типа.

UDP-атака Snork

Snork-атака подобна UDP-бомбе. В ней применяется UDP-блок, содержащий порт источника 7 (эхо) или 19 (генерация символов) и порт адресата 135 (средства адресации (location service) фирмы Microsoft). Результат аналогичный – лавина ненужных передач, способных снизить производительность или вызвать аварийный сбой вовлеченных систем.

Атака WinNuke (атака Windows Out-of-Band)

Атака передачи срочных данных (out-of-band, OOB), иногда называемая Windows OOB bug, использует в своих интересах уязвимость сетей Microsoft. Программа WinNuke (и ее разновидности, такие как Sinnerz и Muerte) выполняет передачу экстренных данных, вызывающих аварийный сбой на компьютере-адресате. Работает она следующим образом: устанавливается соединение TCP/IP с IP-адресом адресата, использующее порт 139 (порт NetBIOS). Затем программа посылает данные, содержащие в заголовке пакета флаг MSG_OOB (или Urgent). Этот флаг заставляет интерфейс Winsock компьютера посылать данные, называемые экстренными или срочными (out-of-band data, OOB). На приеме Windows-сервер, адресат, ожидает указатель в пакете, ссылающийся на позицию завершения экстренных данных, за которой следуют обычные данные. Однако OOB-указатель в пакете, созданном программой WinNuke, ссылается на блок, за которым нет последующих данных.

Компьютер под управлением ОС Windows не знает, как обработать такую ситуацию и прерывает коммуникации в сети, и все последующие попытки пользователей связаться с ним закончатся отказом от их обслуживания. Атака WinNuke обычно требует перезагрузки атакованной системы для восстановления сетевых коммуникаций.

ОС Windows 95 и NT версий 3.5 1 и 4.0 уязвимы для атаки WinNuke, несмотря на установку исправлений, предоставленных фирмой Microsoft.

Операционные системы Windows 98/ME и Windows 2000/2003 не подвержены атакам WinNuke, брандмауэр ISA Server позволяет включить обнаружение попыток атак передачи срочных данных.

Атака Mail Bomb

Атака «почтовая бомба» (mail bomb) – средство переполнения почтового сервера, вызывающее остановку его функционирования и тем самым отказ от обслуживания пользователей. Это относительно простая разновидность атаки, выполняемая с помощью отправки большого массива сообщений электронной почты конкретному пользователю или системе. На хакерских сайтах в Интернете есть программы, позволяющие легко запустить почтовую бомбу, автоматически отправляя лавину сообщений электронной почты на заданный адрес и скрывая при этом авторство злоумышленника.

Разновидностью почтовой бомбы может служить программа, автоматически подписывающая компьютер-адресат на сотни и тысячи рассылок интернет-списков огромного объема, которые заполняют почтовый ящик пользователя и/или почтовый сервер. Бомбисты называют этот вид атаки загрузкой списков рассылки (list linking). К примерам таких программ относятся почтовые бомбы Unabomber, extreme Mail, Avalanche и Kaboom.

Справиться с повторяющимися почтовыми бомбами поможет блокирование с помощью пакетных фильтров трафика из сети, порождающей атаку. К сожалению, этот способ не годится для загрузки списков рассылки, поскольку адрес-источник скрыт, поток трафика приходит от почтовых рассылок списков, на которые жертва была подписана.

Сканирование и подмена адреса подтверждения

Термин сканер (scanner) в контексте сетевой безопасности означает программу, которая используется хакерами для удаленного определения открытых на данной системе и, следовательно, уязвимых для атаки TCP/UDP-

портов. Сканеры также применяются администраторами для выявления слабых мест в их собственных системах и устранения их, прежде чем эти уязвимости обнаружит злоумышленник. Сетевые диагностические средства, такие как известное Security Administrator's Tool for Analyzing Networks (SATAN, Средство автоматизированного контроля безопасности), утилита UNIX, включают развитые функциональные возможности сканирования портов.

Хорошая сканирующая программа может определить местонахождение компьютера-цели в Интернете (одного из уязвимых для атаки), определить, какие TCP/IP-сервисы выполняются на машине, и исследовать слабые места в защите этих сервисов.

ПРИМЕЧАНИЕ

Среди хакеров бытует мнение: «Хороший сканер портов стоит тысячи паролей».

Многие сканирующие программы можно найти в Интернете как свободно распространяемое программное обеспечение.

Сканирование портов

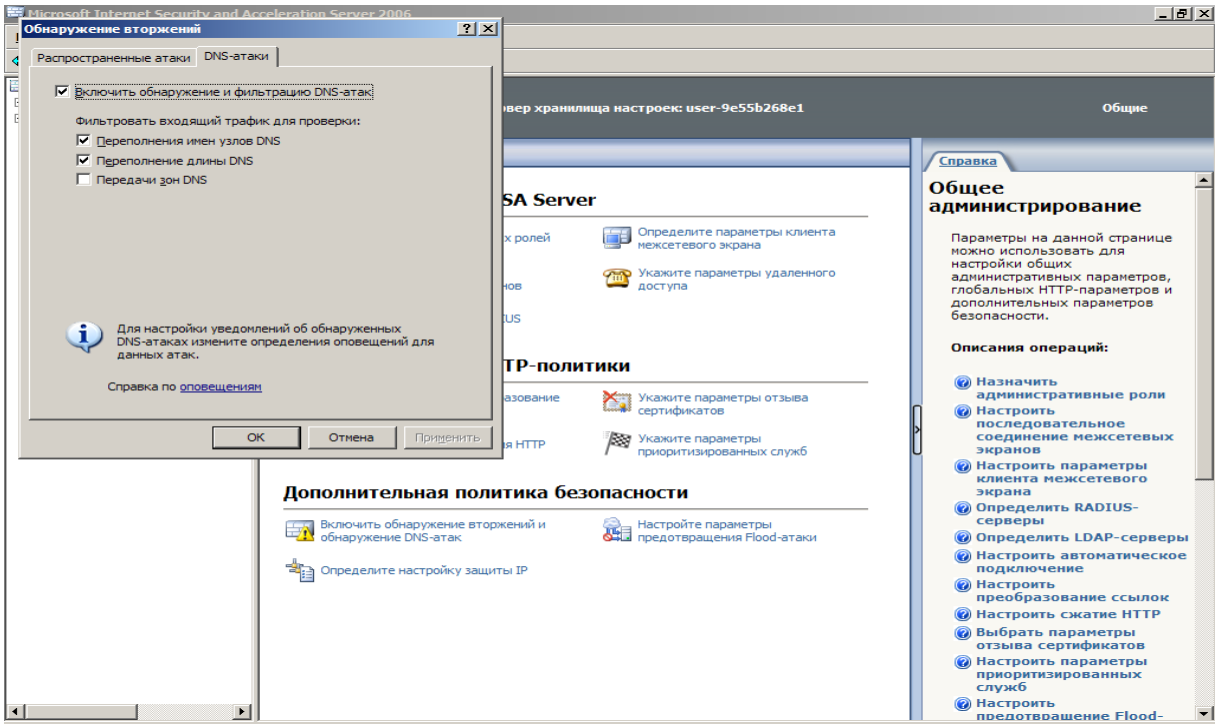
Сканирование портов – это процесс поиска «слушающих» TCP- или UDP-портов на компьютере или маршрутизаторе и получение от слушающих портов максимума сведений об устройстве. TCP- и UDP-сервисы применяют ряд популярных портов (well-known ports), которые широко опубликованы. Хакер использует эти сведения о широко используемых портах для экстраполяции информации.

Например, протокол Telnet обычно использует порт 23. Если хакер обнаружит, что этот порт открыт и ожидает запрос, он догадывается, что на машине, возможно, разрешен Telnet. Затем злоумышленник может попытаться проникнуть в систему, например, подобрав подходящий пароль в ходе атаки грубой силой (brute-force).

Обнаружение и предотвращение DNS-атак

DNS-фильтр брандмауэра ISA защищает DNS-серверы, опубликованные брандмауэром ISA с помощью правил публикования сервера (Server Publishing Rules). К странице конфигурирования предотвращения DNS-атак можно получить доступ в диалоговом окне «Обнаружение вторжений (Intrusion Detection)». Раскройте имя сервера, а затем раскройте узел «Конфигурирование (Configuration)». Щелкните мышью узел «Общие (General)».

На панели «Дополнительная политика безопасности (Details)» щелкните мышью ссылку «Включить обнаружение вторжений и обнаружение DNS-атак (Enable Intrusion Detection and DNS Attack Detection)». В диалоговом окне «Обнаружение вторжений (Intrusion Detection)» щелкните вкладку «DNS-атаки (DNS Attacks)». На вкладке «DNS-атаки (DNS Attacks)» установите флажок «Включить обнаружение и фильтрацию DNS-атак (Enable detection and filtering of DNS attacks)».



После того, как выявление атак включено, можно включить предотвращение и защиту от трех типов атак

- переполнение имен узлов DNS;

- переполнение длины DNS;
- передачи зон DNS.

Атаки типа переполнения имен узлов DNS и переполнения имен DNS представляют собой DoS-атаки. DoS-атаки DNS отличаются по размеру от DNS-запроса и от DNS-ответа, в которых вся пропускная способность сети занимается поддельными DNS-запросами. Для увеличения DNS-трафика атакующий использует DNS-серверы в качестве «усилителей».

Атакующий начинает посылать на каждый DNS-сервер небольшие DNS-запросы, которые содержат поддельный IP-адрес потенциальной «жертвы». Ответы, возвращаемые на небольшие запросы, довольно большие, поэтому, если одновременно имеется много возвращаемых ответов, канал связи перегружается и имеет место отказ от обслуживания (DoS-атака).

Одно из решений этой проблемы состоит в том, что администратор должен конфигурировать DNS-серверы так, чтобы они при получении DNS-запроса от подозрительного или неожиданного источника отвечали отрицательным ответом (refused response), который намного меньше, чем ответ утвердительный.

Конфигурирование брандмауэра ISA для быстрого старта

В этом руководстве по быстрой установке и конфигурированию брандмауэра используется сеть, к которой предъявляются следующие требования:

- в этой сети нет других серверов Windows;
- установка брандмауэра ISA Server 2004 производится на базе ОС Windows Server 2003;
- на компьютере установлена ОС Windows Server 2003 со стандартными настройками и нет другого программного обеспечения;
- на компьютере на базе Windows Server 2003 установлено два сетевых

адаптера. Одна сетевая интерфейсная карта соединена с внутренней сетью, а другая напрямую соединяется с Интернетом через сетевой маршрутизатор;

- компьютеры во внутренней сети настроены как DHCP-клиенты и будут использовать компьютер брандмауэра ISA Server 2004 в качестве своего DHCP-сервера;
- компьютер на базе ОС Windows Server 2003, на котором устанавливается программное обеспечение брандмауэра ISA Server 2004, не является членом домена Windows. Хотя позже рекомендуется сделать брандмауэр ISA членом домена, компьютер, на котором установлено программное обеспечение брандмауэра ISA, не обязательно должен быть членом домена. Это требование необходимо в данном руководстве, потому что предполагается, что в данной сети нет других серверов на базе Windows (но в ней могут быть серверы на базе Linux, Netware и других производителей).

Для быстрой установки и конфигурирования брандмауэра ISA нужно выполнить следующие действия:

- настроить сетевые интерфейсы брандмауэра ISA;
- установить и настроить DNS-сервер на компьютере брандмауэра ISA Server 2004;
- установить и настроить DHCP-сервер на компьютере брандмауэра ISA Server 2004;
- установить и настроить программное обеспечение ISA Server 2004;
- настроить компьютеры внутренней сети как DHCP-клиенты.

Конфигурирование сетевых интерфейсов брандмауэра ISA

У брандмауэра ISA должен быть хотя бы один внутренний сетевой интерфейс и один внешний сетевой интерфейс. Чтобы правильно настроить сетевые интерфейсы на брандмауэре ISA, нужно сделать следующее:

- назначить IP-адреса внутреннему и внешнему сетевым интерфейсам;
- назначить адрес DNS-сервера внутреннему интерфейсу брандмауэра ISA;
- поместить внутренний интерфейс в верх списка сетевых интерфейсов.

Назначение IP-адресов и DNS-сервера

Прежде всего, нужно назначить статические IP-адреса внутреннему и внешнему интерфейсу брандмауэра ISA. Для брандмауэра ISA также требуется адрес DNS-сервера, связанного с его внутренним интерфейсом. Для всех сетевых интерфейсов брандмауэра ISA не используется DHCP-сервер, потому что у внутреннего интерфейса должен всегда быть статический IP-адрес, а внешний интерфейс не поддерживает динамические адреса, поскольку он находится за маршрутизатором.

Если в учетной записи Интернета используется DHCP для присвоения общего адреса, то DSL или кабельный маршрутизатор могут получать и обновлять общий адрес. Кроме того, если для соединения с интернет-провайдером используется PPPoE (Point-to-Point Protocol over Ethernet, протокол «точка-точка» через Ethernet) или VPN, то маршрутизатор также может выполнять эти задачи.

Конфигурирование внутреннего сетевого интерфейса

Внутренний интерфейс должен иметь IP-адрес с того же идентификатора сети, что и другие компьютеры во внутренней сети. Этот адрес должен входить в адресный диапазон частной сети и не должен уже использоваться в сети.

Брандмауэр ISA будет настроен на использование адреса внутреннего интерфейса в качестве адреса DNS-сервера.

На брандмауэре ISA должен быть статический IP-адрес, связанный с его внутренним интерфейсом. На компьютере на базе ОС Windows Server 2003 нужно выполнить следующие действия:

- Правой кнопкой мыши щелкните My Network Places (Сетевое окружение) на рабочем столе и выберите в контекстном меню пункт Properties (Свойства).
- В окне Network Connections (Сетевые подключения) правой кнопкой мыши щелкните внутренний сетевой интерфейс и выберите в контекстном меню пункт Properties (Свойства).
- В диалоговом окне сетевого интерфейса Properties (Свойства) щелкните правой кнопкой мыши Internet Protocol (TCP/IP) (Протокол Интернета, TCP/IP) и выберите в контекстном меню пункт Properties (Свойства).
- В диалоговом окне Internet Protocol (TCP/IP) Properties (Свойства: Протокол Интернета, TCP/IP) выберите Use the following IP address (Использовать следующий IP-адрес). Введите IP-адрес внутреннего интерфейса в текстовое поле IP address (IP-адрес). Введите маску подсети для внутреннего интерфейса в текстовом поле Subnet mask (Маска подсети). Не вводите основной шлюз для внутреннего интерфейса.
- Выберите Use the following DNS server addresses (Использовать следующие адреса DNS-серверов). Введите IP-адрес внутреннего интерфейса брандмауэра ISA в текстовом поле Preferred DNS server (Предпочитаемый DNS-сервер). Это тот же адрес, который был введен в текстовое поле IP-address (IP-адрес) в п. 4.
- Нажмите кнопку ОК в диалоговом окне Internet Protocol (TCP/IP) Properties (Свойства: Протокол Интернета, TCP/IP).
- Нажмите кнопку ОК в диалоговом окне Properties (Свойства) внутреннего интерфейса.

ПРЕДУПРЕЖДЕНИЕ

Если во внутренней сети уже есть DNS-сервер, то следует настроить внутренний интерфейс брандмауэра ISA на использование IP-адреса DNS-сервера внутренней сети. Затем следует настроить DNS-сервер во внутренней сети так, чтобы он разрешал имена хостов в Интернете. DNS-сервер Microsoft автоматически разрешает имена хостов s Интернете, пока файл корневых ссылок заполняется корневыми серверами DNS Интернета. Стандартное правило доступа, создание которого описано в конце этого раздела, разрешает DNS-серверу исходящий доступ к DNS-серверам Интернета с целью разрешения имен хостов.

ПРЕДУПРЕЖДЕНИЕ

Никогда не указывайте адрес основного шлюза на внутреннем интерфейсе. У брандмауэра ISA может быть лишь один интерфейс с основным шлюзом. Даже если на одном брандмауэре ISA установлено 17 сетевых интерфейсных карт, только одна из них может быть настроена с адресом основного шлюза. Все другие шлюзы должны настраиваться в таблице маршрутизации Windows.

Конфигурирование внешнего сетевого интерфейса

Для того чтобы настроить информацию об IP-адресах на внешнем интерфейсе брандмауэра ISA, выполните следующие действия:

- Правой кнопкой мыши щелкните My Network Places (Сетевое окружение) на рабочем столе и в контекстном меню выберите пункт Properties (Свойства).
- В окне Network Connections (Сетевые подключения) правой кнопкой мыши щелкните внешний сетевой интерфейс и в контекстном меню выберите пункт Properties (Свойства).
- В диалоговом окне сетевого интерфейса Properties (Свойства) щелкните мышью Internet Protocol (TCP/IP) (Протокол Интернета, TCP/IP) и выберите пункт меню Properties (Свойства).

- В диалоговом окне Internet Protocol (TCP/IP) Properties (Свойства: протокол Интернета, TCP/IP) выберите Use the following IP address (Использовать следующий IP-адрес). Введите IP-адрес внешнего интерфейса в текстовое поле IP address (IP-адрес). Введите маску подсети для внешнего интерфейса в текстовое поле Subnet mask (Маска подсети). Введите основной шлюз для внешнего интерфейса в текстовое поле Default gateway (Основной шлюз). Основной шлюз — это адрес маршрутизатора в сети.
- Нажмите кнопку ОК в диалоговом окне Properties (Свойства) внешнего интерфейса.

СОВЕТ

Не нужно настраивать адрес DNS-сервера на внешнем интерфейсе. Необходим лишь адрес DNS-сервера на внутреннем интерфейсе.

Порядок сетевых интерфейсов

Внутренний интерфейс компьютера с ISA Server 2004 помещается вверху списка сетевых интерфейсов, чтобы обеспечить лучшую производительность при разрешении имен. Выполните следующие действия, чтобы настроить сетевой интерфейс на компьютере на базе ОС Windows Server 2003:

- Правой кнопкой мыши щелкните My Network Places (Сетевое окружение) на рабочем столе и в контекстном меню выберите пункт Properties (Свойства).
- В окне Network and Dial-up Connections (Сетевые подключения) щелкните мышью меню Advanced (Дополнительно), а затем щелкните мышью Advanced Settings... (Дополнительные параметры...).
- В диалоговом окне Advanced Settings (Дополнительные параметры) щелкните мышью внутренний интерфейс в списке Connections (Подключения) на вкладке Adapters and Bindings (Адаптеры и привязки). После того как выбран внутренний интерфейс, щелкните мышью стрелку

вверх, чтобы переместить его в верх списка интерфейсов.

- Нажмите кнопку OK в диалоговом окне Advanced Settings (Дополнительные параметры).

Установка и конфигурирование DNS-сервера на брандмауэре ISA

На брандмауэре ISA будет установлен DNS-сервер в режиме только кэширования. Это позволит компьютерам во внутренней сети и брандмауэру ISA разрешать имена хостов в Интернете. Отметим, что если во внутренней сети уже есть DNS-сервер, то устанавливать его еще раз не нужно. Если во внутренней сети есть DNS-сервер, то можно попробовать настроить компьютер брандмауэра ISA как DNS-сервер в режиме только кэширования, а затем настроить компьютеры во внутренней сети так, чтобы они использовали компьютер с ISA Server 2004 в качестве DNS-сервера или применяли DNS-сервер внутренней сети, а DNS-сервер внутренней сети настроить так, чтобы он использовал брандмауэр ISA в качестве сервера пересылок DNS.

Установка службы DNS

Служба DNS-сервера не устанавливается по умолчанию в операционных системах Windows для серверов. Сначала нужно установить службу DNS-сервера на компьютере на базе Windows Server 2003, который будет играть роль брандмауэра ISA.

Установка службы DNS-сервера на базе Windows Server 2003

Выполните следующие действия, чтобы установить службу DNS на компьютере с Windows Server 2003:

- Нажмите кнопку Start (Пуск), установите курсор мыши на Control Panel (Панель управления) и щелкните мышью Add or Remove Programs (Установка и удаление программ).
- В окне Add or Remove Programs (Установка и удаление программ)

щелкните мышью Add/Remove Windows Components (Установка компонентов Windows).

- В диалоговом окне Windows Components Wizard (Мастер компонентов Windows) выберите Networking Services (Сетевые службы) из списка Components (Компоненты Windows). Не устанавливайте флажок в поле! Выделив запись Networking Services (Сетевые службы), нажмите кнопку Details (Состав).
- В диалоговом окне Networking Services (Сетевые службы) установите флажок в поле Domain Name System (DNS) и нажмите кнопку ОК.
- Нажмите кнопку Next (Далее) в диалоговом окне Windows Components (Компоненты Windows).
- Нажмите кнопку ОК в диалоговом окне Insert Disk (Вставка диска). В диалоговом окне Files Needed (Требуемые файлы) укажите путь к папке i386 на установочном компакт-диске Windows Server 2003 в текстовом поле Copy files from (Размещение файлов) и нажмите кнопку ОК.
- Нажмите кнопку Finish (Готово) на странице Completing the Windows Components Wizard (Завершение работы мастера компонентов Windows).
- Закройте окно Add or Remove Programs (Установка и удаление программ).

Конфигурирование службы DNS на брандмауэре ISA

DNS-сервер на компьютере с брандмауэром ISA выполняет DNS-запросы имен хостов в Интернете от имени компьютеров внутренней сети. DNS-сервер на брандмауэре ISA настроен в режиме только кэширования. DNS-сервер в режиме только кэширования не имеет информации об общих или частных DNS-именах и доменах. Он разрешает имена хостов в Интернете и кэширует результаты; он не отвечает на DNS-запросы имен в частной DNS-зоне внутренней сети или в общей DNS-зоне.

Если во внутренней сети имеется DNS-сервер, поддерживающий домен Active Directory, то расположенный на брандмауэре ISA DNS-сервер можно настроить в режиме только кэширования так, чтобы направлять клиентские запросы к домену внутренней сети на DNS-сервер внутренней сети. В итоге DNS-сервер в режиме только кэширования на компьютере брандмауэра ISA Server 2004 не будет мешать текущей установке DNS-сервера.

Конфигурирование службы DNS в Windows Server 2003

Для того чтобы настроить службу DNS на компьютере с Windows Server 2003 выполните следующие действия:

- Нажмите кнопку Start (Пуск) и установите курсор мыши на Administrative Tools (Администрирование). Щелкните мышью запись DNS.
- Правой кнопкой мыши щелкните имя сервера в левой панели консоли, установите курсор мыши на View (Вид) и щелкните пункт Advanced (Расширенный).
- Разверните все узлы в левой панели консоли DNS.
- Правой кнопкой мыши щелкните имя сервера в левой панели консоли DNS и в контекстном меню выберите пункт Properties (Свойства).
- В диалоговом окне Properties (Свойства) сервера щелкните мышью вкладку Interfaces (Интерфейсы). Выберите вариант Only the following IP addresses (Только по указанным IP-адресам). Щелкните мышью любой IP-адрес, не связанный с внутренним интерфейсом компьютера. Выделив такой IP-адрес, нажмите кнопку Remove (Удалить). Нажмите кнопку Apply (Применить).
- Щелкните мышью вкладку Forwarders (Пересылка). Введите IP-адрес DNS-сервера интернет-провайдера в текстовое поле Selected domain's forwarder IP address list (Список IP-адресов серверов пересылки для выбранного домена), а затем нажмите кнопку Add (Добавить). Установите

флажок в поле Do not use recursion for this domain (Не использовать рекурсию для этого домена). Этот вариант запрещает попытки DNS-сервера на брандмауэре ISA выполнять разрешение имен самостоятельно. В итоге, если сервер пересылки не может разрешить имя, запрос на разрешение имени отвергается. Нажмите кнопку Apply (Применить).

СОВЕТ

Если производительность разрешения имен оставляет желать лучшего, отключите запись Forwarders (Пересылка). Хорошо настроенный DNS-сервер интернет-провайдера может существенно улучшить производительность разрешения имен, а плохо настроенный DNS-сервер интернет-провайдера может снизить способность локального брандмауэра ISA по разрешению имен хостов в Интернете. Чаще всего лучшей производительности можно добиться, используя DNS-сервер интернет-провайдера, потому что его кэш с разрешенными именами хостов больше, чем кэш на DNS-сервере в режиме только кэширования на локальном брандмауэре ISA.

- Нажмите кнопку ОК в диалоговом окне Properties (Свойства).
- Правой кнопкой мыши щелкните имя сервера, установите курсор на All Tasks (Все задачи) и нажмите кнопку Restart (Перезапустить).

Эти действия нужно выполнять, только если во внутренней сети нет DNS-сервера, который используется для поддержки домена Active Directory. Если во внутренней сети нет DNS-сервера и нет необходимости в разрешении DNS-имен внутренней сети, то пропустите следующий раздел, посвященный конфигурированию зоны-заглушки.

ПРЕДУПРЕЖДЕНИЕ

Если во внутренней сети уже есть DNS-сервер, то не нужно выполнять указанные далее действия. Их нужно выполнять только в тех сетях, где уже есть домены Active Directory в среде Windows 2000 Server или Windows Server 2003. Сначала нужно создать зону обратного просмотра для внутренней сети, в которой расположен идентификатор внутреннего DNS-сервера.

- Правой кнопкой мыши щелкните узел Reverse Lookup Zones (Зоны обратного просмотра) в левой панели консоли и нажмите кнопку New Zone (Создать новую зону).
- Нажмите кнопку Next (Далее) на странице Welcome to the New Zone Wizard (Вас приветствует мастер создания новой зоны).
- На странице Zone Type (Тип зоны) выберите Stub zone (Зона-заглушка) и нажмите кнопку Next (Далее).
- Выберите Network ID (Идентификатор сети ID). На странице Reverse Lookup Zone Name (Имя зоны обратного просмотра) введите в текстовое поле Network ID (Идентификатор сети ID) идентификатор сети, в которой расположен DNS-сервер внутренней сети. Нажмите кнопку Next (Далее).
- На странице Zone File (Файл зоны) оставьте стандартное имя файла и нажмите кнопку Next (Далее).
- На странице Master DNS Servers (Основные DNS-серверы) введите IP-адреса DNS-сервера внутренней сети и нажмите кнопку Add (Добавить). Щелкните мышью кнопку Next (Далее).
- Нажмите кнопку Finish (Готово) на странице Completing the New Zone Wizard (Завершение мастера создания новой зоны).

Затем нужно создать зону прямого просмотра для зоны-заглушки.

- Правой кнопкой мыши щелкните узел Forward Lookup Zones (Зоны прямого просмотра) в левой панели консоли и выберите пункт New Zone... (Создать новую зону...).
- Нажмите кнопку Next (Далее) на странице Welcome to the New Zone Wizard (Мастер создания новой зоны).
- На странице Zone Type (Тип зоны) выберите Stub zone (Зона-заглушка) и щелкните кнопку Next (Далее).
- На странице Zone name (Имя зоны) введите имя домена внутренней сети в текстовое поле Zone name (Имя зоны). Нажмите кнопку Next (Далее).

- На странице Zone File (Файл зоны) оставьте стандартное имя файла зоны и щелкните кнопку Next (Далее). На странице Master DNS Servers (Основные DNS-серверы) введите IP-адрес DNS-сервера внутренней сети и нажмите кнопку Add (Добавить). Нажмите кнопку Next (Далее).
- Нажмите кнопку Finish (Готово) на странице Completing the New Zone Wizard (Завершение мастера создания новой зоны).
- Правой кнопкой мыши щелкните имя сервера в левой панели консоли; установите курсор мыши на пункт All Tasks (Все задачи) и нажмите кнопку Restart (Перезапустить).

