А.М. Голиков

СИСТЕМЫ РАДИОСВЯЗИ И СЕТИ ТЕЛЕРАДИОВЕЩАНИЯ

Компьютерный практикум

Томск

Голиков А.М. Системы радиосвязи и сети телерадиовещания: Компьютерный практикум. – Томск: Томск. гос. ун-т систем управления и радиоэлектроники, 2015. – 229 с.

Сборник содержит описания компьютерных практикумов по курсу «Системы радиосвязи и сети телерадиовещания», являющийся курсом, который включен в Государственный образовательный стандарт по специальности 090302.65 – Информационная безопасность телекоммуникационных систем. Представлены описания программных комплексов и методики выполнения практических работ.

ОГЛАВЛЕНИЕ

Компьютерный практикум 1. Исследование методов скремблирования информации в сетях и системах радиосвязи

1. Цель работы

Ознакомиться с методами цифровой обработки сигналов с использованием dsp-скремблеров, схемами получения шифрованных сигналов и исследованием их свойств. Изучить принципы работы цифровых сигнальных процессоров, а так же основ их программирования.

2. Краткие теоретические сведения

С развитием вычислительной техники и информационных технологий увеличивается сложность систем защиты компьютерной информации. Финансовый кризис обостряет конкуренцию в различных секторах рынка и выводит на первый план вопросы информационной безопасности даже для тех компаний, которые раньше, в более спокойных условиях, не придавали этим вопросам особого значения.

В данном обзоре предпринята попытка сопоставить базовые функции отечественных аппаратных устройств защиты информации (УЗИ) на основе сведений, предоставляемых фирмами-производителями, и выработать рекомендации по выбору устройства.

Преимущественный интерес к отечественным продуктам обусловлен тем, что применение зарубежных средств встречает значительные трудности. С одной стороны, их вывоз из страны происхождения зачастую вообще невозможен: так, в США, которые наряду с Россией остаются лидером мировой криптографии, наложен запрет на экспорт средств шифрования с “сильными” ключами. С другой стороны, легальное применение зарубежных криптографических средств в нашей стране жестко регламентируется, и в этих условиях оправданным представляется сосредоточить внимание на отечественных продуктах.

Как правило, аппаратные средства уступают чисто программным решениям по ряду параметров (скорости шифрования, возможности применения в компьютерах различных конструктивных исполнений — например, ноутбуках), но превосходят их по главному показателю — стойкости. Кроме того, нельзя полностью гарантировать, что в применяемых операционных системах (ОС) и прикладных программах отсутствуют неописанные возможности, невыявленные ошибки или умышленно размещенные “закладки”. Потенциально возможностями их модификации обладают не только активные злоумышленники, но даже обычные пользователи компьютеров: имея навыки программирования и администрирования и доступ к компьютерной системе, они способны модифицировать эту систему, снижая уровень ее надежности.

Для обеспечения должной безопасности следует либо заниматься анализом и аттестацией существующих систем на уровне их исходных текстов, либо разрабатывать собственную, полностью контролируемую ОС и постоянно заботиться о поддержании ее целостности. Чаще всего пользователи выбирают третий путь, отвечающий их реальным возможностям: принимают используемую ОС за контролируемую и — в лучшем случае — стремятся обеспечить ее целостность имеющимися в наличии средствами (антивирусными пакетами и т.п.).

Однако проверку целостности одних программ при помощи других нельзя признать надежной, поскольку под сомнение ставится целостность самой программы проверки целостности. Для получения достоверных сведений необходима некая начальная “точка отсчета”, подлинность которой не вызывает сомнений.

В подобной роли и могут выступить рассматриваемые устройства, применяемые в составе систем защиты информации (СЗИ) и позволяющие обеспечить целостность таких систем аппаратной реализацией функций, критически важных для поддержания надежности СЗИ. К числу таких функций, полностью или частично выполняемых аппаратными средствами, относятся следующие.

Запрет на модификацию процесса загрузки компьютера.

Идентификация и аутентификация пользователя до загрузки ОС.

Контроль целостности операционной системы и прикладного программного обеспечения (ПО).

Управление доступом пользователя к ресурсам компьютера.

Ведение журнала действий пользователя.

Реализация криптографических алгоритмов, гарантия их стойкости и неизменности.

Надежное хранение секретных криптографических элементов (ключей) вне оперативного запоминающего устройства (ОЗУ) компьютера.

Загрузка секретных элементов со специальных носителей: смарт-карт, идентификаторов Touch Memory (TM) и т.п. К примеру, смарт-карты по сравнению с традиционными носителями (дискетами) обладают большей стойкостью к механическим, электрическим, магнитным, климатическим воздействиям, более долговечны (срок хранения данных — до 10 лет) и удобны в пользовании, а микропроцессорные карты, кроме того, обладают еще и высокой степенью защищенности от несанкционированного использования.

Наличие аппаратного датчика случайных чисел. Аппаратный датчик, использующий физический процесс (например, обратный пробой специализированного диода), обеспечивает распределение случайных чисел, наиболее близкое к равновероятному (что недоступно программным датчикам). Таким образом, при формировании криптографических ключей с помощью аппаратного датчика обеспечивается максимальный уровень их надежности.

Полностью реализовать все перечисленные функции одним только аппаратным способом невозможно (а часто и не нужно), поэтому ряд функций может выполняться программно. Программное обеспечение может находиться в постоянном запоминающем устройстве (ПЗУ) УЗИ, либо размещаться на обычных носителях (в этом случае защищать его целостность необходимо организационными методами — особым режимом хранения, ограничением числа лиц, имеющих доступ к этому ПО, и т.д.). В любом случае, ПО должно опираться на возможности, предоставляемые устройством защиты информации.

Скремблирование аналоговых сигналов

Преобразования с инверсией спектра и статическими перестановками спектральных компонент речевого сигнала

Схемотехническая реализация двух рассматриваемых вариантов заметно отличается, что и обусловливает их раздельное рассмотрение. Однако с точки зрения достигаемых результатов по защищенности сигнала в канале связи оба варианта аналогичны.

Процесс инверсии спектра сигнала при передаче и его восстановления при приеме иллюстрируется на рисунке 1.1.

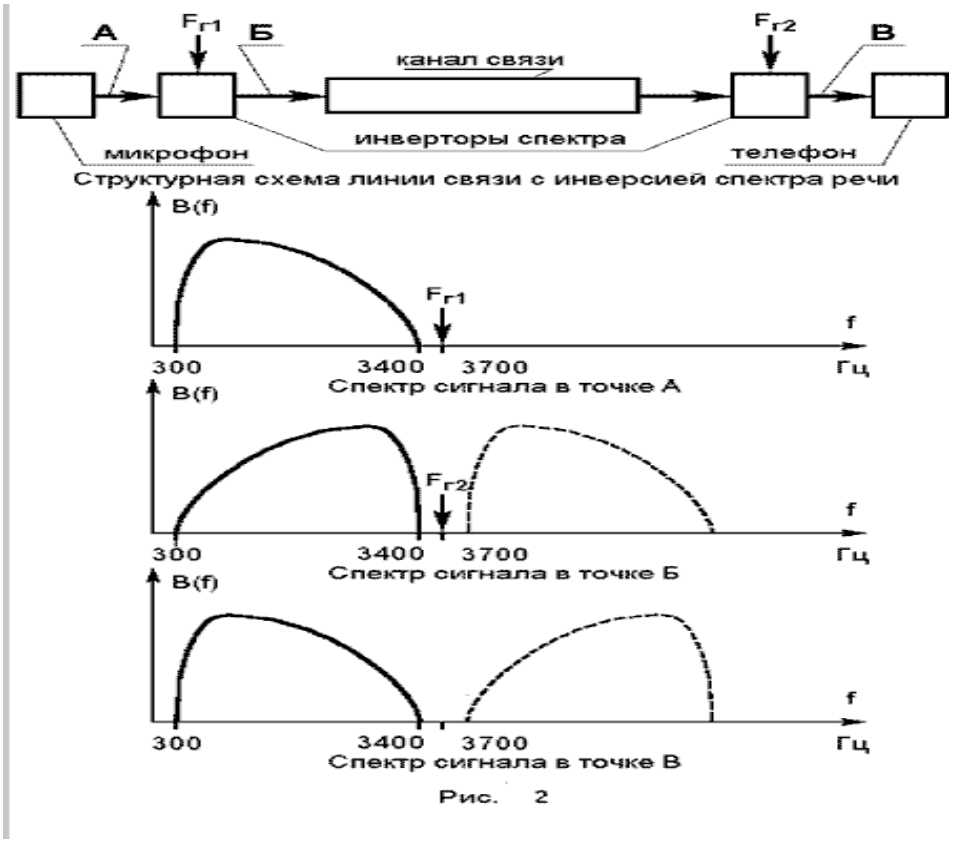


Рисунок 1.1. Процесс инверсии спектра

Схема инвертора представляет собой балансный смеситель. При частоте гетеродина $F_{г,}$ равной сумме граничных частот $F_н$ и $F_в$ преобразуемого сигнала (3700 Гц для стандартного телефонного канала с $F_н$ = 300 Гц и $F_в$ = 3400 Гц) нижняя полоса частот после смесителя воспроизводится в исходной полосе частот, т.е. в полосе канала в инверсном виде. При приеме производится повторная инверсия и исходный сигнал восстанавливается.

Качество восстановленной речи зависит от качества (на передающей и на приемной сторонах) смесителей, фильтров, ограничивающих спектр входного сигнала и выделяющих нижнюю полосу частот преобразованного сигнала, а также от коррекции на приемной стороне частотных искажений канала, влияние которых также сказывается инверсно: затухание канала в высокочастотной части спектра на приеме сказывается в низкочастотной части сигнала и наоборот.

При перехвате сигнал с инвертированным спектром может быть легко восстановлен любым аналогичным аппаратом (не обязательно однотипным), а при соответствующей тренировке — воспринят человеком непосредственно.

Для повышения стойкости защиты некоторые изготовители вводят переменную частоту гетеродина, устанавливаемую партнерами по договоренности в форме числового кода-пароля, вводимого в аппарат при переходе в защищенный режим.

Возможности такого дополнительного частотного сдвига, приводящего к несовпадению спектра передаваемого сигнала и номинальной частотной полосы канала связи и, соответственно, к ухудшению качества восстановленной речи, ограничены несколькими сотнями герц. Достигаемый эффект весьма условен. Действительно, при прослушивании восстановленного сигнала, в случае неравенства частот гетеродинов на передаче и на приеме, в первый момент возникает ощущение неестественной и непонятной речи, которое, однако, почти не мешает воспринимать ее смысл после некоторой адаптации.

Процесс преобразования с фиксированными перестановками спектральных компонент речевого сигнала при передаче и его восстановления при приеме иллюстрируется на рисунке 1.2.

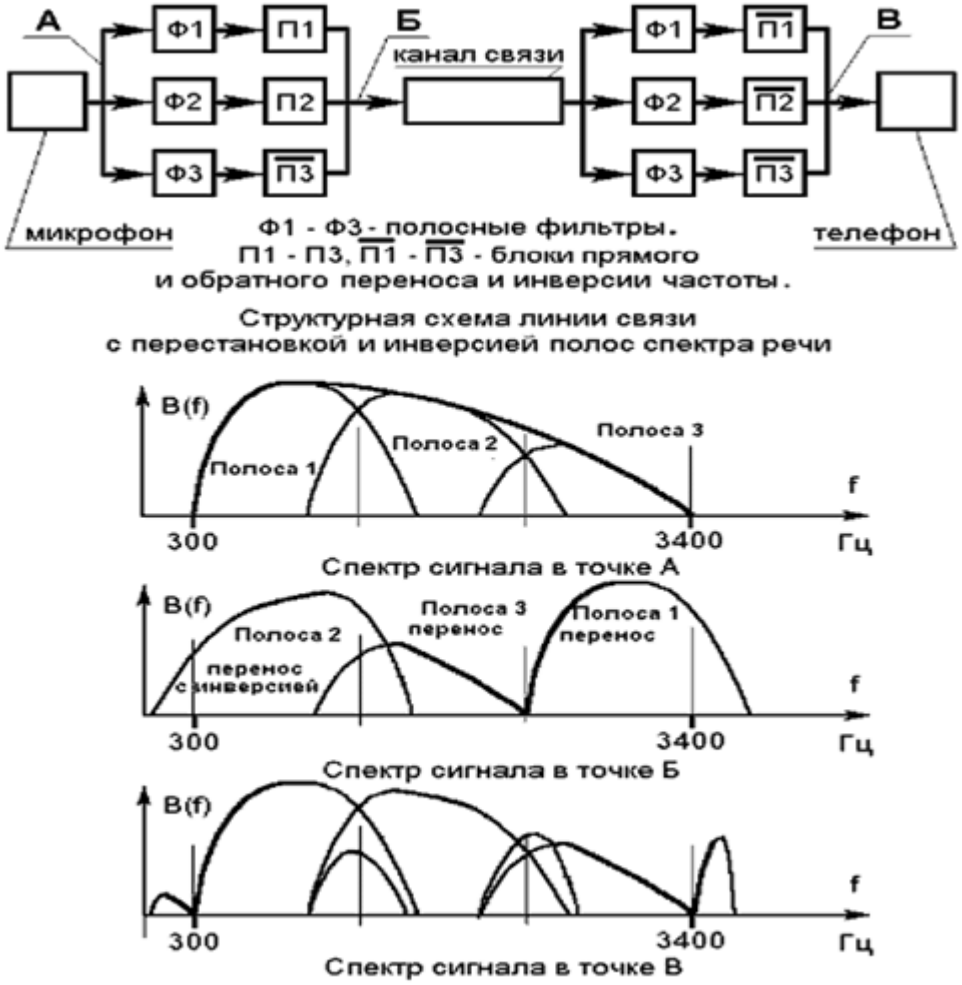


Рисунок 1.2. Преобразование с фиксированными перестановками

При таком преобразовании разборчивость речевого сигнала нарушается в значительно большей степени, чем при простой инверсии. Следует, однако, учитывать, что выбор вариантов частотных перестановок весьма ограничен. Фильтры, выделяющие частотные полосы в исходном и в линейном сигнале, имеют конечную крутизну характеристики, в результате чего на заметном частотном интервале в окрестности границы частотных полос будет происходить заметное невосстановимое смешение различных компонент сигнала. Полная полоса частот (300-3400 Гц) составляет 3,5 октавы. При формировании трех полос (по 1,2 октавы на каждую полосу) и при использовании фильтров 8-го порядка (нарастание затухания около 48 дБ/октаву) затухание в середине (!) соседней полосы составит не более 30 дБ, что предопределяет низкое качество восстановленной речи. Существенное увеличение порядка фильтров настолько усложняет аппаратуру, что она теряет преимущества перед другими вариантами преобразователей. В тоже время число возможных перестановок из трех полос — всего лишь 6, из четырех полос — 24, т.е. даже в условиях прямого перехвата, не говоря уже об анализе записи, подбор нужной подстановки не составит труда.

Наиболее существенным положительным качеством рассматриваемых преобразователей является их автономность, т.е. отсутствие необходимости во взаимной синхронизации передающего и приемного аппарата и, соответственно, отсутствие задержки связи на время проведения синхронизации и возможных срывов защищенного режима из-за качества канала, недостаточного для проведения синхронизации. Если удалось установить связь в открытом режиме после включения партнерами инверторов будет реализован и защищенный режим.

Положительными качествами такой аппаратуры также являются:

- дешевизна (цены инверторов спектра порядка 30 — 50 USD);
- возможность построения схем, не вносящих задержку сигнала;
- малая критичность к качеству используемого канала связи и предельная простота в управлении.

Аппаратура может включаться между телефонным аппаратом и линией в стандартный двухпроводной стык между телефонным аппаратом и микротелефонной трубкой, может использоваться в виде накладки на микротелефонную трубку с акустической передачей преобразованного сигнала. Переход в защищенный режим происходит по взаимной договоренности партнеров после установления соединения. Переход происходит немедленно после нажатия соответствующей клавиши (или другого управляющего действия). Включение и выключение защищенного режима осуществляется каждым партнером самостоятельно, синхронизация действий не требуется.

При разговоре в линии прослушивается характерный сигнал, по структуре полностью повторяющий передаваемую речь. Восстановленный сигнал имеет высокое качество. В дешевых аппаратах с недостаточной фильтрацией возможно наличие свистящих тонов и изменение тембра голоса говорящего. Наличие посторонних шумов в помещении, из которого ведется передача, сказывается на качестве восстановленного сигнала так же, как в открытом режиме, на стойкость защитного преобразования почти не влияет.

Преобразования с временными перестановками (скремблированием) и временной инверсией элементов речевого сигнала со статическим законом перестановки

Принцип работы аппаратуры сходен с разрушением и последующим восстановлением мозаичной картины, что обусловило появление названия “аппаратура мозаичных преобразований”.

Данный класс аппаратуры требует наличия в своем составе блока запоминания сигнала с управляемым доступом по записи и считыванию, поэтому аналоговой такую аппаратуру можно назвать условно. Временная перестановка элементарных отрезков речевого сигнала и восстановление их последовательности на приеме занимают соответствующий интервал времени. Поэтому обязательным свойством такой аппаратуры является заметная задержка сигнала на приемной стороне. Процессы преобразования сигнала показаны на рисунке 1.3.

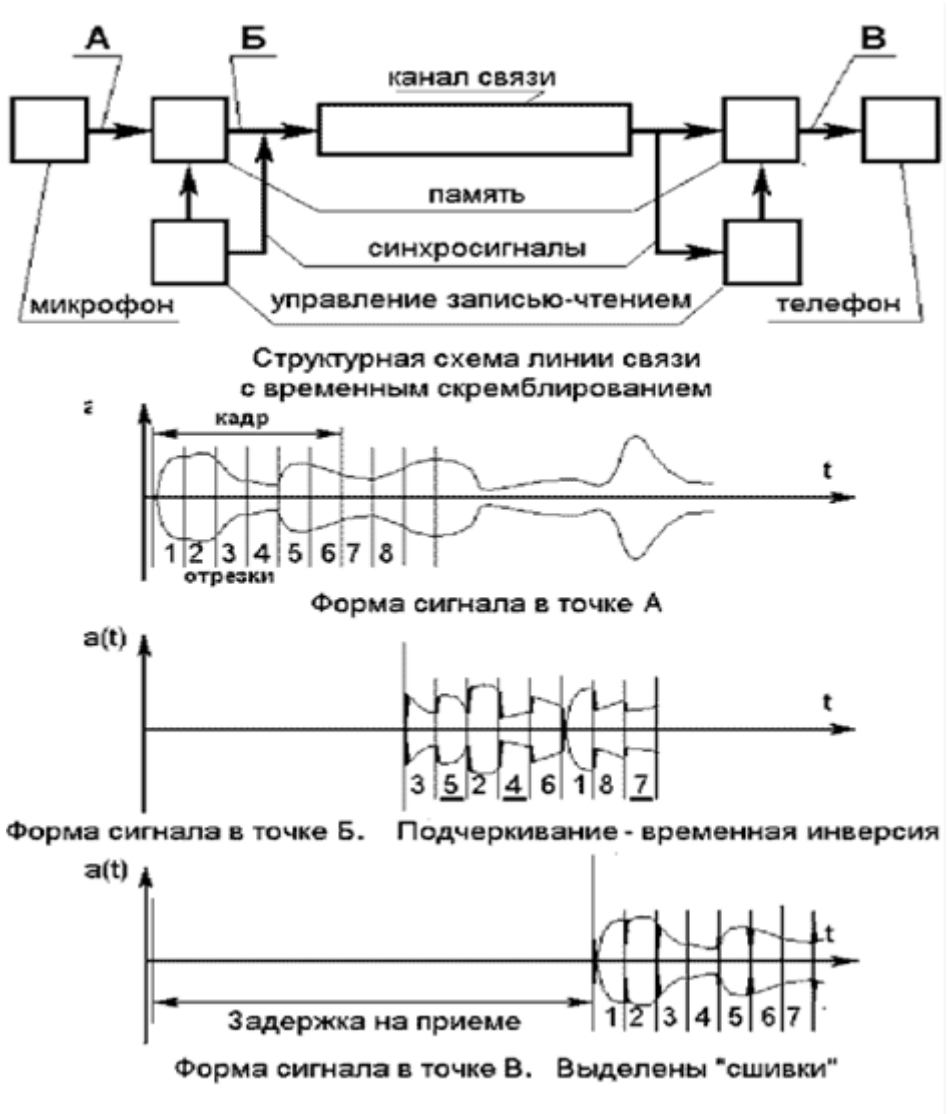


Рисунок 1.3. Процесс преобразования сигнала

Чем меньше длительность элементарных отрезков, на которые разбивается исходный речевой сигнал и чем больше элементов участвуют в операции перестановки, тем сложнее процесс восстановления речи по перехваченному линейному сигналу.