Конфигурирование службы DNS на DNS-сервере внутренней сети

Если в организации имеется инфраструктура DNS, то следует настроить DNS-сервер внутренней сети на использование DNS-сервера на брандмауэре ISA Server 2004 в качестве сервера пересылки в DNS. Такая конфигурация DNS является более безопасной, потому что DNS-сервер внутренней сети никогда напрямую не взаимодействует с не вызывающим доверия DNS-сервером в Интернете.

DNS-сервер внутренней сети пересылает DNS-запросы на DNS-сервер на брандмауэре ISA Server 2004, а DNS-сервер на брандмауэре ISA Server 2004 разрешает имя, сохраняет результат в своем кэше, а затем возвращает IP-адрес на DNS-сервер во внутренней сети.

ПРЕДУПРЕЖДЕНИЕ

Перечисленные далее действия следует выполнять, только если во внутренней сети имеется DNS-сервер, а внутренний интерфейс брандмауэра ISA был настроен на использование внутреннего DNS-сервера. Если внутреннего DNS-сервера нет, то эти действия выполнять не нужно.

Выполните следующие действия на DNS-сервере внутренней сети, чтобы настроить его на использование DNS-сервера на брандмауэре ISA в качестве сервера пересылок:

- Нажмите кнопку Start (Пуск) и установите курсор мыши на Administrative tools (Администрирование) и щелкните пункт DNS.
- В консоли DNS Management (Управление DNS-сервером) правой кнопкой мыши щелкните имя сервера в левой панели консоли и в контекстном меню выберите пункт Properties (Свойства).
- В диалоговом окне Properties (Свойства) щелкните мышью вкладку Forwarders (Пересылка)
- На вкладке Forwarders (Пересылка) введите IP-адрес внутреннего интерфейса брандмауэра ISA Server 2004 в текстовое поле Selected domain's forwarder IP address list (Список IP-адресов серверов пересылки для выбранного домена). Нажмите кнопку Add (Добавить).
- IP-адрес внутреннего интерфейса брандмауэра ISA Server 2004 появится в списке адресов серверов пересылки.
- Установите флажок в поле Do not use recursion for this domain (Не использовать рекурсию для этого домена). Этот параметр запрещает DNS-серверу внутренней сети разрешать имя самостоятельно в случае, если сервер пересылок на брандмауэре ISA не способен разрешить имя.

Обратите внимание, что DNS-сервер во внутренней сети еще не способен разрешать имена хостов в Интернете. Еще нужно создать правило доступа, которое разрешает DNS-серверу доступ к DNS-серверу на брандмауэре ISA. Далее в этом разделе показано, как создавать такое правило доступа.

Установка и конфигурирование DHCP-сервера на брандмауэре ISA

У каждого компьютера должен быть IP-адрес и другая информация, позволяющая ему взаимодействовать с другими компьютерами в сети и в

Интернете. Служба DHCP-сервера может быть установлена на брандмауэре ISA, она предоставляет информацию об IP-адресах компьютерам во внутренней сети. Предположим, что брандмауэр ISA будет использоваться в качестве DHCP-сервера. Если в сети уже есть DHCP-сервер, то следующий раздел можно пропустить.

ПРЕДУПРЕЖДЕНИЕ

В сети не должно быть других DHCP-серверов. Если в сети есть еще один компьютер, выступающий в роли DHCP-сервера, то нужно отключить на нем службу DHCP так, чтобы брандмауэр ISA Server 2004 выступал в роли единственного DHCP-сервера в сети.

Установка службы DHCP

Службу DHCP-сервера можно установить на базе ОС Windows 2000 Server и Windows Server 2003- Процесс установки немного отличается для этих двух операционных систем. В этом разделе рассматривается установка службы DHCP-сервера на базе Windows 2000 Server и Windows Server 2003.

Установка службы DHCP-сервера на базе Windows Server 2003

Для того чтобы установить службу DNS-сервера на базе Windows Server 2003, выполните следующие действия:

- Нажмите кнопку Start (Пуск), установите курсор мыши на Control Panel (Панель управления) и выберите пункт Add or Remove Programs (Установка и удаление программ).
- В окне Add or Remove Programs (Установка или удаление программ) щелкни

  те мышью Add/Remove Windows Components (Установка/Удаление компонентов Windows).
- В диалоговом окне Windows Components Wizard (Мастер компонентов Windows) выберите Networking Services (Сетевые службы) из списка

Components(Компоненты Windows). Не уста на вливайте флажок в поле! Выделив запись Networking Services (Сетевые службы) нажмите кнопку Details... (Состав...).

- В диалоговом окне Networking Services (Сетевые службы) (рис. 6.21) установите флажок в поле Dynamic Host Configuration Protocol (DHCP) и нажмите кнопку OK
- Нажмите кнопку Next (далее) в диалогором окне Windows Components (Компоненты Windows).
- Нажмите кнопку Finish (Готово) на странице Completing the Windows Components Wizard (Завершение мастера компонентов Windows).
- Закройте окно Add or Remove Programs (Установка или удаление программ).

Конфигурирование службы DHCP

DHCP-сервер должен быть сконфигурирован с набором IP-адресов, которые он может присваивать компьютерам в частной сети. DHCP-сервер также предоставляет дополнительную информацию помимо IP-адреса, включающую адрес DNS-сервера, основной шлюз и первичное имя домена.

Адреса DNS-сервера и основного шлюза, назначаемые компьютеру, совпадают с IP-адресом внутреннего интерфейса брандмауэра ISA. DHCP-сервер использует область DHCP, чтобы предоставить эту информацию клиентам внутренней сети. Необходимо создать область DHCP, которая предоставляет клиентам внутренней сети правильную информацию об IP-адресах.

ПРИМЕЧАНИЕ

DHCP-сервер не должен назначать адреса, которые уже используются в сети. Нужно создать исключения для этих IP-адресов. В качестве примера можно привести статические или зарезервированные адреса, назначенные печатным, файловым, почтовым или Web-серверам, это лишь несколько

примеров устройств или серверов, которые постоянно используют одни и те же назначенные им на постоянной основе IP-адреса. Если для этих адресов не создать исключения, то DHCP-сервер выполнит разрешение адресов, а когда он обнаружит, что эти адреса уже используются, то он поместит их в группу плохих адресов (bad address group). Кроме того, хорошо сконфигурированная сеть сгруппирует компьютеры в смежные блоки IP-адресов. Например, все компьютеры, которым должны быть назначены статические IP-адреса, входят в один блок.

Для того чтобы настроить DHCP-сервер на базе Windows Server 2003 с областью, которая будет назначать правильную информацию об IP-адресах клиентам внутренней сети, выполните следующие действия:

ПРЕДУПРЕЖДЕНИЕ

Если в корпоративной сети уже есть DHCP-сервер, не выполняйте эти действия и не устанавливайте DHCP-сервер на брандмауэре ISA. DHCP-сервер следует устанавливать на брандмауэре ISA, только если во внутренней сети нет DHCP-сервера.

- Нажмите кнопку Start (Пуск) и установите курсор мыши на Administrative Tools (Администрирование). Нажмите кнопку DHCP.
- Разверните все узлы в левой панели консоли DHCP. Правой кнопкой мыши щелкните имя сервера в левой панели консоли и нажмите кнопку New Scope (Создать область).
- Нажмите кнопку Next (Далее) на странице Welcome to the New Scope Wizard (Вас приветствует мастер создания области).
- Введите SecureNAT Client Scope (Область для клиента SecureNAT) в текстовом поле Name (Имя) на странице Scope Name (Имя области). Нажмите кнопку Next (Далее).
- На странице IP Address Range (Диапазон адресов) введите первый IP-адрес и последний IP-адрес диапазона в текстовые поля Start IP address (Начальный IP-адрес) и End IP address (Конечный IP-адрес). Например,

при использовании идентификатора сети 192.168.1.0 с маской подсети 255.255.255-0 введите начальный IP-адрес 192.168.1.1, а конечный IP-адрес 192.168.1.254. Нажмите кнопку Next (Далее).

- На странице Add Exclusions (Добавление исключений) введите IP-адрес внутреннего интерфейса брандмауэра ISA в текстовое поле Start IP address (Начальный IP-адрес) и нажмите кнопку Add (Добавить). Если в сети имеются серверы или рабочие станции со статическими IP-адресами, которые не нужно менять, добавьте эти адреса в список исключений. Нажмите кнопку Next (Далее), после того как будут добавлены все адреса, которые нужно исключить из области DHCP.
- На странице Lease Duration (Срок действия аренды адреса) оставьте стандартное значение и нажмите кнопку Next (Далее).
- На странице Configuring DHCP Options (Настройка параметров DHCP) выберите Yes, I want to configure these options now (Да, настроить эти параметры сейчас) и щелкните кнопку Next (Далее).
- На странице Router (Маршрутизатор, основной шлюз) введите IP-адрес внутреннего интерфейса брандмауэра ISA и нажмите кнопку Add (Добавить). Нажмите кнопку Next (Далее).
- На странице Domain Name and DNS Servers (Имя домена и DNS-серверы) введите IP-адрес внутреннего интерфейса брандмауэра ISA в текстовое поле IP address (IP-адрес) и нажмите кнопку Add (Добавить). Если во внутренней сети имеется домен Active Directory, введите имя домена внутренней сети в текстовое поле Parent domain (Родительский домен). Не вводите имя домена в текстовое поле Parent domain (Родительский домен), если во внутренней сети нет домена Active Directory. Щелкните кнопку Next (Далее).
- Не вводите никакую информацию на странице WINS Servers (WINS-серверы),

если во внутренней сети нет WINS-сервера. Если во внутренней сети имеется WINS-сервер, введите этот IP-адрес в текстовое поле IP address (IP-адрес). Нажмите кнопку Next (Далее).

- Выберите Yes, I want to activate this scope now (Да, я хочу активировать эту область сейчас) на странице Activate Scope (Активировать область) и нажмите кнопку Yes (Да).
- Нажмите кнопку Finish (Готово) на странице Completing the New Scope Wizard (Завершение мастера создания области).

Установка и конфигурирование программного обеспечения ISA Server 2004

Теперь можно приступить к установке программного обеспечения брандмауэра ISA.

Чтобы установить программное обеспечение брандмауэра ISA на компьютере на базе ОС Windows Server 2003 с двумя сетевыми адаптерами, выполните следующие действия:

- Вставьте установочный компакт-диск для ISA Server 2004 в дисковод для компакт-дисков или установите соединение с общим сетевым ресурсом, в котором находятся установочные файлы ISA Server 2004. Если программа установки не запустится автоматически, дважды щелкните мышью файл isaautorun.exe в корне дерева установочных файлов.
- На странице Microsoft Internet Security and Acceleration Server 2004 щелкните мышью Review Release Notes (Информация о версии) и прочтите информацию о версии. Эта информация о версии содержит полезные данные о важных моментах и возможностях конфигурирования. После просмотра информации о версии щелкните мышью Read Setup and Feature Guide (Прочесть руководство по установке и функциям). Не обязательно читать все руководство сразу, его можно распечатать и прочесть потом. Щелкните мышью Install ISA Server 2004 (Установить ISA Server 2004).

- Нажмите кнопку Next (Далее) на странице Welcome to the Installation Wizard for Microsoft ISA Server 2004 (Мастер установки Microsoft ISA Server 2004).
- Выберите вариант I accept the terms in the license agreement (Я согласен) на странице License Agreement (Лицензионное соглашение). Нажмите кнопку Next (Далее).
- На странице Customer Information (Информация о пользователе) введите имя пользователя и название организации в текстовые поля User Name (Имя) и Organization (Организация). Введите серийный номер в текстовое поле Product Serial Number (Серийный номер). Щелкните кнопку Next (Далее).
- На странице Setup Type (Тип установки) щелкните мышью вариант Custom (Пользовательская). Если не нужно устанавливать программное обеспечение брандмауэра ISA на диске C:, щелкните мышью кнопку Change (Изменить), чтобы изменить место установки программы на жестком диске. Нажмите кнопку Next (Далее).
- На странице Custom Setup (Пользовательская установка) выберите устанавливаемые компоненты. По умолчанию устанавливаются компоненты Firewall Services, Advanced Logging и ISA Server Management. Средство контроля SMTP- сообщений (Message Screener), которое используется для того, чтобы контролировать спам и вложения, поступающие в сеть и исходящие из нее, не устанавливается по умолчанию. Прежде чем устанавливать Message Screener, нужно установить SMTP-службу IIS 6.0 на компьютере брандмауэра ISA Server 2004. В данном случае будет установлен общий ресурс с установочными файлами для клиента брандмауэра Firewall Client Installation Share, чтобы впоследствии можно было установить клиент брандмауэра на других компьютерах во внутренней сети. Щелкните мышью значок x слева от параметра Firewall Client Installation Share и щелкните мышью This feature,

and all subfeatures, will be installed on the local hard drive (Эта функция и все подфункции будут установлены на локальном жестком диске). Использование клиента брандмауэра позволяет лучше защитить сеть, по возможности следует всегда устанавливать клиент брандмауэра на клиентских компьютерах во внутренней сети. Нажмите кнопку Next (Далее).

- На странице Internal Network (Внутренняя сеть) нажмите кнопку Add (Добавить). Внутренняя сеть отличается от таблицы локальных адресов (LAT, Local Address Table), которая использовалась в брандмауэре ISA Server 2000. Внутренняя сеть включает в себя доверяемые сетевые службы, с которыми должен взаимодействовать брандмауэр ISA. В качестве примера таких служб можно при вести контроллеры домена Active Directory, DNS, DHCP, службы терминалов и др. Системная политика брандмауэра использует определение внутренней сети во многих правилах системной политики.
- На странице Internal Network (Внутренняя сеть) нажмите кнопку Select Network Adapter (Выбрать сетевой адаптер).
- На странице Configure Internal Network (Настроить внутреннюю сеть) снимите флажок в поле Add the following private ranges... (Добавить следующие частные диапазоны...). Оставьте флажок в поле Add address ranges based on the Windows Routing Table (Добавить диапазоны адресов на основе таблицы маршрутизации Windows). Установите флажок в поле рядом с адаптером, соединенным со внутренней сетью. В данном случае сетевые интерфейсы были переименованы так, чтобы имя интерфейса отражало его расположение. Нажмите кнопку ОК.
- Нажмите кнопку ОК в диалоговом окне с сообщением о том, что внутренняя сеть была определена на основании таблицы маршрутизации Windows.
- Щелкните кнопку ОК в диалоговом окне Internal network address ranges

(Диапазоны адресов внутренней сети).

- Нажмите кнопку Next (Далее) на странице Internal Network (Внутренняя сеть).
- Не устанавливайте флажок в поле Allow computers running earlier versions of Firewall Client software to connect (Разрешить соединения компьютерам с более ранними версиями программного обеспечения клиента брандмауэра). Этот параметр предполагает применение клиента брандмауэра нового бранд мауэра ISA. Предыдущие версии клиента брандмауэра (входящие в Proxy 2.0 и ISA Server 2000) не поддерживаются. Этот параметр также разрешает клиенту брандмауэра отправлять верительные данные пользователя по зашифрованному каналу на брандмауэр ISA и проходить проверку подлинности на брандмауэре ISA в прозрачном режиме. Щелкните кнопку Next (Далее).
- На странице Services (Службы) отметьте, чтобы службы SNMP и IIS Admin Service были остановлены на время установки. Если на компьютере брандмауэра ISA Server 2004 установлены службы Internet Connection Firewall (ICF)/Internet Connection Sharing (ICF) и/или служба IP Network Address Translation, то они будут отключены, т. к. они конфликтуют с программным обеспечением брандмауэра ISA Server 2004.
- Щелкните кнопку Install (Установить) на странице Ready to Install the Program (Установка программы).
- На странице Installation Wizard Completed (Завершение работы мастера установки) нажмите кнопку Finish (Готово).
- Щелкните кнопку Yes (Да) в диалоговом окне Microsoft ISA Server, в котором сообщается, что нужно перезапустить сервер.
- Выполните вход в систему как администратор после перезапуска компьютера.

- Нажмите кнопку Start (Пуск) и установите курсор на All Programs (Программы). Установите курсор на Microsoft ISA Server и выберите пункт ISA Server Management. Откроется консоль управления Microsoft Internet Security and Acceleration Server 2004, и появится страница Welcome to Microsoft Internet Security and Acceleration Server 2004.

Конфигурирование брандмауэра ISA

Теперь можно настроить политику доступа на брандмауэре ISA. Нужно создать пять правил доступа:

- правило, разрешающее клиентам внутренней сети доступ к DHCP-серверу на брандмауэре ISA;
- правило, разрешающее брандмауэру ISA отправлять DHCP-сообщения хостам во внутренней сети;
- правило, разрешающее DNS-серверу внутренней сети использовать брандмауэр ISA в качестве своего DNS-сервера. Это правило следует создавать, только если во внутренней сети имеется DNS-сервер;
- правило, разрешающее клиентам внутренней сети доступ к DNS-серверу в ре жиме только кэширования на брандмауэре ISA. Это правило используется, только если во внутренней сети нет DNS-сервера или если нужно использовать брандмауэр ISA в качестве DNS-сервера в режиме только кэширования с зоной-заглушкой, указывающей на домен внутренней сети;
- правило «все открыто», разрешающее клиентам внутренней сети доступ ко всем протоколам и узлам Интернета.

ПРЕДУПРЕЖДЕНИЕ

Последнее правило, «все открыто», используется только для того, чтобы начать работу. Это правило позволяет протестировать способность брандмауэра ISA устанавливать соединение с Интернетом, но оно не обеспечивает никакого

контроля исходящего доступа, как это делают большинство аппаратных брандмауэров с фильтрацией пакетов. Брандмауэр ISA способен обеспечить контроль входящего и исходящего трафика, поэтому нужно выключить это правило и создать правила для пользователей/групп, для протоколов и для узлов после того, как базовые соединения с Интернетом через брандмауэр ISA окажутся успешными.

Помимо этих правил доступа, следует настроить системную политику брандмауэра, чтобы разрешить DHCP-ответы с DHCP-серверов внешней сети.

Правило «DHCP Request to Server»

Для того чтобы создать правило «DHCP Request to Server» (DHCP-запрос к серверу), выполните следующие действия:

- В консоли управления Microsoft Internet Security and Acceleration Server 2004 разверните имя сервера и щелкните пункт Firewall Policy (Политика брандмауэра
- В узле Firewall Policy (Политика брандмауэра) щелкните вкладку Tasks (Задачи). На панели задач щелкните мышью пункт Create a New Access Rule (Создать новое правило доступа).
- На странице Welcome to the New Access Rule Wizard (Мастер создания нового правила доступа) введите DHCP Request to Server (DHCP-запрос к серверу) в текстовое поле Access Rule name (Имя правила доступа). Щелкните кнопку Next (Далее).
- На странице Rule Action (Действие правила) выберите Allow (Разрешающее)
  и нажмите кнопку Next (Далее).
- На странице Protocols (Протоколы) выберите вариант Selected protocols (К выбранным протоколам) из списка This rule applies to (Это правило при меняется) и щелкните кнопку Add (Добавить).

- В диалоговом окне Add Protocols (Добавить протоколы) щелкните папку Infrastructure (Инфраструктура). Дважды щелкните мышью запись DHCP
  (request) (DHCP, запрос) и нажмите кнопку Close (Закрыть).
- Нажмите кнопку Next (Далее) на странице Protocols (Протоколы).
- На странице Access Rule Sources (Источники для правила доступа) щелкните
  кнопку Add (Добавить).
- В диалоговом окне Add Network Entities (Добавить сетевые объекты) щелкните мышью папку Computer Sets (Подмножества компьютеров). Дважды щелкните мышью запись Anywhere (Везде) и нажмите кнопку Close (Закрыть).
- Нажмите кнопку Next (Далее) на странице Access Rule Sources (Источники для правила доступа). На странице Access Rule Destinations (Адресаты правила доступа) щелкните
  кнопку Add (Добавить).
- В диалоговом окне Add Network Entities (Добавить сетевые объекты) щелкните
  мышью папку Networks (Сети) и дважды щелкните мышью Local Host (Локальный хост). Щелкните кнопку Close (Закрыть).
- Нажмите кнопку Next (Далее) на странице Access Rule Destinations (Адресаты правила доступа).
- На странице User Sets (Подмножества пользователей) оставьте значение по умолчанию All Users (Все пользователи) и щелкните, кнопку Next (Далее).
- На странице Completing the New Access Rule Wizard (Завершение работы ма
  стера создания нового правила доступа) проверьте настройки и нажмите кнопку Finish (Готово).

Правило «DHCP Reply from Server»

Для создания правила «DHCP Reply from Server» (DHCP-ответ от сервера) выполните следующие действия:

- В консоли управления Microsoft Internet Security and Acceleration Server 2004 разверните имя сервера и нажмите кнопку Firewall Policy (Политика брандмауэра).
- В узле Firewall Policy (Политика брандмауэра) щелкните мышью вкладку Tasks(Задачи) на панели задач. На панели задач щелкните мышью Create a New Access Rule (Создать новое правило доступа).
- На странице Welcome to the New Access Rule Wizard (Мастер создания нового правила доступа) введите DHCP Reply from Server (DHCP-ответ от сервера) в текстовое поле Access Rule name (Имя правила доступа). Щелкните кнопку Next (Далее).
- На странице Rule Action (Действие правила) выберите Allow (Разрешающее) и щелкните кнопку Next (Далее).
- На странице Protocols (Протоколы) выберите вариант Selected protocols (К выбранным протоколам) из списка This rule applies to (Это правило применяется) и щелкните кнопку Add (Добавить).
- В диалоговом окне Add Protocols (Добавить протоколы) щелкните мышью папку Infrastructure (Инфраструктура). Дважды щелкните мышью запись DHCP (reply) (DHCP, ответ) и нажмите кнопку Close (Закрыть).
- Нажмите кнопку Next (Далее) на странице Protocols (Протоколы).
- На странице Access Rule Sources (Источники для правила доступа) щелкните кнопку Add (Добавить).
- В диалоговом окне Add Network Entities (Добавить сетевые объекты) щелкните мышью папку Networks (Сети). Дважды щелкните мышью запись Local Host (Локальный хост) и нажмите кнопку Close (Закрыть).

- Нажмите кнопку Next (Далее) на странице Access Rule Sources (Источники для правила доступа).
- На странице Access Rule Destinations (Адресаты для правила доступа) щелкните кнопку Add (Добавить).
- В диалоговом окне Add Network Entities (Добавить сетевые объекты) щелкните мышью папку Networks (Сети) и дважды щелкните мышью запись Internal (Внутренняя). Нажмите кнопку Close (Закрыть).
- Нажмите кнопку Next (Далее) на странице Access Rule Destinations (Адресаты правила доступа).
- На странице User Sets (Подмножества пользователей) оставьте значение по умолчанию (All Users (Все пользователи)) и щелкните кнопку Next (Далее).
- На странице Completing the New Access Rule Wizard (Завершение работы мастера создания нового правила доступа) проверьте настройки и нажмите кнопку Finish (Готово).

Правило «Internal DNS Server to DNS Forwarder»

Для создания правила «Internal DNS Server to DNS Forwarder» (От внутреннего DNS-сервера к серверу пересылок DNS) выполните следующие действия:

- В консоли управления Microsoft Internet Security and Acceleration Server 2004 разверните имя сервера и щелкните мышью пункт Firewall Policy (Политика брандмауэра).
- В узле Firewall Policy (Политика брандмауэра) щелкните мышью вкладку Tasks (Задачи) на панели задач. На панели задач щелкните мышью пункт Create a New Access Rule (Создать новое правило доступа)На странице Welcome to the New Access Rule Wizard (Мастер создания нового правила доступа) введите Internal DNS Server to DNS Forwarder (От внутреннего

DNS-сервера к серверу пересылок DNS) в текстовом поле Access Rule name (Имя правила доступа). Нажмите кнопку Next (Далее).

- На странице Rule Action (Действие правила) выберите Allow (Разрешающее) и щелкните кнопку Next (Далее).
- На странице Protocols (Протоколы) выберите вариант Selected protocols (К выбранным протоколам) из списка This rule applies to (Это правило применяется) и щелкните кнопку Add (Добавить).
- В диалоговом окне Add Protocols (Добавить протоколы) щелкните мышью папку Infrastructure (Инфраструктура). Дважды щелкните мышью запись DNS и щелкните кнопку Close (Закрыть). Нажмите кнопку Next (Далее) на странице Protocols (Протоколы).
- На странице Access Rule Sources (Источники для правила доступа) щелкните кнопку Add (Добавить).
- В диалоговом окне Add Network Entities (Добавить сетевые объекты) щелкните мышью меню New (Новый), а затем Computer (Компьютер).
- В диалоговом окне New Computer Rule Element (Новый элемент правила для компьютера) введите Internal DNS Server (Внутренний DNS-сервер) в текстовое поле Name (Имя). Введите 10.0.0.2 в текстовое поле Computer IP Address (IP-адрес компьютера). Нажмите кнопку ОК.
- В диалоговом окне Add Network Entities (Добавить сетевые объекты) щелкните мышью папку Computers (Компьютеры) и дважды щелкните мышью запись Internal DNS Server (Внутренний DNS-сервер). Нажмите кнопку Close (Закрыть).
- Нажмите кнопку Next (Далее) на странице Access Rule Sources (Источники для правила доступа).
- Нажмите кнопку Add (Добавить) на странице Access Rule Destinations (Адресаты правила доступа).
- В диалоговом окне Add Network Entities (Добавить сетевые объекты)

щелкните мышью папку Networks (Сети) и дважды щелкните мышью Local Host (Локальный хост). Нажмите кнопку Close (Закрыть).

- Нажмите кнопку Next (Далее) на странице Access Rule Destinations (Адресаты правила доступа).
- На странице User Sets (Подмножества пользователей) оставьте значение по умолчанию All Users (Все пользователи) и нажмите кнопку Next (Далее).
- На странице Completing the New Access Rule Wizard (Завершение работы мастера создания нового правила доступа) проверьте настройки и нажмите кнопку Finish (Готово).

Правило «Internal Network to DNS Server»

Для создания правила «Internal Network to DNS Server» (Из внутренней сети к DNS-серверу) выполните следующие действия:

- В консоли управления Microsoft Internet Security and Acceleration Server 2004 разверните имя сервера и щелкните мышью Firewall Policy (Политика брандмауэра).
- В узле Firewall Policy (Политика брандмауэра) щелкните мышью вкладку Tasks (Задачи) на панели задач. На панели задач щелкните мышью Create a New Access Rule (Создать новое правило доступа).
- На странице Welcome to the New Access Rule Wizard (Мастер создания нового правила доступа) введите Internal Network to DNS Server (Из внутренней сети к DNS-серверу) в текстовое поле Access Rule name (Имя правила доступа). Нажмите кнопку Next (Далее).
- На странице Rule Action (Действие правила) выберите Allow (Разрешающее) и нажмите кнопку Next (Далее). На странице Protocols (Протоколы) выберите вариант Selected protocols (К выбранным протоколам) из списка This rule applies to (Это правило при-

меняется) и нажмите кнопку Add (Добавить).

- В диалоговом окне Add Protocols (Добавить протоколы) щелкните мышью папку Common Protocols (Общие протоколы). Дважды щелкните мышью запись DNS и нажмите кнопку Close (Закрыть).
- Нажмите кнопку Next (Далее) на странице Protocols (Протоколы).
- На странице Access Rule Sources (Источники для правила доступа) нажмите кнопку Add (Добавить).
- В диалоговом окне Add Network Entities (Добавить сетевые объекты) щелкните мышью папку Networks (Сети). Дважды щелкните мышью Internal (Внутренняя сеть) и нажмите кнопку Close (Закрыть).
- Нажмите кнопку Next (Далее) на странице Access Rule Sources (Источники для правила доступа).
- Нажмите кнопку Add (Добавить) на странице Access Rule Destinations (Адресаты правила доступа).
- В диалоговом окне Add Network Entities (Добавить сетевые объекты) щелкните мышью папку Networks (Сети) и дважды щелкните мышью Local Host (Локальный хост). Нажмите кнопку Close (Закрыть).
- Нажмите кнопку Next (Далее) на странице Access Rule Destinations (Адресаты правила доступа).
- На странице User Sets (Подмножества пользователей) оставьте значение по умолчанию All Users (Все пользователи) и нажмите кнопку Next (Далее).
- На странице Completing the New Access Rule Wizard (Завершение работы мастера создания нового правила доступа) проверьте настройки и нажмите кнопку Finish (Готово).

Правило «All Open»

Для создания правила «All Open» (Все открыто) выполните следующие действия:

- В консоли управления Microsoft Internet Security and Acceleration Server 2004 разверните имя сервера и щелкните мышью Firewall Policy (Политика брандмауэра).
- В узле Firewall Policy (Политика брандмауэра) щелкните мышью вкладку Tasks (Задачи) на панели задач. На панели задач щелкните мышью Create a New Access Rule (Создать новое правило доступа).
- На странице Welcome to the New Access Rule Wizard (Вас приветствует мастер создания нового правила доступа) введите All Open (Все открыто) в текстовое поле Access Rule name (Имя правила доступа). Нажмите кнопку Next (Далее).
- На странице Rule Action (Действие правила) выберите Allow (Разрешающее) и нажмите кнопку Next (Далее).
- На странице Protocols (Протоколы) выберите вариант All outbound traffic (Ко всему исходящему трафику) из списка This rule applies to (Это правило применяется) и нажмите кнопку Next (Далее).
- Нажмите кнопку Next (Далее) на странице Protocols (Протоколы).
- На странице Access Rule Sources (Источники для правила доступа) нажмите кнопку Add (Добавить).
- В диалоговом окне Add Network Entities (Добавить сетевые объекты) щелкните мышью папку Networks (Сети). Дважды щелкните мышью Internal (Внутренняя) и нажмите кнопку Close (Закрыть).
- Нажмите кнопку Next (Далее) на странице Access Rule Sources (Источники для правила доступа).
- Нажмите кнопку Add (Добавить) на странице Access Rule Destinations (Адресаты правила доступа).
- В диалоговом окне Add Network Entities (Добавить сетевые объекты) щелкните мышью папку Networks (Сети) и дважды щелкните мышью External (Внешняя). Нажмите кнопку Close (Закрыть).

- Нажмите кнопку Next (Далее) на странице Access Rule Destinations (Адресаты правила доступа).
- На странице User Sets (Подмножества пользователей) оставьте значение по умолчанию All Users (Все пользователи) и нажмите кнопку Next (Далее).
- На странице Completing the New Access Rule Wizard (Завершение работы мастера создания нового правила доступа) проверьте настройки и нажмите кнопку Finish (Готово).
- Правило доступа должно выглядеть, как на рис. 6.28. В данном случае не нужно менять порядок правил. При создании расширенных правил доступа для контроля исходящего и входящего доступа, возможно, потребуется изменить порядок правил, чтобы добиться желаемых результатов.

Конфигурирование компьютеров внутренней сети

Компьютеры внутренней сети настраиваются как клиенты SecureNAT ISA Server. Клиент SecureNAT — это компьютер, адрес основного шлюза которого настроен как IP-адрес сетевого устройства, маршрутизирующего запросы из Интернета на внутренний IP-адрес брандмауэра ISA Server 2004.

Когда компьютеры внутренней сети имеют тот же идентификатор сети, что и внутренний интерфейс брандмауэра ISA, основной шлюз компьютеров внутренней сети настраивается как внутренний IP-адрес на компьютере брандмауэра ISA. Так настраивается область DHCP на DHCP-сервере, расположенном на брандмауэре ISA.

В этом разделе описывается конфигурирование компьютеров внутренней сети, имеющих тот же идентификатор сети, что и внутренний интерфейс брандмауэра ISA Server 2004, и клиентов, которые могут иметь другой идентификатор сети. Чаще всего второй случай встречается в крупных сетях, в которых для внутренней сети есть более одного идентификатора сети.

Настройка клиентов внутренней сети как DHCP-клиентов

DHCP-клиенты запрашивают информацию об IP-адресах с DHCP-сервера. В этом разделе описывается, как настроить клиент Windows 2000 (Server или Professional) как DHCP-клиент. Эта процедура схожа для всех клиентов на базе Windows. Для того чтобы настроить клиент внутренней сети как DHCP-клиент, выполните следующие действия:

- Правой кнопкой мыши щелкните значок My Network Places (Сетевое окружение) на рабочем столе и в контекстном меню выберите пункт Properties (Свойства).
- В окне Network Connections (Сетевые подключения) правой кнопкой мыши щелкните внешний сетевой интерфейс и выберите пункт Properties (Свойства).
- В диалоговом окне Properties (Свойства) сетевого интерфейса щелкните мышью запись Internet Protocol (TCP/IP) (Протокол Интернета, TCP/IP) и щелкните мышью пункт меню Properties (Свойства).
- В диалоговом окне Internet Protocol (TCP/IP) Properties (Свойства протокол Интернета TCP/IP) (рис. 6.29) выберите Obtain an IP-address automatically (Получить IP-адрес автоматически).
- Выберите Use the following DNS server addresses (Использовать следующие адреса DNS-серверов). Введите IP-адрес внутреннего интерфейса в текстовое поле Preferred DNS server (Предпочитаемый DNS-сервер). Нажмите кнопку ОК в диалоговом окне Internet Protocol (TCP/IP) Properties (Свойства протокола Интернета TCP/IP).

VPN-соединение

Обзор использования VPN межсетевым экраном ISA

Постоянный рост популярности виртуальных частных сетей (VPN) превратил их в стандарт для компаний, имеющих надомных работников, администраторов и продавцов, которым необходим доступ к сети вне офиса, а

также партнеров и клиентов, нуждающихся в доступе к ресурсам корпоративной сети. Задача VPN – разрешить удаленный доступ к ресурсам корпоративной сети, которые в противном случае могут быть доступными только при непосредственном подключении пользователя к локальной сети. С помощью VPN-соединения пользователь получает «виртуальное», конфигурации узел-в-узел соединение удаленного VPN-пользователя с корпоративной сетью. Пользователь может работать так, как будто он (она) находится в офисе; приложения и сервисы, выполняющиеся на компьютерах пользователей, интерпретируют VPN-линию связи как типичное соединение Ethernet. Интернет, через который клиент соединяется с корпоративной сетью, полностью скрыт от пользователей и приложений (прозрачен для них).

Одно из главных преимуществ применения VPN-соединения по сравнению с клиент-серверным Web-приложением заключается в том, что VPN-пользователи, находящиеся далеко от локальной сети, могут получить доступ ко всем протоколам и серверам корпоративной сети. Программное обеспечение VPN-клиента встроено во все современные операционные системы Windows. VPN-пользователю не нужны никакие специальные программные средства для подключения к любому из этих сервисов и нет необходимости создавать специальные приложения прокси, разрешающие вашим пользователям подсоединяться к этим ресурсам.

ISA Server 2000 был первым брандмауэром корпорации Microsoft, обеспечивающим тесную интеграцию VPN и управление ими. В состав ISA Server 2000 были включены удобные мастера, упрощающие создание VPN-соединений удаленного доступа и межшлюзовых.или узел-в-узел VPN-соединений с брандмауэром ISA Server 2000/VPN-сервером. Но сформированную структуру все еще можно было улучшить. VPN-сервер брандмауэра ISA Server 2000 требовал от администратора брандмауэра значительных затрат времени на точную настройку конфигурации VPN-сервера

с помощью консоли сервиса Routing and Remote Access (маршрутизация и удаленный доступ).

В ISA Server 2006 существенно усовершенствованы VPN-компоненты, которые включены в состав брандмауэра из сервиса Routing and Remote Access (RRAS) операционных систем Windows 2000 и Windows Server 2003. Теперь администратор имеет возможность конфигурировать VPN-сервер и шлюзовые компоненты и управлять ими непосредственно на консоли управления брандмауэра ISA Server 2006, не переключаясь между консолью управления ISA MMC и консолью управления RRAS MMC. Вам очень редко понадобится консоль сервиса маршрутизации и удаленного доступа для конфигурирования VPN-компонентов.

К другим усовершенствованиям функциональных возможностей использования VPN в ISA Server 2006 можно отнести следующие:

- политику брандмауэра, применяемую к соединениям VPN-клиентов;
- политику брандмауэра, применяемую к VPN-соединениям конфигурации узел-в-узел;
- VPN-карантин или временную изоляцию;
- отображение пользователей для VPN-клиентов;
- поддержку клиентов SecureNAT для VPN-соединений;
- виртуальную частную сеть конфигурации «узел-в-узел» с применением туннельного режима протокола IPSec;
- публикацию VPN-серверов по протоколу PPTP (Point-to-Point Tunneling Protocol, сквозной туннельный протокол);
- поддержку аутентификации секретным ключом Pre-shared Key для VPN-соединений по протоколу IPSec;
- улучшенная работа сервера имен для VPN-клиентов;
- мониторинг соединений VPN-клиентов.

Эти новые свойства VPN-сервера и шлюза делают ISA 2006 одной из наиболее мощных реализаций как VPN, так и брандмауэров, представленных сегодня на рынке.

Создание VPN-сервера удаленного доступа по протоколу PPTP

VPN-сервер удаленного доступа принимает VPN-вызовы от компьютеров VPN-клиентов. Он разрешает отдельным компьютерам клиента и пользователям получать доступ к сетевым ресурсам после того, как установлено VPN-соединение. VPN-шлюз, напротив, соединяет целые сети друг с другом и разрешает многочисленным хостам в каждой сети соединяться с другими сетями с помощью VPN-канала типа узел-в-узел.

Для соединения с VPN-сервером можно использовать любое клиентское программное обеспечение, поддерживающее протоколы PPTP или L2TP/IPSec. Идеальным выбором может служить VPN-клиент Microsoft, входящий в состав всех версий ОС Windows. Но если вы хотите использовать протокол L2TP/IPSec с секретными ключами (pre-shared keys), обходящий NAT (NAT traversal), следует загрузить и установить обновленный клиент L2TP/IPSec с сайта загрузки корпорации Microsoft.

В этом разделе мы рассмотрим процедуры, необходимые для создания на брандмауэре ISA VPN-сервера удаленного доступа по протоколу PPTP. Выполним следующие конкретные шаги:

- активизируем компонент VPN-сервера брандмауэра ISA;
- создадим правило доступа, разрешающее VPN-клиентам доступ к внутренней сети;
- разрешим удаленный доступ по телефонной линии (Dial-in) для учетных записей пользователей VPN;
- протестируем VPN-соединение по протоколу PPTP.

Включение VPN-сервера

Необходимо включить компонент VPN-сервера, так как он по умолчанию отключен. Первый шаг – активизация функции VPN-сервера и конфигурирование его компонентов. Делается это на консоли управления Microsoft Internet Security and Acceleration Server 2006 (Сервер защищенного быстрого доступа к сети Интернет 2006), а не на консоли сервиса RRAS.

Большая часть проблем конфигурации VPN брандмауэра ISA была связана с применением неопытными администраторами брандмауэра ISA консоли сервиса RRAS (Routing and Remote Access Services, сервис маршрутизации и удаленного доступа) для настройки VPN-компонентов. Несмотря на то, что возможны ситуации, в которых нам понадобится эта консоль, подавляющая часть конфигурирования VPN-сервера брандмауэра ISA и VPN-шлюза выполняется на консоли управления Microsoft Internet Security and Acceleration Server 2006 (Сервер защищенного быстрого доступа к сети Интернет 2006).

Выполните следующие шаги для включения и настройки VPN-сервера ISA 2006:

- Откройте консоль управления Microsoft Internet Security and Acceleration Server 2006 (Сервер защищенного быстрого доступа к сети Интернет 2006) и раскройте окно, связанное с именем сервера.
- Щелкните кнопкой мыши узел Virtual Private Networks (VPN) (Виртуальные частные сети).
- Щелкните мышью вкладку Tasks (Задачи) на панели задачи.
- Щелкните кнопкой мыши ссылку Enable VPN Client Access (Включить доступ VPN-клиентов).
- Щелкните мышью кнопку Apply (Применить) для сохранения изменений обновления политики брандмауэра.
- Щелкните мышью кнопку ОК в диалоговом окне Apply New Configuration (Сохранение изменений конфигурации).

- На вкладке Tasks (Задачи) щелкните кнопкой мыши ссылку Configure VPN Client Access (Настроить доступ VPN-клиентов).
- На вкладке General (Общие) в диалоговом окне VPN Clients Properties (Свойства: VPN-клиенты) измените значение параметра Maximum number of VPN clients allowed (Максимальное разрешенное количество VPN-клиентов) с 5 на 10. Версия Standard Edition брандмауэра ISA поддерживает до 1000 параллельных VPN-соединений. Это жестко заданный предел, и он не меняется независимо от количества VPN-соединений, поддерживаемых операционной системой Windows, в которой установлен брандмауэр ISA. У версии Enterprise edition бранд-мауэра ISA нет жестко заданного лимита и количество поддерживаемых VPN-соединений определяется базовой операционной системой. Точно число неизвестно, но если брандмауэр ISA установлен в ОС Windows Server 2003 версии Enterprise, вы можете создать к брандмауэру ISA 16 000 VPN-подключений по протоколу PPTP и 30 000 – по протоколу L2TP/IPSec.

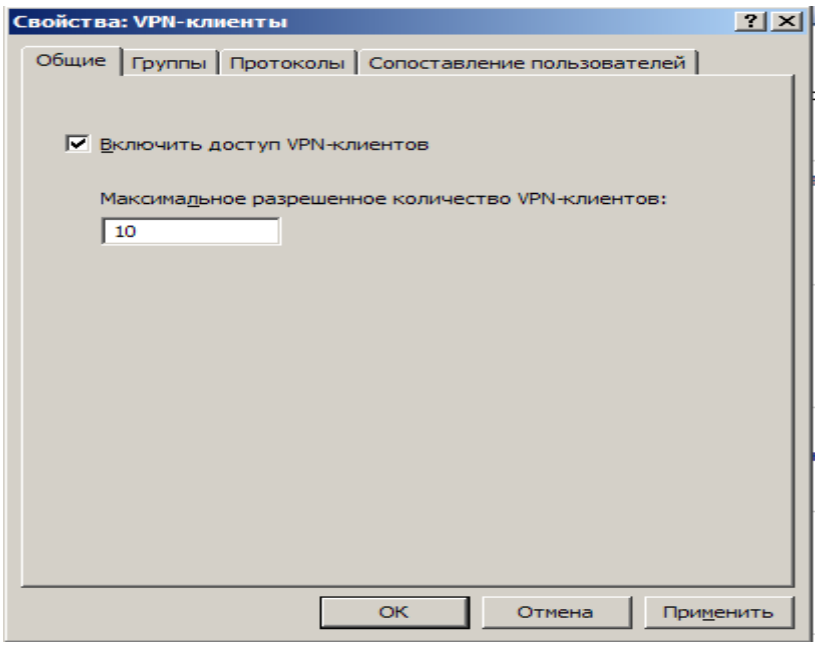


Рис.11. Вкладка «Общие (General)»

Убедитесь, что имеется количество IP-адресов для VPN-клиентов, по меньшей мере, равное числу, указанному в текстовом поле Maximum number of VPN clients allowed (Максимальное разрешенное количество VPN-клиентов). Определите количество VPN-клиентов, которые необходимо соединить с брандмауэром ISA, а затем добавьте единицу для самого брандмауэра ISA. Это и будет число, которое нужно ввести в данное текстовое поле.

- Щелкните кнопкой мыши вкладку Groups (Группы). На этой вкладке щелкните мышью кнопку Add (Добавить).
- В диалоговом окне Select Groups (Выбор: «Группы») щелкните мышью кнопку Locations (Размещение). В диалоговом окне Locations (Размещение) щелкните кнопкой мыши адрес USER-9E55B268E1, а затем кнопку ОК.
- В диалоговом окне Select Groups (Выбор: «Группы») в текстовое поле Enter the object names to select (Введите имена выбираемых объектов) введите VPN-клиенты. Щелкните мышью кнопку Check Names (Проверить имена). Как только имя группы будет найдено в базе данных Active Directory, оно будет подчеркнуто. Щелкните мышью кнопку ОК.
- Щелкните кнопкой мыши вкладку Protocols (Протоколы). На этой вкладке установите флажок Enable PPTP (Разрешить протокол PPTP) (рис. 12)

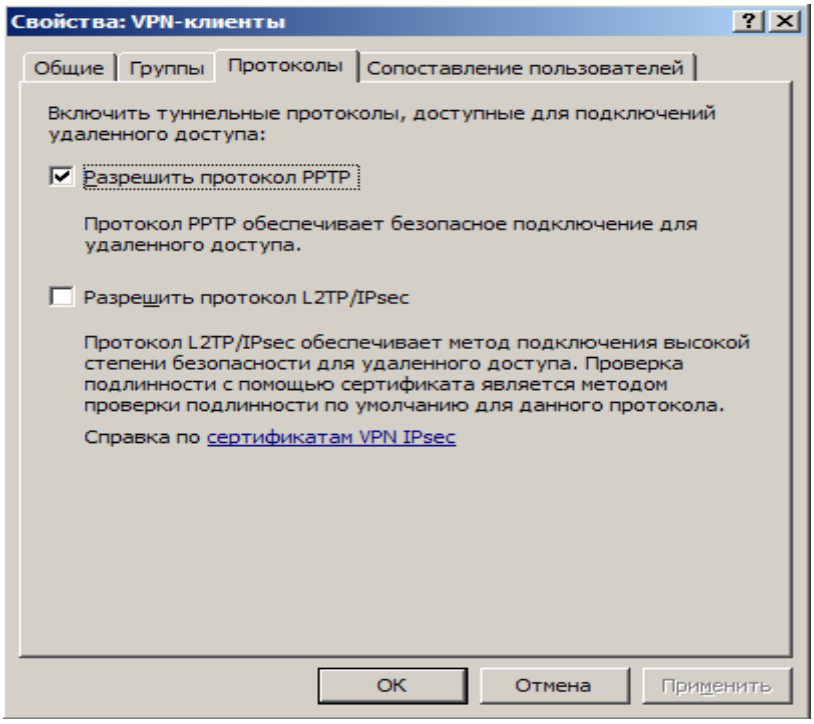


Рис. 12. Вкладка «Протоколы (Protocols)»

- Щелкните кнопкой мыши вкладку User Mapping (Сопоставление пользователей) (рис. 5.2.1.3). Установите флажок Enable User Mapping (Включить сопоставление пользователей) и флажок When username does not contain a domain, use this domain (Если в имени пользователя не содержится домен, использовать данный домен). Введите имя USER-9E55B268E1 в текстовое поле Domain Name (Доменное имя). Имейте в виду, что эти установки будут применяться при использовании аутентификации RADIUS/EAR Они игнорируются, когда используется аутентификация Windows (например, когда машина с брандмауэром ISA 2004 принадлежит домену и пользователь явно вводит верительные данные домена).

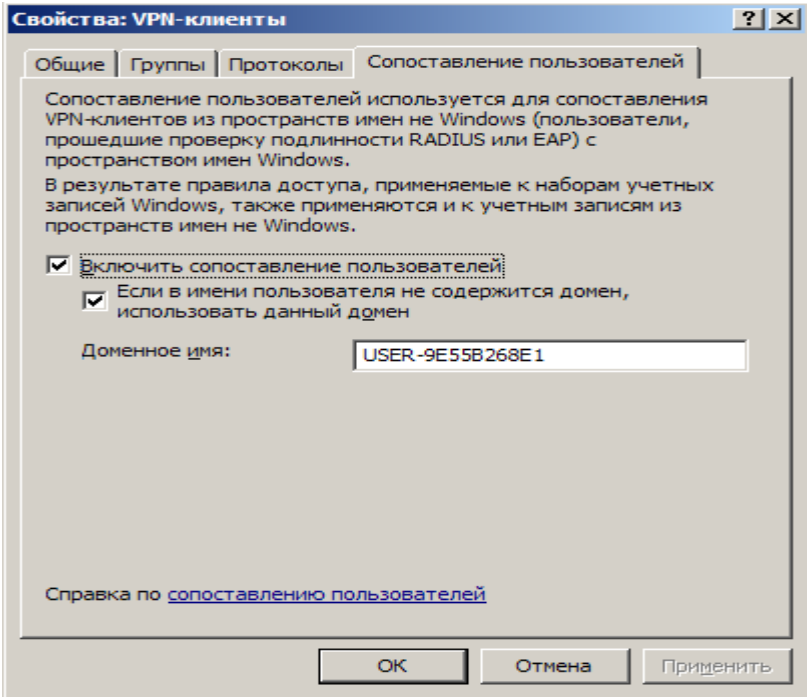


Рис. 13. Вкладка «Сопоставление пользователей (User Mapping)»

- Щелкните мышью кнопки Apply (Применить) и OK. Вы увидите диалоговое окно Microsoft Internet Security and Acceleration Server 2006 (Сервер защищенного быстрого доступа к сети Интернет 2006), информирующее вас о том, что необходимо перезапустить компьютер для ввода в действие установленных параметров. Если так, щелкните мышью кнопку OK в диалоговом окне.
- На вкладке Tasks (Задачи) щелкните кнопкой мыши строку Select Access Networks (Выбрать сети доступа).
- В диалоговом окне Virtual Private Networks (VPN) Properties (Свойства: Виртуальные частные сети) (рис. 5.2.1.4) щелкните кнопкой мыши вкладку Access Networks (Сети доступа). Обратите внимание на то, что установлен флажок External (Внешняя). Это означает, что внешний интерфейс ожидает входящие соединения от VPN-клиентов. Если вы хотите внутренних пользователей подключить к брандмауэру ISA, выберите флажок Internal (Внутренняя)

Есть также варианты, разрешающие VPN-подключения из All Networks (and Local Host Network) (Все сети, и локальный компьютер) и All Protected Networks (Все защищенные сети).

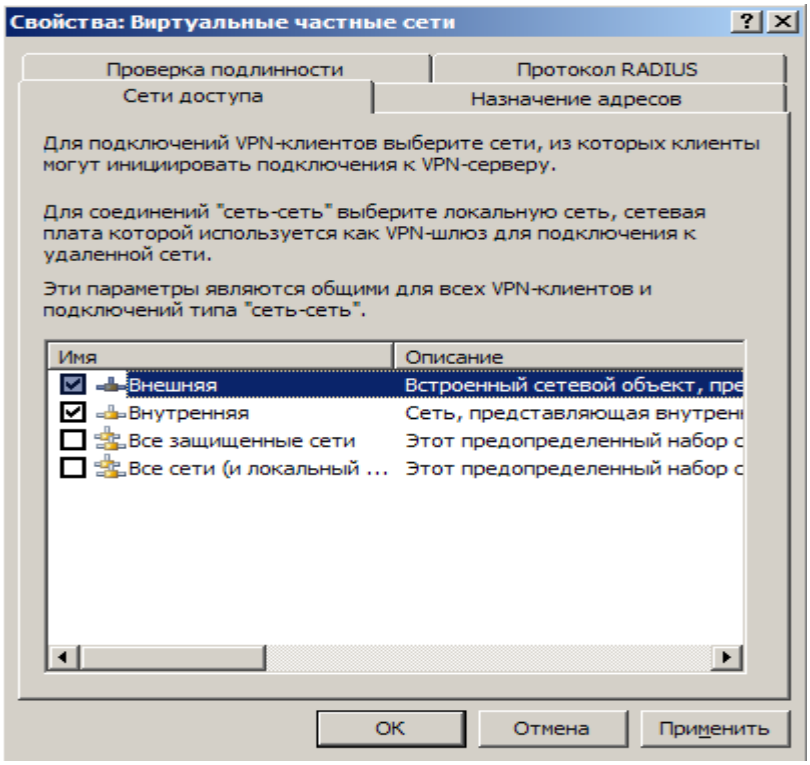


Рис. 14. Выбор сетей доступа

Возможность выбора VPN-соединений из разных сетей может быть полезна, если у вас есть небезопасные сети, расположенные за брандмауэром ISA. Предположим, что у вас есть трехадаптерный брандмауэр ISA, имеющий внешний интерфейс, внутренний интерфейс и интерфейс WLAN (Wireless Local Area Network, беспроводная локальная сеть). Интерфейс WLAN применяется для пользователей портативных компьютеров (laptop), которые не управляются вашей организацией. Вы можете потребовать также и от пользователей управляемых компьютеров использовать сегмент WLAN, когда они приносят портативные компьютеры, которые перемещаются между корпоративной сетью и сетями, не заслуживающими доверия.

Вы настраиваете правила доступа на брандмауэре ISA, запрещающие соединения из сегмента WLAN. Но вы формируете правила доступа,

разрешающие VPN-соединения с интерфейсом WLAN для подключения к ресурсам корпоративной внутренней сети. В этом случае никто из пользователей, соединяющихся с сегментом WLAN, не способен получить доступ к ресурсам в корпоративной внутренней сети, за исключением тех корпоративных пользователей, кто может установить VPN-соединение с интерфейсом WLAN на брандмауэре ISA и предоставить соответствующие верительные данные для завершения VPN-соединения. Другой сценарий, в котором вы можете разрешить VPN-соединение с брандмауэром ISA, – функционирование брандмауэра ISA как внешнего (front-end) брандмауэра. В этом случае вы, возможно, не захотите разрешать прямые соединения по протоколу RDP (Remote Desktop Protocol, протокол удаленного рабочего стола) или удаленные соединения MMC с брандмауэром ISA. У вас есть возможность разрешить RDP-соединения только от VPN-клиентов и затем разрешить VPN-клиентам доступ по протоколу RDP к сети локального хоста (Local Host Network). В этом случае пользователь должен установить защищенное VPN-соединение с внешним брандмауэром ISA, прежде чем может быть установлено RDP-соединение. Хостам, соединяющимся с помощью любых других средств, запрещается доступ к RDP-протоколам.

- Щелкните кнопкой мыши вкладку Address Assignment (Назначение адресов) (рис. 5.2.1.5). Выберите в раскрывающемся списке Use the following network to obtain DHCP, DNS and WINS services (Использовать следующую сеть для получения доступа к службам DHCP, DNS и WINS) элемент Internal (Внутренняя). Это важная установка, поскольку она определяет сеть, в которой осуществляется доступ к сервису DHCP.