Однако при передаче по каналу связи возникают краевые искажения элементарных отрезков. При восстановлении речи на приемной стороне это приводит к появлению “сшивок”, ухудшающих качество восстановленного сигнала. С учетом характеристик реальных телефонных каналов длительность элементарных отрезков сигнала ограничена снизу на уровне 15 — 20 миллисекунд.

Увеличение числа перемешиваемых элементов мозаики — увеличение “глубины перестановки” — ограничено возрастанием задержки восстановленного сигнала на приеме. При диалоге заметные неудобства возникают при задержке более 0,3 сек, а при задержке более 1 сек диалог становится невозможным. Оба указанных фактора определяют глубину перестановки на уровне 16 — 64 элементарных отрезков речи.

Маскирующее воздействие на структуру сигналов в линии связи может быть достигнуто временной инверсией (воспроизведением в обратном направлении по отношению к записи) всех или отдельных отрезков. Такое преобразование неэффективно на коротких отрезках (с продолжительностью менее длительности одного элементарного звука речи). Применение длинных отрезков уменьшает возможность их перемешивания. Поэтому временная инверсия применяется исключительно как дополнительное преобразование в

комбинации с временными перестановками. При этом наиболее эффективна временная инверсия всех отрезков.

Временные перестановки и временная инверсия при правильном выборе параметров перестановки исключают непосредственное прослушивание речи в канале связи, но при анализе записи или при оперативном анализе сигнала на месте перехвата статическая перестановка, повторяющаяся из кадра в кадр, легко выявляется по спектральным и амплитудным связям отрезков, в результате чего исходная речь может быть восстановлена с применением несложной аппаратуры (ПЭВМ с аудиоплатой).

В то же время по своему составу и сложности алгоритма аппаратура с фиксированными перестановками незначительно отличается от аппаратуры с переменными перестановками, управляемыми криптоблоком. Поэтому в настоящее время для цепей защиты информации применяются почти исключительно аппараты с переменными перестановками.

Преобразования с временными или частотными перестановками (скремблированием) с переменными перестановками под управлением криптоблока и комбинированные мозаичные преобразования

Применение переменных перестановок позволяет значительно затруднить восстановление исходной речи по перехвату сигнала в канале. При правильном выборе криптоалгоритма удачный подбор перестановки на одном интервале никак не способствует подбору перестановок на последующих интервалах. Кроме того, введение криптоалгоритма с индивидуальным ключом исключает возможность использования для перехвата однотипного аппарата.

Аппаратура строится, как правило, на базе сигнальных процессоров , имеет в своем составе АЦП, ЦАП, криптоблок управления перестановкой, систему ввода или формирования ключа. Обязательным этапом рабочего процесса является начальная синхронизация взаимодействующих аппаратов и их последующая подсинхронизация.

Как следствие, эта аппаратура заметно дороже аппаратуры частотной инверсии — 200 - 400 USD за единицу.

При переходе в защищенный режим по договоренности абонентов возникает интервал прерывания речевой связи, который занимает процесс синхронизации и установления взаимодействия криптоблоков. В ряде изделий в это же время абонент, используя тастатуру телефонного аппарата или тастатуру скремблера, или персональный узел памяти, должен ввести ключ. В результате переход в защищенный режим может занимать до 10 — 20 секунд. При этом надо учитывать, что при плохом качестве канала синхронизация и переход в защищенный режим могут не состояться, хотя связь в открытом режиме, пусть и при плохом качестве, поддерживается.

Наличие временной задержки при передаче сигнала при работе по двухпроводной линии неизбежно приводит к возникновению “эха” (это же характерно и для статических временных перестановок). В современной аппаратуре связи отработаны весьма совершенные алгоритмы подавления эха, широко применяемые в скоростных модемах. Однако человеческое ухо реагирует на уровни эхо-сигналов, заведомо несущественные для модемов. Поэтому даже в наиболее удачных моделях скремблеров подавление эха до не замечаемого абонентом уровня достигается только при случайном удачном сочетании параметров линии связи.

Криптоблок, управляющий процессом перестановок, может использовать как симметричную, так и несимметричную (“с открытым ключом”) ключевую систему. Варианты с несимметричной системой предпочтительнее, так как упрощают эксплуатационный процесс и исключают вскрытие записи при хищении личного ключа. Однако и в этом случае применение личного пароля полезно, так как исключает вхождение в связь посторонних лиц.

Учитывая то вышеуказанное обстоятельство, что при самом совершенном криптоалгоритме передаваемая речь может быть восстановлена по перехвату линейного сигнала по остаточным признакам взаимного расположения элементарных отрезков, применение в скремблерах очень мощных криптоалгоритмов и ключевых кодов большой длины не оправдано. Вполне достаточной является длина ключевого кода порядка 9 десятичных (30 двоичных) знаков в симметричной ключевой системе и 30 десятичных (около 100 двоичных) — в несимметричной ключевой системе. При разговоре в линии прослушивается характерный “рваный” сигнал, в котором достаточно легко определяется структура передаваемой речи. Восстановленный сигнал имеет высокое качество, мало отличающееся от качества речи в открытом режиме на том же канале. Наличие посторонних шумов в помещении, из которого ведется передача, сказывается на качестве восстановленного сигнала так же, как в открытом режиме. Однако ритмические помехи, создающие “шкалу времени” параллельную преобразуемому сигналу, могут повлиять на стойкость защитного преобразования. Аппаратура может включаться между телефонным аппаратом и линией в стандартный двухпроводной стык, между телефонным аппаратом и микротелефонной трубкой, может использоваться в виде накладки на микротелефонную трубку с акустической передачей преобразованного сигнала.

Таким образом, основными положительными качествами аппаратуры мозаичных преобразований — скремблеров — являются:

- относительно высокая стойкость защиты передаваемого речевого сигнала, исключающая его непосредственное прослушивание даже при наличии группы высокотренерованных аудиторов и требующая для восстановления речи значительных затрат времени при использовании специализированных измерительно-вычислительных комплексов, применяемых государственными спецслужбами;
- относительно низкая стоимость;
- простота эксплуатации (для моделей, специально разработанных для непрофессионального пользователя).

К недостаткам данного класса аппаратуры следует отнести:

- задержку восстановленного сигнала на приемной стороне, требующую привыкания и затрудняющую диалог;
- наличие эха, зависящего от параметров коммутируемой линии связи;
- задержку связи на время прохождения процесса синхронизации аппаратов;
- возможность срыва синхронизации на плохих каналах.

По совокупности качеств этот класс аппаратуры представляется наиболее приемлемым для использования в корпоративных системах защищенного обмена речевой информацией оперативного характера, не требующей длительного периода секретности.

Скремблирование цифровых сигналов

Суть скремблирования заключается в побитном изменении проходящего через систему потока данных. Практически единственной операцией, используемой в скремблерах является XOR – "побитное исключающее ИЛИ". Параллельно прохождению информационного потока в скремблере по определенному правилу генерируется поток бит – кодирующий поток. Как прямое, так и обратное шифрование осуществляется наложением по XOR кодирующей последовательности на исходную.

Генерация кодирующей последовательности бит производится циклически из небольшого начального объема информации – ключа по следующему алгоритму. Из текущего набора бит выбираются значения определенных разрядов и складываются по XOR между собой. Все разряды сдвигаются на 1 бит, а только что полученное значение ("0" или "1") помещается в освободившийся самый младший разряд. Значение, находившееся в самом старшем разряде до сдвига, добавляется в кодирующую последовательность, становясь очередным ее битом (см. рис.1.4).

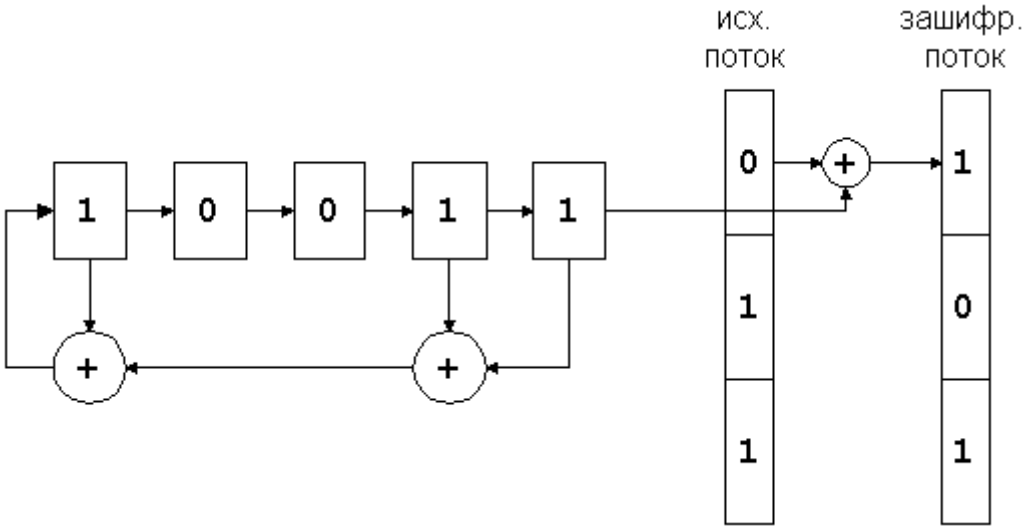


Рисунок 1.4. Схема скремблирования

Из теории передачи данных криптография заимствовала для записи подобных схем двоичную систему записи. По ней изображенный на рисунке скремблер записывается комбинацией "10011_2" – единицы соответствуют разрядам, с которых снимаются биты для формирования обратной связи.

Как видим, устройство скремблера предельно просто. Его реализация возможна как на электронной, так и на электрической базе, что и обеспечило его широкое применение в полевых условиях. Более того, тот факт, что каждый бит выходной последовательности зависит только от одного входного бита, еще более упрочило положение скремблеров в защите потоковой передачи данных. Это связано с неизбежно возникающими в канале передаче помехами, которые могут исказить в этом случае только те биты, на которые они приходятся, а не связанную с ними группу байт, как это имеет место в блочных шифрах.

Декодирование заскремблированных последовательностей происходит по той же самой схеме, что и кодирование. Именно для этого в алгоритмах применяется результирующее кодирование по "исключающему ИЛИ" – схема, однозначно восстановимая при раскодировании без каких-либо дополнительных вычислительных затрат. Произведем декодирование полученного фрагмента.

Как Вы можете догадаться, главная проблема шифров на основе скремблеров - синхронизация передающего (кодирующего) и принимающего (декодирующего) устройств. При пропуске или ошибочном вставлении хотя бы одного бита вся передаваемая информация необратимо теряется. Поэтому, в системах шифрования на основе скремблеров очень большое внимание уделяется методам синхронизации. На практике для этих целей обычно применяется комбинация двух методов: а) добавление в поток информации синхронизирующих битов, заранее известных приемной стороне, что позволяет ей при ненахождении такого бита активно начать поиск синхронизации с отправителем, и б) использование высокоточных генераторов временных импульсов, что позволяет в моменты потери синхронизации производить декодирование принимаемых битов информации "по памяти" без синхронизации.

Число бит, охваченных обратной связью, то есть разрядность устройства памяти для порождающих кодирующую последовательность бит называется разрядностью скремблера. Изображенный выше скремблер имеет разрядность 5. В отношении параметров криптостойкости данная величина полностью идентична длине ключа блочных шифров, который будет проанализирован далее. На данном же этапе важно отметить, что чем больше разрядность скремблера, тем выше криптостойкость системы, основанной на его использовании.

При достаточно долгой работе скремблера неизбежно возникает его зацикливание. По выполнении определенного числа тактов в ячейках скремблера создастся комбинация бит, которая в нем уже однажды оказывалась, и с этого момента кодирующая последовательность начнет циклически повторяться с фиксированным периодом. Данная проблема неустранима по своей природе, так как в N разрядах скремблера не может пребывать более 2^N комбинаций бит, и, следовательно, максимум, через, 2^N-1 циклов повтор комбинации обязательно произойдет. Комбинация "все нули" сразу же исключается из цепочки графа состояний скремблера – она приводит скремблер к такому же положению "все нули". Это указывает еще и на то, что ключ "все нули" неприменим для скремблера. Каждый генерируемый при сдвиге бит зависит только от нескольких бит хранимой в данный момент скремблером комбинации. Поэтому после повторения некоторой ситуации, однажды уже встречавшейся в скремблере, все следующие за ней будут в точности повторять цепочку, уже прошедшую ранее в скремблере.

Возможны различные типы графов состояния скремблера. На рисунке 1.5 приведены примерные варианты для 3-разрядного скремблера. В случае "А" кроме всегда присутствующего цикла "000">>"000" мы видим еще два цикла – с 3-мя состояниями и 4-мя. В случае "Б" мы видим цепочку, которая сходится к циклу из 3-х состояний и уже никогда оттуда не выходит. И наконец, в случае "В" все возможные состояния кроме нулевого, объединены в один замкнутый цикл. Очевидно, что именно в этом случае, когда все 2^N-1 состояний системы образуют цикл, период повторения выходных комбинаций максимален, а корреляция между длиной цикла и начальным состоянием скремблера (ключом), которая привела бы к появлению более слабых ключей, отсутствует.

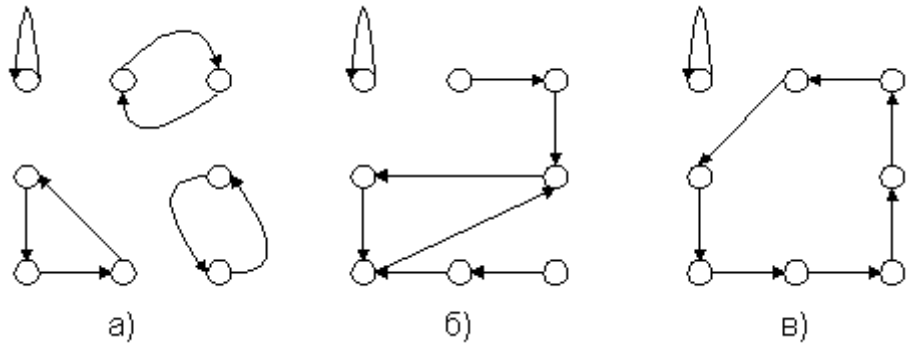


Рисунок 1.5. Графы для трех разрядного скремблера

И вот здесь математика преподнесла прикладной науке, каковой является криптография, очередной подарок. Следствием одной из теорем доказывается (в терминах применительно к скремблированию), что для скремблера любой разрядности N всегда существует такой выбор охватываемых обратной связью разрядов, что генерируемая ими последовательность бит будет иметь период, равный 2^N-1 битам. Так, например, в 8-битном скремблере, при охвате 0-го, 1-го, 6-го и 7-го разрядов действительно за время генерации 255 бит последовательно проходят все числа от 1 до 255, не повторяясь ни разу.

Схемы с выбранными по данному закону обратными связями называются генераторами последовательностей наибольшей длины (ПНД), и именно они используются в скремблирующей аппаратуре. Из множества генераторов ПНД заданной разрядности во времена, когда они реализовывались на электрической или минимальной электронной базе выбирались те, у которых число разрядов, участвующих в создании очередного бита, было минимальным. Обычно генератора ПНД удавалось достичь за 3 или 4 связи. Сама же разрядность скремблеров превышала 30 бит, что давало возможность передавать до 2^{40} бит = 100 Мбайт информации без опасения начала повторения кодирующей последовательности.

ПНД неразрывно связаны с математической теорией неприводимых полиномов. Оказывается, достаточно чтобы полином степени N не был представим по модулю 2 в виде произведения никаких других полиномов, для того, чтобы скремблер, построенный на его основе, создавал ПНД. Например, единственным неприводимым полиномом степени 3 является x^3+x+1, в двоичном виде он записывается как 1011_2 (единицы соответствуют присутствующим разрядам). Скремблеры на основе неприводимых полиномов образуются отбрасыванием самого старшего разряда (он всегда присутствует, а следовательно, несет информацию только о степени полинома), так на основе указанного полинома, мы можем создать скремблер 011_2 с периодом зацикливания $7(=2^3-1)$. Естественно, что на практике применяются полиномы значительно более высоких порядков. А таблицы неприводимых полиномов любых порядков можно всегда найти в специализированных математических справочниках.

Существенным недостатком скремблирующих алгоритмов является их нестойкость к фальсификации. Подробнее данная проблема рассмотрена на следующей лекции, применительно к созданию целых криптосистем.

Генераторы псевдослучайной последовательности.

Как уже говорилось выше, скремблеры и дескремблеры цифрового сигнала строятся на основе генераторов псевдослучайных последовательностей битов. Генераторы чаще всего выполняются с использованием M-разрядных сдвиговых регистров RG с цепями обратной связи (рис. 1.6).

Показанные устройства различаются периодом генерируемых последовательностей битов. В генераторе по схеме на рис. 1.6, регистр RG исходно установлен в некоторое ненулевое состояние (цепь начальной установки не показана). Под действием фронтов синхросигнала CLK хранимый в регистре код непрерывно циркулирует в нем и одновременно видоизменяется благодаря преобразованию битов логическим элементом «Исключающее ИЛИ» (XOR). Генерируемая последовательность битов снимается с выхода этого элемента или с выхода любого разряда регистра. Направление сдвига данных в регистре показано стрелкой. В полном цикле работы генератора в регистре однократно формируются все возможные M-разрядные коды за исключением нулевого. Циклы следуют один за другим без пауз.