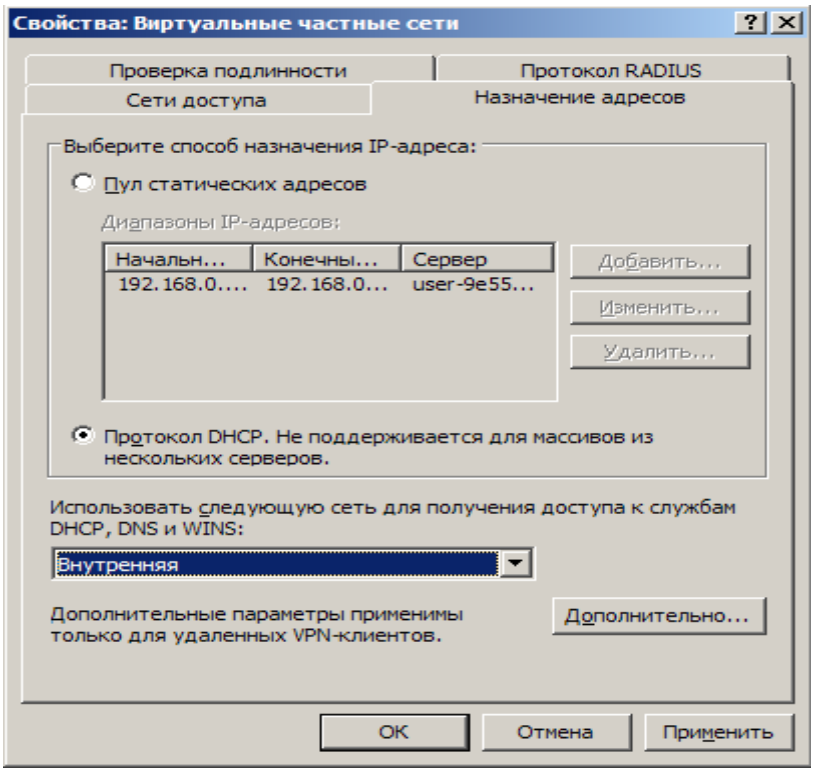


Рис. 15. Вкладка «Назначение адресов (Address Assignment)»

Заметьте, что это не единственно возможный выбор. Можно выбрать любой из адаптеров брандмауэра ISA в списке Use the following network to obtain DHCP, DNS and WINS services (Использовать следующую сеть для получения сервисов DHCP, DNS и WINS). Ключевой вывод заключается в том, что вы выбираете адаптер, на котором есть корректная информация сервера имен и наиболее вероятный кандидат – внутренний интерфейс брандмауэра ISA. У вас также есть возможность использовать Static address pool (Пул статических адресов) для назначения адресов VPN-клиентам. Проблема применения пула статических адресов заключается в том, что при назначении адресов из подсети (адреса в сети с тем же сетевым идентификатором (ID), что и один из интерфейсов брандмауэра ISA) необходимо удалять эти адреса из сети, к которой подсоединен брандмауэр ISA.

Предположим, что у брандмауэра ISA есть два сетевых интерфейса: внешний и внутренний. Внутренний интерфейс соединен с вашей внутренней сетью по умолчанию и ее сетевой идентификатор – 192.168.1.0/24. Если вы хотите назначить адреса VPN-клиентам из диапазона адресов внутренней сети,

используя пул статических адресов, например 192.168.1.200/211 (всего 10 адресов), вам нужно будет вручную удалить эти адреса из определения внутренней сети, прежде чем вы сможете создать из них пул статических адресов. Если вы попытаетесь создать пул статических адресов с сохранением этих адресов в подсети (on subnet), то увидите сообщение об ошибке.

- Щелкните кнопкой мыши вкладку Authentication (Проверка подлинности). Отметьте, что установлен только флажок Microsoft encrypted authentication version 2 (MS-CHAPv2) (Шифрованная аутентификация версии 2, Протокол проверки подлинности запроса-подтверждения Microsoft версии 2).

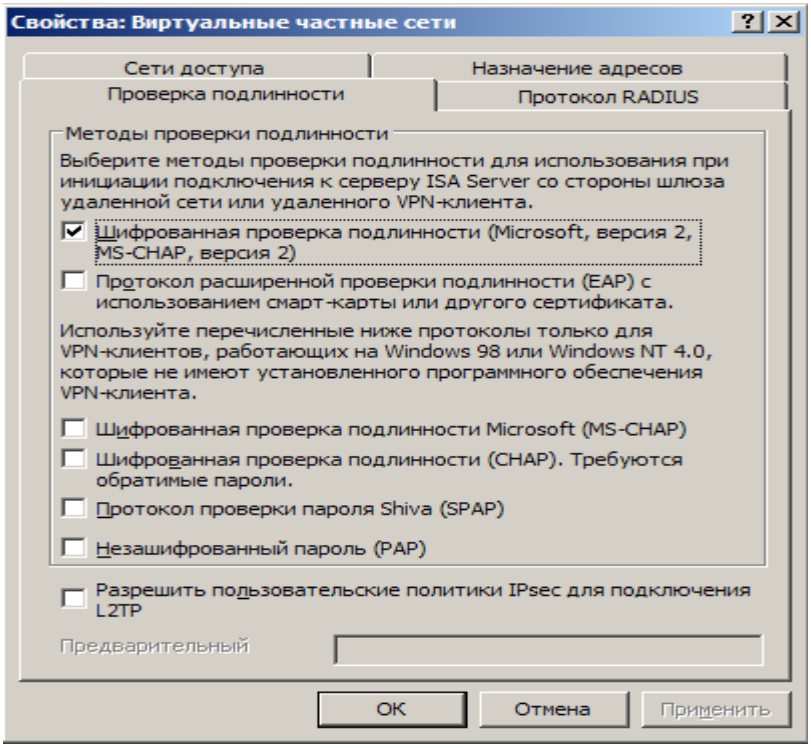


Рис.16. Вкладка «Проверка подлинности (Authentication)»

- Щелкните кнопкой мыши вкладку Протокол RADIUS (Remote Authentication Dial-In User Service, служба аутентификации удаленного дозванивающегося (коммутируемого) пользователя). На этой вкладке можно настроить VPN-сервер брандмауэра ISA 2006 для применения аутентификации VPN-пользователей с помощью сервиса RADIUS. Преимущество подтверждения подлинности

средствами RADIUS заключается в том, что можно привлечь базу данных пользователей службы Active Directory (или других каталогов) для аутентификации пользователей без обязательного членства в домене брандмауэра ISA.

- В диалоговом окне Virtual Private Networks (VPN) Properties (Свойства: Виртуальные частные сети) щелкните мышью кнопку Apply (Применить) и затем кнопку ОК.
- Щелкните мышью кнопку Apply (Применить) для сохранения изменений и обновления политики брандмауэра
- Щелкните мышью кнопку ОК в диалоговом окне Apply New Configuration (Применить новую конфигурацию).
- Перезапустите машину с брандмауэром ISA.

Создание правила доступа, предоставляющего VPN-клиентам доступ к разрешенным ресурсам

Брандмауэр ISA после перезапуска компьютера сможет принимать входящие VPN-соединения. Но VPN-клиенты не получат доступ к ресурсам, поскольку нет правил доступа, разрешающих им получать что-либо. Следует создать правила доступа, разрешающие членам сети VPN-клиентов обращаться к ресурсам, которые вы захотите им предоставить. Этот вариант значительно отличается от других комбинированных решений брандмауэра/VPN-сервера, в которых применяются отслеживающие состояние соединений фильтрация и проверка на прикладном уровне всех соединений VPN-клиентов.

В следующем примере создается правило доступа, разрешающее любому трафику проходить из сети VPN-клиентов во внутреннюю сеть. В производственной среде вам пришлось бы создавать более строгие правила доступа, для того чтобы пользователи сети VPN-клиентов получали доступ только к тем ресурсам, которые им необходимы.

Выполните следующие шаги для создания правила доступа, обеспечивающего неограниченный доступ для VPN-клиентов.

- На консоли управления The Microsoft Internet Security and Acceleration Server 2006 (Сервер защищенного быстрого доступа к сети Интернет 2004) раскройте окно, связанное с именем сервера, и щелкните кнопкой мыши узел Firewall Policy (Политика межсетевого экрана). Щелкните правой кнопкой мыши узел Firewall Policy (Политика брандмауэра), укажите левой кнопкой мыши команду New (Создать) и затем Access Rule (Правило доступа).
- На странице New Access Rule Wizard (Мастер создания правила доступа) введите название правила в текстовое поле Access Rule name (Имя правила доступа). В данном примере – VPN Client to Internal. Щелкните мышью кнопку Next (Далее).
- На странице Rule Action (Действие правила) выберите вариант Allow (Разрешить) и щелкните мышью кнопку Next (Далее).
- На странице Protocols (Протоколы) выберите вариант All outbound protocols (Весь исходящий трафик) в списке This rule applies to (Данное правило применяется к). Щелкните мышью кнопку Next (Далее).
- На странице Access Rule Sources (Источники правил доступа) щелкните мышью кнопку Add (Добавить). В диалоговом окне Add Network Entities (Добавление сетевых сущностей) щелкните кнопкой мыши папку Networks (Сети) и дважды щелкните мышью узел VPN Clients (VPN-клиенты). Щелкните мышью кнопку Close (Закрыть).
- Щелкните мышью кнопку Next (Далее) на странице Access Rule Sources (Источники правил доступа).
- На странице Access Rule Destinations (Пункты назначения правил доступа) щелкните мышью кнопку Add (Добавить). В диалоговом

окне Add Network Entities (Добавление сетевых сущностей) щелкните кнопкой мыши папку Networks (Сети) и дважды щелкните мышью узел Internal (Внутренняя) и Local Computer (Локальный компьютер). Щелкните мышью кнопку Close (Закрыть).

- На странице User Sets (Наборы учетных записей) согласитесь с установкой по умолчанию All Users (Все пользователи) и щелкните мышью кнопку Next (Далее).
- Щелкните кнопку Finish (Готово) на странице Completing the New Access Rule Wizard (Завершение мастера создания Правило доступа).
- Щелкните мышью кнопку Apply (Применить) для сохранения изменений и обновления политики брандмауэра.
- Щелкните мышью кнопку ОК в диалоговом окне Apply New Configuration (Применить новую конфигурацию). Политика VPN-клиента теперь отражена в верхнем правиле доступа, приведенном в списке политики доступа.

С этого момента VPN-клиенты, успешно подтвердившие свою подлинность и имеющие разрешение на соединение по телефонной линии, имеют возможность доступа ко всем ресурсам внутренней сети с помощью любого протокола.

Разрешение удаленного доступа по телефонной линии

В доменах Active Directory, находящихся в неосновном режиме (non-native mode), для всех учетных записей пользователей по умолчанию удаленный доступ по телефонной линии (dial-in) запрещен. Вы должны разрешить такой доступ, основываясь на учетных записях для этих доменов Active Directory, находящихся в неосновном режиме. Напротив, в доменах Active Directory, находящихся в основном режиме (native mode), по умолчанию удаленный доступ по телефонной линии управляется политикой удаленного доступа

(Remote Access Policy). В доменах ОС Windows NT 4.0 удаленный доступ по телефонной линии управляется посредством учетных записей пользователя.

Выполните следующие шаги на контроллере домена для разрешения удаленного доступа по телефонной линии для учетной записи Administrator.

- Щелкните мышью кнопку Start (Пуск) и строку Administrative Tools (Администрирование). Щелкните мышью оснастку Active Directory Users and Computers (Active Directory – пользователи и компьютеры).
- В оснастке Active Directory Users and Computers (Active Directory – пользователи и компьютеры) щелкните мышью узел Users (Пользователи) на левой панели. Дважды щелкните кнопкой мыши учетную запись Administrator на правой панели оснастки.
- Щелкните кнопкой мыши вкладку Dial-in (Соединение по телефонной линии). В области Remote Access Permission (Dial-in or VPN) (Разрешение удаленного доступа, по модему или через сеть VPN) выберите переключатель Allow access (Разрешить доступ). Щелкните мышью кнопку Apply (Применить) и затем кнопку ОК.
- Закройте оснастку Active Directory Users and Computers (Active Directory – пользователи и компьютеры).

Другой вариант – создать группы на самом брандмауэре ISA и поместить их в группы. Этот метод позволит применить установочные параметры по умолчанию в учетных записях пользователей, созданных на брандмауэре, для которых по умолчанию выбран для удаленного доступа по телефонной линии Control access via Remote Access Policy (Контроль доступа с помощью политики удаленного доступа).

Несмотря на то, что этот вариант не слишком хорошо регулируется, он вполне жизнеспособен в тех организациях, у которых ограниченное количество VPN-пользователей и которые не хотят применять подтверждения подлинности с помощью системы RADIUS или не имеют RADIUS-сервера для использования.

Выполните следующие шаги для создания группы пользователей, имеющих доступ к VPN-серверу брандмауэра ISA.

- На рабочем столе брандмауэра ISA щелкните правой кнопкой пиктограмму My Computer (Мой компьютер) и щелкните левой кнопкой мыши команду Manage (Управление).
- На консоли Computer Management (Управление компьютера) раскройте узел System Tools (Служебные программы) и затем узел Local Users and Groups (Локальные пользователи и группы). Щелкните правой кнопкой мыши папку Groups (Группы) и левой кнопкой мыши щелкните команду New Group (Новая группа).
- В диалоговом окне New Group (Новая группа) введите имя группы в текстовое поле Group Name (Имя группы). В данном примере мы назовем группу VPN Users. Щелкните мышью кнопку Add (Добавить).
- В диалоговом окне Select: users (Выбор: пользователи) щелкните мышью кнопку Advanced (Дополнительно).
- В диалоговом окне Select: users (Выбор: пользователи) выберите пользователей или группы, которые вы хотите сделать членами группы VPN-Клиенты. В этом примере мы выберем Authenticated Users (Аутентифицированные пользователи). Щелкните мышью кнопку ОК. Щелкните мышью кнопку ОК в диалоговом окне Select: users (Выбор: пользователи).
- Щелкните мышью кнопку Create (Создать), а затем кнопку Close (Закрыть).

Теперь настроим компонент VPN-сервера брандмауэра ISA для разрешения доступа членам группы VPN-Клиенты.

- На консоли управления Microsoft Internet Security and Acceleration Server 2004 (Сервер защищенного быстрого доступа к сети Интернет

2006) раскройте окно, связанное с именем сервера, и щелкните кнопкой мыши узел Virtual Private Networking (VPN) (Виртуальные частные сети). Щелкните кнопкой мыши строку Configure VPN Client Access (Настроить доступ VPN-клиентов) на вкладке Tasks (Задачи) на панели задачи.

- В диалоговом окне VPN Clients Properties (Свойства: VPN-клиенты) на вкладке Groups (Группы) щелкните мышью кнопку Add (Добавить).
- В диалоговом окне Select Groups (Выбор: «Группы») введите VPN-Клиенты в текстовое поле Enter the object name to select (Введите имена выбираемых объектов) и щелкните мышью кнопку Check Names (Проверить имена). Найденное имя группы будет подчеркнуто. Щелкните мышью кнопку ОК.

В данном примере мы ввели локальную группу VPN-Клиенты на вкладке Groups (Группы), потому что VPN-доступ может контролироваться с помощью режима Control access through Remote Access Policy (Контроль доступа с помощью политики удаленного доступа), установленного для учетных записей пользователей в локальном диспетчере SAM (Security Accounts Manager, диспетчер учетных записей безопасности) брандмауэра ISA. Вы также можете ввести пользователей и группы домена (если брандмауэр ISA является членом домена пользователей), если домен поддерживает удаленный доступ по телефонной линии с помощью политики удаленного доступа.

- Щелкните мышью кнопку Apply (Применить), а затем кнопку ОК в диалоговом окне VPN Client Properties (Свойства: VPN-клиенты)
- Щелкните мышью кнопку Apply (Применить) для сохранения изменений и обновления политики брандмауэра.
- Щелкните мышью кнопку ОК в диалоговом окне Apply New Configuration (Применить новую конфигурацию).

Тестирование VPN-соединения по протоколу PPTP

Теперь VPN-сервер брандмауэра ISA 2006 готов для приема соединений от VPN-клиентов.

Выполните следующие шаги для тестирования VPN-сервера.

- На машине внешнего клиента с ОС Windows XP щелкните правой кнопкой мыши пиктограмму My Network Places (Сетевое окружение) на рабочем столе и выберите команду Properties (Свойства).
- Дважды щелкните кнопкой мыши строку New Connection Wizard (Мастер новых подключений) в окне Network Connections (Сетевые подключения).
- Щелкните мышью кнопку Next (Далее) на странице Welcome to the New Connection Wizard (Вас приветствует мастер новых подключений).
- На странице Network Connection Type (Тип сетевого подключения) выберите переключатель Connect to a private network at my workplace (Подключить к сети на рабочем месте) и щелкните мышью кнопку Next (Далее).
- На странице Network Connection (Сетевое подключение) выберите переключатель Virtual Private Network connection (Подключение к виртуальной частной сети) и щелкните мышью кнопку Next (Далее).
- На странице Connection Name (Имя подключения) введите VPN в текстовое поле Company Name (Организация) и щелкните мышью кнопку Next (Далее).
- На странице VPN Server Selection (Выбор VPN-сервера) введите IP-адрес на внешнем интерфейсе брандмауэра ISA в текстовое поле Host name or IP address (Имя компьютера или IP-адрес). Щелкните мышью кнопку Next (Далее).

- Щелкните мышью кнопку Finish (Готово) на странице Completing the New Connection Wizard (Завершение Мастера новых подключений).
- В диалоговом окне Connect VPN (VPN-подключение) введите имя пользователя Administrator и пароль для учетной записи администратора (если брандмауэр ISA – член домена, введите имя компьютера или имя домена перед именем пользователя в формате NAME\username). Щелкните мышью кнопку Connect (Подключиться).
- VPN-клиент устанавливает соединение с VPN-сервером брандмауэра ISA 2006.Щелкните мышью кнопку ОК в диалоговом окне Connection Complete (Соединение установлено), информирующем об установке соединения.
- Дважды щелкните кнопкой мыши пиктограмму соединения на системной панели задач, а затем щелкните мышью вкладку Details (Сведения). Вы увидите шифрование MPPE 128 (Microsoft Point-to-Point Encryption), применяемое для защиты данных, и IP-адрес, назначенный VPN-клиенту. Щелкните мышью кнопку Close (Закрыть).
- Щелкните правой кнопкой мыши по пиктограмме соединения на панели задач и щелкните левой кнопкой мыши кнопку Disconnect (Отключить).

Защита границ корпоративной сети предприятия от внешних угроз, контроль входящего и исходящего Интернет трафика и маршрутизация внутри локальных подсетей являются важными элементами системы безопасности. С каждым разом угроза заражения данных вирусами и уровень хакерских атак на сеть возрастают, а нерадивые пользователи стремятся "обойти" установленные ограничения. Решить задачи по контролю маршрутизации пакетов можно с помощью профессиональных программных брандмауэров.

Одним из таких решений является **Microsoft Internet Security and Acceleration Server 2006 (ISA Server**). Этот брандмауэр может контролировать сетевой трафик на пяти уровнях стека протоколов TCP/IP, кроме канального и физического уровней. Он способен контролировать не только заголовки пакетов, но и раскрывать их содержимое, анализировать скрытую информацию. Этой системой также, безусловно, поддерживается контроль адресов пакетов.

ISA Server можно использовать не только как внешний сетевой экран, с помощью которого корпоративная сеть отделяется от Интернета, но также и как контролер Интернет-трафика во внутренней сети. Также ISA Server можно использовать в качестве прокси. Он способен кэшировать содержимое внешних web-узлов. При этом их содержимое будет сохраняться в локальной сети. В случае повторного обращения пользователей к внешнему web-серверу ответ даст ISA Server компании, что существенно разгрузит внешний канал связи. Его кэш достаточно производителен, т.к. содержимое сохраняется не только на жестких дисках, но и в оперативной памяти сервера. При этом сам кэш представляет собой единый индексированный файл, что существенно ускоряет поиск нужной информации. Кэшировать объекты можно по расписанию.

Это полезно если клиенты корпоративной сети часто пользуются одним и тем же сайтом, информация на котором меняется. В этом случае ISA Server может загружать новую версию сайта раз в несколько минут, предоставляя пользователям максимально адекватную времени информацию. В случае если на предприятии используются несколько ISA Serverов, между ними можно распределить задачи по кэшированию.

Располагая ISA Server на границе корпоративной сети и внешнего Интернета, можно использовать его как брандмауэр. В этом случае внешний адрес присваивается только ISA Server, который проводит безопасную идентификацию внешних пользователей и осуществляет их связь с внутренними серверами компании. При этом внутренние серверы компании не видны из

Интернета, но прошедшие проверку пользователи могут получить доступ к их сервисам.

Как брандмауэр ISA Server поддерживает множество фильтров, пакетов, каналов и приложений, что позволяет дать доступ только к явно указанным ресурсам в случае необходимости. Используя комбинацию фильтров можно защитить данные даже тогда, когда протоколы, по которым происходит связь, сами по себе являются небезопасными. Также брандмауэр способен определять вторжение в автоматическом режиме по заранее заданным шаблонам.

ISA Server имеет очень гибкий инструмент по настройке внутренней и внешней сетевой топологии. Этот элемент является важным, т.к. позволяет отделить внутренние сети от внешних и применять различные политики доступа к различным сетевым сегментам. Компьютеры объединяются в группы в соответствии с диапазонами адресов, что позволяет в настройках ISA Server'а создать максимально точную модель корпоративной сетевой топологии. Поэтому можно управлять потоками данных не только между внутренней сетью и внешним Интернетом, но и между отдельными сетевыми сегментами предприятия.

4. Рекомендуемая литература

1 Томас В. Шиндер, Дебра Л. Шиндер / ISA Server 2004. – БХВ-Петербург, Русская Редакция, 2005. – 1064 с.

2 http://www.microsoft.com

3 http://www.isadocs.ru

4 http://www.isaserver.ru

Лабораторная работа 5. Исследование и развертывание сетевой инфраструктуры Microsoft Windows Exchange Server

1. Цель работы

Выполнить комплекс лабораторных работ, направленных на проектирование, внедрение, управление и поддержку сетевой инфраструктуры Microsoft Windows Server 2003. Данный комплекс работ может рассматриваться как одна из возможных реализаций по развертыванию IT-инфраструктуры небольшого предприятия.

2. Краткие теоретические сведения

IT-инфраструктура – это комплекс взаимосвязанных систем передачи данных, аппаратных и программных информационных систем, служб и набор средств управления, настольными и переносными компьютерами, серверами, системами хранения данных, сетевыми устройствами, операционными системами и приложениями, удовлетворяющих потребностям бизнеса, действующих в режиме повышенной готовности, отказоустойчивости и безопасности, и имеющие потенциал для масштабирования, не снижающего эффективность управления информационной системой.

Сегодня IT-инфраструктура компании имеет критически важное значение для ее успешной деятельности. Это утверждение одинаково применимо как к крупному, так и к малому и среднему бизнесу во всех отраслях экономики.

Бизнес-приложения, корпоративные сети, серверы и центры обработки данных уже давно стали неотъемлемой частью корпоративной инфраструктуры любой компании и обеспечивают жизненно необходимые бизнес-процессы.

Внедрение Информационных Технологий сопровождается повышенными требованиями к адаптивности, производительности и масштабируемости оборудования, к защите информации и доступности данных и приложений, к надежности эксплуатации.

Структура предприятия

При проектировании IT-инфраструктуры в первую очередь следует знать, как устроена та или иная организация.

В рамках данной работы предприятием, для которого необходимо разработать IT-инфраструктуру, является вымышленная компания «ДéвельСофт», занимающаяся разработкой и продажей программного обеспечения.

Структура компании (рис. 1) состоит из следующих организационных единиц:

- Руководство компанией;
- Отдел кадров;
- Бухгалтерия;
- Плановый отдел;
- Отдел проектирования и разработки;
- Отдел продаж;
- Отдел по работе с клиентами;
- Юридический отдел;
- Рекламно-маркетинговый отдел;
- IT-отдел.

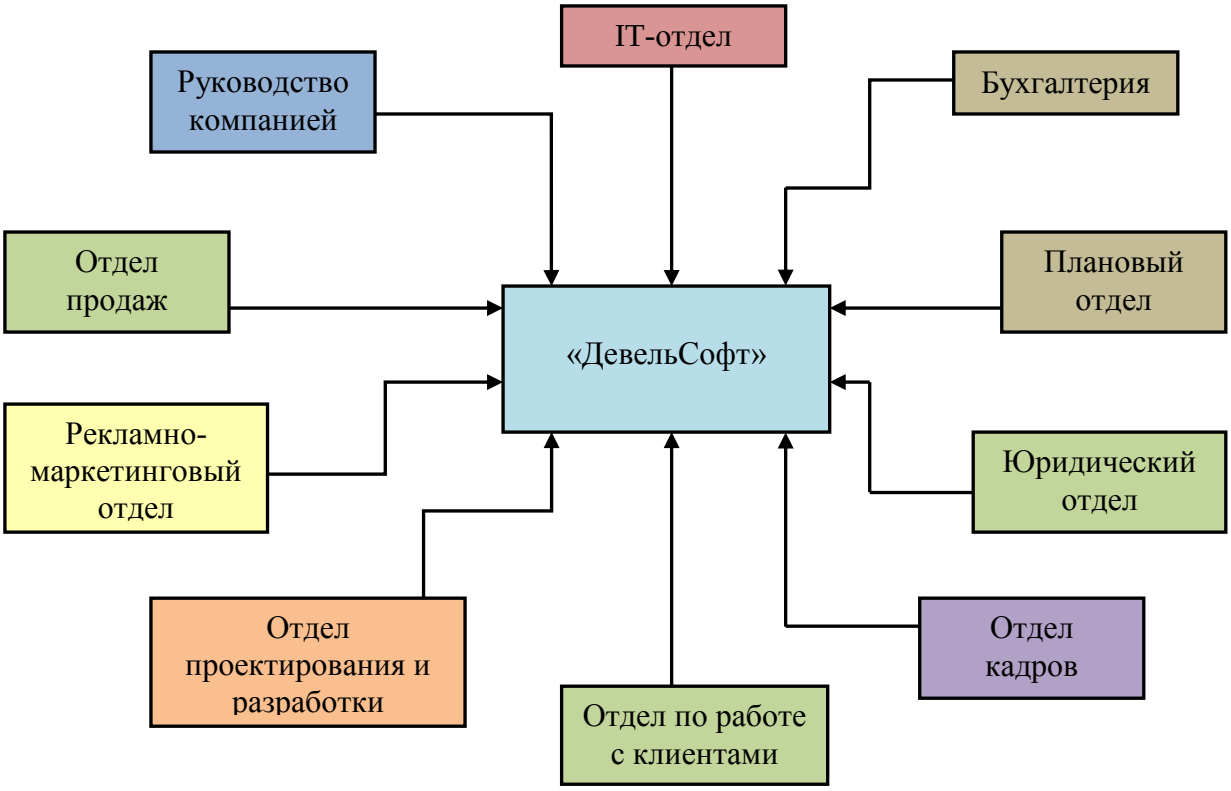


Рис. 1. Структура компании «ДевельСофт»

Информационные ресурсы предприятия

Для ведения бизнеса компании «ДевельСофт» необходимы следующие информационные ресурсы:

- Файловый сервер;
- Сервер печати;
- Почтовый сервер.