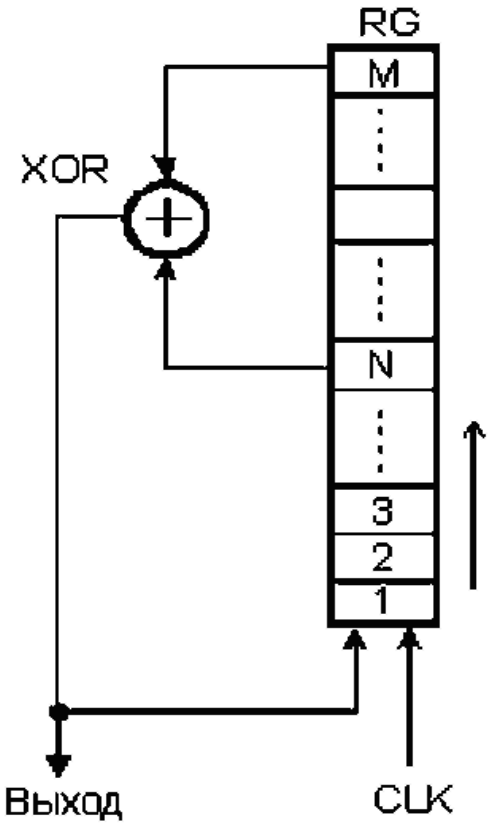


Рисунок 1.6. Генератор псевдослучайной последовательности

В общем случае при использовании M-разрядного регистра цепь обратной связи подключается к разрядам с номерами M и N (M > N). Для того чтобы на выходе генератора формировалась псевдослучайная последовательность битов с периодом повторения, равным 2^M-1, следует выбирать точки подключения цепи обратной связи в соответствии с:

M=3 4 5 6 7 9 10 11 15 17 18 20 21 22 23 25 28 29 31 33 35 36 39 …

N=2 3 3 5 6 5 7 9 14 14 11 17 19 21 18 22 25 27 28 20 33 25 35

Отметим, что не для любой разрядности регистра M возможно построение генератора с периодом 2^M-1 по такой простой схеме.

Псевдослучайная последовательность битов с периодом повторения, равным 2^M-1, обладает следующими свойствами.

• В полном цикле (2^M-1 тактов) число лог. 1, формируемых на выходе генератора, на единицу больше, чем число лог. 0. Добавочная лог. 1 появляется за счет исключения состояния, при котором в регистре присутствовал бы нулевой код. Это можно интерпретировать так, что вероятности появления логического 0 и 1 на выходе генератора практически одинаковы.

Вероятности появления логической единицы и логического нуля в каждой последующей позиции потока битов одинаковы и не зависят от предыстории. Применительно к телекоммуникационным системам скремблирование повышает надежность синхронизации устройств, подключенных к линии связи, и уменьшает уровень помех, излучаемых на соседние линии многожильного кабеля. Есть и иная область применения скремблеров — защита передаваемой информации от несанкционированного доступа.

В полном цикле (2^M-1 тактов) половина серий из последовательных лог. 1 имеет длину 1, одна четвертая серий — длину 2, одна восьмая — длину 3 и т. д. Такими же свойствами обладают и серии из лог. 0 с учетом пропущенного лог. 0. Это говорит о том, что вероятности появления «орлов» и «решек» не зависят от исходов предыдущих

«подбрасываний». Поэтому вероятность того, что серия из последовательных лог. 1 или 0 закончится при следующем подбрасывании, равна $1/_2$.

Если последовательность полного цикла (2^M-1 тактов) сравнивать с этой же последовательностью, но циклически сдвинутой на любое число тактов W (W не является нулем или числом, кратным 2^M-1), то число несовпадений будет на единицу больше, чем число совпадений.

Усовершенствованный вариант генератора (рис. 1.7) формирует псевдослучайную последовательность битов с периодом повторения, равным 2^M. К нему также применима таблица, приведенная на рис. 1, в. В регистре RG в определенном порядке формируются все возможные коды, включая нулевой. Генератор дополнительно содержит элемент «ИЛИ-НЕ», инвертор и мультиплексор MS. Сигнал Z на выходе элемента «ИЛИ-НЕ» задает направление передачи данных через мультиплексор. При Z = 0 на выход мультиплексора транслируется сигнал с выхода элемента «Исключающее ИЛИ», а при Z = 1 — сигнал с выхода инвертора.

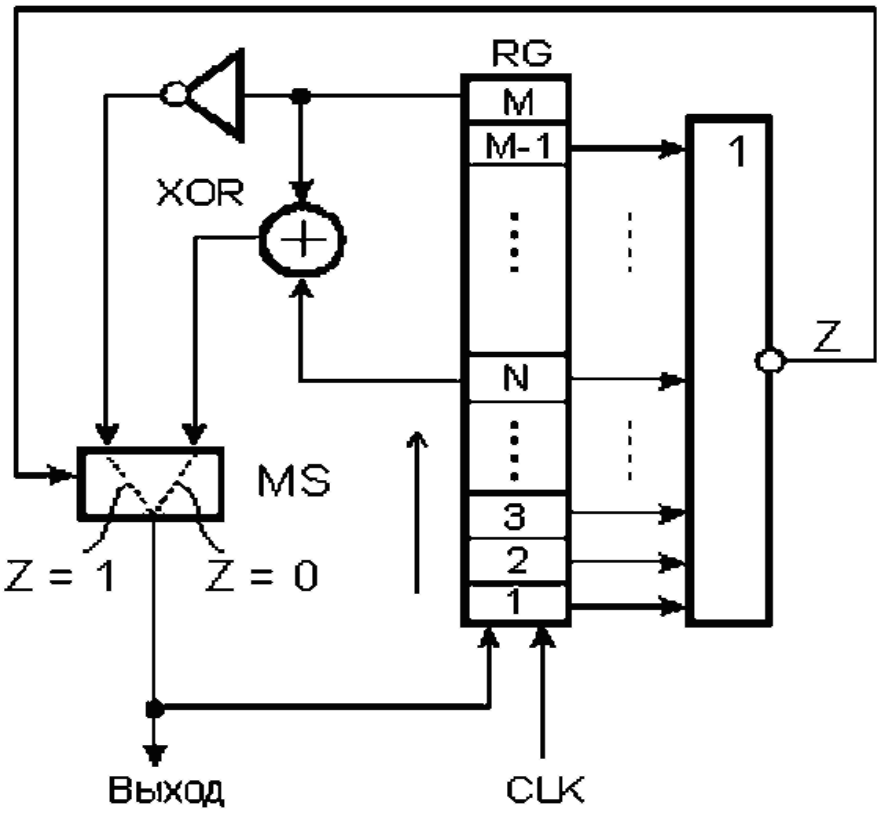


Рисунок 1.7. Усовершенствованный вариант генератора псевдослучайной последовательности

До тех пор, пока на входах элемента «ИЛИ-НЕ» присутствует хотя бы одна лог. 1, на его выходе будет сигнал Z = 0. В этом случае мультиплексор MS в каждом такте передает в освободившийся (нижний) разряд сдвигового регистра бит с выхода элемента «Исключающее ИЛИ» так же, как и в схеме, показанной на рис. 1.6.

В некотором такте i в регистре фиксируется код, содержащий единственную лог. 1, размещенную в разряде M-1. Так как в разрядах M и N присутствуют лог. 0, то на выходе элемента «Исключающее ИЛИ» сформирован сигнал лог. 0, который к началу такта i+1 поступает на вход регистра. В начале такта i+1 лог. 1 перемещается из разряда M-1 в разряд M, на входах элемента «ИЛИ-НЕ» формируется нулевой код. Сигнал Z = 1 переводит мультиплексор MS в состояние, при котором на вход нижнего разряда сдвигового регистра

поступает бит с выхода инвертора. В данном случае этот бит равен 0, поэтому в такте i+2 в регистре фиксируется нулевой код.

К началу такта i+3 на вход сдвигового регистра с выхода инвертора поступает лог. 1, поэтому по фронту синхросигнала CLK в регистре фиксируется код, содержащий лог. 0 во всех разрядах, кроме первого. Сигнал Z вновь принимает нулевое значение, мультиплексор переключается в состояние передачи сигнала с выхода элемента «Исключающее ИЛИ» и т. д. Таким образом регистр проходит через все состояния, включая нулевое. Возможны и иные варианты построения генераторов с числом состояний, равным 2^M.

Система с неизолированными генераторами.

В системе, показанной на рис. 1.8, скремблер и дескремблер содержат фрагменты рассмотренного ранее генератора (рис. 1.6) псевдослучайных последовательностей битов. В скремблере цепь обратной связи генератора на основе сдвигового регистра RG1 дополнительно содержит элемент «Исключающее ИЛИ» XOR2. В дескремблере применен аналогичный генератор на основе сдвигового регистра RG2 с разомкнутой цепью обратной связи.

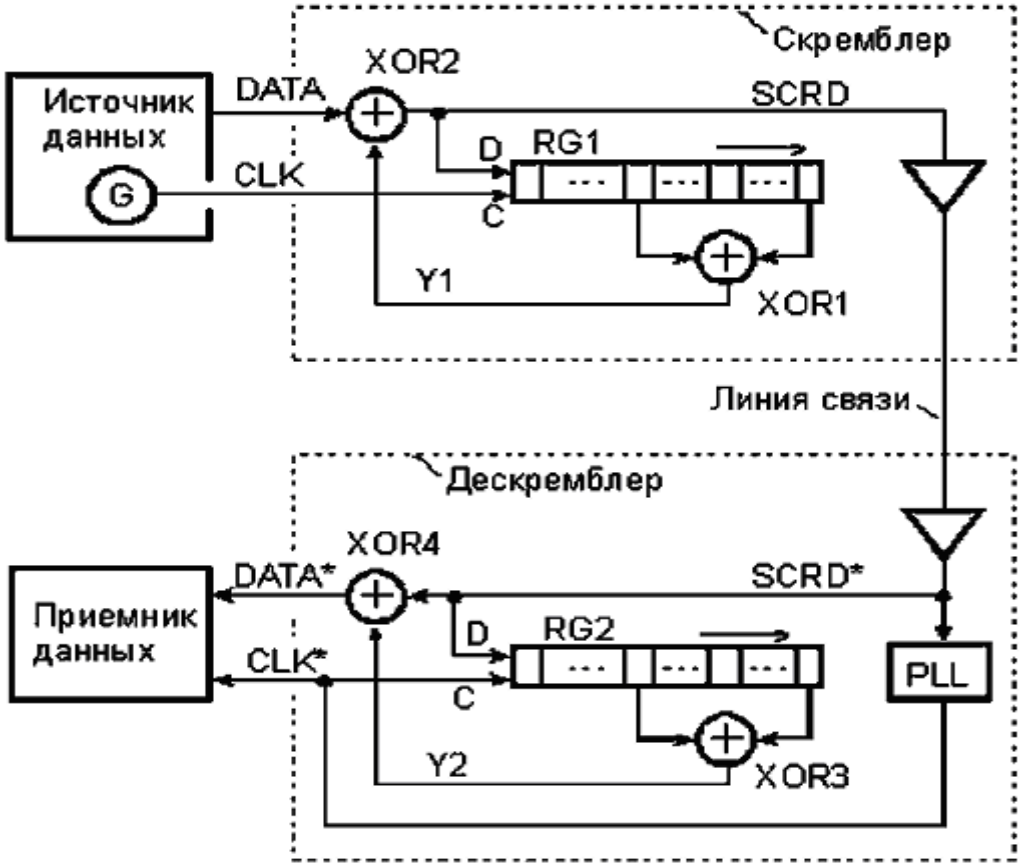


Рисунок 1.8. Скремблер и дескремблер с неизолированным генератором

На этом рисунке показана система «скремблер — дескремблер» с неизолированными генераторами псевдослучайных последовательностей битов.

Все процессы, протекающие в системе, синхронизируются от тактового генератора G, размещенного в источнике данных (возможно также его размещение в скремблере). Тактовый генератор формирует сигнал CLK — непрерывную последовательность тактовых импульсов со скважностью, равной двум. В каждом такте по фронту сигнала CLK на вход скремблера подается новый бит передаваемых данных DATA, а код в его сдвиговом регистре RG1 продвигается на один разряд вправо, причем в этот же момент в освободившийся разряд

заносится старый бит данных, просуммированный по модулю два со старым битом Y с выхода элемента XOR1.

Строго говоря, на границах между битовыми интервалами на выходе элемента XOR2 могут сформироваться короткие ложные импульсы в результате неодновременного формирования новых сигналов на его входах (сигнал Y1 приходит чуть позже сигнала DATA). Для устранения ложных импульсов можно ввести в цепь сигнала SCRD D-триггер, синхронизируемый спадом сигнала CLK (триггер на рисунке не показан). Короткими ложными импульсами пока пренебрегаем для упрощения изложения основных идей построения систем «скремблер — дескремблер».

Если источник данных посылает в скремблер длинную последовательность сигналов лог. 0 (DATA ≡ 0), то элемент XOR2 можно рассматривать как повторитель сигнала Y1. Тогда регистр RG1 фактически оказывается замкнутым в кольцо и генерирует точно такую же псевдослучайную последовательность битов, как и в рассмотренной ранее схеме генератора, приведенной на рис. 1.6. Отметим, что в этой ситуации при неблагоприятном стечении обстоятельств есть опасность потери работоспособности скремблера, если в регистре RG1 к началу передачи последовательности сигналов лог. 0 зафиксирован нулевой код (подробнее этот случай рассмотрим ниже). Если от источника данных поступает произвольная битовая последовательность, то она взаимодействует с последовательностью битов с выхода элемента XOR1. В результате формируется новая (скремблированная) последовательность битов данных SCRD, по структуре близкая к случайной. Эта последовательность, в свою очередь, продвигается по регистру RG1, формирует поток битов Y1 на выходе элемента XOR1 и т. д.

Скремблированная последовательность битов SCRD проходит через передающий усилитель и по линии связи поступает в дескремблер, где проходит через приемный усилитель. Линия связи может быть выполнена, например, в виде витой пары проводов многожильного кабеля городской телефонной сети. С помощью генератора PLL (Phase Locked Loop) с фазовой автоподстройкой частоты из входного сигнала SCRD* выделяется тактовый сигнал CLK*, который передается на синхронизирующие входы регистра RG2 и приемника данных.

Генератор PLL с фазовой автоподстройкой частоты может быть построен по одной из известных схем (например, [6]). Он предназначен для формирования высокостабильного синхросигнала CLK* на основе непрерывного слежения за входным сигналом SCRD*. В данном случае спад сигнала CLK* привязан к моментам изменения сигнала SCRD* (0 →> 1 или 1 →> 0), так что фронт сигнала CLK* формируется в середине битового интервала сигнала SCRD*, что соответствует его установившемуся значению. Сдвиг данных в регистре RG2 и прием очередного бита SCRD* в его освободившийся разряд происходят по фронту сигнала CLK*. Дескремблированные данные DATA* поступают в приемник данных и фиксируются в нем по фронтам сигнала CLK*. Благодаря достаточной инерционности генератора PLL сигнал CLK* практически нечувствителен к «дрожанию фазы» сигнала SCRD* и иным его кратковременным искажениям, вызванным помехами в линии связи.

Потоки данных DATA и DATA* совпадают с точностью до задержки передачи. Действительно, в установившемся режиме в сдвиговых регистрах RG1 и RG2 присутствуют одинаковые коды, так как на входы D этих регистров поданы одни и те же данные SCRD = SCRD* (с учетом задержки передачи), а тактовая частота одна и та же. Поэтому Y2 = Y1 и с учетом этого DATA* = SCRD* © Y2 = SCRD © Y2 = (DATA © Y1) © Y2 = DATA © Y1 © Y1 = DATA © 0 = DATA.

Рассмотренный способ скремблирования-дескремблирования данных не требует применения какой-либо специальной процедуры начальной кодовой синхронизации, после которой коды в обоих регистрах становятся одинаковыми и, следовательно, начинает выполняться условие Y2 = Y1. Синхронизация достигается автоматически после заполнения регистров одинаковыми данными. Это, пожалуй, единственное преимущество данного варианта перед классическим устройством с изолированными генераторами (рис. 3).

К сожалению, есть и существенные недостатки. О первом из них уже вскользь упоминалось — это плохая устойчивость по отношению к некоторым неблагоприятным кодовым ситуациям, которые могут возникнуть как при нормальной работе системы, так и в результате злого умысла. Этот недостаток и меры его устранения будут подробно рассмотрены далее.

Второй недостаток состоит в размножении ошибок. При появлении одиночной ошибки в линии связи идентичность содержимого регистров RG1 и RG2 временно нарушается, но затем автоматически восстанавливается, как только правильные данные вновь заполнят регистр RG2. Однако в процессе продвижения ошибочного бита по сдвиговому регистру RG2, а именно в периоды его попадания сначала на один, а затем на другой вход элемента XOR3 сигнал Y2 дважды принимает неправильное значение. Это приводит к размножению одиночной ошибки — она впервые появляется в сигнале DATA* в момент поступления из линии и затем возникает еще два раза при последующем искажении сигнала Y2.

Система с изолированными генераторами

В системе, показанной на рис. 1.9, применены изолированные от линии связи генераторы псевдослучайных битовых последовательностей. Преимущества этой системы перед предыдущей заключаются в том, что ошибки, поступающие из линии, не размножаются, и как будет показано ниже, такая система более устойчива по отношению к неблагоприятным последовательностям битов, которые формируются в силу случайных стечений обстоятельств, либо в результате преднамеренных действий пользователя.

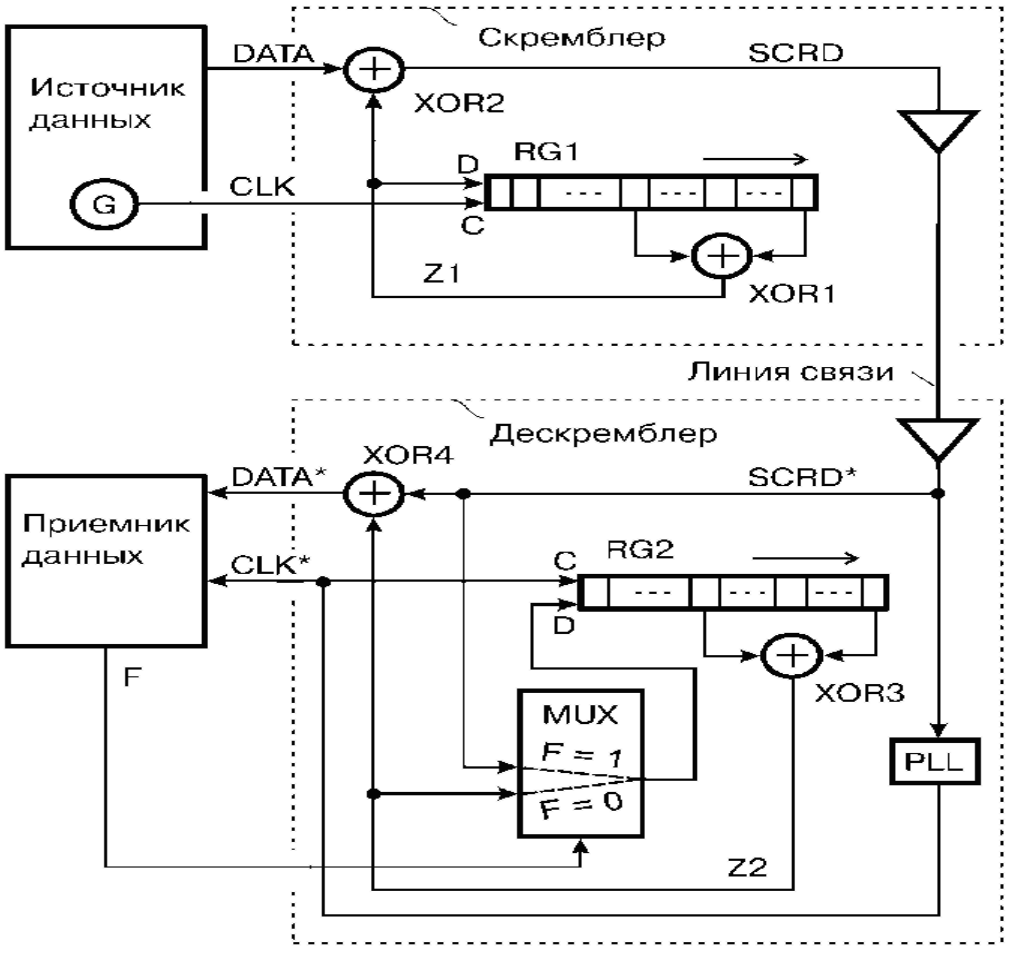


Рисунок 1.9. Скремблер и дескремблер с изолированным генератором

Недостаток этой системы — сложность установления кодовой синхронизации. Отметим, что в конце статьи предложено решение, лишенное этого недостатка — оно предусматривает автоматическое установление и поддержание синхронной работы изолированных генераторов псевдослучайных битовых последовательностей.

Начальная кодовая синхронизация системы с изолированными генераторами псевдослучайных последовательностей битов (рис.1.9) осуществляется с использованием аппаратных средств дескремблера и программных средств источника и приемника данных. К аппаратным средствам относятся мультиплексор MUX и программно-управляемый выход приемника данных, на котором формируется управляющий сигнал F. При нормальной работе системы приемник данных постоянно поддерживает на выходе сигнал F = 0. На выход мультиплексора транслируется сигнал Z2 с выхода элемента «Исключающее ИЛИ» XOR3. Генератор псевдослучайной битовой последовательности на основе регистра RG2 изолирован от внешних воздействий со стороны линии связи.

Предположим, что в исходном состоянии дескремблер не синхронизирован со скремблером. Такая ситуация может возникнуть, например, после включения напряжения питания аппаратуры приемной стороны, после ошибки в работе генератора PLL дескремблера из-за воздействия помех на линию связи или по иным причинам. При отсутствии кодовой синхронизации между скремблером и дескремблером содержимое регистров RG1 и RG не совпадает, поток принимаемых данных DATA* ошибочен и не совпадает с потоком передаваемых данных DATA.

При обнаружении устойчивого «хаоса» в данных DATA* (когда в потоке нет обусловленного протоколом обмена разделения на информационные кадры и т. п.) приемник формирует сигнал F = 1. Вследствие этого мультиплексор начинает транслировать на вход D регистра RG2 сигнал скремблированных данных SCRD*, как в ранее рассмотренной системе.

Протокол обмена предусматривает пересылку данных в виде последовательности кадров. Группы обычных кадров перемежаются со служебными кадрами. Например, после группы из 1000 обычных кадров следует один служебный. Он, в частности, содержит синхронизирующую последовательность из некоторого числа (например, 256) нулевых битов. При выдаче этих битов (DATA = 0) в скремблер элемент XOR2 выполняет функцию повторителя сигнала Z1 с выхода элемента XOR1. Поэтому в данном случае скремблированный сигнал SCRD представляет собой фрагмент «истинной» псевдослучайной битовой последовательности в том смысле, что она не смешана с потоком произвольных данных DATA и порождается только генератором скремблера.

Эта последовательность загружается в регистр RG2 и проходит через него, так как F = 1. После того как содержимое регистров RG1 и RG2 оказывается одинаковым, сигнал Z2 начинает повторять сигнал Z1. Кодовая синхронизация достигнута. На вход приемника данных подается непрерывная последовательность лог. 0, так как DATA* = = DATA ≡ 0. После уверенного обнаружения достаточно длинной (например, содержащей 220 бит) последовательности лог. 0 приемник данных формирует сигнал F = 0 и тем самым возвращает генератор псевдослучайной последовательности битов дескремблера в режим изолированной работы. Теперь кодовая синхронизация не только достигнута, но и «сохранена» благодаря логической изоляции регистра RG2 от линии связи. После окончания передачи служебного (синхронизирующего) кадра источник данных приступает к передаче группы из 1000 обычных кадров согласно принятому в системе протоколу обмена.

Таким образом, в рассмотренной системе для поддержания синхронной работы сдвиговых регистров скремблера и дескремблера (в случае нарушения синхронизации или при первоначальном включении приемной части системы) необходимо периодически прерывать передачу полезных данных и передавать по линии связи служебные информационные кадры, содержащие достаточно длинные цепочки синхронизирующих битов (DATA ≡ 0). В результате уменьшается эффективная скорость передачи данных по линии, усложняется протокол обмена. Кроме того, с увеличением интервалов между служебными кадрами (что способствует более эффективной передаче пользовательских данных)

увеличивается время ожидания этих кадров дескремблером в случае потери кодовой синхронизации. В течение времени ожидания передача полезных данных невозможна.

Повышение устойчивости синхронизации.

Следует рассмотреть вопросы улучшения синхронизации и устойчивости скремблеров по отношению к нежелательным последовательностям битов.При передаче данных по линии связи применяют различные способы кодирования. В частности, широкое распространенное получило NRZ-KO-дирование и его модификации. Для передачи нулевых и единичных битов выделяются одинаковые интервалы времени — «битовые интервалы». В каждом битовом интервале в зависимости от значения передаваемого бита (лог. 1 или 0) между проводами витой пары (двухпроводной линии) присутствует положительное или отрицательное напряжение. Применительно к оптоволоконным линиям в каждом битовом интервале по оптическому волокну передается или не передается световой поток. Такое кодирование неприменимо в случаях, когда по линии могут передаваться очень длинные цепочки из одинаковых битов. Тогда состояние линии будет оставаться неизменным на протяжении длительного интервала времени, и синхронизация приемника с передатчиком может нарушиться. Действительно, приемник надежно восстанавливает синхросигнал только тогда, когда паузы между изменениями сигнала в линии не слишком велики. Изменение сигнала в линии после незначительной паузы позволяет всякий раз корректировать «ход часов» приемника. С увеличением паузы надежность «службы времени» падает. Например, после передачи серии из 10000 нулей приемник, вероятнее всего, не сможет с уверенностью определить, находится ли последующая единица на позиции 9999, 10000 или 10001. То же относится и к передаче длинных цепочек лог. 1. Другими словами, при передаче достаточно большой последовательности нулей или единиц приемник теряет синхронизацию с передатчиком.

На практике данные группируют в кадры постоянной или переменной длины. Каждый кадр содержит некоторую служебную информацию, например, флаговый код начала кадра, причем эта информация заведомо не является последовательностью одинаковых битов. Это облегчает поддержание синхронизации, так как возможная однородность пользовательских данных периодически нарушается заведомо неоднородными служебными данными. Тем не менее, для повышения надежности синхронизации желательно исключить из потока пользовательских данных длинные последовательности нулевых или единичных битов. Это и делается с помощью скремблирования — це-почки нулевых или единичных битов (и не только они) преобразуются в псевдослучайные битовые последовательности, в которых вероятность изменения уровня сигнала в каждом последующем битовом интервале (по отношению к текущему уровню) равна $^{1}/_{2}$

В подтверждение сказанного об устойчивости синхронизации рассмотрим цепь выделения синхросигнала и данных из сигнала в линии.

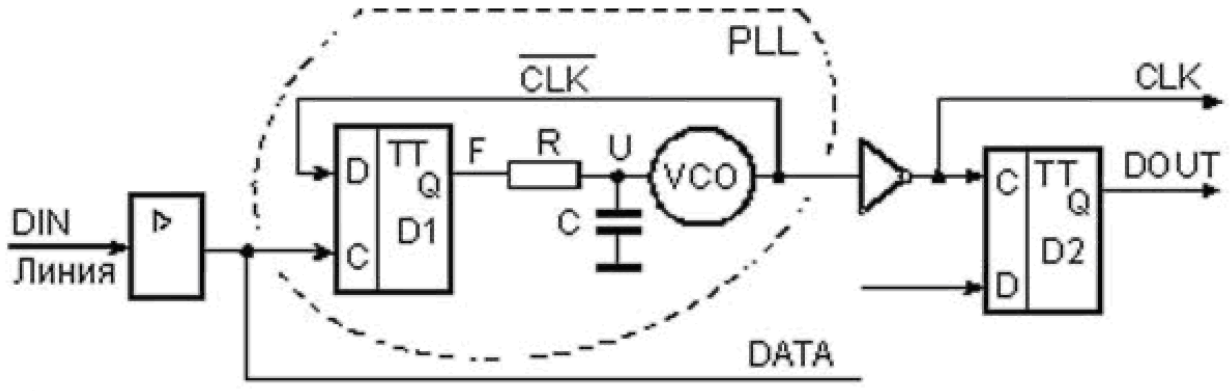


Рисунок 1.10. Цепь выделения синхросигнала

Узел содержит входной усилитель, генератор PLL с фазовой автоподстройкой частоты, инвертор и триггер D2. Генератор PLL включает в себя триггер D1, фильтр низких частот (RC-цепь) и генератор VCO (Voltage Controlled Oscillator), управляемый напряжением U. Триггеры D1 и D2 принимают данные с входов D по фронту сигнала на входе C. Генератор VCO формирует выходной синхросигнал CL. Частота этого сигнала в незначительных пределах может изменяться в зависимости от напряжения U на его управляющем входе. С повышением этого напряжения частота уменьшается, и наоборот.

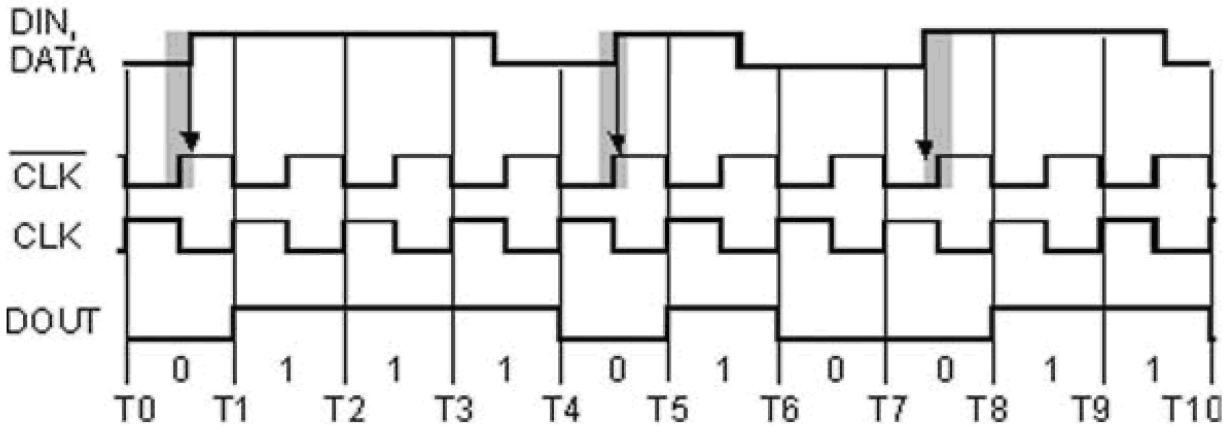


Рисунок 1.11. Формирование синхросигнала

Данные DATA представлены кодом NRZ. Границы битовых интервалов примерно соответствуют моментам формирования спадов сигнала CLK, а середины этих интервалов — моментам T0—T10.

Обратите внимание на нестандартный режим работы триггера D1. Обычно на вход C синхронизации D-триггера подается синхроимпульс, а на вход D — данные. При этом согласно техническим условиям на триггер к моменту формирования фронта синхроимпульса сигнал на входе D данных должен принять установившееся значение в течение некоторого «времени предустановки» и сохранять это значение в течение «времени удержания», которое отсчитывается от того же фронта. Здесь же реализован некий противоположный режим. В качестве данных на D-вход триггера поступает синхросигнал, а в качестве синхросигнала данные. При этом в идеальном случае фронт сигнала на входе C должен совпадать с фронтом сигнала на входе D.

Как показано на рис. 1.11 затемненными прямоугольниками, существуют области неопределенности моментов формирования фронтов сигнала данных. Неопределенность обусловлена так называемым джиттером (дрожанием фронтов). Джиттеру в равной мере подвержены и спады входного сигнала, но они нас в данном случае не интересуют.

Предположим, что генератор VCO уже вошел в синхронизацию с сигналом, поступающим из линии. В этом случае фронты сигнала DATA с равной вероятностью совмещены во времени с нулевыми или единичными уровнями инвертированного сигнала CLK. На рисунке вертикальные стрелки показывают, что два фронта сигнала DATA совмещены с единичным уровнем инвертированного сигнала CLK, а третий — с нулевым уровнем. При равновероятном приеме в триггер D1 лог. 0 и 1 сигнал F на его выходе постоянно изменяется, но в среднем пребывает в состоянии лог. 0 столько же времени, сколько и в состоянии лог. 1. При этом напряжение U на выходе интегрирующей RC-цепи примерно равно половине напряжения, соответствующего уровню лог. 1 на выходе триггера D1.

Предположим теперь, что вертикальные стрелки в большинстве своем указывают на нулевые состояния синхросигнала с выхода генератора VCO. Это означает, что следует

слегка увеличить частоту синхросигнала, что приведет к его незначительному фазовому опережению, т. е. к некоторому «сжатию влево» его временной диаграммы. Это и произойдет благодаря тому, что в данной ситуации сигнал управления F будет преимущественно нулевым, напряжение U снизится, частота сигнала CLK незначительно увеличится.

В противоположной ситуации временная диаграмма синхросигнала исходно чуть смещена влево относительно показанной на рисунке. Тогда стрелки должны преимущественно попадать на единичные состояния синхросигнала. Это означает, что синхросигнал вырабатывается с опережением, и его следует задержать. Средством задержки служит незначительное снижение частоты. Оно достигается благодаря тому, что в данной ситуации управляющий сигнал F преимущественно равен единице, напряжение U повышается, частота незначительно снижается.

В результате малых постоянных колебаний около равновесного состояния осуществляется статистически наиболее правильная привязка синхросигнала CLK к сигналу DATA. Такая привязка обеспечивает стабильность данных на входе D триггера D2 в момент прохождения фронта сигнала CLK. Таким образом, на выходе схемы формируется синхросигнал и данные, выделенные из входного сигнала DIN.

Если сигнал DIN в течение длительного времени остается неизменным, то управление генератором VCO теряется, так как постоянно действующий на него через интегрирующую цепь нулевой или единичный сигнал F вызывает неуклонное повышение или снижение частоты синхросигнала. Скремблирование передаваемого по линии сигнала предотвращает его длительную фиксацию, т. е. повышает надежность синхронизации.

3. Порядок выполнения работы

Описание лабораторной установки

Лабораторная установка позволяет осуществить физический анализ сигналов, лабораторная установка включает в себя аппаратную и программную часть, аппаратная часть состоит из (отладочная плата DSP и персонального компьютера соединенного с ней по шине USB) программная часть включает в себя (программный код, среда проектирования visual dsp). Структурная схема приведена на рисунке 1.12.

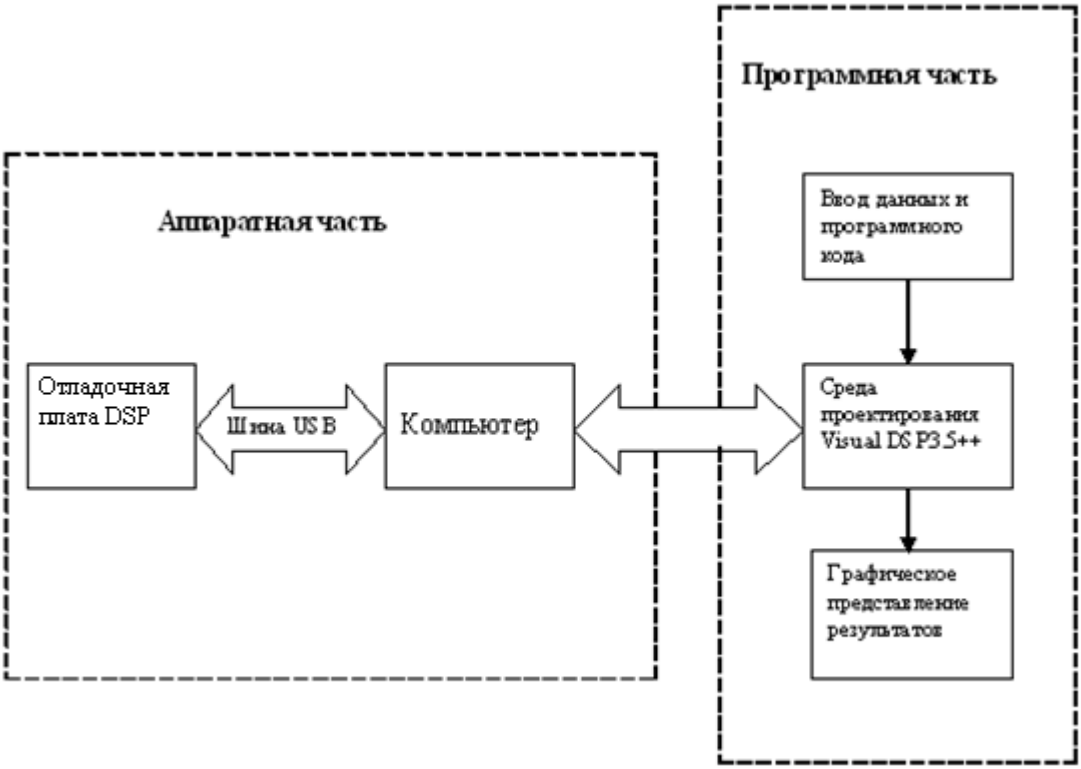


Рисунок 1.12. Структурная схема лабораторного макета

Порядок выполнения лабораторной работы

1. Уяснить функциональное назначение отдельных узлов макета, и принципы шифрования данных
2. Собрать лабораторную установку для исследования методов Цифровой обработки сигналов
3. Включить лабораторную установку.
4. Выполнить исследование открытых сигналов, псевдослучайной последовательности, шифр сигналов, формируемых в лабораторной установки.

Примечание. Предполагается изменять по указанию преподавателя параметры:

Скорость ввода информационной последовательности

Начальное состояние регистров (ключ шифрования)

Длину сдвигового регистра и расположение отводов.

Изображения получаемых сигналов при изменении указанных параметров рекомендуется помещать на графиках один под другим при неизменном масштабе по оси времени.

Исследование проводить в следующем порядке:

1. Запустить VisualDSP++ Environment (на рисунке представлен интерфейс программы).
2. В закладке Project выбрать New.
3. Нажать CTRL+N и написать исходный текст.
4. Сохранить с расширением asm.
5. Подключить этот файл в проект, Project->Add to Project->File.
6. Для создания файла архитектуры процессора необходимо выполнить 2-4 пункты, но сохранить с расширением ldf.
7. Для использования готового файла архитектуры процессора необходимо выполнить пункт 5 и найти его.
8. Для подключения файлов с расширением dat (например, содержащих коэффициенты

фильтра), необходимо нажать закладки Project->Add to Project->New Folder.

9. Подключить в папку файлов данных необходимые файлы, однократным нажатием левой кнопкой мышки на созданной папке, и щелчком правой кнопкой мышки выбрать Add File(s) to folder.
10. Отредактировать текст исходной программы и откомпилировать нажатием клавиши F7.
11. При появлении ошибок в Output window, посмотреть номера строки, отредактировать и снова выполнить пункт 10.
12. Пошагово отлаживать клавишей F11
13. Исследовать характеристики входного сигнала;
14. Исследовать псевдослучайной последовательности при изменении начального состояния регистров, Длину сдвигового регистра и расположение отводов
15. Исследовать характеристики шифр сигнала, для различных параметров измененных в п2.
16. Определить криптостойкость шифр последовательности для 3 значений длинны сдвигового регистра.
17. Сделать необходимые выводы по каждому из пунктов исследования.