Также требуется обеспечить служащим безопасный доступ в сеть Интернет.

К внутренней сети компании необходим защищенный удаленный доступ, как для сотрудников, так и для партнеров компании.

На одном из серверов будет размещаться веб-сайт организации.

В таблице 1 приведено количество стационарных и мобильных рабочих станций сотрудников компании.

Таблица 1. Количество рабочих станций

Организационная единица	Количество рабочих станций	
	стационарных	мобильных
Руководство компанией	0	3
Отдел кадров	2	0
Бухгалтерия	3	0
Плановый отдел	3	0
Отдел проектирования и разработки	10	0
Отдел продаж	0	5
Отдел по работе с клиентами	0	3
Юридический отдел	1	0
Рекламно-маркетинговый отдел	5	5
IT-отдел	3	0

Физическая структура сети и схема IP-адресации

На рис. 2 приведена схема сети компании.

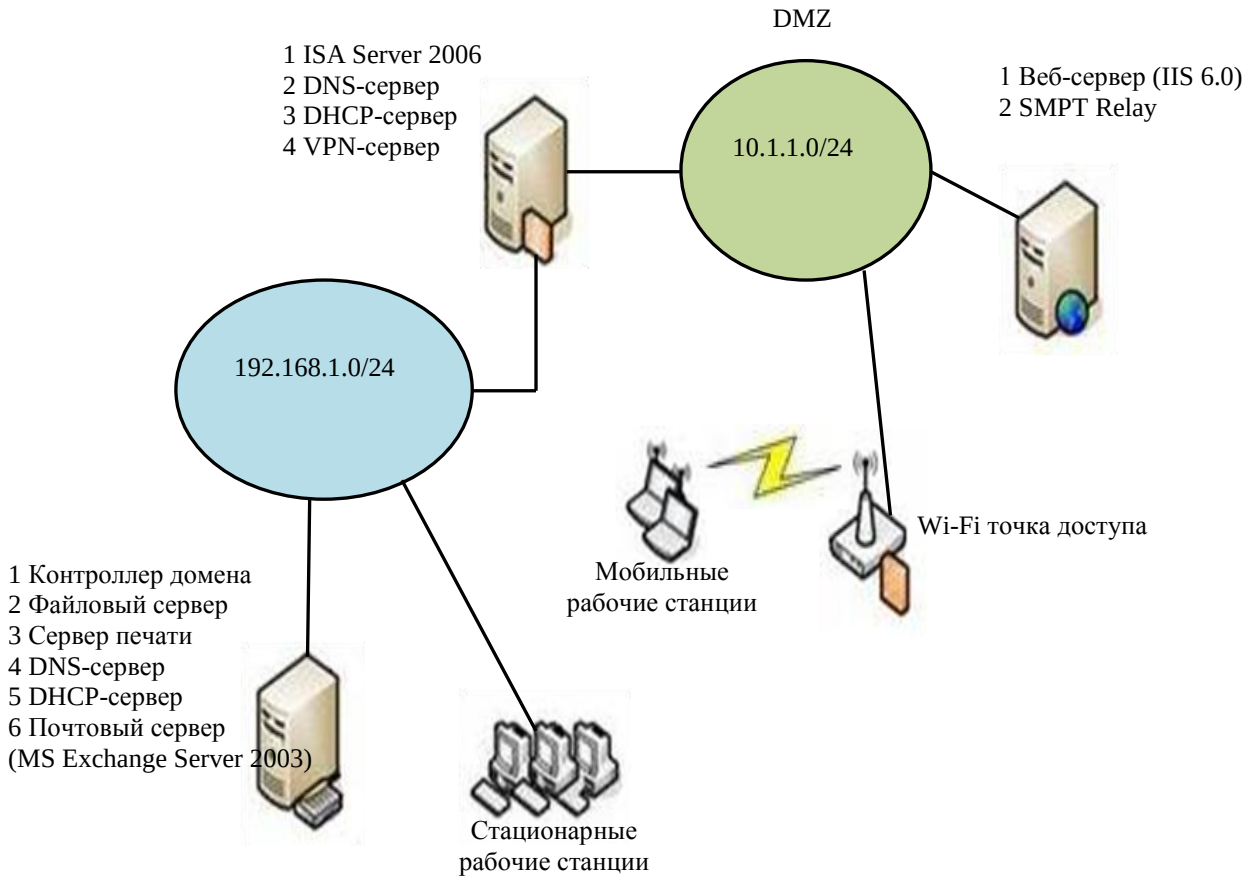


Рис. 2. Общая схема сети компании

Один из серверов будет использоваться в качестве межсетевого экрана (ISA Server) между внутренней сетью компании, демилитаризованной зоной (DMZ) и сетью Интернет, поэтому на нем будут задействованы три сетевых адаптера.

ДМЗ (демилитаризованная зона, DMZ) – технология обеспечения защиты информационного периметра, при которой серверы, отвечающие на запросы из внешней сети, находятся в особом сегменте сети (который и называется ДМЗ) и ограничены в доступе к основным сегментам сети с помощью межсетевого экрана, с целью минимизировать ущерб, при взломе одного из общедоступных сервисов находящихся в ДМЗ.

ISA Server позволит обезопасить внутреннюю сеть организации от атак из сети Интернет, организовать удаленный доступ к сети компании с помощью технологии VPN, проводить ограничение доступа к сети Интернет для отдельных групп пользователей и вести статистику использования сети Интернет сотрудниками компании.

Другой сервер будет хранить централизованную базу учетных записей пользователей, политики безопасности, а также предоставлять сервисы назначения IP-адресов клиентским компьютерам (DHCP) и разрешения имен (DNS). Также этот сервер будет выполнять функции файлового сервера, сервера печати и почтового сервера (MS Exchange Server).

Третий сервер (IIS) находится в ДМЗ и используется для размещения содержимого Интернет-сайта организации. Также на нем будет размещена служба SMPT Relay для повышения безопасности электронной почты и установлена программа блокирования спама и проверки почты на вирусы. Это позволит затруднить атаки, явно направленные против MS Exchange Server. Вся входящая почта будет приходить сначала на SMTP Relay, где будет проверяться на вирусы и спам, а затем уже будет пересылаться на MS Exchange Server.

Политики именования объектов сети

Политики представлены в таблице 2.

Таблица 2. Шаблоны имен сетевых объектов

Сетевые объекты	Шаблон имени
Рабочие станции	*отдел-номер_станции* Пример: **razrabotki-07, buhgalterija-01**
Печатающие устройства	*отдел-количество_цветов_печати* Пример: **reklamnyj-color, planovyj-monochrome**

Логическая организация сетевой инфраструктуры.

Схема Active Directory

В качестве централизованного средства администрирования и управления сетевой средой используется служба каталогов Active Directory. Для организаций, внедряющих Microsoft Windows Server 2003, модель домена Active Directory является наиболее предпочтительной и рекомендованной компанией Microsoft. База данных службы каталогов устанавливается на один или несколько компьютеров – контроллеров домена.

В данном проекте в сети организации используется один домен - **develsoft.local**. В качестве DNS-суффикса домена используется ".local", что является рекомендованным к применению в частных сетях. Для работы Active Directory требуется служба DNS, поэтому контроллер домена DomainController является также севером DNS, который, в свою очередь, является основным методом разрешения имен хостов в сети.

Для назначения IP-конфигурации рабочим станциям внутренней сети и беспроводным клиентам применяется служба DHCP. При этом компьютер ISAServer самостоятельно обслуживает область адресов, которые выдаются беспроводным клиентам, а область адресов, соответствующая внутренней сети, обслуживается компьютерами DomainController и ISAServer одновременно, в соответствие с правилом 80/20. Таким образом, в случае отказа одного из серверов, второй сервер примет на себя его функции по предоставлению IP-конфигурации клиентам внутренней сети и обеспечит бесперебойную работу.

Схема Active Directory приведена на рисунке 3.

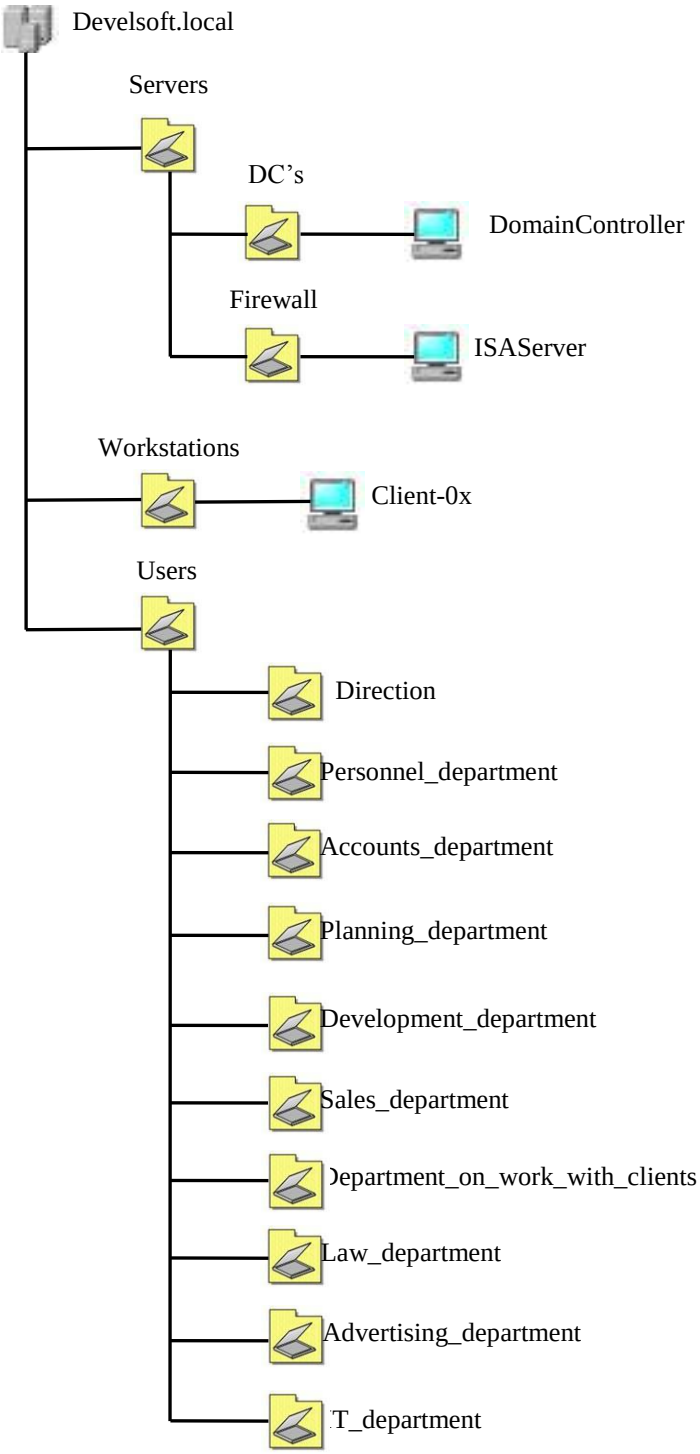


Рис. 3. Схема Active Directory

Структура каталогов для хранения данных

Предлагается использовать следующую структуру каталогов для организации файлового архива компании (рис. 4)

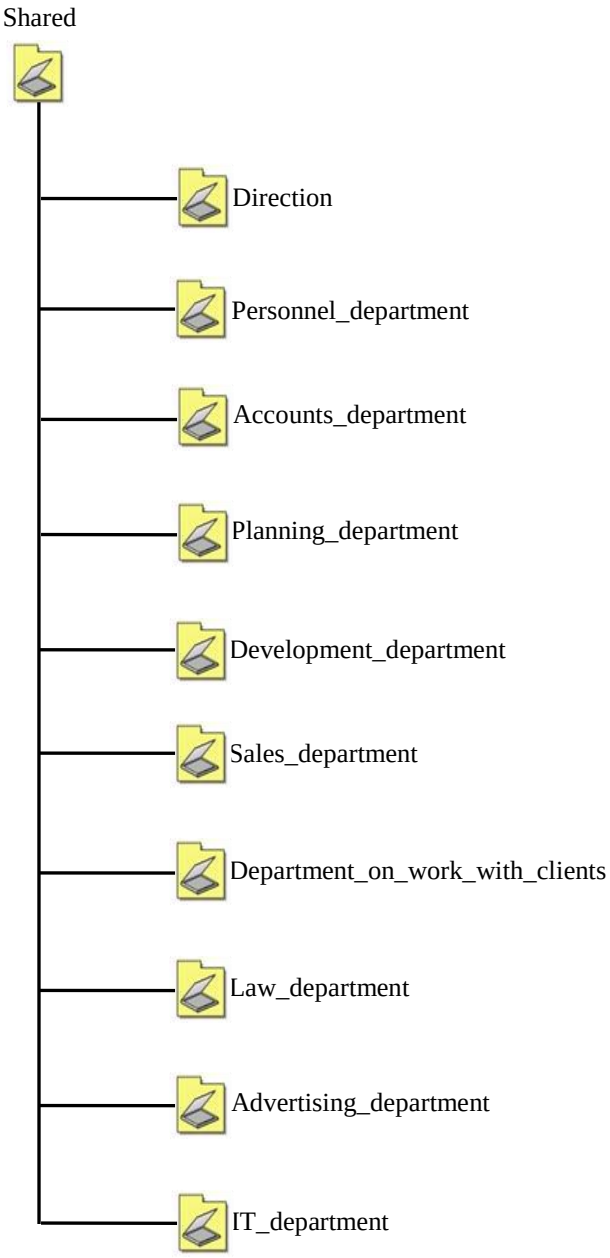


Рис. 4. Структура каталогов для хранения данных

3. Порядок выполнения работы

Установка и настройка Windows Server 2003

Характерные этапы установки Windows Server 2003 описаны в задании №1.

После установки и активации Windows можно настроить сервер, используя хорошо продуманную страницу **Управление данным сервером (Manage Your Server)** (рис. 5), которая автоматически открывается при входе в систему. Эта страница упрощает установку некоторых служб, инструментов и конфигураций в зависимости от роли сервера. Щелкните кнопку **Добавить или удалить роль (Add Or Remove A Role),** появится окно *Мастера настройки сервера* (Configure Your Server Wizard).

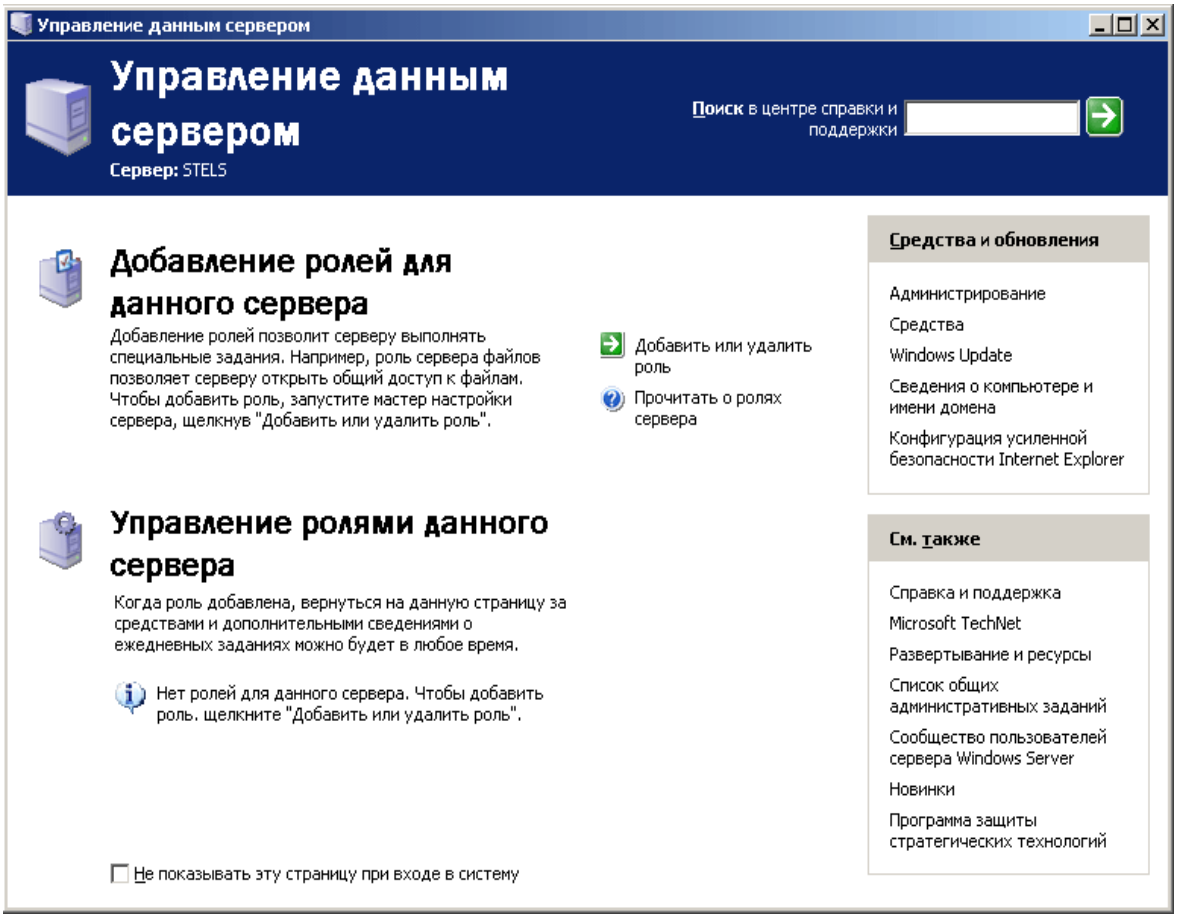


Рис. 5. Страница Управление данным сервером

Если установить переключатель **Типовая настройка для первого сервера (Typical Configuration For A First Server),** мастер сделает сервер контроллером нового домена, установит службы Active Directory и при необходимости службы DNS (Domain Name Service), DHCP (Dynamic Host Configuration Protocol) и RRAS (Routing And Remote Access).

Если установить переключатель **Особая конфигурация (Custom Configuration),** мастер может настроить следующие роли.

- **Файловый сервер (File Server).** Обеспечивает централизованный доступ к файлам и каталогам для пользователей, отделов и организации в целом. Выбор этого варианта позволяет управлять пользовательским дисковым пространством путем включения и настройки средств управления дисковыми квотами и ускорить поиск в файловой системе за счет активизации *Службы индексирования* (Indexing Service).
- **Сервер печати (Print Server).** Обеспечивает централизованное управление печатающими устройствами, предоставляя клиентским компьютерам доступ к общим принтерам и их драйверам. Если выбрать этот вариант, запустится *Мастер установки принтеров* (Add Printer), позволяющий установить принтеры и соответствующие драйверы. Кроме того, мастер устанавливает службы IIS 6.0 (Internet Information Services), настраивает протокол печати IPP (Internet Printing Protocol) и Web - средства управления принтерами.
- **Application Server IIS, ASP.NET (Сервер приложений IIS, ASP.NET).** Предоставляет компоненты инфраструктуры, которые требуются для поддержки размещения Web - приложений. Эта роль устанавливает и настраивает I IS 6.0, ASP.NET и COM+.

- **Mail Server POP3, SMTP (Почтовый сервер POP3, SMTP).** Устанавливает POP3 и SMTP , чтобы сервер мог выступать в роли почтового сервера для клиентов POP3.
- **Сервер терминалов (Terminal Server).** Позволяет множеству пользователей с помощью клиенского ПО *Службы терминалов* (Terminal Services) или *Дистанционное управление рабочим столом* (Remote Desktop) подключаться к приложениям и ресурсам сервера, например принтерам или дисковому пространству, как если бы эти ресурсы были установлены на их компьютерах. В отличие от Windows 2000, Windows Server 2003 предоставляет *Дистанционное управление рабочим столом* автоматически. Роли сервера терминалов требуются, только когда нужно размещать приложения для пользователей на сервере терминалов.
- **Сервер удаленного доступа или VPN-сервер (Remote Access/VPN Server).** Обеспечивает маршрутизацию по нескольким протоколам и службы удаленного доступа для коммутируемых, локальных (LAN) и глобальных (WAN) вычислительных сетей. *Виртуальная частная сеть* (virtual private network, VPN) обеспечивает безопасное соединение пользователя с удаленными узлами через стандартные интернет-соединения.
- **Контроллер домена Active Directory (Domain Controller Active Directory).** Предоставляет службы каталогов клиентам сети. Этот вариант позволяет создать контроллер нового или существующего домена и установить DNS . Если выбрать эту роль, запускается *Мастер установки Active Directory* (Active Directory Installation Wizard).
- **DNS Server (DNS -сервер).** Обеспечивает разрешение имен узлов: DNS - имена преобразуются в IP-адреса (прямой поиск) и обратно (обратный поиск). Если выбрать этот вариант, устанавливается служба DNS и запускается *Мастер настройки DNS-сервера* (Configure A DNS Server Wizard).

- **DHCP-сервер (DHCP Server).** Предоставляет службы автоматического выделения IP-адресов клиентам, настроенным на динамическое получение IP-адресов. Если выбрать этот вариант, устанавливаются службы DHCP и запускается *Мастер создания области* (New Scope Wizard), позволяющий определить один или несколько диапазонов IP-адресов в сети.
- **Сервер потоков мультимедиа (Streaming Media Server).** Предоставляет службы WMS (Windows Media Services), которые позволяют серверу передавать потоки мультимедийных данных в интрасети или через Интернет. Содержимое может храниться и предоставляться по запросу или в реальном времени. Если выбрать этот вариант, устанавливается сервер WMS.
- **WlNS-сервер (WINS Server).** Обеспечивает разрешение имен компьютеров путем преобразования имен NetBIOS в IP-адреса. Устанавливать службу WINS (Windows Internet Name Service) не требуется, если вы не поддерживаете старые ОС, например Windows 95 или NT. Такие ОС, как Windows 2000 и XP не требуют WINS, хотя старым приложениям, работающим на этих платформах, может понадобиться разрешать имена NetBIOS. Если выбрать этот вариант, устанавливается сервер WINS.

Сети Microsoft Windows поддерживают две модели служб каталогов: *рабочую группу* (workgroup) и *домен* (domain). Для огранизаций, внедряющих Windows Server 2003, модель домена наиболее предпочтительна. Модель домена характеризуется единым каталогом ресурсов предприятия — Active Directory, — которому доверяют все системы безопасности, принадлежащие домену. Поэтому такие системы способны работать с субъектами безопасности (учетными записями пользователей, групп и компьютеров) в каталоге, чтобы обеспечить защиту ресурсов. Служба Active Directory, таким образом, играет роль идентификационного хранилища и сообщает «кто есть кто» в этом домене. Впрочем, Active Directory — не просто база данных. Это коллекция файлов,

включая журналы транзакций и системный том (Sysvol), содержащий сценарии входа в систему и сведения о групповой политике. Это службы, поддерживающие и использующие БД, включая протокол LDAP (Lightweight Directory Access Protocol), протокол безопасности Kerberos, процессы репликации и службу FRS (File Replication Service). БД и ее службы устанавливаются на один или несколько контроллеров домена. Контроллер домена назначается *Мастером установки Active Directory,* который можно запустить с помощью *Мастера настройки сервера* (как показано в лабораторной работе № 1, упражнение 2). После того как сервер становится контроллером домена, на нем хранится копия (реплика) Active Directory, и изменения БД на любом контроллере реплицируются на все остальные контроллеры домена.

Active Directory не может существовать без домена и наоборот. Домен — это основная административная единица службы каталогов. Однако предприятие может включить в свой каталог Active Directory более одного домена. Когда несколько моделей доменов совместно используют непрерывное пространство имен DNS, они образуют логические структуры, называемые *деревьями* (tree).

Домены Active Directory с разными корневыми доменами образуют несколько деревьев. Они объединяются в самую большую структуру Active Directory — *лес* (forest). Лес Active Directory содержит все домены в рамках службы каталогов. Лес может состоять из нескольких доменов в нескольких деревьях или только из одного домена. Когда доменов несколько, приобретает важность компонент Active Directory, называемый *глобальным каталогом* (global catalog): он предоставляет информацию об объектах, расположенных в других доменах леса.

Служба DNS

Сервер каталогов Active Directory тесно связан со службой DNS. Собственно говоря, без нее он работать не будет. Он использует эту службу для поиска информации в сети точно так же, как и клиентские компьютеры. Сервер DNS — еще один важный компонент для правильного функционирования домена Active Directory.

В нашей сети мы уже установили сервер DNS и создали зону DNS под именем, соответствующим задуманному имени домена Active Directory develsoft.local. Исходя из того, что служба DNS — неотделимая составная часть домена Active Directory, мастер установки домена производит ее поиск и, если она еще не установлен, предлагает ее автоматическую установку и настройку.

Зона DNS — это непрерывная часть пространства имен, обслуживаемая полномочным сервером. Сервер может выполнять роль полномочным в одной или нескольких зонах, а зона может содержать один или несколько смежных доменов. Сервер DNS является полномочным для зоны, если он обслуживает ее в качестве основного или дополнительного DNS-сервера. Зона DNS хранит записи ресурсов, необходимые для ответов на запросы в пределах своей части пространства имен DNS.

DNS-серверы являются полномочными для зон, которые на них размещаются. Зоны прямого просмотра отвечают на запросы об IP-адресах, а зоны обратного просмотра — на запросы о полных доменных именах.

DNS-сервер, на котором размещается основная зона, называется основным DNS-сервером. Основные DNS-серверы хранят исходную зонную информацию. В Windows Server 2003 можно использовать зоны двух типов: стандартные основные зоны или зоны, интегрированные с Active Directory. В последнем случае данные зоны хранятся в Active Directory.

DNS-сервер, на котором размещается дополнительная зона, называется дополнительным DNS-сервером. Дополнительные DNS-серверы являются полномочными резервными серверами для основного сервера. Серверы, от

которых дополнительные серверы получают зонную информацию, называются главными. Главным может быть как основной сервер зоны, так и другой дополнительный сервер.

DHCP

Протокол DHCP (Dynamic Host Configuration Protocol) совместно с *системой доменных имен* (Domain Name System, DNS) играет ключевую роль в сетевой инфраструктуре Microsoft Windows Server 2003. Во всех сетях, за исключением, пожалуй, самых маленьких, DHCP обеспечивает настройку параметров IP-протокола, необходимых для взаимодействия с другими компьютерами сети. Как минимум определяются IP-адрес и маска подсети, но обычно дополнительно назначаются суффикс основного контроллера домена, основной шлюз, основной и дополнительные DNS- и WINS-серверы, а также некоторые другие свойства. В отсутствие надежных и автоматических средств предоставления клиентам конфигурационных параметров администраторы не справляются с быстро растущей ручной работой по настройке IP-протокола.

DHCP — стандартное средство протокола IP, призванное упростить администрирование IP-конфигураций.

При наличии в сети DHCP-сервера поддерживающие протокол DHCP клиенты автоматически получают IP-адреса и связанные с ними параметры при каждом запуске и подключении к сети. DHCP-сервер предоставляет конфигурацию обратившимся клиентам в форме аренды адреса.

Одно из основных преимуществ протокола DHCP заключается в том, что DHCP- серверы значительно сокращают время настройки компьютеров в сети. DHCP упрощает администрирование не только за счет предоставления клиентам IP-адресов, но и (при необходимости) адреса основного шлюза, адресов DNS- и WINS-серверов, а также других необходимых клиентам серверов. У DHCP есть еще одно преимущество: автоматическое назначение IP-адресов позволяет избежать ошибок конфигурирования, неизбежных при ручном определении

параметров IP на каждом сетевом узле. В частности, DHCP предотвращает конфликты адресов, возникающие из-за ошибочного присвоения одинаковых IP-адресов двум сетевым узлам.