4. Рекомендуемая литература

1. General DSP Training and Workshops: http://www.analog.com/industry/dsp/training
2. DSP Designer's Reference (DSP Solutions) CD-ROM, Analog Devices, 1999.
4. Марпл-мл. С. Л. Цифровой спектральный анализ и его приложения. - М.: Мир, 1990, - 234с.
5. Гольденберг Л.М., Матюшкин Б.Д., Поляк М.Н.. Цифровая обработка сигналов. - М: Радио и связь, 1985, - 340 с.
6. Эммануил С. Айфичер, Барри У. Джервис. Цифровая обработка сигналов: практический подход, 2-е издание.- М.: Изд-во Вильямс, 2004. – 992 с.

Компьютерный практикум 2. Исследование аппаратных средств шифрования информации в сетях и системах радиосвязи

1. Цель работы

Объектом исследования является аппаратный шифратор для реализации стандарта криптографической защиты AES. Создан аппаратный комплекс для обеспечения безопасной передачи данных и исследования стандарта криптографической защиты. Комплекс представляет собой аппаратный продукт для IBM-PC совместимых ПК, реализующий алгоритм шифрования Rijndael. В качестве аппаратной составляющей используется плата фирмы Analog Devices – EzKit Lite.

2. Краткие теоретические сведения

В современном конкурентном мире наблюдается тенденция постоянного увеличения стоимости важной коммерческой информации и, соответственно, возникает необходимость шифрования информации для сокрытия ее от несанкционированного пользования. В дипломном проекте разрабатывается аппаратный шифратор для шифрования файлов и обеспечения информационной защиты. В связи с тем, что существует угроза доступа к конфиденциальным данным со стороны злоумышленников, конкурентов, следует осознать, что шифрование файлов и текстов – это гарантия целостности и конфиденциальности всех сведений, отчетов и данных.

С повышением ценности и значимости информации растет и важность ее защиты, поэтому разработка аппаратного шифратора для обеспечения беспрецедентного уровня шифрования информации является очень актуальной задачей на сегодняшний день.

Аппаратные шифраторы позволяют обеспечивать высочайший уровень шифрования информации для предотвращения утечки и утраты информации и, соответственно, минимизации материального и морального ущерба. Также информация – это одна из важных составляющих процесса управления, а несанкционированное вмешательство в этот процесс может привести к катастрофическим последствиям.

Вне зависимости от того, хотите ли Вы обезопасить сведения от доступа злоумышленников, собственных сотрудников, родственников или конкурентов аппаратный AES-шифратор, как криптографический средство нового поколения, обеспечит надежное шифрование информации и гарантию полной информационной безопасности.

Стандарт криптографической защиты AES (Advanced Encryption Standard – Усовершенствованный стандарт шифрования) является на сегодняшний день наиболее надежным с точки зрения длины ключа и, как следствие, наиболее востребованным.

Если взглянуть на любую деятельность человека, где есть место для коммерческой информации, мы можем встретить стандарт криптографической защиты AES. Будь то телекоммуникация, где нормой стало использование модулей шифрования, или передача данных через электронную почту и т.д.

Шифрование

С развитием информационных технологий все большую актуальность приобретает проблема защиты информации — предотвращение ее утечки, несанкционированных и непреднамеренных воздействий на нее. Одна из важнейших областей этой деятельности – криптография, которая призвана обеспечить аутентичность и конфиденциальность передаваемых сообщений. Для решения первой задачи используется технология электронной

цифровой подписи как компьютерного аналога подписи ответственного лица и печати организации, для решения второй – шифрование.

Под шифром в криптографии понимается совокупность обратимых преобразований множества возможных открытых данных во множество возможных зашифрованных данных, расшифровать и понять которые нелегальный пользователь (злоумышленник) не в силах. Эти преобразования осуществляются по определенному алгоритму с применением ключа — конкретного секретного состояния некоторых параметров криптоалгоритма, обеспечивающего выбор одного преобразования из всей совокупности вариантов, возможных для данного алгоритма. Стойкие криптоалгоритмы (к числу которых, например, относится отечественный ГОСТ 28147_89 или американский AES) способны обеспечить конфиденциальность сообщений даже при условии, что злоумышленнику известны открытые и зашифрованные тексты и сами правила преобразования. Иными словами, в открытых криптосистемах необходимо сохранять в тайне только ключи.

При этом полностью исключены ситуации, когда, скажем, кража шифратора или публикация текста алгоритма даст злоумышленнику возможность раскрыть зашифрованные данные.

Схема криптографической системы, обеспечивающей шифрование передаваемой информации, представлена на рис.2.1.

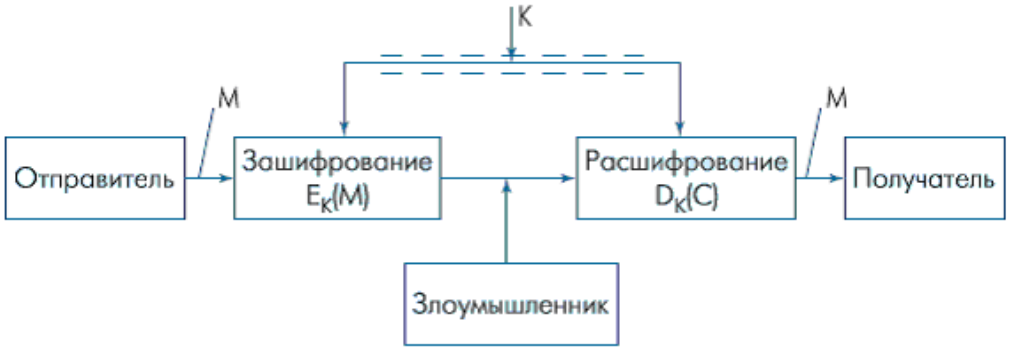


Рисунок 2.1. Схема криптографической системы

Отправитель генерирует открытый текст исходного сообщения M, которое должно быть передано законному получателю по незащищенному каналу. Для того чтобы злоумышленник не смог узнать содержание сообщения M, отправитель зашифровывает его по ключу K с помощью обратимого преобразования E_K и создает шифртекст (или криптограмму) C = E_K (M), который отправляет получателю. Законный получатель, приняв шифртекст C, расшифровывает его с помощью обратного преобразования $D_K(C) = E_K^{-1}$(C) = и получает исходное сообщение в виде открытого текста M: $D_K(C) = E_K^{-1}[E_K(M)] = M$. Данная система шифрования называется симметричной, поскольку зашифрование и расшифрование производятся с помощью одного и того же ключа K. При этом необходимо обеспечение конфиденциальности этого ключа (симметричные системы именуются также одноключевыми или системами с секретным ключом).

Как раз для реализации целей шифрования существуют устройства называемые шифраторами.

Классификация методов шифрования информации

Основные объекты изучения классической криптографии показаны на рисунок 1.2, где A и B - законные пользователи, W - противник или криптоаналитик. Учитывая, что схема на рисунке 1.2а фактически является частным случаем схемы на рисунке 1.2б при B = A, в дальнейшем будет рассматриваться только она.

Процедуры зашифрования (encryption) и расшифрования (decryption) можно представить в следующем виде:

$c = E_k(p)$,
$p = D_k(c)$,

где

p и **c** - открытый (**plaintext**) и зашифрованный (**ciphertext**) тексты;

k_e и **k_d** - соответственно ключи зашифрования и расшифровиииия;

E_k и **D_k**- функции зашифрования с ключом $к_e$ и расшифрования с ключом k_d соответственно, причем для любого открытого текста p справедливо $D_k(E_k(p))=p$.

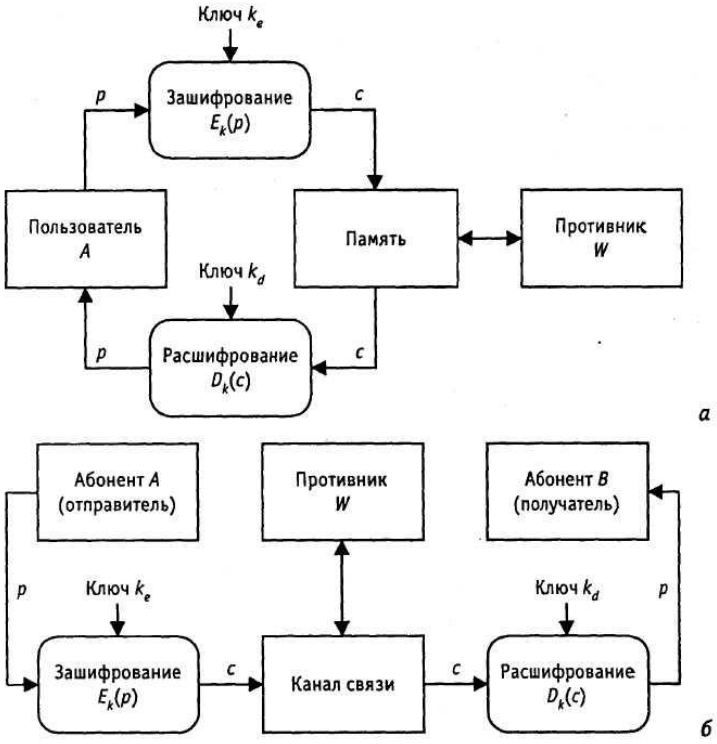


Рисунок 2.2. Криптозащита: а - при хранении информации; б - при передаче информации по каналу связи

На рисунке приведена классификация методов шифрования информации. Различают два типа алгоритмов шифрования: симметричные (с секретным ключом) и асимметричные (с открытым ключом). В первом случае обычно ключ расшифрования совпадает с ключом зашифрования, т. е.

$k_e = k_d = k$,

либо знание ключа зашифрования позволяет легко вычислить ключ расшифрования. В асимметричных алгоритмах такая возможность отсутствует: для зашифрования и расшифрования используются разные ключи, причем знание одного из них не дает практической возможности определить другой.

Рисунок 2.3. Классификация методов шифрования информации

В процессе шифрования информация делится на порции величиной от одного до сотен бит. Как правило, поточные шифры оперируют с битами открытого и закрытого текстов, а блочные - с блоками фиксированной длины. Но главное отличие между этими двумя методами заключается в том, что в блочных шифрах для шифрования всех порций используется один и тот же ключ, а в поточных - для каждой порции используется свой ключ той же размерности. Иначе говоря, в поточных шифрах имеет место зависимость результата шифрования порции информации от ее позиции в тексте, а в некоторых случаях и от результатов шифрования предыдущих порций текста. Таким образом, при реализации поточной криптосистемы возникает необходимость в элементах памяти, изменяя состояние которых, можно вырабатывать последовательность (поток) ключевой информации. Блочную же криптосистему можно рассматривать как зависящую от ключа подстановку на множестве значений блоков открытого текста.

Достоинством поточных шифров является высокая скорость шифрования, которая и определяет область их использования шифрование данных, требующих оперативной доставки потребителю, например, аудио- и видеоинформации. Учитывая, что при применении классических блочных шифров одинаковым блокам открытого текста соответствуют одинаковые блоки шифротекста, что является серьезным недостатком, на практике получили наибольшее распространение комбинированные методы шифрования, использующие один из следующих принципов:

- "сцепление" блоков;
- формирование потока ключей (гаммы шифра) с помощью так называемых генераторов псевдослучайных кодов (ГПК), в качестве функции обратной связи которых используется функция зашифрования блочного шифра.

Блочные составные шифры

В общем случае детерминированный шифр G определяется следующим образом

G = (P,C,K,F),

где

P - множество входных значений,

C - множество выходных значений,

К - пространство ключей,

F - функция зашифрования

$$\mathbf{F: P \times K \rightarrow C}$$

Пусть составной шифр определяется семейством преобразований $\mathbf{G_i}$, имеющими общие пространства входных и выходных значений, т. е. $\mathbf{P_i = C_i - = M}$, при этом результат действия функции $\mathbf{F_i}$ зависит от ключевого элемента $\mathbf{k_i \in K_i}$. На основе этого семейства с помощью операции композиции можно построить шифр, задаваемый отображением

$$\mathbf{F: M \times (K_1 \times K_2 \times ... \times K_r) \rightarrow M_r,}$$

причем

$$\mathbf{F = F_r \cdot ... F_2 \cdot F_1,}$$

а ключом является вектор

$$\mathbf{(k_1, k_2, ..., k_r) \in K_1 \times K_2 \times \ldots \times K_r}$$

Преобразование $\mathbf{F_i}$ называется **i-м** раундом шифрования, ключ $\mathbf{k_i}$ - раундовым ключом. В некоторых случаях раундовые ключи получаются из ключа всей системы с помощью алгоритма выработки раундовых ключей (при этом размер ключа системы существенно меньше суммарного размера всех раундовых ключей). Если ключевые пространства $\mathbf{K_i}$ и преобразования $\mathbf{F_i}$ для всех раундов совпадают, такой составной шифр называется **итерационным**, представляющим собой композицию одной и той же криптографической функции, используемой с разными ключами.

Идея, лежащая в основе составных (или композиционных) блочных шифров, состоит в построении криптостойкой системы путем многократного применения относительно простых криптографических преобразований, в качестве которых К.Шеннон предложил использовать преобразования подстановки (substitution) и перестановки (permutation), схемы, реализующие эти преобразования, называются SP-сетями.

Многократное использование преобразований подстановки и перестановки (рис.1.4) позволяет обеспечить два свойства, которые должны быть присущи стойким шифрам:

рассеивание (diffusion) и

перемешивание (confusion) (рисунок).

Рассеивание предполагает распространение влияния одного знака открытого текста, а также одного знака ключа на значительное количество знаков шифротекста. Наличие у шифра этого свойства позволяет:

скрыть статистическую зависимость между знаками открытого текста, иначе говоря, перераспределить избыточность исходного языка посредством распространения ее на весь текст;

не позволяет восстанавливать неизвестный ключ по частям.

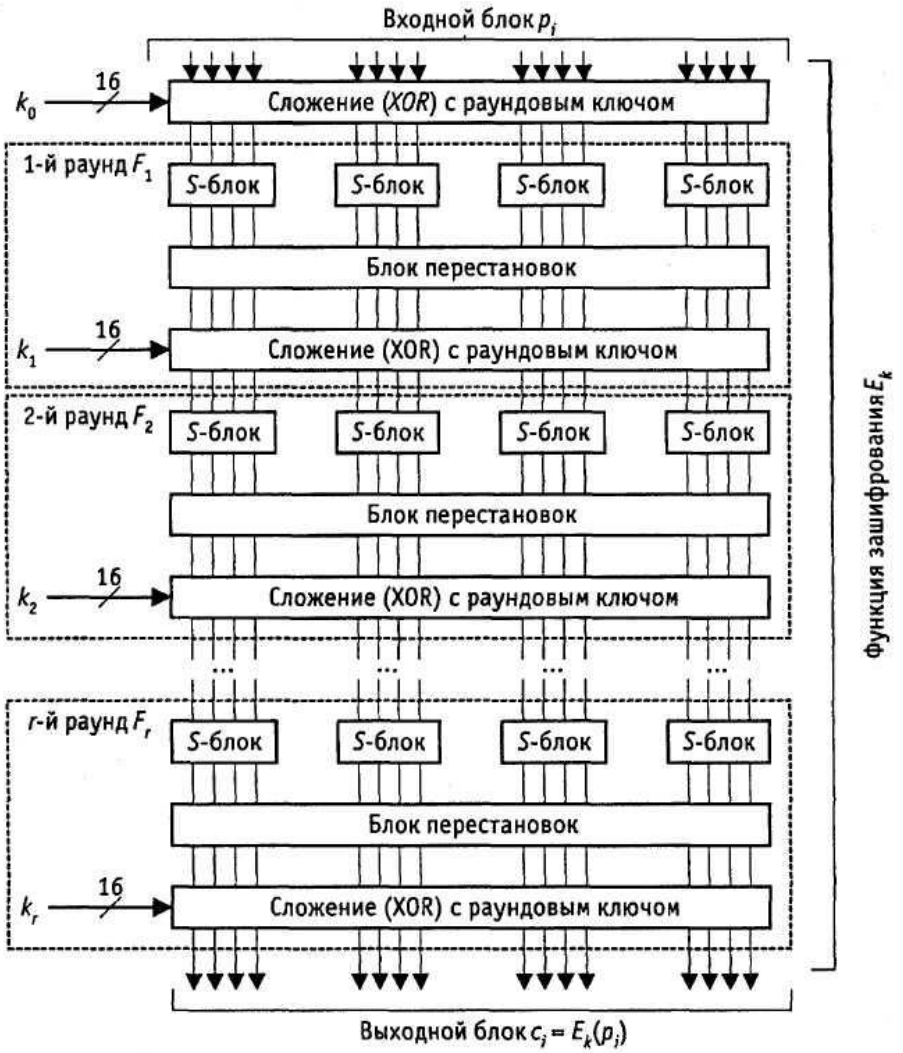


Рисунок 2.4. Схема простейшего итерационного шифра

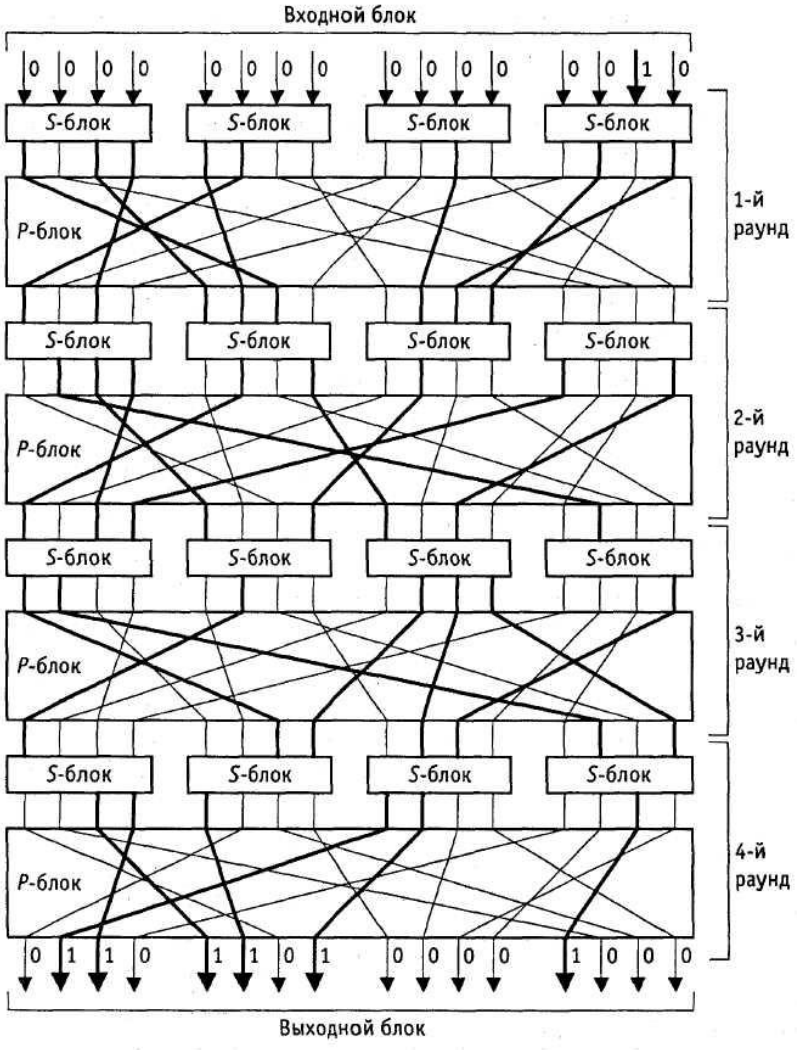


Рисунок 2.5. Рассеивание и перемешивание в SP-сети

Цель перемешивания - сделать как можно более сложной зависимость между ключом и шифротекстом. Криптоаналитик на основе статистического анализа перемешанного текста не должен получить сколь–нибудь значительного количества информации об использованном ключе.

Применение рассеивания и перемешивания порознь не обеспечивает необходимую стойкость, надежная криптосистема получается только в результате их совместного использования.

В современных блочных криптосистемах раундовые шифры строятся в основном с использованием операций замены двоичных кодов небольшой разрядности (схемы, реализующие эту нелинейную операцию, называются S-блоками; как правило, именно от их свойств в первую очередь зависит стойкость всей системы), перестановки элементов двоичных кодов, арифметических и логических операций над двоичными кодами. Каждый раундовый шифр может являться преобразованием, слабым с криптографической точки зрения. Единственное ограничение при построении составного шифра заключается в запрете на использование в двух соседних раундах шифрования преобразований, имеющих общую прозрачность.

Пусть F: x —> y, x, y ∈ M, и на множестве M определены преобразования g и h. Если F(g(x)) = h(y), F прозрачно для g, а g прозрачно для F.

Примерами прозрачных операций могут являться операции циклического сдвига, замены и т. п. Если два преобразования, выбранные в качестве соседних раундов, имеют общую прозрачность g, и при этом существует простое преобразование, не прозрачное для g,

это преобразование следует поместить между двумя раундами шифрования, и полученная композиция уже не будет прозрачной для g. Такие преобразования, чаще всего не зависящие от ключа, называются буферами. Помимо внутренних иногда применяют и внешние буфера, выполняющие преобразования, зависящие или не зависящие от ключа.

Важным достоинством многих составных шифров является их симметричность относительно операций зашифрования и расшифрования, которые по этой причине могут быть реализованы на одном устройстве. Переход от одного режима к другому обеспечивается заменой последовательности раундовых ключей на обратную.

Составные шифры, использующие в качестве раундовых криптографически слабые преобразования, становятся нестойкими, если становятся известными какие-либо промежуточные результаты преобразований. По этой причине использование этой информации при криптоанализе составных шифров является некорректным.

Необходимые и достаточные условия абсолютной стойкости шифра:

- полная случайность ключа;
- равенство длин ключа и открытого текста;
- однократное использование ключа.Классификация шифраторов

Возможная классификация современных коммерческих шифраторов приведена на рис. 2.6.

Рисунок 2.6. Классификация шифраторов

Алгоритмы защиты информации, в частности, алгоритмы шифрования, могут быть реализованы как программным, так и аппаратным способом. Оба варианта имеют ярко выраженные достоинства и недостатки. Основной недостаток устройств шифрования, реализующих аппаратное шифрование информации, - это их относительно высокая стоимость. К достоинствам же относится:

аппаратная реализация алгоритма криптографического преобразования, что гарантирует целостность алгоритма;

шифрование и ключи шифрования хранятся в самой плате, а не в оперативной памяти компьютера;

аппаратный датчик случайных чисел создает действительно случайные числа для формирования надежных ключей шифрования и электронной цифровой подписи;

загрузка ключей шифрования в устройство производится напрямую, минуя ОЗУ и системную шину компьютера, что исключает возможность перехвата ключей;

хранение ключей шифрования не в ОЗУ компьютера (как в случае с программной реализацией), а в памяти шифропроцессора;

на базе аппаратных шифраторов можно создавать системы защиты информации от

несанкционированного доступа и разграничения доступа к компьютеру;

применение специализированного шифропроцессора для выполнения криптографических преобразований разгружает центральный процессор компьютера; возможна также установка на одном компьютере нескольких устройств, что еще более повысит скорость шифрования;

использование парафазных шин в архитектуре шифропроцессора исключает угрозу снятия ключевой информации по возникающим в ходе криптографических преобразований колебаниям электромагнитного излучения в цепях «земля—питание» микросхемы.

обеспечение наряду со всеми перечисленными достоинствами сопоставимой с программными продуктами скорости шифрования.

Что же мешает широкому применению аппаратных шифраторов — или, выражаясь точнее, обусловливает их меньшую распространенность по сравнению с криптографическим ПО?

Прежде всего цена — в любом случае стоимость аппаратного шифратора будет выше, чем чисто программного решения. Но для организаций, всерьез заботящихся об информационной безопасности, использование аппаратных шифраторов в силу перечисленных выше причин безусловно желательно — во всяком случае, для защиты наиболее важных ресурсов. Производители аппаратных криптографических средств постоянно дополняют свои продукты новыми возможностями, и по соотношению цена/качество (если понимать под последним прежде всего функциональность) аппаратные шифраторы выглядят более предпочтительно, если их сравнивать с соответствующим ПО.

Зачастую у пользователей отсутствует полное понимание всех нюансов, связанных с правовым регулированием практики применения криптографических средств. Вероятно, здесь имеет место и психологический эффект. Кажется, гораздо проще переписать из Интернета одну из бесплатных или условно-бесплатных программ шифрования и активно ее использовать, в том числе для защиты информационного обмена со сторонними организациями, в то время как закупка аппаратного шифратора представляется началом долгого процесса получения всевозможных лицензий, сбора согласующих виз и т. п.. Иными словами, на первый план выходят даже не денежные соображения, а попытки сэкономить время и облегчить себе жизнь.

Однако, в нормативных актах регулирующих практику применения криптографических (шифровальных) средств, не проводится различий между программными и аппаратными средствами: оформлять использование криптосредств надо в любом случае. Другое дело, что документы эти могут быть разными — или лицензия ФАПСИ на использование криптосредств, или договор с организацией, имеющей необходимую лицензию ФАПСИ на предоставление услуг по криптографической защите конфиденциальной информации. Поэтому переход к применению аппаратных шифраторов можно совместить с оформлением упомянутых выше документов.

Аппаратные шифраторы

Аппаратный шифратор по виду и по сути представляет собой обычное компьютерное «железо», чаще всего это плата расширения, вставляемая в разъем ISA или PCI системной платы ПК. Бывают и другие варианты, например через разъем USB.

Использовать целую плату только для функций шифрования — непозволительная роскошь, поэтому производители аппаратных шифраторов обычно стараются насытить их различными дополнительными возможностями, среди которых:

Генерация случайных чисел. Это нужно прежде всего для получения криптографических ключей. Кроме того, многие алгоритмы защиты используют их и для других целей, например алгоритм электронной подписи ГОСТ Р 34.10 - 2001. При каждом вычислении подписи ему необходимо новое случайное число.

Контроль входа на компьютер. При включении ПК устройство требует от пользователя ввести персональную информацию (например, вставить дискету с ключами). Работа будет разрешена только после того, как устройство опознает предъявленные ключи и сочтет их "своими". В противном случае придется разбирать системный блок и вынимать оттуда шифратор, чтобы загрузиться (однако, как известно, информация на ПК тоже может быть зашифрована).

Контроль целостности файлов операционной системы. Это не позволит злоумышленнику в ваше отсутствие изменить какие-либо данные. Шифратор хранит в себе список всех важных файлов с заранее рассчитанными для каждого контрольными суммами (или хэш-значениями), и если при следующей загрузке не совпадет эталонная сумма хотя бы одного из них, компьютер будет блокирован.

Плата со всеми перечисленными возможностями называется устройством криптографической защиты данных — УКЗД.

Шифратор, выполняющий контроль входа на ПК и проверяющий целостность операционной системы, называют также «электронным замком». Понятно, что последним не обойтись без программного обеспечения — необходима утилита, с помощью которой формируются ключи для пользователей и ведется их список для распознавания «свой/чужой». Кроме того, требуется приложение для выбора важных файлов и расчета их контрольных сумм. Эти программы обычно доступны только администратору по безопасности, который должен предварительно настроить все УКЗД для пользователей, а в случае возникновения проблем разбираться в их причинах.

УЗКД проявится через несколько секунд после включения кнопки Power, как минимум сообщив о себе и попросив ключи. Шифратор всегда перехватывает управление при загрузке ПК (когда BIOS компьютера поочередно опрашивает все вставленное в него «железо»), после чего не так-то легко получить его обратно . УКЗД позволит продолжить загрузку только после всех своих проверок. Кстати, если ПК по какой-либо причине не отдаст управление шифратору, тот, немного подождав, все равно его заблокирует. И это также прибавит работы администратору по безопасности.

Структура шифраторов

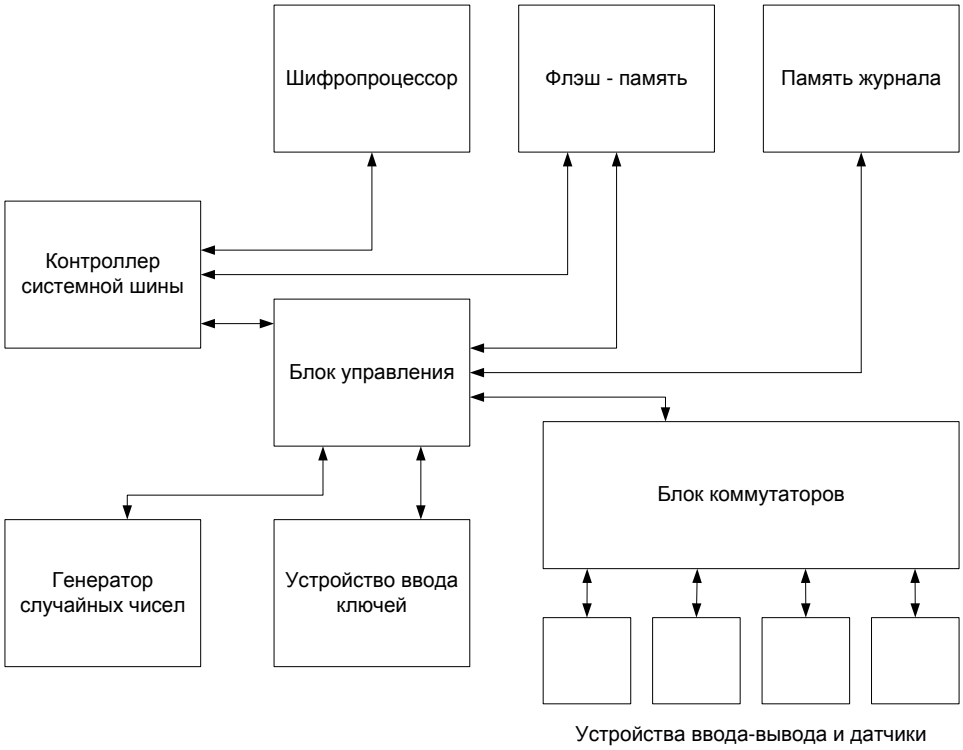


Рисунок 2.7. Структура шифратора

Блок управления - основной модуль шифратора, который "заведует" работой всех остальных. Обычно реализуется на базе микроконтроллера, сейчас их предлагается немало и можно выбрать подходящий. Главное - быстродействие и достаточное количество внутренних ресурсов, а также внешних портов для подключения всех необходимых модулей.

Контроллер системной шины ПК (например, PCI). Через него осуществляется основной обмен данными между УКЗД и компьютером.

Энергонезависимое запоминающее устройство (ЗУ) - обычно на базе микросхем флэш-памяти. Оно должно быть достаточно емким (несколько мегабайт) и допускать большое число циклов записи. Здесь размещается программное обеспечение микроконтроллера, которое выполняется при инициализации устройства (т. е. когда шифратор перехватывает управление при загрузке компьютера).

Память журнала. Также представляет собой энергонезависимое ЗУ; это действительно еще одна флэш-микросхема: во избежание возможных коллизий память для программ и для журнала не должны объединяться.

Шифропроцессор (или несколько) - это специализированная микросхема или микросхема программируемой логики PLD - Programmable Logic Device. Собственно, он и шифрует данные. Подробнее об этом немного позже.

Генератор случайных чисел. Обычно представляет собой некое устройство, дающее статистически случайный и непредсказуемый сигнал - белый шум. Это может быть, например, шумовой диод. А перед использованием по специальным правилам белый шум преобразуется в цифровую форму.

Блок ввода ключевой информации. Обеспечивает защищенный прием ключей с ключевого носителя, через него также вводится идентификационная информация о пользователе, необходимая для решения вопроса "свой/чужой".

Блок коммутаторов. Помимо перечисленных выше основных функций, УКЗД может по велению администратора безопасности отключать возможность работы с внешними устройствами: дисководами, CD-ROM, параллельным и последовательным портами, шиной USB и т. д. Если пользователь работает с настолько важной информацией, что ее нельзя ни печатать, ни копировать, УКЗД при входе на компьютер заблокирует все внешние устройства, включая даже сетевую карту.

Шифропроцессор

Основное назначение УКЗД - шифрование данных. Эта операция выполняется шифропроцессором, представляющим собой специализированную микросхему, которая выполняет криптографические операции, или микросхему программируемой логики, либо цифровой сигнальный процессор. Шифропроцессоров может быть несколько для повышения скорости и/или надежности шифрования. Для повышения скорости информацию распараллеливают между ними. Для обеспечения надежности производят обработку одних и тех же данных двумя шифропроцессорами с последующим сравнением результатов перед их выдачей.

Шифрование в УКЗД должно выполняться так, чтобы посторонним невозможно было узнать ключи и каким-либо образом повлиять на реализуемые в нем алгоритмы. Иногда бывает полезно засекретить и правила преобразования ключей. Поэтому шифропроцессор логически состоит из нескольких структурных единиц (рис. 1.8):

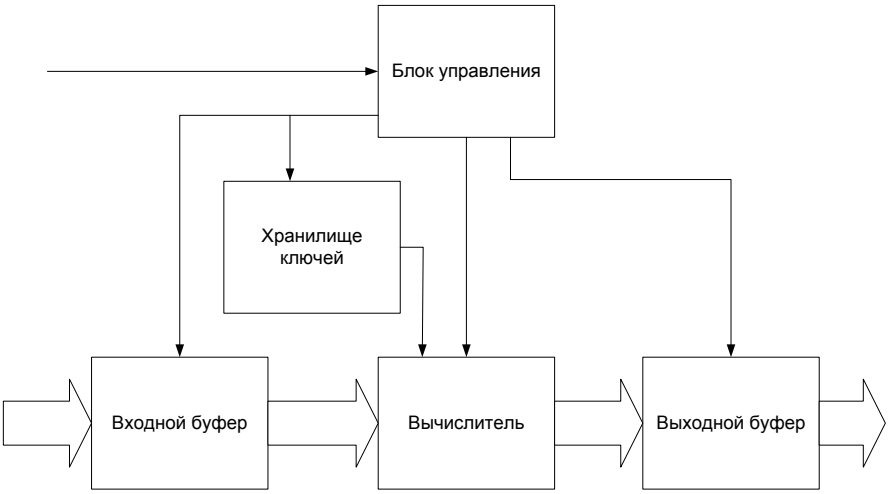


Рисунок 2.8. Структура шифропроцессора

Вычислитель - набор регистров, сумматоров, блоков подстановки и т. п., связанных между собой шинами передачи данных. Собственно, он и выполняет криптографические действия, причем должен делать это максимально быстро. На вход вычислитель получает открытые данные, которые следует зашифровать, и ключ шифрования, который, как известно, является случайным числом. А шифрование - это сложное математическое преобразование, поэтому его результат тоже очень похож на набор случайных величин (попробуйте сжать зашифрованный файл каким-нибудь архиватором - при использовании серьезного алгоритма защиты это будет невозможно).

Блок управления. На самом деле это аппаратно реализованная программа, управляющая вычислителем. Если по какой-либо причине программа изменится, его работа начнет давать сбои. Это чревато, например, появлением данных в открытом виде вместо зашифрованного (хотя это крайний случай; более вероятно получение такой шифровки, которую ни вы сами, ни кто-либо еще уже не расшифрует никогда L). Поэтому программа должна не только надежно храниться и устойчиво функционировать, но и регулярно проверять сама себя. Кстати, внешний блок управления (описанный выше) тоже периодически посылает ей контрольные задачи. На практике для большей уверенности ставят два шифропроцессора, которые постоянно сравнивают свои результаты (если они не совпадают, шифрование придется повторить). Все это требуется для обеспечения неизменности алгоритма шифрования.

Буфер ввода-вывода необходим для повышения производительности устройства: пока шифруется первый блок данных, загружается следующий и т. д. То же самое происходит и на выходе. Такая конвейерная передача данных серьезно увеличивает скорость шифрования.

Быстродействие

Любому пользователю ПК желательно, чтобы присутствие в его компьютере шифратора не отражалось на удобстве работы (конечно, если человек выполняет только разрешенные действия). Но, естественно, шифрование данных отнимает некоторое время, еще несколько лет назад шифраторы отвлекали на себя значительные ресурсы процессора. Современные шифраторы шифруют данные без помощи центрального процессора ПК. В шифратор лишь передается команда, а затем он сам извлекает данные из ОЗУ компьютера, шифрует их и кладет в указанное место. Процессор же при этом вполне может выполнять другие задачи. Исследования современных УКЗД показывают, что во время их работы производительность ПК практически не снижается.

Возможно применение и нескольких УКЗД на одном компьютере, например на криптографическом маршрутизаторе: один шифрует отправляемую в Интернет информацию,

второй — принимаемую. Производительность такой системы не вносит задержек в работу локальной сети Fast Ethernet (100 Мбит/с).

Потоковая скорость обработки данных — это один из основных параметров, по которым оценивают аппаратные шифраторы. Она измеряется в мегабайтах в секунду и зависит прежде всего от сложности алгоритма шифрования. Проще всего оценить ее по формуле:

$$V = F \text{ i } K / n, \qquad (2.1)$$

где F — тактовая частота,
K — размер стандартного блока шифрования,
n — число тактов, требующееся на преобразование стандартного блока.

Например, отечественный алгоритм ГОСТ 28147—89 имеет быстродействие 32 такта на 64-битовый блок, а значит, теоретически скорость шифрования должна стремиться к 25 Мбайт/с при тактовой частоте 100 МГц. Однако последние опубликованные достижения скорости аппаратной реализации этого алгоритма — 9 Мбайт/с. Ограничения являются чисто технологическими: отсутствие необходимого уровня разработок или элементной базы. Хотелось бы отметить, что программная реализация криптоГОСТа на самых современных ПК достигает 12—16 Мбайт/с при тактовой частоте процессора 1 ГГц. Хотя в этом случае аппаратная скорость шифрования теоретически могла бы быть около 250 Мбайт/с.

Другой пример, американский стандарт шифрования AES имеет быстродействие 10 тактов (может быть и 14 тактов, если размер блока и ключа – 256 бит) на 128-битовый блок, а значит, теоретически скорость шифрования должна стремиться к 160 Мбайт/с при тактовой частоте 100 МГц. Хотя для этого алгоритма также имеются чисто технологические ограничения. Кроме того формула не учитывает платформу на которой будет реализованы данные алгоритмы. При реализации на 32-битовых платформах ГОСТ проиграет AES всего 10-30%, тогда как при реализациях на 8-ми битовых платвормах разница в скоростях будет в 4-5 раза.