При наличии работоспособного DHCP-сервера компьютеры, настроенные на автоматическое получение IP-адреса, при загрузке запрашивают и получают IP-параметры от DHCP-сервера. В сетях с Active Directory DHCP-серверы должны обязательно проходить авторизацию.

Область DHCP — это непрерывный диапазон IP-адресов, определенных в единой логической подсети, которые DHCP-сервер предоставляет клиентам. После определения и настройки области ее надо активировать — только после этого DHCP-сервер сможет обслуживать клиентов.

Служба WINS

Служба WINS (Windows Internet Name Service) выполняет задачи, аналогичные задачам службы DNS, — динамическая регистрация имен компьютеров и других сетевых узлов и их IP-адресов в БД сервера WINS и разрешение имен компьютеров в IP-адреса. Главное отличие в том, что WINS функционирует в совершенно ином пространстве имен, т.н. пространстве имен NetBIOS, которое никак не пересекается с пространством FQDN-имен, в котором работает служба DNS. По этой причине службу WINS еще иначе называют NetBIOS Name Service (NBNS). До появления системы Windows 2000 сетевой программный интерфейс NetBIOS был основным сетевым интерфейсом для обмена данными между компьютерами в сетях на базе технологий Microsoft (технология SMB — предоставление совместного доступа к файлам и печати — работала только с помощью сетевого интерфейса NetBIOS), и поэтому служба WINS была основной службой разрешения имен компьютеров в IP-адреса. После выхода Windows 2000 служба файлов и печати может работать без NetBIOS, и основной технологией разрешения имен в IP-адреса стала служба DNS. Если в вашей сети нет операционных систем Windows 95/98/ME/NT, то вам служба WINS может вообще не потребоваться.

Процесс разрешения имен в пространстве NetBIOS

Когда один компьютер пытается использовать ресурсы, предоставляемые другим компьютером через интерфейс NetBIOS поверх протокола TCP/IP, то первый компьютер, называемый клиентом, вначале должен определить IP-адрес второго компьютера, называемого сервером, по имени этого компьютера. Это может быть сделано одним из трех способов:

- широковещательный запрос;
- обращение к локальной базе данных NetBIOS-имен, хранящейся в файле LMHOSTS (этот файл хранится в той же папке, что и файл hosts, отображающий FQDN-имена);
- обращение к централизованной БД имен NetBIOS, хранящейся на сервере WINS.

В зависимости от *типа* узла NetBIOS, разрешение имен осуществляется с помощью различных комбинаций перечисленных способов:

- **b-узел** (*broadcast node, широковещательный узел*) — разрешает имена в IP-адреса посредством широковещательных сообщений (компьютер, которому нужно разрешить имя, рассылает по локальной сети широковещательное сообщение с запросом IP-адреса по имени компьютера);
- **p-узел** (*peer node, узел "точка — точка"*) — разрешает имена в IP-адреса с помощью WINS-сервера (когда клиенту нужно разрешить имя компьютера в IP-адрес, клиент отправляет серверу имя, а тот в ответ посылает адрес);
- **m-узел** (*mixed node, смешанный узел*) — комбинирует запросы b- и p-узла (WINS-клиент смешанного типа сначала пытается применить широковещательный запрос, а в случае неудачи обращается к WlNS-серверу; поскольку разрешение имени начинается с широковещательного запроса, m-узел загружает сеть широковещательным трафиком в той же степени, что и b-узел);
- **h-узел** (*hybrid node, гибридный узел*) — также комбинирует запросы b-узла и p-узла, но при этом сначала используется запрос к WINS-серверу и лишь в

случае неудачи начинается рассылка широковещательного сообщения, поэтому в большинстве сетей h-узлы работают быстрее и меньше засоряют сеть широковещательными пакетами.

С точки зрения производительности, объема сетевого трафика и надежности процесса разрешения NetBIOS-имен самым эффективным является *h-узел*.

Если в свойствах протокола TCP/IP Windows-компьютера нет ссылки на WINS-сервер, то данный компьютер является b-узлом. Если в свойствах протокола TCP/IP имеется ссылка хотя бы на один WINS-сервер, то данный компьютер является h-узлом. Другие типы узлов настраиваются через реестр системы Windows.

Служба RRAS

Служба *RRAS* (*Routing and Remote Access Service, Служба Маршрутизации и Удаленного Доступа*) — служба системы Windows Server, позволяющая решать следующие задачи:

- подключение мобильных (или домашних) пользователей к корпоративной сети через коммутируемые телефонные линии и другие средства коммуникаций (например, сети Frame Relay, X.25);
- подключение к сети главного офиса компании удаленных офисов (через телефонные линии и сети Frame Relay, X.25);
- организация защищенных соединений (виртуальные частные сети) между мобильными пользователями, подключенными к сетям общего пользования (например, Интернет), и корпоративной сетью;
- организация защищенных соединений между офисами компании, подключенными к сетям общего пользования;
- маршрутизация сетевого трафика между различными подсетями корпоративной сети, соединенными как с помощью технологий локальных сетей, так и с помощью различных средств удаленных коммуникаций (например, по коммутируемым телефонным линиям).

Служба RRAS обладает богатым набором функций и возможностей. Мы рассмотрим базовые функции и возможности данной службы, которые в первую очередь необходимо знать любому сетевому администратору.

Службы удаленного доступа, реализованные различными производителями, используют два основных коммуникационных протокола, которые образуют уровень, промежуточный между средствами коммуникаций (коммутируемые телефонные линии, Frame Relay, X.25) и сетевыми протоколами (TCP/IP, IPX/SPX):

- протокол *SLIP* (*Serial Line Interface Protocol*) — достаточно старый протокол, реализованный преимущественно на серверах удаленного доступа, функционирующих в системах семейства UNIX (разработан специально для подключения пользователей к сети Интернет); системы семейства Windows поддерживают данный протокол только на клиентской части (SLIP позволяет работать только с сетевым стеком TCP/IP, требует написания специальных сценариев для подключения клиента к серверу, не позволяет создавать виртуальные частные сети);
- протокол *PPP* (*Point-to-Point Protocol*) — используемый повсеместно коммуникационный протокол (точнее, семейство протоколов), позволяющий пользователям прозрачно подключаться к серверу удаленного доступа, использовать различные сетевые протоколы (TCP/IP, IPX/SPX, NetBEUI, AplleTalk), создавать виртуальные частные сети (служба удаленного доступа серверов Windows использует именно этот коммуникационный протокол).

Использование службы RADIUS

Служба RADIUS (*Remote Authentication Dial-in User Service*) является промежуточным звеном между сервером удаленного доступа (который в данном случае называют клиентом RADIUS) и службой каталогов корпоративной сети. Сервер RADIUS позволяет решить две основные задачи:

- интеграция в единую систему серверов удаленного доступа от различных производителей;
- централизованное управление доступом в корпоративную сеть (служба RRAS в системе Windows Server настраивается *индивидуально для каждого сервера* RRAS).

Служба RADIUS работает по следующей схеме:

1. вначале устанавливается телефонное (или иное) соединение между клиентом и сервером удаленного доступа;
2. пользователь пересылает серверу RAS запрос на аутентификацию (свои имя и пароль);
3. сервер удаленного доступа (являющийся клиентом сервера RADIUS) пересылает данный запрос серверу RADIUS;
4. сервер RADIUS проверяет запрос на аутентификацию в службе каталогов (например, в службе Active Directory) и посылает в ответ RAS-серверу разрешение или запрещение данному пользователю на подключение к серверу удаленного доступа;
5. сервер удаленного доступа либо подключает пользователя к корпоративной сети, либо выдает отказ в подключении.

Реализация службы RADIUS в системе Windows Server называется службой *IAS* (*Internet Authentication Service*).

Настройка параметров безопасности (Шаблоны безопасности, Анализ и настройка безопасности)

В работе рассмотрим работу с очень полезными оснастками, которые могут помочь начинающему сетевому администратору ознакомиться с некоторыми стандартными шаблонами политик безопасности, которые имеются в самой системе Windows Server, и проводить анализ и текущих настроек сервера в сравнении со этими стандартными шаблонами.

1. Сначала откроем чистую консоль mmc.

Кнопка "*Пуск*" — "*Выполнить*" — mmc — кнопка "*ОК*".

2. Добавим в новую консоль оснастки "*Шаблоны безопасности*" и "*Анализ и настройка безопасности*".

Меню "*Консоль*" — "*Добавить или удалить оснастку*" — кнопка "*Добавить*" — выбрать оснастку "*Анализ и настройка безопасности*" — кнопка "*Добавить*" — выбрать оснастку "*Шаблоны безопасности*" — кнопка "*Добавить*" — кнопка "*Закрыть*" — кнопка "*ОК*" (рис. 6.).

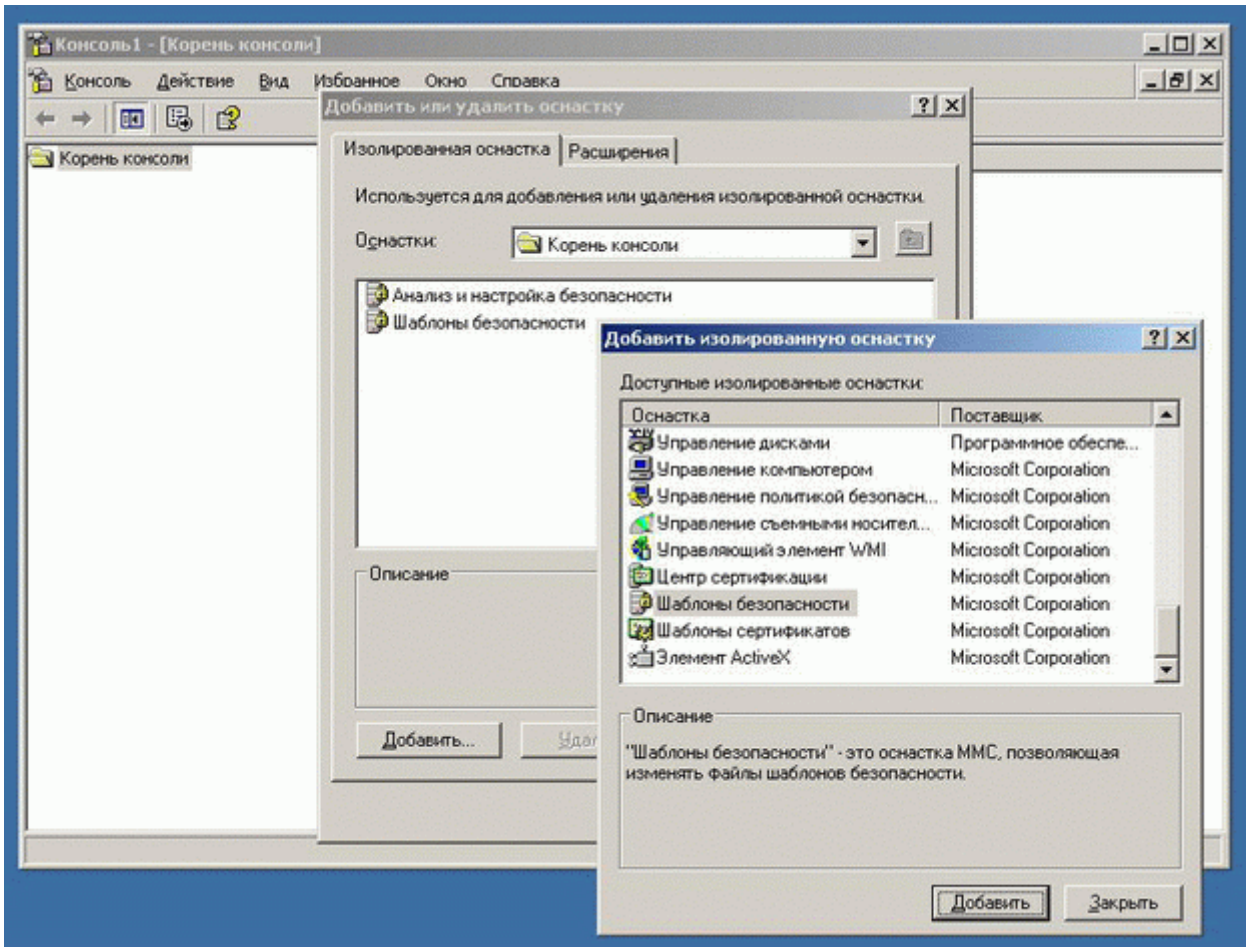


Рис. 6. Окна для добавления оснастки

В полученной консоли (ее можно будет сохранить и использовать в дальнейшем неоднократно) можно делать следующее:

- изучить параметры стандартных шаблонов безопасности (оснастка "Шаблоны безопасности") и даже попробовать сконструировать собственные шаблоны на основе стандартных (можно сохранить какой-либо шаблон с другим именем и изменить какие-либо параметры шаблона);

- провести анализ (сравнение) текущих параметров безопасности сервера (оснастка "*Анализ и настройка безопасности*").

Приведем краткие характеристики стандартных шаблонов безопасности:

- **DC security** — используемые по умолчанию параметры безопасности контроллера домена;
- **securedc** — защищенный контроллер домена (более высокие требования к безопасности по сравнению с шаблоном *DC security*, отключается использование метода аутентификации *LanManager*);
- **hisecdc** — контроллер домена с высоким уровнем защиты (более высокие требования к безопасности по сравнению с шаблоном *securedc*, отключается метод аутентификации *NTLM*, включается требование цифровой подписи пакетов SMB);
- **compatws** — совместимая рабочая станция или совместимый сервер (ослабляет используемые по умолчанию разрешения доступа группы "Пользователи" к реестру и к системным файлам для того, чтобы приложения, не сертифицированные для использования в данной системе, могли работать в ней);
- **securews** — защищенная рабочая станция или защищенный сервер (аналогичен шаблону *securedc*, но предназначен для применения к рабочим станциям и простым серверам);
- **hisecws** — рабочая станция или защищенный сервер с высоким уровнем защиты (аналогичен шаблону *hisecdc*, но предназначен для применения к рабочим станциям и простым серверам);
- **setup security** — первоначальные настройки по умолчанию (параметры, устанавливаемые во время инсталляции системы);
- **rootsec** — установка стандартных (назначаемых во время инсталляции системы) NTFS-разрешений для папки, в которую установлена операционная система.

В работе на примере рассмотрено, как проводить анализ настроек безопасности:

1. Откроем базу данных, в которой будут сохраняться настройки проводимого нами анализа.

Щелкнем правой кнопкой мыши на значке оснастки "*Анализ и настройка безопасности*", выберем "*Открыть базу данных*", укажем путь и название БД (по умолчанию БД создается в папках профиля того администратора, который проводит анализ), нажмем кнопку "*Открыть*", выберем нужный нам шаблон (например, *hisecdc*) и нажмем "*ОК*" (рис. 7.):

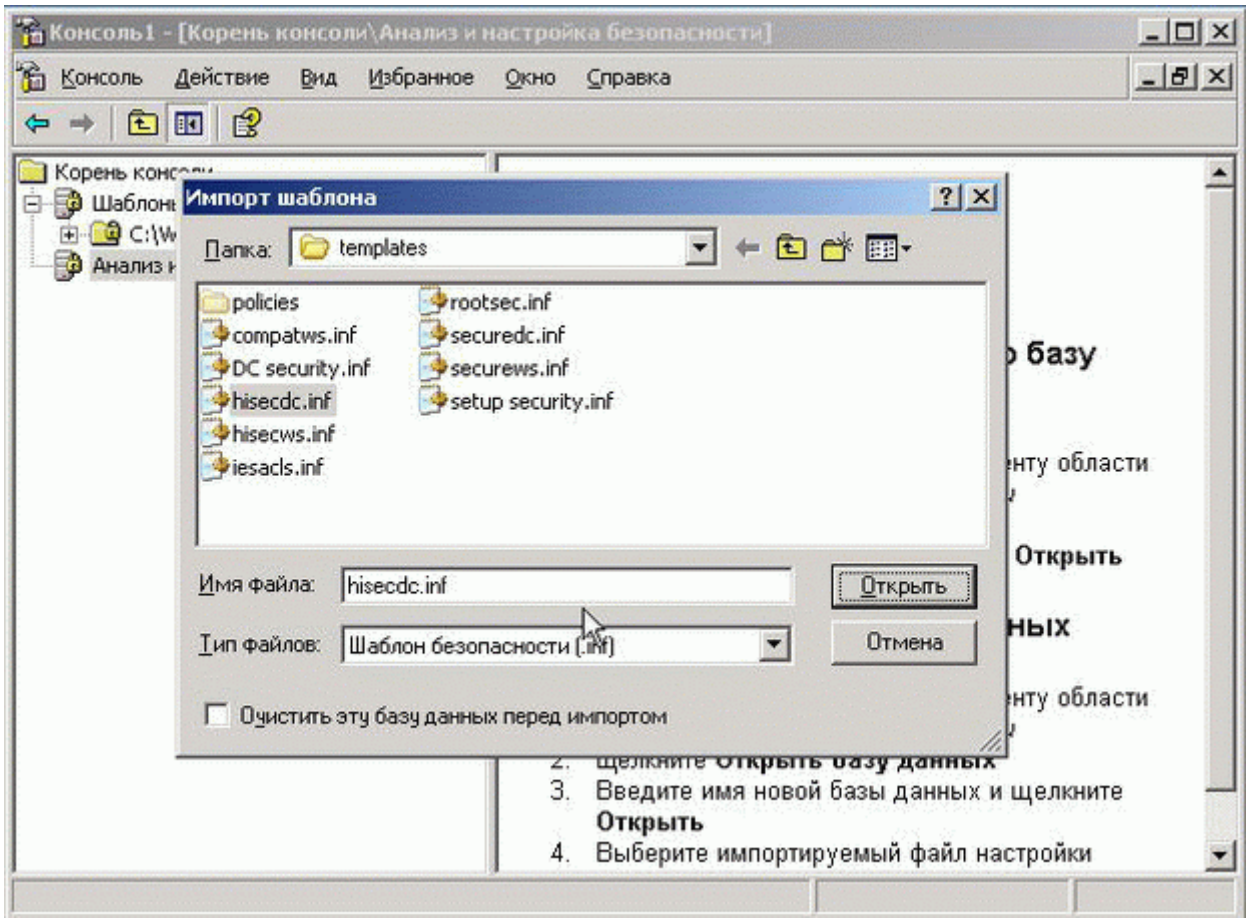


Рис. 7**.** Путь к БД

2. Выполним анализ настроек безопасности.

Щелкнем правой кнопкой мыши на значке оснастки "*Анализ и настройка безопасности*", выберем "*Анализ компьютера*", укажем путь и название файла с журналом ошибок (т.е. протоколом проведения анализа), нажмем "ОК", будет выполнено сравнение текущих настроек с параметрами шаблона (рис. 8.):

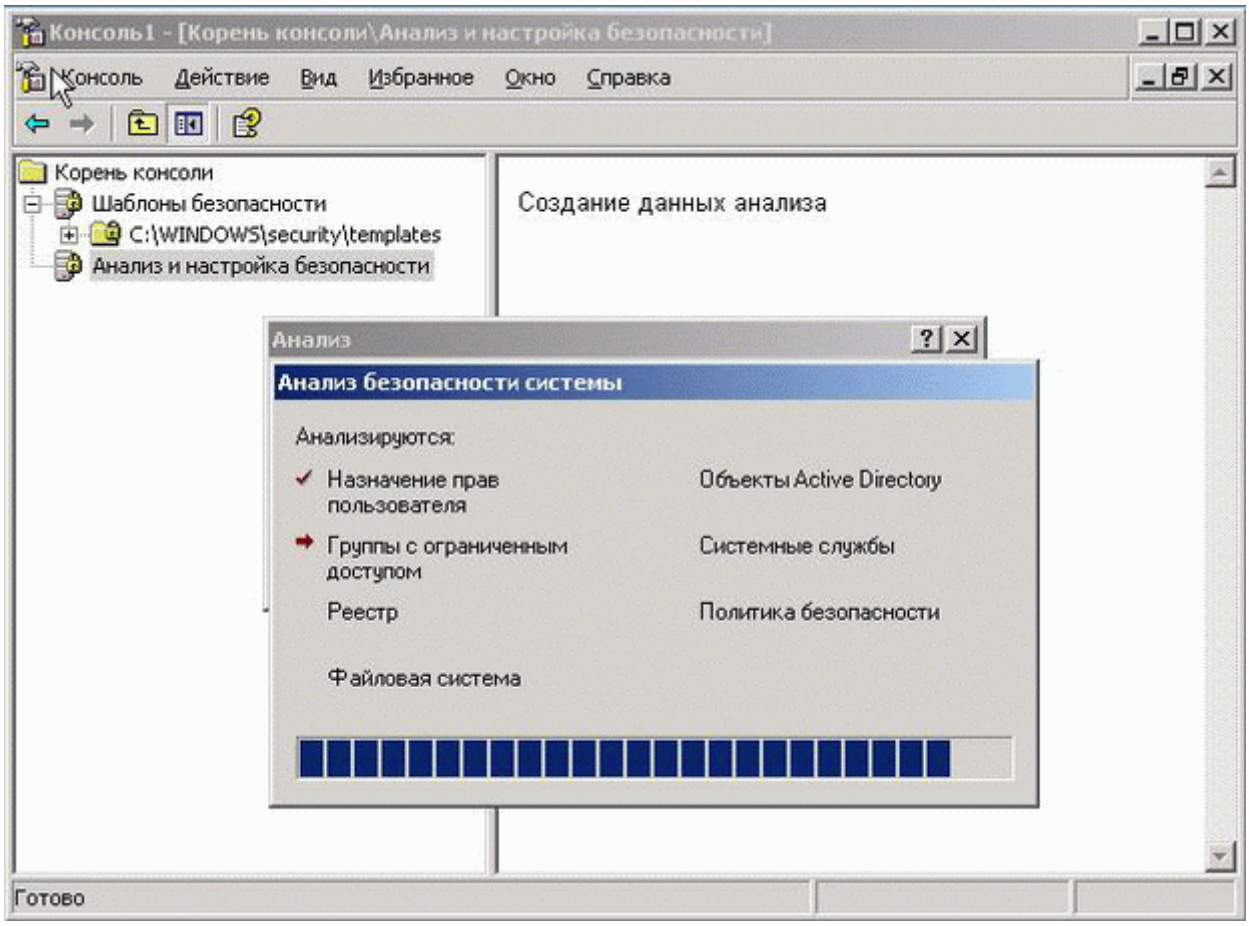


Рис. 8. Сравнение текущих настроек с параметрами шаблона

3. Теперь можно провести уже настоящий анализ настроек безопасности. Откроем любой раздел оснастки (например, "*Политики паролей*", рис. 9.)

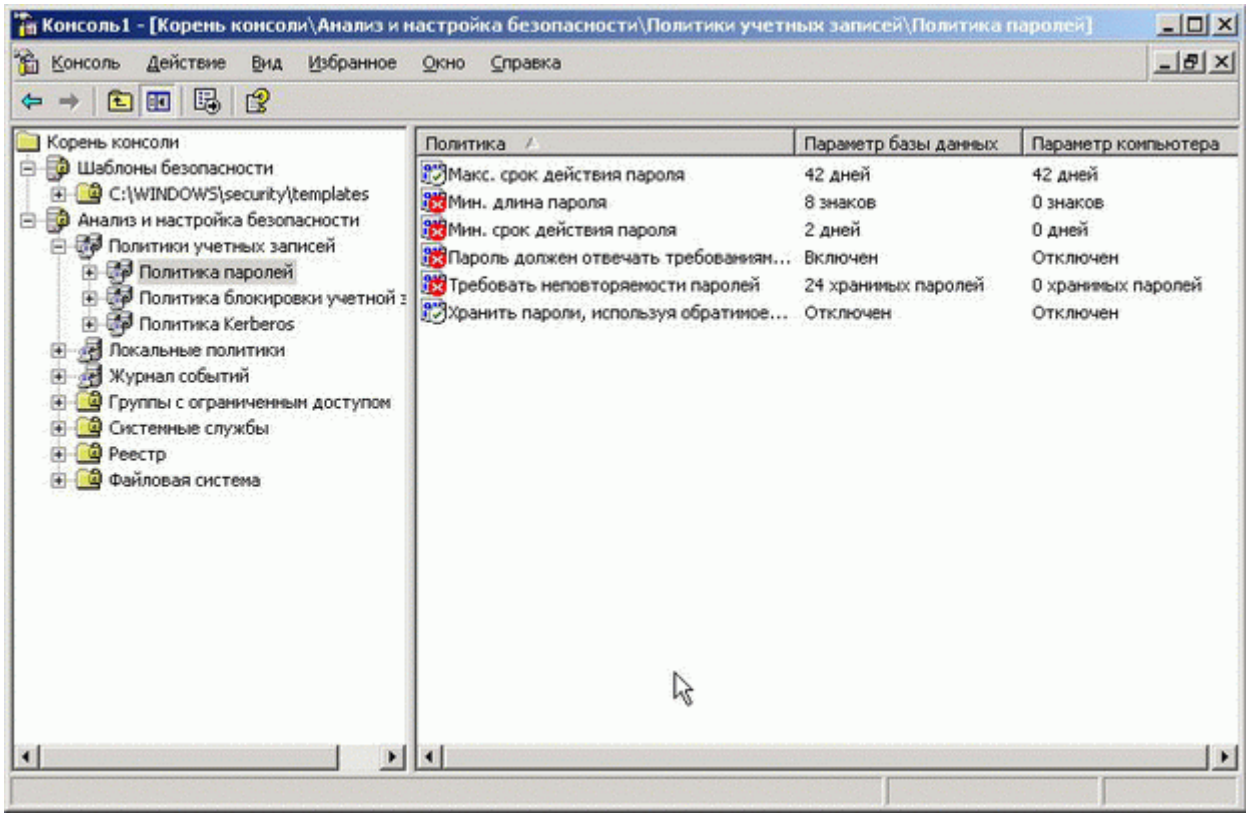


Рис. 9. Оснастка «Политика паролей»

На рисунке сразу видны расхождения между настройками нашего сервера (столбец "*Параметр компьютера*") и настройками шаблона (столбец "*Параметр базы данных*") — видно, как мы понизили настройке безопасности для проведения практических занятий.

Аналогично проводится анализ всех остальных разделов политик безопасности.

Этой же оснасткой можно одним действием привести настройки нашего компьютера в соответствии с параметрами шаблона (щелкнуть правой кнопкой мыши на значке оснастки "*Анализ и настройка безопасности*", выбрать "*Настроить компьютер*"). Не рекомендуем это делать, не изучив в деталях, какие последствия это может повлечь для всей сети. Высокие требования к параметрам безопасности препятствуют работе в домене Active Directory компьютеров с системами Windows 95/98/ME/NT. Например, данные системы поддерживают уровень аутентификации NTLM версии 2 (который назначается шаблонами *hisecdc* и *hisecws*) только при проведении определенных настроек на

компьютерах со старыми системами. Поэтому, прежде чем принимать решение об установке более высоких параметров безопасности в сети, необходимо тщательно изучить состав сети, какие требования к серверам и рабочим станциям предъявляют те или иные шаблоны безопасности, предварительно установить нужные обновления и настроить нужные параметры на "старых" системах и только после этого применять к серверам и рабочим станциям Windows 2000/XP/2003 шаблоны с высокими уровнями сетевой безопасности.