Шифраторы для защиты сетей

Для защиты передаваемой в Сеть информации можно использовать как обычный аппаратный шифратор, так и проходной шифратор (ПШ), который, помимо всего вышеперечисленного, является также полноценным сетевым адаптером Ethernet (т. е. шифратор и сетевой адаптер выполнены в качестве одной PCI-платы). Его достоинство в том, что он полностью контролирует весь обмен данными по сети, а обойти его (как изнутри, так и снаружи) просто невозможно.

ПШ являются достаточно сложными устройствами, так как они вместо центрального процессора компьютера вынуждены выполнять дополнительные функции по обработке информации. Обычно в ПШ ставят два шифропроцессора: один из них отвечает за шифрование отправляемых данных, а другой расшифровывает принимаемые. Такое устройство может хранить в себе несколько сотен ключей, чтобы каждый блок информации был зашифрован на своем, отличном от других. Это делает все ключи абсолютно недоступными злоумышленникам, но несколько затрудняет процесс управления ими.

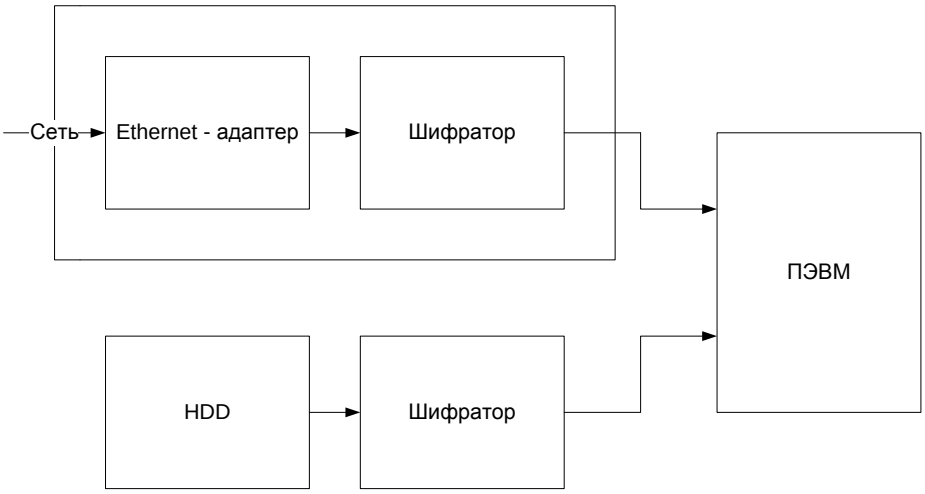


Рисунок 2.9. Структура проходного шифратора

Технические трудности не позволяли до последнего времени разработать надежные и быстродействующие ПШ. Однако с недавним появлением на рынке дорогих, но очень качественных микросхем решаются многие проблемы создания сложных многофункциональных устройств, что стимулировало выпуск первых проходных шифраторов.

Кстати, ПШ допускает и другое применение: он может стоять в разрыве между жестким диском компьютера и его контроллером. В этом случае все, что пишется на HDD, будет также автоматически шифроваться.

Разработчики аппаратных шифраторов и программного обеспечения для них, полагают, что уже скоро будут созданы ПШ, осуществляющие управление не только работой дисководов, CD-ROM и портов ввода-вывода, но всеми ресурсами ПК. В ближайшем будущем компьютеру останется только передавать открытые данные между процессором и оперативной памятью и обрабатывать их, все остальное сделает сам шифратор. Ясно, что абсолютному большинству пользователей это не потребуется. Но там, где ведется работа с важными и конфиденциальными документами, информация должна быть серьезно защищена.

Программные интерфейсы

Установленный на компьютере шифратор может использоваться сразу несколькими программами, например программой прозрачного шифрования, «прогоняющей» данные сквозь шифратор, и программой электронной подписи, использующей для вычисления подписи получаемые от шифратора случайные числа.

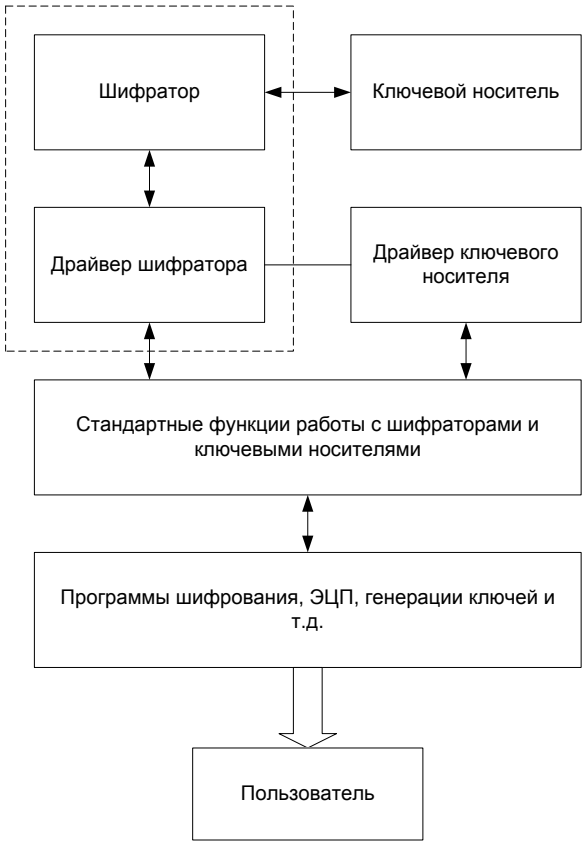


Рисунок 2.10. Программный интерфейс шифратора

Для того чтобы не возникало коллизий при одновременном обращении к шифратору разных программ (представим, что одна из них шифрует логический диск, а вторая на другом ключе расшифровывает файл: если не управлять очередью выполнения шифратором их требований, получится абракадабра), ставят специальное программное обеспечение управления им. Такое ПО выдает команды через драйвер шифратора и передает последнему данные, следя за тем, чтобы потоки информации от разных источников не пересекались, а также за тем, чтобы в шифраторе всегда находились нужные ключи. Таким образом, УКЗД выполняет два принципиально разных вида команд:

перед загрузкой операционной системы - команды, зашитые в память шифратора. Они осуществляют все необходимые проверки и устанавливают требуемый уровень безопасности - допустим, отключают внешние устройства.

после загрузки, например, Windows - команды, поступающие через модуль управления шифраторами: шифровать данные, перезагружать ключи, вычислять случайные числа и т. д.

Такое разделение необходимо из соображений безопасности — после выполнения команд первого блока, которые нельзя обойти, злоумышленник уже не сможет сделать что-либо запрещенное.

Еще одно назначение ПО управления шифраторами — обеспечить возможность замены одного шифратора на другой (скажем, на более «продвинутый» или быстрый), не меняя программного обеспечения. Это происходит аналогично, например, смене сетевой карты: шифратор поставляется вместе с драйвером, который позволяет программам выполнять стандартный набор функций. Те же программы шифрования и не заметят такой подмены, но будут работать в несколько раз быстрее.

Таким же образом можно заменить аппаратный шифратор на программный. Для этого программный шифратор выполняют обычно в виде драйвера, предоставляющего тот же набор функций.

Впрочем, такое ПО нужно вовсе не всем шифраторам — в частности, ПШ, стоящий по

дороге к HDD, достаточно настроить один раз, после чего о нем можно просто забыть.

Математические пространство алгоритма шифрования AES

Алгоритм оперирует байтами, которые рассматриваются как элементы конечного поля $GF(2^8)$.

Элементами поля $GF(2^8)$ являются многочлены степени не более 7, которые могут быть заданы строкой своих коэффициентов. Если представить байт в виде
$b_7, b_6, b_5, b_4, b_3, b_2, b_1, b_0,$
то элемент поля описывается многочленом с коэффициентами из {0, 1}:
$b_7 x^7 + b_6 x^6 + b_5 x^5 + b_4 x^4 + b_3 x^3 + b_2 x^2 + b_1 x^1 + b_0$

Например, байту {11001011} (или {cb} в шестнадцатеричной форме) соответствует многочлен $x^7 + x^6 + x^3 + x + 1$.

Для элементов конечного поля определены аддитивные и мультипликативные операции.

Сложение

Сложение суть операция поразрядного XOR и поэтому обозначается как ⊕. Пример выполнения операции сложения:
$(x^6 + x^4 + x^2 + x + 1) \oplus (x^7 + x + 1) = x^1 + x^6 + x^4 + x^2$ (в виде многочленов)
{01010111} ⊕ {10000011} = {11010100} (двоичное представление)
{57}⊕{83} = {d4} (шестнадцатеричное представление)

В конечном поле для любого ненулевого элемента a существует обратный элемент -a, при этом a + (-a) = 0, где нулевой элемент -это {00}. В $GF(2^8)$ справедливо a + a = 0, т. е. каждый ненулевой элемент является своей собственной аддитивной инверсией.

Умножение

Умножение, обозначаемое далее как •, более сложная операция. Умножение в $GF(2^8)$ - это операция умножения многочленов со взятием результата по модулю неприводимого многочлена m(x) восьмой степени и с использованием операции XOR при приведении подобных членов. В RIJNDAEL выбран $m(x) = x^8 + x^4 + x^3 + x + 1$, или в шестнадцатеричной форме 1{1b} (такая запись обозначает, что присутствует «лишний» девятый бит). Пример операции умножения:

$\{57\} \cdot \{83\} = \{c1\}$,

или

$\mathbf{(x^6 + x^4 + x^2 + x + 1)\ (x^7 + x + 1) = x^{13} + x^{11} + x^9 + x^8 + x^7 + x^7 + x^5 + x^3 + x^2 + x + x^6 + x^4 + x^2 + x + 1 = x^{13} + x^{11} + x^9 + x^8 + x^6 + x^5 + x^4 + x^3 + 1}$

Следовательно,

$x^{13} + x^{11} + x^9 + x^8 + x^6 + x^5 + x^4 + x^8 + 1 \bmod (x^8 + x^4 + x^3 + x + 1) = x^7 + x^6 + 1$

Результат является двоичным полиномом не выше 8 степени. В отличие от сложения, простой операции умножения на уровне байтов не существует.

Умножение, определенное выше, является ассоциативным, и существует единичный элемент ('01'). Для любого двоичного полинома b(x) не выше 8-й степени можно использовать расширенный алгоритм Евклида для вычисления полиномов a(x) и c(x) таких, что
$b(x)\ a(x) + m(x)\ c(x) = 1$

Следовательно,
$a(x)\ b(x) \bmod m(x) = 1$
или
$b\text{-}1(x) = a(x) \bmod m(x)$

Более того, можно показать, что
$a(x)\ (b(x) + c(x)) = a(x)\ b(x) + a(x)\ c(x)$

Из всего этого следует, что множество из 256 возможных значений байта образует конечное поле GF (2^8) с XOR в качестве сложения и умножением, определенным выше.

Умножение на x

Если умножить

$b(x) = b_7 x^7 + b_6 x^6 + b_5 x^5 + b_4 x^4 + b_3 x^3 + b_2 x^2 + b_1 x^1 + b_0$

на полином x, мы будем иметь:

$b_7 x^8 + b_6 x^7 + b_5 x^6 + b_4 x^5 + b_3 x^4 + b_2 x^3 + b_1 x^2 + b_0 x$

Если $b_7 = 0$, то мы сразу получаем результат умножения. Если $b_7 = 1$, то m(x) следует вычесть из результата (т.е. XOR) Из этого следует, что умножение на x может быть реализовано на уровне байта как левый сдвиг и возможно последующий побитовый XOR с {1b}.

Пусть функция *xtime()* осуществляет операцию умножения на x вышеописанным способом. Применяя функцию n раз можно получить результат умножения на x^n, а суммируя степени x можно получить любой элемент поля. Например:

{57} • {13} = {fe}, так как

{57} • {02=x}= xtime({57})= {ae}

{57} • {04}= xtime({ae})= {47}

{57} • {08}= xtime({47})= {8e}

{57} • {10}= xtime({8e})= {07}, откуда

{57} • {13}= {57} • ({01}⊕ {02}⊕ {10})= {57} ⊕ {ae} ⊕ {07}= {fe}

Полиномы с коэффициентами из GF (2^8)

Раундовые преобразования RIJNDAEL оперируют 32-разрядными словами. Четырехбайтовому слову может быть поставлен в соответствие многочлен a(x) с коэффициентами из GF(2^8) степени не более трех:

$a(x) = a_3 x^3 + a_2 x^2 + a_1 x^1 + a_0$

Полиномы могут быть сложены простым сложением соответствующих коэффициентов. Как сложение в GF (2^8) является побитовым XOR, так и сложение двух слов является простым побитовым XOR:

$a(x)+b(x) = (a_3 \oplus b_3)x^3 + (a_2 \oplus b_2)x^2 + (a_1 \oplus b_1)x^1 + (a_0 \oplus b_0)$

Умножение представляет собой более сложное действие. Предположим, что мы имеем два полинома в GF (2^8).

$a(x) = a_3 x^3 + a_2 x^2 + a_1 x^1 + a_0,$
$b(x) = b_3 x^3 + b_2 x^2 + b_1 x^1 + b_0,$

$c(x) = a(x)\, b(x),$
определяется следующим образом:
$c(x) = c_6 x^6 + c_5 x^5 + c_4 x^4 + c_3 x^3 + c_2 x^3 + c_1 x^1 + c_0,$
$c_0 = a_0 b_0,$
$c_1 = a_1 b_0 \oplus a_0 b_1,$
$c_2 = a_2 b_0 \oplus a_1 b_1 \oplus a_0 b_2,$
$c_3 = a_3 b_0 \oplus a_2 b_1 \oplus a_1 b_2 \oplus a_0 b_3,$
$c_4 = a_3 b_1 \oplus a_2 b_2 \oplus a_1 b_3,$
$c_5 = a_3 b_2 \oplus a_2 b_3,$

$c_6 = a_3 b_3$.

Для того чтобы результат умножения мог быть представлен 4-байтовым словом, необходимо взять результат по модулю многочлена степени не более 4. Авторы шифра выбрали многочлен

$M(x) = x^4 + 1$

так как

$x^i \bmod (x^4 + 1) = x^{i \bmod 4}$

Рузультат, получаемый из a(x) и b(x), обозначаемый $d(x) = a(x) \otimes b(x)$, получается следующим образом:

$d_0 = a_0 b_0 \oplus a_3 b_1 \oplus a_2 b_2 \oplus a_1 b_3$

$d_1 = a_1 b_0 \oplus a_0 b_1 \oplus a_3 b_2 \oplus a_2 b_3$

$d_2 = a_2 b_0 \oplus a_1 b_1 \oplus a_0 b_2 \oplus a_3 b_3$

$d_3 = a_3 b_0 \oplus a_2 b_1 \oplus a_1 b_2 \oplus a_0 b_3$

Операция, состоящая из умножения фиксированного полинома a(x), может быть записана как умножение матрицы, где матрица является циклической:

$$\begin{bmatrix} d_0 \\ d_1 \\ d_2 \\ d_3 \end{bmatrix} = \begin{bmatrix} a_0 & a_3 & a_2 & a_1 \\ a_1 & a_0 & a_3 & a_2 \\ a_2 & a_1 & a_0 & a_3 \\ a_3 & a_2 & a_1 & a_0 \end{bmatrix} . \begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \end{bmatrix}$$

Пусть

$b(x) = b_3 x^3 + b_2 x^2 + b_1 x^1 + b_0$,

умножению на x многочлена b(x) с коэффициентами из $GF(2^8)$ по модулю $x^4 + 1$, учитывая свойство последнего, соответствует циклический сдвиг байтов в пределах слова в сторону старшего байта, та как

$x \otimes b(x) = b_2 x^3 + b_1 x^2 + b_0 x^1 + b_3$.

2.1 Алгоритм шифрования AES.

В Rijndael Блоки открытых и зашифрованных данных, соответственно $\boldsymbol{T}$ и $\boldsymbol{T'}$, представляются в виде массивов из 16, 24 или 32 байтов:

$\boldsymbol{T} = (\boldsymbol{t}_1, \boldsymbol{t}_2, ..., \boldsymbol{t}_N)$

$\boldsymbol{T'} = (\boldsymbol{t'}_1, \boldsymbol{t'}_2, ..., \boldsymbol{t'}_N)$

$| \boldsymbol{t} | = | \boldsymbol{t'} | = 8$, $\boldsymbol{N} \in \{16, 24, 32\}$.

В соответсвии с использованными архитектурными принципами в ходе криптографических преобразований исходный и зашифрованный блоки данных, а также все промежуточные результаты процесса шифрования интерпретируются как матрицы байтов размером $4 \times \boldsymbol{n}$, откуда получаем $\boldsymbol{n} = \boldsymbol{N}/4$, $\boldsymbol{n} \in \{4, 6, 8\}$. Матрицы заполняются байтами входного блока (открытых данных при зашифровании и зашифрованных данных при расшифровании соответсвенно) по столбцам сверху вниз и слева направо, и в точно таком же порядке извлекаются байты из матрицы-результата:

$$\boldsymbol{T} = \begin{bmatrix} \boldsymbol{t}_1 & \boldsymbol{t}_5 & \dots & \boldsymbol{t}_{N-3} \\ \boldsymbol{t}_2 & \boldsymbol{t}_6 & \dots & \boldsymbol{t}_{N-2} \\ \boldsymbol{t}_3 & \boldsymbol{t}_7 & \dots & \boldsymbol{t}_{N-1} \\ \boldsymbol{t}_4 & \boldsymbol{t}_8 & \dots & \boldsymbol{t}_N \end{bmatrix}, \quad \boldsymbol{T'} = \begin{bmatrix} \boldsymbol{t'}_1 & \boldsymbol{t'}_5 & \dots & \boldsymbol{t'}_{N-3} \\ \boldsymbol{t'}_2 & \boldsymbol{t'}_6 & \dots & \boldsymbol{t'}_{N-2} \\ \boldsymbol{t'}_3 & \boldsymbol{t'}_7 & \dots & \boldsymbol{t'}_{N-1} \\ \boldsymbol{t'}_4 & \boldsymbol{t'}_8 & \dots & \boldsymbol{t'}_N \end{bmatrix}.$$

Схема преобразования данных при зашифровании показана на рисунке и схема соответсвующего алгоритма - на русунке 2.1 и 2.2.

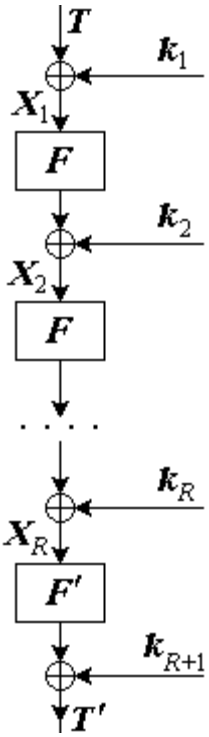


Рисунок 2.11. Цикл шифрования Rijndael - схема преобразования данных

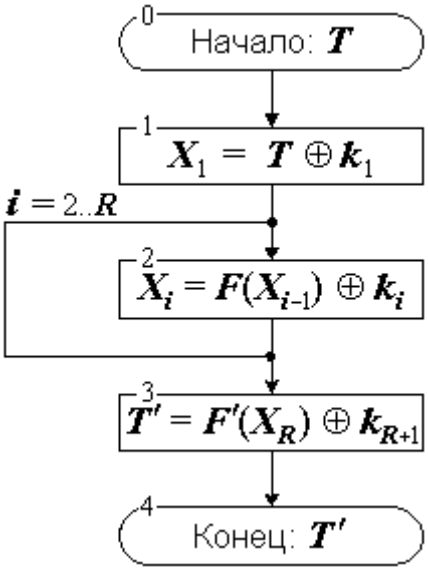


Рисунок 2.12. Цикл шифрования Rijndael - схема алгоритма

На рисунках использованы следующие обозначения:
T, ***T′*** - открытый и зашифрованный блоки данных соответственно;
k_i - ***i***-тый ключевой элемент;
F, ***F′*** - регулярное нелинейное преобразование и преобразование последнего раунда соответсвенно;
X_i - промежуточное состояние шифруемого блока после прибавления ***i***-того ключевого элемента.