Заметим дополнительно, что данные оснастки имеются не только на серверах, но и на рабочих станциях под управлением Windows 2000/XP Professional, и они позволяют производить аналогичный анализ и настройки на рабочих местах пользователей.

Задание № 1. ***Установка и настройка Windows Server 2003***

Цель работы: настроить компьютер для работы под управлением Windows Server 2003. Сделать сервер контроллером домена develsoft.local.

Упражнение 1. Установка Windows Server 2003

Это упражнение следует выполнять на компьютере, совместимом с Windows Server 2003. Предполагается, что основной жесткий диск полностью чист. Если диск уже разбит на разделы, можно изменить упражнение согласно конфигурации вашей системы.

1. В BIOS компьютера или контроллера диска задайте загрузку с CD-ROM. Если вы не знаете, как это сделать, обратитесь к соответствующей документации.
2. Вставьте установочный компакт-диск Windows Server 2003 в привод CD-ROM и перезагрузите компьютер.
3. Если основной диск не пуст, появится сообщение с предложением нажать любую клавишу, чтобы загрузить компьютер с компакт-диска. Если вы увидите такое сообщение, нажмите любую клавишу. После загрузки

компьютера ненадолго появится сообщение об анализе конфигурации системы, а затем откроется окно **Установка Windows (Windows Setup).**

4. Если компьютеру нужны специальные драйверы для запоминающих устройств, которых нет в комплекте Windows Server 2003, нажмите F6, когда появится соответствующее сообщение, и предоставьте соответствующие драйверы.
5. Система предложит нажать F2, чтобы выполнить ***автоматическое аварийное восстановление системы*** (Automated System Recovery , ASR). Это новая функция Windows Server 2003, пришедшая на смену функции ***диск аварийного восстановления*** (Emergency Repair Disk) в предыдущих версиях Windows. Не нажимайте F2 на этом этапе. Установка продолжится. Заметьте: серый индикатор внизу экрана показывает, что выполняется проверка компьютера и загрузка файлов. Это необходимо для запуска ОС с минимальным набором драйверов.
6. Если вы устанавливаете пробную версию Windows Server 2003, откроется окно Setup Notification, прочитайте информацию и для продолжения нажмите клавишу Enter. Программа установки отобразит окно приветствия. Заметьте, что помимо установки Windows Server 2003 на чистый диск, программу Setup можно использовать для восстановления поврежденной системы Windows.
7. Прочитайте информацию в окне **Вас приветствует программа установки (Welcome To Setup)** и для продолжения нажмите клавишу Enter. Появится окно **Лицензионное соглашение (License Agreement).**
8. Прочитайте лицензионное соглашение: для прокрутки текста вниз нажимайте клавишу Page Down.
9. Нажмите F8, чтобы принять условия соглашения. Откроется окно Windows Server 2003 Setup с предложением выбрать область свободного пространства или существующий раздел, куда будет установлена ОС. На данном этапе вы можете создать или удалить разделы на жестком диске.

Для выполнения упражнений необходимо создать достаточно большой раздел, на котором поместится ОС (рекомендуется не менее 3 Гб), и минимум 1 Гб нераспределенного пространства. Дальнейшие действия предполагают, что размер вашего диска не менее 4 Гб и он в данный момент чист. Вы можете скорректировать процедуру по ситуации.

10. Нажмите клавишу C, чтобы создать раздел.
11. Чтобы создать раздел размером 3 Гб, в поле **Создать раздел размером (МБ) [Create Partition Of Size (In MB)]** введите 3072 и нажмите Enter.
12. Выберите **C: Раздел1 [Новый (неформ.)] (C: Partition 1 [New(Raw)])** и нажмите клавишу Enter. Вам будет предложено выбрать файловую систему для этого раздела.
13. Убедитесь, что установлен переключатель **Форматировать раздел в системе NTFS (Format The Partition Using The NTFS File System)** и нажмите Enter. Программа установки отформатирует раздел под NTFS, проверит жесткий диск на наличие физических ошибок, которые могут помешать установке, скопирует файлы на жесткий диск и начнет установку. Это займет несколько минут. После этого появится красная строка состояния, отсчитывающая назад 15 секунд до перезагрузки компьютера и перехода процесса установки в графический режим.
14. После завершения установки в текстовом режиме система перезагружается. Не нажимайте клавишу для загрузки с компакт-диска, если появится соответствующее сообщение. Windows Setup запустит графический пользовательский интерфейс, демонстрирующий на левой панели процесс установки. Вы увидите, что отмечены флажки **Сбор информации (Collecting Information), Динамическое обновление (Dynamic Update)** и **Подготовка к установке (Preparing Installation).** Сбор информации был завершен до перехода в графический режим, а динамическое обновление не применяется при запуске с компакт-диска. Теперь система готовится к установке и копирует файлы на жесткий диск.

15. На странице **Язык и региональные стандарты (Regional And Language Options)** выберите необходимые параметры и щелкните **Далее (Next).**

Совет*:** Вы сможете изменить региональные параметры после установки ОС, используя элемент **Язык и региональные стандарты (Regional And Language Options)** из ***Панели управления.

16. Программа установки отобразит страницу **Настройка принадлежности программ (Personalize Your Software),** где вам будет предложено указать свое имя и название организации.
17. В поле **Имя (Name)** введите свое имя, а в поле **Организация (Organization)** — название организации, после чего щелкните **Далее (Next).** Откроется страница **Ключ продукта (Your Product Key)**.
18. Введите ключ продукта, прилагаемый к установочному компакт-диску Windows Server 2003, и щелкните **Далее (Next)**. Откроется диалоговое окно **Режимы лицензирования (Licensing Modes)** с предложением выбрать режим лицензирования.
19. Убедитесь, что в поле **«На сервер». Число одновременных подключений (Per Server Number Of Concurrent Connections)** указано 5, и щелкните **Далее (Next)**.

Внимание! *Такой вариант лицензирования и пять одновременных подключений — рекомендуемые значения для самостоятельного обучения. Вы должны вводить количество одновременных подключений согласно приобретенной лицензии. Также можно выбрать вариант* ***«На устройство или на пользователя» (Per Device Or Per User).***

Откроется страница **Имя компьютера и пароль администратора (Computer Name And Administrator Password).** Заметьте, что программа установки предлагает имя компьютера на основе названия вашей организации. Если вы оставили это поле пустым, программа установки сгенерирует часть имени компьютера, используя ваше имя.

20. В поле **Имя компьютера (Computer Name)** введите Server2003. Имя компьютера отображается заглавными буквами независимо от того, в каком регистре вы его вводите. В практических упражнениях всего комплекса будет упоминаться Server2003.

Внимание! *Если ваш компьютер подключен к сети, посоветуйтесь с сетевым администратором, прежде чем назначать имя.*

21. В полях **Пароль администратора (Administrator Password)** и **Подтверждение пароля (Confirm Password)** введите сложный пароль для учетной записи ***Администратор*** (Administrator) (такой, который нельзя просто угадать). Запомните его, поскольку при выполнении большинства практических упражнений курса вы будете входить в систему под учетной записью ***Администратор.***

Внимание! *Если вы устанавливаете Windows Server 2003 вручную, то не сможете пе рейти к последующим шагам, пока не введете пароль администратора, удовлетворяющий требованиям сложности. Допускается ввести пустой пароль, хотя это крайне нежелательно.*

Если на сервере установлен модем, откроется диалоговое окно **Сведения о модеме (Modem Dialing Information).**

22. Введите междугородний телефонный код вашей местности и щелкните **Далее (Next)**. Откроется страница **Настройка времени и даты (Date And Time Settings)**.
23. Введите точную дату, время и часовой пояс и щелкните **Далее (Next)**.

Внимание! *Работа служб Windows Server 2003 зависит от настроек даты и времени. Убедитесь, что дата и время заданы точно и указан правильный часовой пояс для вашей местности.*

24. На странице **Сетевые параметры (Networking Settings)** выберите **Обычные параметры (Typical Settings)** и щелкните **Далее (Next)**. Откроется страница **Рабочая группа или домен (Workgroup Or Computer Domain)**.

25. Убедитесь, что выбран первый вариант, а имя группы — Workgroup, после чего щелкните **Далее (Next)**. Программа Setup установит и настроит остальные компоненты ОС. После завершения установки компьютер автоматически перезагрузится, и откроется диалоговое окно **Операционная система Windows (Welcome To Windows)**.
26. Нажмите **Ctrl + Alt + Delete**, чтобы инициировать вход в систему, и введите пароль, который вы задали для учетной записи ***Администратор*** (Administrator).

Примечание: *Некоторые редакции Windows Server 2003 требуют активации через Интернет или по телефону в течение 14 дней после установки. Лицензию на Windows Server 2003 не требуется активировать, если она приобретена в рамках одной из массовых программ лицензирования Microsoft .*

27. Щелкните подсказку на системной панели, чтобы начать активацию Windows Server 2003. Следуйте инструкциям на экране.

Примечание: *Для активации через Интернет необходимо подсоединить Server2003 к сети и при необходимости указать нужный IP-адрес, маску подсети, шлюз по умолчанию и адрес DNS-сервера в настройках протокола TCP/IP для сетевой платы.*

Упражнение 2. Настройка сервера

В этом упражнении вы сделаете сервер первым контроллером в домене Active Directory с именем develsoft.local.

Примечание *Описанный ниже процесс установки предполагает, что* **Мастер установки Active Directory** *запускается в изолированной сети. Если вы подключены к сети с другим контроллером домена, процесс установки будет отличаться, и вы можете либо изменить выбор согласно конфигурации вашей сети, либо отключиться от сети перед выполнением этого упражнения.*

1. Откройте страницу **Управление данным сервером (Manage Your Server)** в группе программ **Администрирование (Administrative Tools)**.
2. Щелкните **Добавить или удалить роль (Add Or Remove A Role)**. Откроется окно ***Мастер настройки сервера*** (Configure Your Server Wizard).
3. Щелкните **Далее (Next)**, мастер попытается определить сетевые параметры.
4. Щелкните **Типовая настройка для первого сервера (Typical Configuration For A First Server),** а затем **Далее (Next).**
5. В поле **Имя домена в Active Directory (Active Directory Domain Name)** введите develsoft.local.
6. Убедитесь, что в поле **NetBIOS- имя домена (NetBIOS Domain Name)** указано DEVELSOFT, и щелкните **Далее (Next)**.
7. Убедитесь, что окно **Сводка выбранных параметров (Summary Of Selections)** соответствует показанному на рис. 2.6, и щелкните **Далее (Next).**

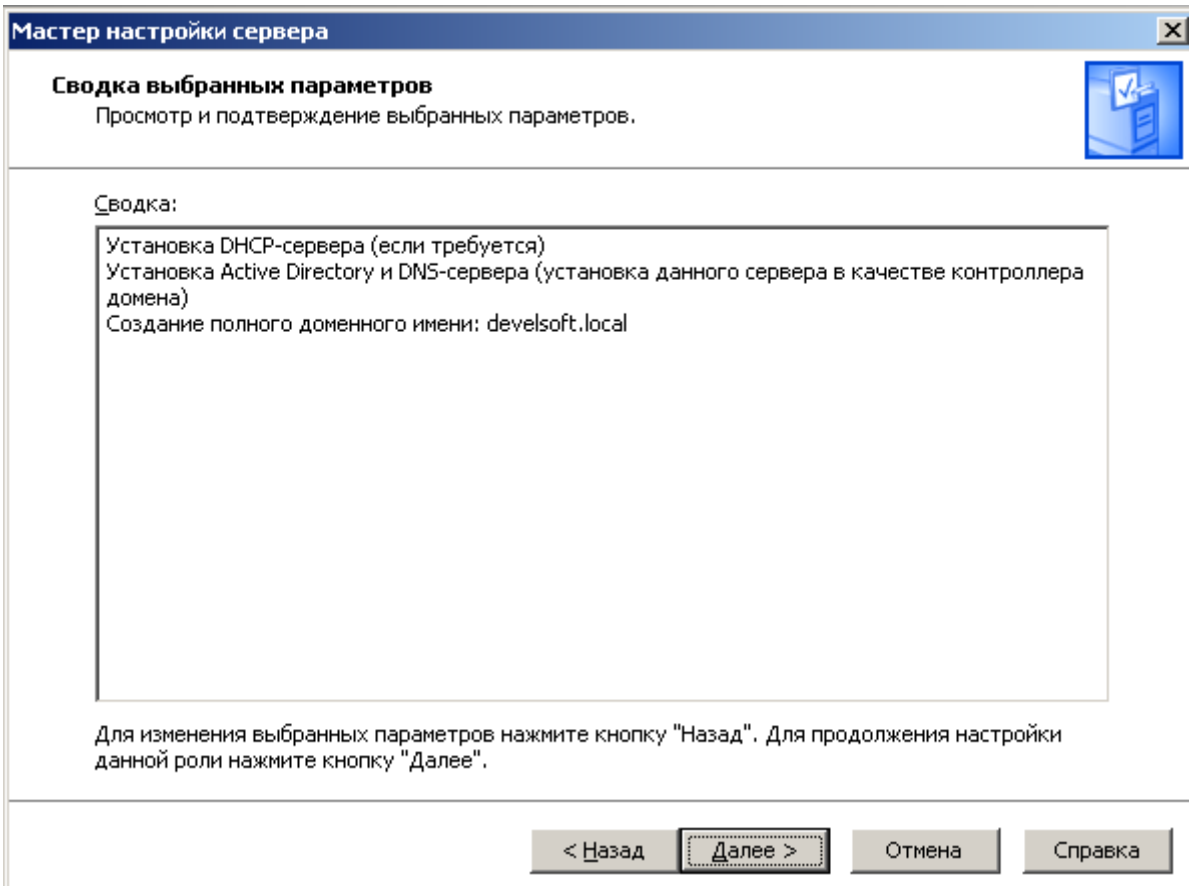


Рис. 10. Окно «**Сводка выбранных параметров»** мастера настройки сервера

8. Мастер напомнит, что система будет перезагружена, и попросит закрыть все открытые программы.
9. Щелкните **Да (Yes).**
10. После перезагрузки войдите в систему как ***Администратор*** (Administrator).
11. Мастер настройки сервера резюмирует установку (рис. 11.).
12. Щелкните **Далее (Next)**, а затем **Готово (Finish)**.
13. Откройте консоль ***Active Directory — пользователи и компьютеры*** (Active Directory Users And Computers). Убедитесь, что домен develsoft.local создан: раскройте его и найдите учетную запись компьютера для Server2003 в ОП Domain Controllers.

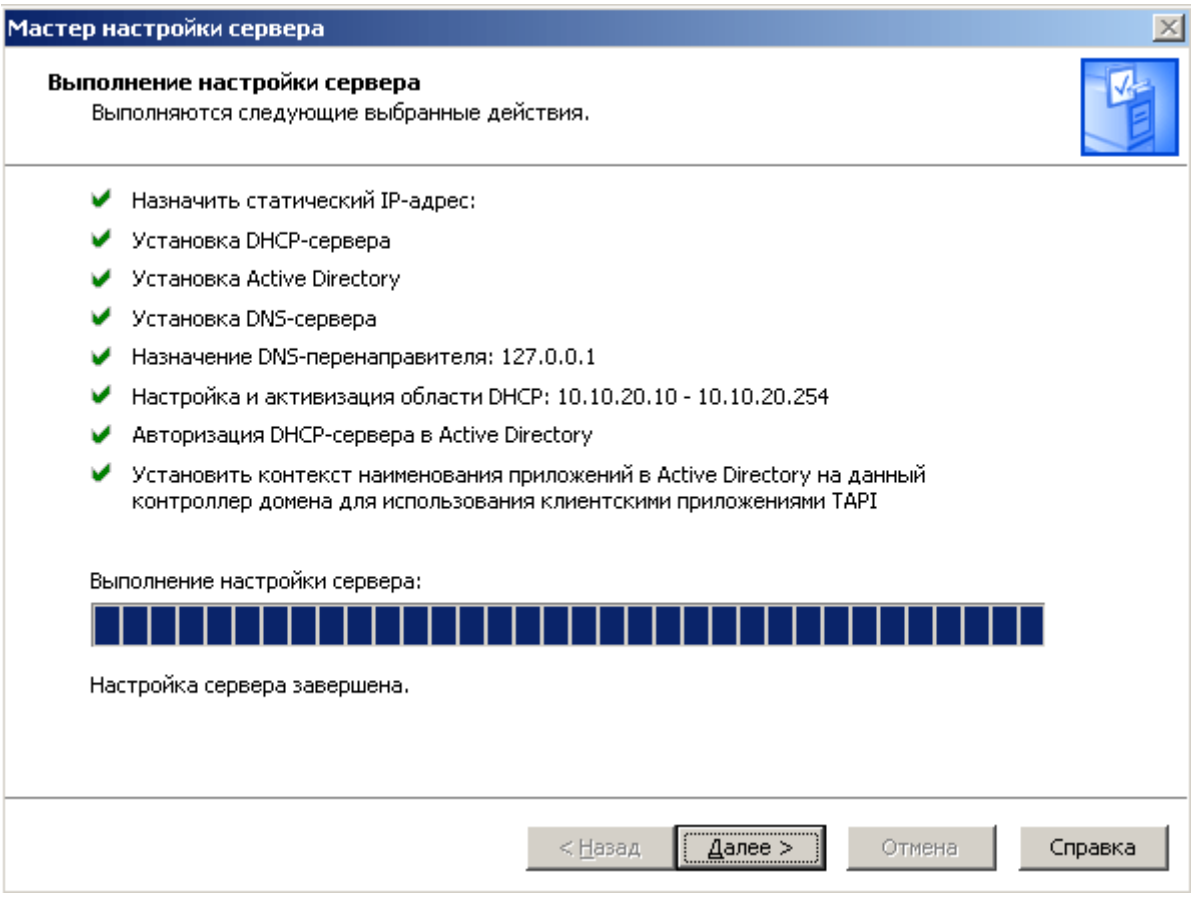


Рис. 11**.** Окно «**Выполнение настройки сервера**» мастера настройки сервера

Задание № 2. ***Настройка DNS-сервер***

Цели работы:

- научиться конфигурировать зоны DNS;
- научиться тестировать службу DNS.

Упражнение 1. Создайте зону прямого просмотра develsoft.local.

Указания к выполнению

В задании №1 при выполнении упражнения 2, мы сделали сервер контроллером домена develsoft.local, и при этом мы сразу сделали зону прямого просмотра.

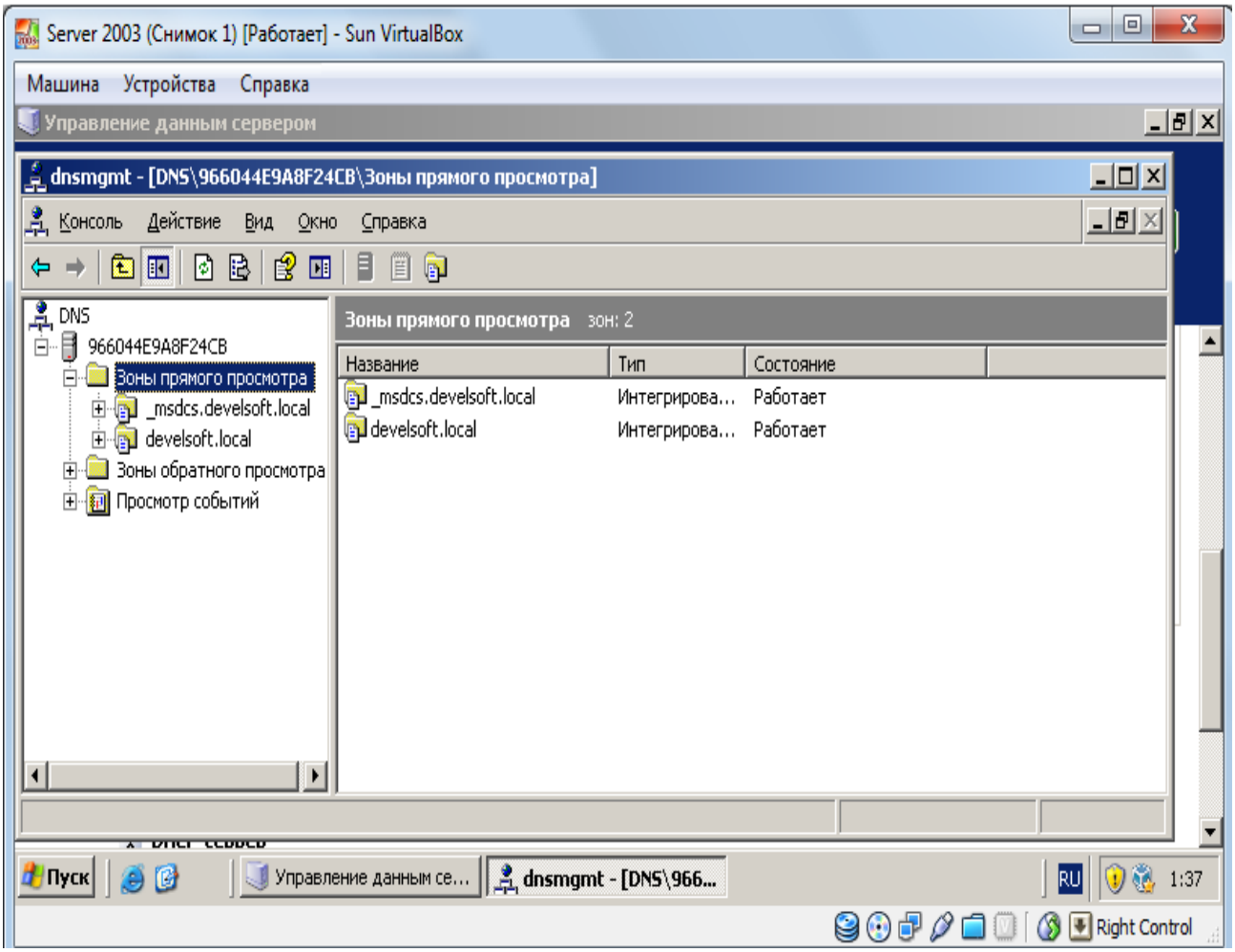


Рис. 12. Зона прямого просмотра develsoft.local

Упражнение 2. Создайте зону обратного просмотра (для преобразования IP-адреса в доменное имя)

Указания к выполнению

1. В узле Reverse Lookup Zones (Зоны обратного просмотра) щелкните правой кнопкой мыши и выберите New zone (Мастер создания новой зоны).

2. В окне Zone Type (Тип зоны) укажите Primary Zone (Основная зона) и нажмите Next.

3. Убедитесь, что выбран переключатель Network ID (Номер сети). В поле под ним введите адрес вашей сети (192.168.1). Поле Reverse Lookup Zone Name (Имя зоны обратного просмотра) внизу окна должно выглядеть так: 1.168.192.in-addr.arpa.

4. Завершите работу мастера, оставив все настройки по умолчанию.

5. Щелкните правой кнопкой мыши по новому узлу в Reverse Lookup Zones (192.168.1.x Subnet) и выберите New Pointer (Новый указатель). Последнее число установите равным последнему числу в IP-адресе. В поле Host name (Имя хоста) запишите полное имя узла, например server.develsoft.local.

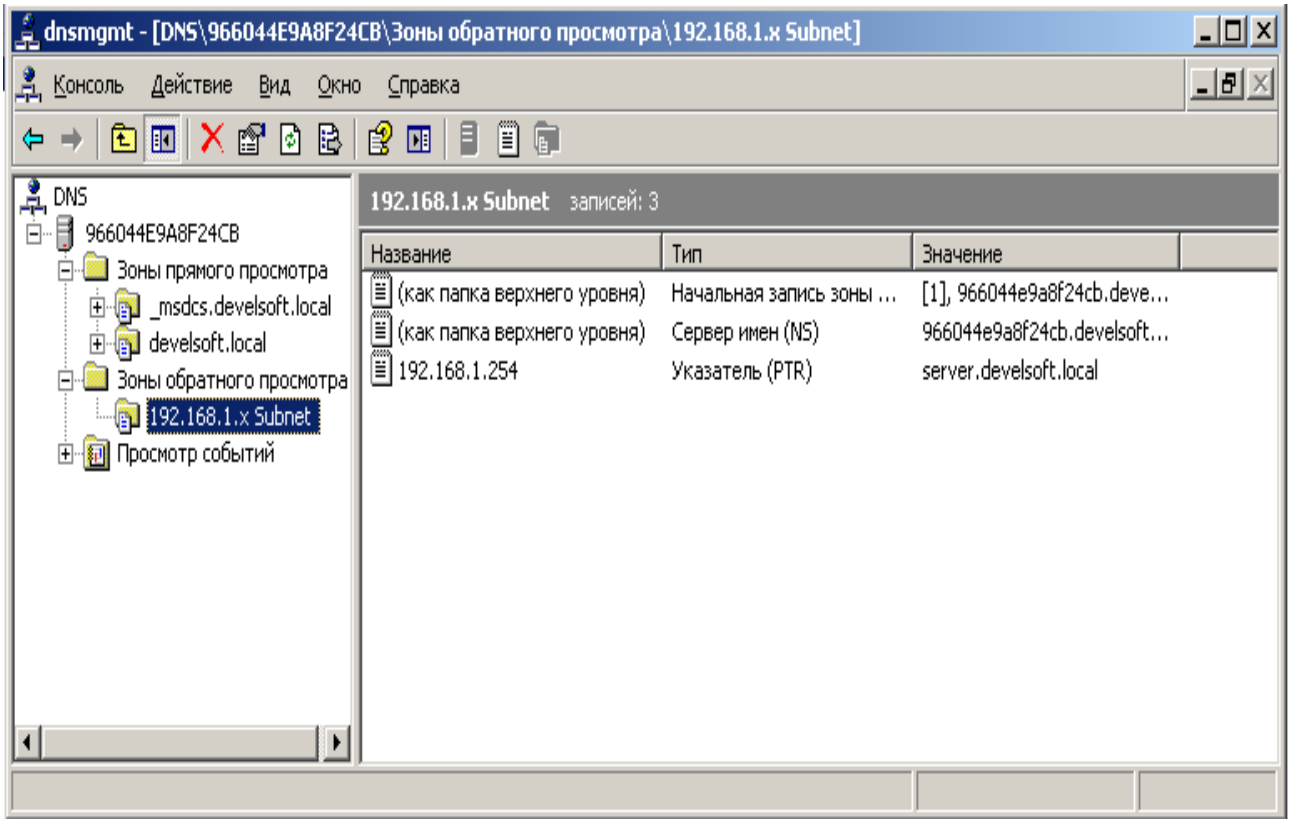


Рис. 13. Зоны обратного просмотра

Упражнение 3. Протестируйте работу службы DNS

Указания к выполнению

Используйте утилиты ping, nslookup.

В дереве консоли откройте свойства узла через команду контекстного меню Properties (Свойства).

Перейдите на вкладку Monitoring (Наблюдение).

В группе Select A Test Type (Выберите тип теста) пометьте флажки A Simple Query Against This DNS Server (Простой запрос к этому DNS-серверу) и

Recursive Query To Other DNS Servers (Рекурсивный запрос к другим DNS-серверам). Щелкните кнопку Test Now (Тестировать).

В списке Test Results (Результаты теста) против обеих записей вы увидите PASS (тест пройден). Если вы работаете на автономном сервере, напротив Recursive Query (Рекурсивный запрос) вы увидите FAIL (ошибка).

Упражнение 4. Сконфигурируйте клиента для использования службы DNS

Указания к выполнению

1. На клиенте откройте диалоговое окно его свойств TCP/IP. Настройте систему для автоматического получения адреса DNS (это обеспечивает сервер DHCP) или вручную укажите IP-адреса предпочтительного и дополнительного серверов DNS.

2. Для настройки дополнительных параметров DNS щелкните кнопку Advanced (Дополнительно). Чтобы задать параметры DNS, в диалоговом окне Advanced TCP/IP Settings (Дополнительные параметры TCP/IP) перейдите на вкладку DNS. Здесь можно сконфигурировать и параметры, обеспечивающие разрешение имен узлов, для которых не было указано полное доменное имя, и настроить параметры регистрации DNS.

Задание № 3. ***Настройка DHCP-сервер***

Цель работы. Научиться настраивать область действия DHCP-сервера.

Чтобы настроить сервер DHCP, вам нужно проделать следующую последовательность действий:

1. Запустите консоль управления DHCP.
2. В левой части окна консоли щелкните правой кнопкой мыши по серверу server.develsoft.local и из контекстного меню выберите команду **Создать область.** По этой команде запустится Мастер создания области. Нажмите **Далее.**

3. В диалоговом окне **Имя области** введите название области (например, ≪Scope1≫) и ее описание (можно оставить по умолчанию). Нажмите **Далее.**
4. В диалоговом окне **Диапазон IP-адресов** введите в поле **Начальный IP-адрес** первый незанятый адрес в вашей подсети (например,192.168.1.1), а в поле **Конечный IP-адрес** — значение 192.168.1.254.

   Поля маски будут заполнены по умолчанию текущей маской сети (в нашем случае 24\255.255.255.0). Нажмите **Далее.**
5. В диалоговом окне **Добавление исключений** оставьте все значения пустыми и нажмите **Далее.**
6. В диалоговом окне **Срок действия аренды адреса** оставьте значение по умолчанию и нажмите **Далее.**
7. В диалоговом окне **Настройка параметров DHCP** выберите **Да, настроить эти параметры сейчас** и нажмите **Далее.**
8. В диалоговом окне **Маршрутизатор (основной шлюз)** не вводите ничего, а нажмите **Далее.**
9. В диалоговом окне **Имя домена и DNS-серверы** оставьте поле **Родительский домен** пустым, а в поле **IP-адрес** введите адрес 192.168.10.2. Затем нажмите кнопку **Добавить** и продолжите нажатием кнопки **Далее.**
10. В диалоговом окне **WINS-серверы,** если вы установили сервер WINS на SRVR001, введите в поле **IP-адрес** адрес 192.168.10.2 и нажмите кнопку **Добавить.** Нажмите **Далее.**
11. В диалоговом окне **Активировать область** отметьте поле **Нет, я активирую эту область позже** и нажмите **Далее**
12. Завершите работу мастера нажатием на кнопку **Готово.**

Проверьте, правильно ли вы задали параметры области, по консоли DHCP (рис. 14)

• В списке **Пул адресов** вы должны увидеть введенный диапазон IP-адресов (192.168.1.1 до 192.168.1.254).

• В списках **Арендованные адреса** и **Резервирование** не должно быть ни одного значения.

• В списке **Параметры области** должно быть три параметра: **006 DNS-серверы, 044 WINS\NBNS-сереepbi** и **046 Тип узла WINS\NBT.**

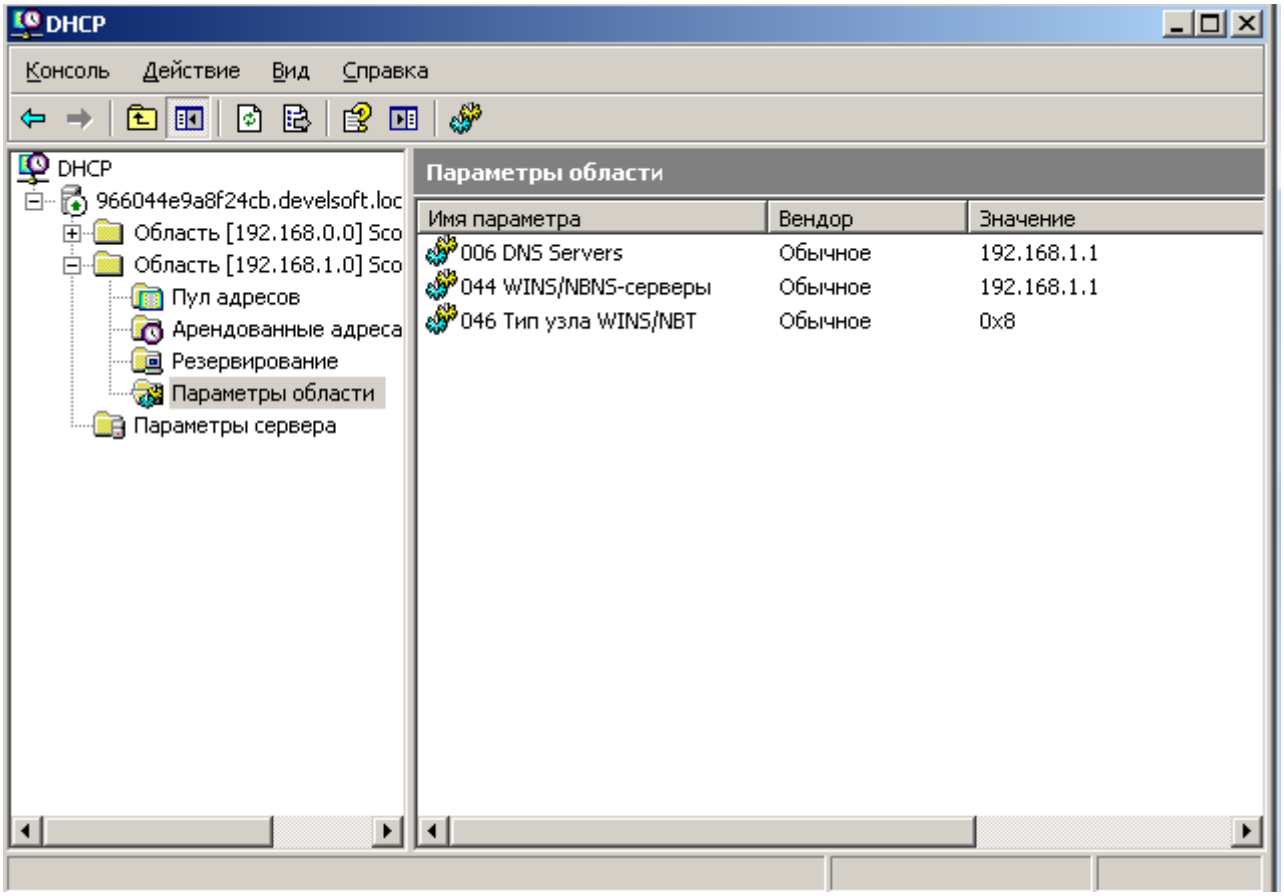


Рис. 14. Параметры области, по консоли DHCP

Если все в порядке, можно провести активацию области. Щелкните правой кнопкой мыши по области ≪Scope1≫ в левой части окна консоли и из контекстного меню выберите команду **Активировать.** После ее выполнения из метки области исчезнет красная стрелка, отмечающая неактивные области.

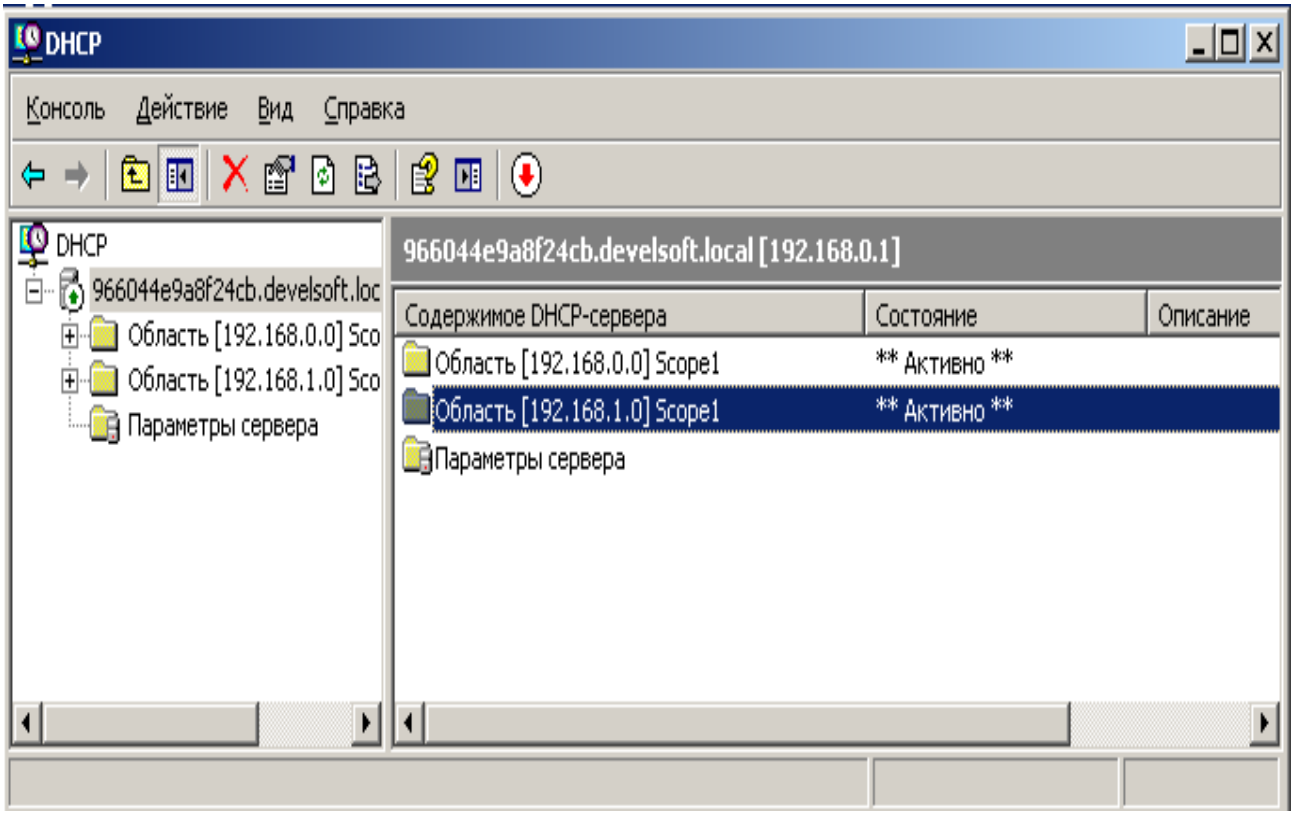


Рис. 15. Область ≪Scope1≫ активирована

Задание № 4. ***Установка и настройка сервера WINS***

Цели работы. Изучить процесс установки и настройки сервера WINS.

Упражнение 1. Установка службы WINS

Установите в системе службу WINS:

1. Кнопка "Пуск" — "Панель управления" — "Установка и удаление программ"
2. Кнопка "Установка компонентов Windows" — Выберите "Сетевые службы"
3. Кнопка "Состав" — Выберите "WINS" — Кнопка "ОК"
4. Кнопка "Далее" (если необходимо, укажите путь к дистрибутиву системы)
5. Кнопка "Готово"

Упражнение 2. Настройка клиентской части протокола TCP/IP на использование службы WINS

Настройка сервера как клиента службы WINS состоит из следующих этапов:

1. Вызовите окно свойств **Подключение по локальной сети** и откройте свойства **Протокол сети Интернет (TCP\1P).**

2. В диалоговом окне **Протокол сети Интернет (TCP\1P) — свойства** нажмите кнопку **Дополнительно** и затем на вкладке **WINS** нажмите на кнопку **Добавить.**

3. Введите IP-адрес сервера SRVR001 (192.168.10.2) и нажатием на кнопку **Добавить** добавьте его. Закройте диалоговое окно нажатием на клавишу ОК.

4. Закройте все диалоговые окна.

Упражнение 3. Анализ записей, зарегистрированных службой WINS.

1. Откройте консоль управления службой WINS
2. Раскройте информацию о вашем сервере
3. Щелкните правой кнопкой мыши на *"Активные регистрации"* — *"Отобразить записи"* — Кнопка *"Найти"*
4. Выберите мышью *"Активные регистрации"*
5. Изучите записи севера WINS

Задание № 5. ***Установка и настройка службы маршрутизации и удаленного доступа, настройка клиентских подключений, управление доступом через Active Directory и политики службы маршрутизации и удаленного доступа***

Цель работы. Изучить установку и настройку службы маршрутизации и удаленного доступа, настройку клиентских подключений, настройку политик службы маршрутизации и удаленного доступа.

Упражнение 1. Включение и настройка службы маршрутизации и удаленного доступа .

1. Откройте консоль *"Маршрутизация и удаленный доступ":*

Кнопка *"Пуск" —"Все программы" — "Администрирование" — "Маршрутизация и удаленный доступ"*

2. Запустите мастер настройки службы:

a) Щелкнуть правой кнопкой мыши на имени сервера
b) Выбрать *"Настроить и включить маршрутизацию и удаленный доступ"*
c) Кнопка *"Далее"*
d) Выбрать *"Особая конфигурация"* — Кнопка *"Далее"*
e) Выбрать все службы — Кнопка *"Далее"*
f) Кнопка *"Готово"*
g) Кнопка *"Да"* (система произведет запуск службы)

Упражнение 2. Настройка параметров сервера и настройка разрешений на подключение к серверу через Active Directory.

Настройте параметры сервера:

1. Консоль *"Маршрутизация и удаленный доступ"*
2. Щелкнуть правой кнопкой мыши на имени сервера — *"Свойства"* — Закладка *"IP"*
3. Выбрать *"статический пул адресов"* — Кнопка *"Добавить"*
4. *"Начальный IP-адрес"* — ввести 192.168.NNN.1
5. *"Конечный IP-адрес"* — ввести 192.168.NNN.10 — Кнопка *"ОК"*

Примечание: параметр NNN — 3 последние цифры IP-адреса вашего сервера;

Разрешите пользователю *"Администратор"* подключения к службе удаленного доступа:

1. Консоль *"Active Directory - пользователи и компьютеры"*
2. Свойства пользователя *"Администратор"*
3. Закладка *"Входящие звонки"* — Выбрать *"Разрешить доступ"* — Кнопка *"ОК.*

Задание № 6. *Настройка параметров безопасности (Шаблоны безопасности, Анализ и настройка безопасности)*

Цель работы. Изучить применение оснасток *"Шаблоны безопасности"*, *"Анализ и настройка безопасности"* для анализа и настройки параметров безопасности сервера.

Упражнение 1. Создание консоли с оснастками "Шаблоны безопасности", "Анализ и настройка безопасности"

1. Откройте новую консоль mmc Кнопка *"Пуск"* - *"Выполнить"* - Введите "mmc" - Кнопка *"ОК"*

2. Добавьте оснастки Меню "Консоль" -

Выберите *"Добавить или удалить оснастку"* -

Кнопка *"Добавить"* -

Выберите *"Шаблоны безопасности"* -

Кнопка *"Добавить"* -

Выберите *"Анализ и настройка безопасности"* -

Кнопка *"Добавить"* -

Кнопка *"Закрыть"* -

Кнопка *"ОК"*

Упражнение 2. Изучение стандартных шаблонов безопасности

1. Откройте оснастку *"Шаблоны безопасности"*

2. Изучите имеющиеся в системе стандартные шаблоны. Обратите внимание на шаблоны:

hisecdc

securedc

setupsecurity

3. Изучите в шаблонах разделы:

- *Политики учетных записей*
  - *Политика паролей*
  - *Политика блокировки учетной записи*
- *Локальные политики*
  - *Политика аудита*
  - *Назначение прав пользователя*
  - *Параметры безопасности*
- *Журнал событий*

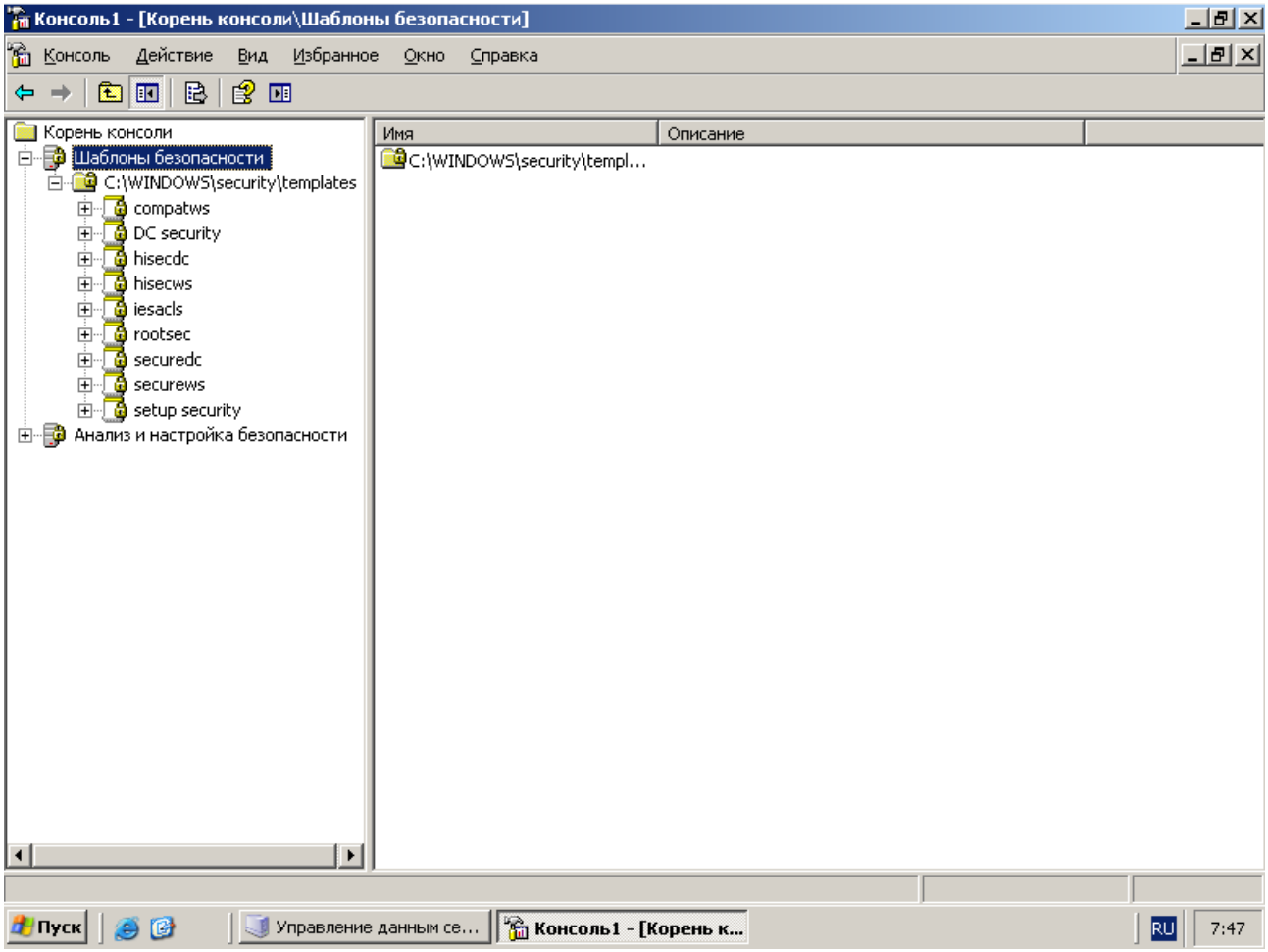


Рис. 16. Окно «Шаблона безопасности»

Упражнение 3. Создание базы данных для анализа и настройки безопасности

Создайте новую базу данных:

1. В левой части окна новой консоли выберите оснастку *"Анализ и настройка безопасности"*
2. Меню *"Действие"* -

   Выберите *"Открыть базу данных"* -

   Укажите имя базы данных (например, *БД*) и путь для сохранения базы (например, C:\мои документы\Securiti\Database) -

   Кнопка *"Открыть"* -

   Выберите шаблон для импорта (выберите шаблон hisecdc.inf -

шаблон контроллера домена с высоким уровнем безопасности) -

Кнопка *"Открыть"*

Упражнение 4. Проведение анализа настроек безопасности

Проведите анализ настроек системы безопасности вашего компьютера:

1. В левой части окна новой консоли выберите оснастку *"Анализ и настройка безопасности"*
2. Меню *"Действие"* -

   Выберите *"Анализ компьютера"* -

   Укажите путь к файлу журнала ошибок (например, C:\мои документы \Securiti \Database) -

   Кнопка *"ОК"*
3. Изучите результаты анализа настроек безопасности:

   В оснастке *"Анализ и настройка безопасности"* просмотрите разделы

   - *Политики учетных записей*
     - *Политика паролей*
     - *Политика блокировки учетной записи*
   - *Локальные политики*
     - *Политика аудита*
     - *Назначение прав пользователя*
     - *Параметры безопасности*
   - *Журнал событий*

   В каждом разделе сравните значения параметров базы данных (т.е. выбранного вами стандартного шаблона безопасности) и значения соответствующих параметров вашего компьютера.

   Найдите различия в настройках.
4. Закройте консоль

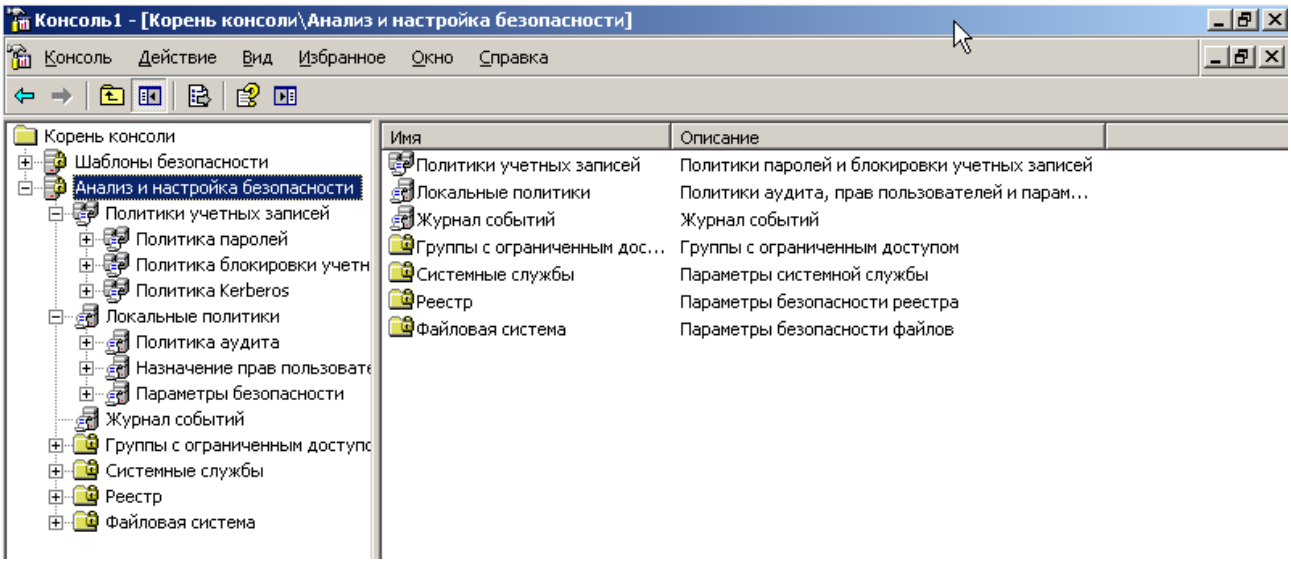


Рис. 17. Окно «Анализ и настройка безопасности»

Заключение

В наше время невозможно себе представить деятельность успешной, развивающейся компании без эффективного использования информационных технологий. Мир информации расширяется и неуклонно движется вперед гигантскими шагами. Те технологии, которые находились в стадии разработки еще вчера, уже сегодня становятся неотъемлемыми средствами ведения бизнеса.

Именно поэтому создание качественной современной информационной инфраструктуры офиса на сегодня является одной из приоритетных задач для любой компании. От того, насколько качественно и удобно организована информационная инфраструктура офиса, в той или иной степени зависит успешное протекание всех бизнес-процессов.

Деловая переписка по электронной почте, телефонные переговоры, подготовка и печать документов - все это необходимые инструменты для функционирования любого бизнеса, вне зависимости от отрасли и сектора занимаемого рынка. Стоит ли говорить о том, что компания, не обладающая современной, оптимизированной, связанно работающей IT инфраструктурой, сегодня просто не способна вести эффективный конкурентоспособный бизнес в своей отрасли.

Мы все давно привыкли к компьютерам, работающим по сети, интернет-серверам, телефонам, факсам, копировальной технике, программным продуктам и другим технологиям, окружающим нас в офисах наших компаний уже много лет. Использование технических средств и информационных технологий в работе офиса давно стало стандартом, и мы уже не задумываемся об этом, совершая звонки, ведя деловую переписку по Интернету, осуществляя работу с различными базами данных или просто распечатывая очередной документ. Фундаментом для эффективной и бесперебойной работы любого офиса, сегодня является профессионально организованная и стабильно поддерживаемая IT инфраструктура.

IT инфраструктура включает в себя следующие звенья:

- ✓ компьютеры (рабочие станции пользователей);
- ✓ сервера (выделенные сервера, выполняющие разные задачи);
- ✓ программное обеспечение серверов и рабочих станций;
- ✓ оргтехнику (принтеры, копиры, факс аппараты, сканеры);
- ✓ сети передачи данных, телефонные сети;
- ✓ активное сетевое оборудование и телефонию (маршрутизаторы, коммутаторы, телефонные станции).

Совместная, связанная работа всех звеньев IT системы, их функциональная и техническая совместимость, а также оптимизация в работе и удобство в использовании, являются основными требованиями, предъявляемыми к современной, качественной IT инфраструктуре. Грамотный подбор и организация работы элементов IT дают реальную возможность в большой степени повысить эффективность и бесперебойность протекания всех бизнес процессов в целом.

Создание и обеспечение стабильного функционирования IT инфраструктуры это многогранный процесс, который необходимо планировать изначально и лучше всего осуществлять в комплексе. Использование комплексного подхода при внедрении IT инфраструктуры в офисе поможет

сэкономить значительные денежные средства и избежать многих проблем, связанных с функционированием системы в будущем.

При проектировании IT инфраструктуры учитываются не только все существующие на данный момент требования к функционированию системы, но и возможности ее расширения и увеличения количества выполняемых ею задач.

Комплексный подход исключает ошибки, которые могут быть допущены на этапе проектирования системы, что позволяет избежать снижения эффективности работы предприятия в будущем.

4.Список использованных источников

1. Шетка П. Microsoft Windows Server 2003. Практическое руководство по настройке сети. – СПб.: Наука и Техника, 2006. – 608 с.
2. Гленн У., Инглиш Б. Microsoft Exchange Server 2003. Справочник администратора. – М.: Изд-во «СП ЭКОМ», 2005. – 720 с.