Как видно из рисунков 2.11 и 2.12, процесс зашифрования состоит из чередующихся прибавлений ключевых элементов к блоку данных и нелинейного преобразования этого блока:

$$T' = E_K(T) = k_{R+1} \oplus F'(k_R \oplus F(k_{R-1} \oplus \ldots F(k_2 \oplus F(k_1 \oplus T))\ldots)).$$

Число ***R*** раундов шифрования переменное и зависит от размера блока данных и ключа. Прибавление ключевых элементов, которым начинается и заканчивается процесс шифрования, а также некоторые другие операции раундового преобразования выполняется побайтно в конечном поле Галуа $GF(2^8)$, полевой операцией сложения в нем является побитовое суммирование по модулю 2. Соответсвенно, каждый ключевой элемент является байтовой матрицей того же самого размера, что и блок данных. За один раунд шифрования преобразуется полный блок данных, а не его часть, как в сетях Фейстеля. На последнем раунде функция нелинейного преобразования отличается от аналогичной функции, используемой в остальных раундах - это сделано для обеспечения алгоритмической эквивалентности прямого и обратного преобразований шифрования.

Процесс расшифрования блока данных алгоритмически идентичен процессу его зашифрования и, следовательно, рисунки 2.1 и 2.2 также справедливы и для него, если через ***T*** обозначить блок зашифрованных данных, а через ***T′*** - открытых. Однако различия между этими двумя процедурами в архитектуре "Квадрат" несколько более существенны, чем в сетях Фейстеля - они различаются не только порядком использовани ключевых элементов в раундах шифрования, но и самими этими элементами, и некоторыми другими константами, используемыми в алгоритме. Соответсвующие вопросы рассмотрены ниже.

Rijnael это блочный шифр с различной длиной блока шифрования и длиной ключа.

Длины блока и ключа шифрования могут быть 128, 192 и 256 бит. Шифрование блока осуществляется за несколько раундов, так, например, при длине блока 128 бит и длине ключа 128 бит алгоритм включает 10 раундов.

Таблица 2.1. Зависимость количества раундов шифрования от длины блока и длины ключа шифрования

Nr	Nb = 4	Nb = 6	Nb = 8
Nk = 4	10	12	14
Nk = 6	12	12	14
Nk = 8	14	14	14

Число столбцов обозначено как **Nb** и равно длине блока, деленной на 32. Ключ шифрования также представлен в виде прямоугольного массива с четырьмя строками. Число столбцов обозначено как **Nk** и равно длине ключа, деленной на 32.

Первому раунду предшествует операция добавления кругового ключа.

В отличие от DES, раунды Rijnael не обладают фейстелевской структурой. Вместо этого каждый раунд включает различные обратимые преобразования под названием слои. Схематически каждый раунд, кроме последнего, можно представить в виде 4 операций. Далее мы будем рассматривать вариант шифрования 128 битного блока при длине ключа 128 бит. При других длинах блока шифрования и длины ключа схема алгоритма не меняется, изменяются лишь некоторые константы реализации алгоритма (число раундов и прочее).

Для дальнейшего описания введем следующие обозначения: Состояние (State)- промежуточный результат шифрования. Состояние можно представить как прямоугольный массив байтов. При этом байты состояния формируют блок данных следующим образом: $a_{0,0}$, $a_{1,0}, a_{2,0}, a_{3,0}, a_{4,0}, a_{0,1}, a_{0,2}, a_{0,3}$ …….

$a_{0,0}$	$a_{0,1}$	$a_{0,2}$	$a_{0,3}$
$a_{1,0}$	$a_{1,1}$	$a_{1,2}$	$a_{1,3}$
$a_{2,0}$	$a_{2,1}$	$a_{2,2}$	$a_{2,3}$
$a_{3,0}$	$a_{3,1}$	$a_{3,2}$	$a_{3,3}$

$k_{0,0}$	$k_{0,1}$	$k_{0,2}$	$k_{0,3}$
$k_{1,0}$	$k_{1,1}$	$k_{1,2}$	$k_{1,3}$
$k_{2,0}$	$k_{2,1}$	$k_{2,2}$	$k_{2,3}$
$k_{3,0}$	$k_{3,1}$	$k_{3,2}$	$k_{3,3}$

Массив состоит из четырех строк и четырех столбцов. Также нам понадобится представление этого блока как одномерного массива 4-байтных векторов, где каждый вектор состоит из соответствующего столбца прямоугольного массива. Ключ шифрования представляется аналогичным образом.

Каждый раунд, кроме последнего, можно представить следующим образом:

```
Round
{
ByteSub()
ShiftRow()
MixColomn()
AddRoundKey()
}
```

Последний раунд не содержит операции MixColomn().

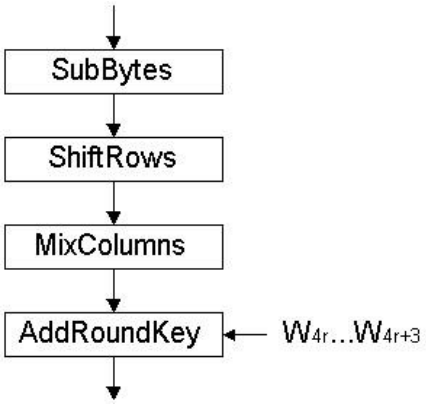


Рисунок 2.13. Раунд алгоритма

ByteSub (Замена байтов)
ShiftRow (Сдвиг строк)
MixColomn (Смешивание столбцов)
В каждом раунде алгоритма выполняются следующие преобразования (см. рис. 2.3):

Операция SubBytes, представляющая собой табличную замену каждого байта массива данных согласно следующей таблице (см. рис. 2.4):

Таблица 2.2 – Таблица замен используемая стандартом AES

63	7C	77	7B	F2	6B	6F	C5	30	01	67	2B	FE	D7	AB	76
CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
04	C7	23	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75
09	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	2F	84
53	D1	00	ED	20	FC	B1	5B	6A	CB	BE	39	4A	4C	58	CF
D0	EF	AA	FB	43	4D	33	85	45	F9	02	7F	50	3C	9F	A8
51	A3	40	8F	92	9D	38	F5	BC	B6	DA	21	10	FF	F3	D2
CD	0C	13	EC	5F	D7	44	17	C4	A7	7E	3D	64	5D	19	73
60	81	4F	DC	22	2A	90	88	46	EE	B8	14	DE	5E	0B	DB
E0	32	3A	0A	49	06	24	5C	C2	D3	AC	62	91	95	E4	79
E7	C8	37	6D	8D	D5	4E	A9	6C	56	F4	EA	65	7A	AE	08
BA	78	25	2E	1C	A6	B4	C6	E8	DD	74	1F	4B	BD	8B	8A
70	3E	B5	66	48	03	F6	0E	61	35	57	B9	86	C1	1D	9E
E1	F8	98	11	69	D9	8E	94	9B	1E	87	E9	CE	55	28	DF
8C	A1	89	0D	BF	E6	42	68	41	99	2D	0F	B0	54	BB	16

Таблица меняет входное значение 0 на 63 (шестнадцатеричное значение), 1 – на 7C, 2 – на 77 и т.д.

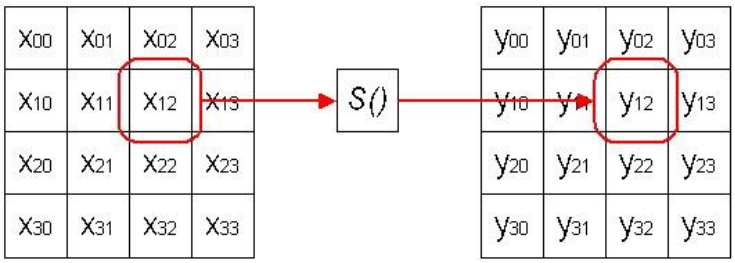


Рисунок 2.14. Операция SubBytes

Вместо данной табличной замены можно выполнить эквивалентную ей комбинацию двух операций:

. Вычисление мультипликативной обратной величины от входного значения в конечном поле GF(2^8); обратной величиной от 0 является 0.

. Выходное значение **b** вычисляется следующим образом:

$\mathbf{b_i = a_i \oplus a_{i+4 \bmod 8} \oplus a_{i+5 \bmod 8} \oplus a_{i+6 \bmod 8} \oplus a_{i+7 \bmod 8} \oplus c_i}$

где $\mathbf{n_i}$ обозначает **i**-й бит величины **n,**

a – результат предыдущей операции,

c – шестнадцатеричная константа 63.

Замена байтов представляет собой нелинейную замену байтов, действующую на каждый байт состояния независимо. Таблица замены является обратимой и строится на основе произведения двух преобразований:

вычисляется "обратный байт" (обратимость понимается над полем GF(256), а 0 элемент отображается в себя).

К полученному байту применяется афинное преобразование:

$$\begin{bmatrix} y_0 \\ y_1 \\ y_2 \\ y_3 \\ y_4 \\ y_5 \\ y_6 \\ y_7 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{bmatrix} \begin{bmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \end{bmatrix} + \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix}$$

Рисунок 2.15. Операция SubBytes в матричной форме

Для выполнения обратной замены байтов применяется обратная таблица замены, которая получается следующим образом: сначала производится обратное афинное преобразование, а затем вычисляется обратный элемент над GF(256).

2. Операция ShiftRows, которая выполняет циклический сдвиг влево всех строк массива данных, за исключением нулевой. Сдвиг **i**-й строки массива (для **i** = 1, 2, 3) производится на **i** байт.

Рисунок 2.16. Операция ShiftRows

3. Операция MixColumns. Смешивание столбцов происходит следующим образом: столбец состояния рассматривается как полином над GF(256) и умножается по модулю x^4+1 на фиксированный полином $a(x)$, где $a(x)='03'x^3+'01'x^2+'01'x+'02'$. Это преобразование

обратимо, поскольку полином $a(x)$ взаимно прост с x^4+1.

Это преобразование можно записать в матричном виде: $y(x)=a(x)\otimes x(x)$,

$$\begin{bmatrix} y_0 \\ y_1 \\ y_2 \\ y_3 \end{bmatrix} = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \begin{bmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \end{bmatrix}$$

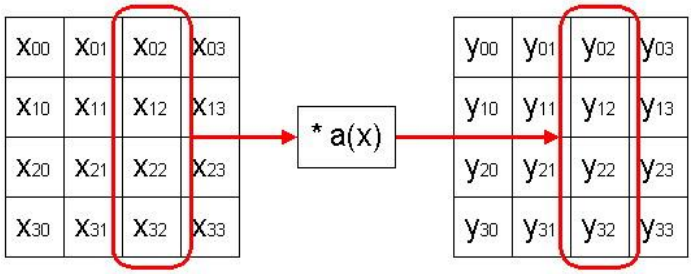


Рисунок 2.17. Операция MixColumns

Для выполнения обратного преобразования необходимо произвести умножение на полином $d(x)='0B'x^3+'0D'x^2+'09'x+'0E'$.

4. Операция AddRoundKey выполняет наложение на массив данных материала ключа. А именно, на **i**-й столбец массива данных (**i** = 0…3) побитовой логической операцией «исключающее или» (XOR) накладывается определенное слово расширенного ключа $\mathbf{W_{4r+i}}$, где **r** – номер текущего раунда алгоритма, начиная с 1 (процедура расширения ключа будет описана ниже). Операция AddRoundKey представлена на рис. 13.

Количество раундов алгоритма **R** зависит от размера ключа следующим образом:

Таблица 2.3 - Количество раундов алгоритма в зависити от размера ключа

Размер ключа, бит	**R**
128	10
192	12
256	14

Перед первым раундом алгоритма выполняется предварительное наложение материала ключа с помощью операции AddRoundKey, которая выполняет наложение на открытый текст первых четырех слов расширенного ключа $\mathbf{W_0…W_3}$.

Последний же раунд отличается от предыдущих тем, что в нем не выполняется операция MixColumns.

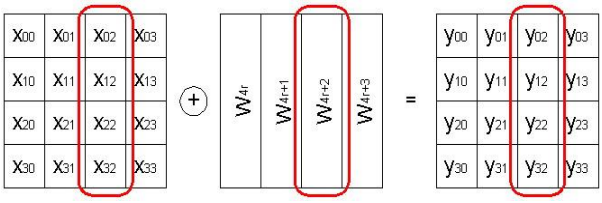


Рисунок 2.18. Операция AddRoundKey

Получение кругового ключа.

Ключ шифрования для каждого раунда получается следующим образом: Сначала происходит расширение ключа, а затем последовательная выборка из расширенного ключа для каждого раунда.

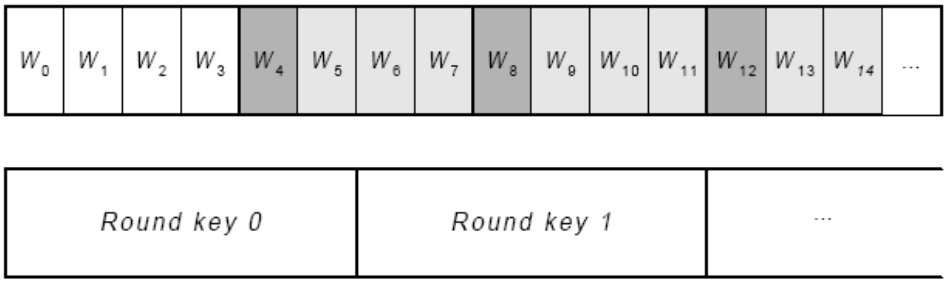


Рисунок 2.19. Расширение ключа и выборка из расширенного ключа ключа для каждого раунда

Полное число битов кругового ключа, необходимго для шифрования, равно длине блока умноженной на количество раундов плюс 1, те для блока длиной 128 бит и 10 раундов необходимо 1408 бит. Первые 128 бит кругового ключа совпадают с самим ключом.

Формирование ключа происходит следующим образом: первые четыре столбца (с номерами 0-3)совпадают с самим ключом, далее столбец с номером четыре получается из третьего с помощью следующей композиции преобразований:

$K_4 = SubByte(RotByte(K_3)) \oplus C_1$, далее для столбцов 5-7 имеем: $K_i = K_{i-4} \oplus K_{i=1}$. Дальнейший процесс определяется рекурсивно, меняется лишь константа С. Здесь SubByte – применение операции замены байт, а RotByte- сдвиг, преобразующий столбец (a,b,c,d) в (b,c,d,a).

Расширение ключа выполняется в два этапа, на первом из которых производится инициализация слов расширенного ключа (обозначаемых как $\mathbf{W_i}$): первые **Nk** (**Nk** – размер исходного ключа шифрования **K** в словах, т.е. 4, 6 или 8) слов $\mathbf{W_i}$ (т.е. **i** = 0…**Nk-1**) формируются их последовательным заполнением байтами ключа (см. рис. 2.20).

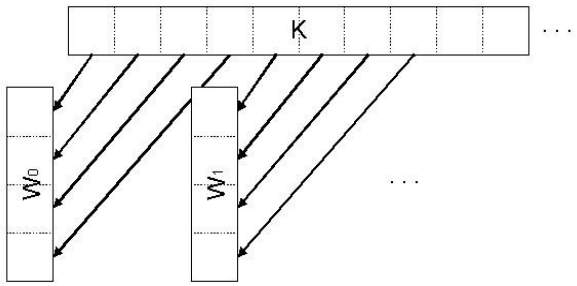


Рисунок 2.20. Инициализация первых слов расширенного ключа

Последующие слова $\mathbf{W_i}$ формируются следующей последовательностью операций для каждого **i** = **Nk**…4*(**R**+1)-1:

Инициализируется временная переменная **T**:

T = $\mathbf{W_{i-1}}$.

Данная переменная модифицируется следующим образом:

если **i** кратно **Nk**, то:

T = SubWord(RotWord(T)) □ RC□i/Nk□;
операции SubWord, RotWord будут описаны ниже, а константы $\mathbf{RC_n}$ представляют собой слова, в которых все байты, кроме первого являются нулевыми, а первый байт имеет значение 2^{n-1} mod 256;

если **Nk** = 8 и (**i** mod **Nk**) = 4, то:

T = SubWord(T);

в остальных случаях модификация переменной **T** не выполняется.

Формируется **i**-е слово расширенного ключа:

$\mathbf{W_i = W_{i-Nk} \square T.}$

Операция SubWord выполняет над каждым байтом входного значения табличную замену, которая была описана выше – см. операцию SubBytes.

Операция RotWord побайтно вращает входное слово на 1 байт влево.

Как видно, процедура расширения ключа является достаточно простой по сравнению со многими другими современными алгоритмами шифрования. Процедура расширения ключа имеет также несомненное достоинство в том, что расширение ключа может быть выполнено «на лету» (on-the-fly), т.е. параллельно с зашифрованием данных.

Авторы алгоритма в [3] пишут также, что не следует задавать напрямую расширенный ключ – программная или аппаратная реализация алгоритма должна именно получать исходный ключ шифрования **K** и выполнять процедуру расширения ключа. Здесь стоит снова вспомнить алгоритм DES – известно, что DES с независимо задаваемыми ключами раундов оказался слабее против некоторых атак, чем исходный алгоритм DES.

Тогда весь процесс шифрования можно записать так:

Изначальное добавление кругового ключа
N-1 раунд
Последний раунд.

Алгоритм дешифрования AES

Выше было отмечена реализация обратного к каждому из преобразований раунда:

{
Добавление кругового ключа
Обратное смешивание столбцов
Обратный сдвиг строк
Обратная замена байт
}

Единственное что необходимо это изменить порядок операций каждого раунда. Сложность операций для алгоритма шифрования не изменяется. Однако исходя из алгебраических свойств входящих в раунд преобразований, можно прийти к структуре, не отличающийся от прямого алгоритма. Рассмотрим двухраундовый обратный алгоритм:

```
AddRoundKey();
InvShiftRow();
InvByteSub();
AddRoundKey();
InvMixColumn();
InvShiftRow();
InvByteSub();
AddRoundKey();
```

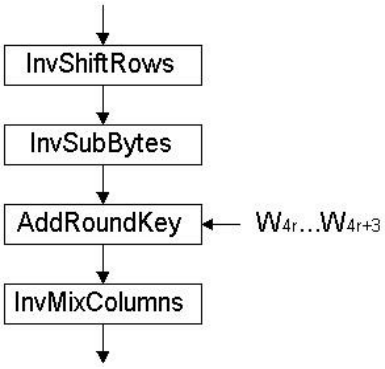


Рисунок 2.21. Раунд расшифрования

Легко заметить, что операции сдвига строк и замены байт можно поменять местами, т.к. замена байт действует на каждый байт независимо. Кроме того, последовательность
AddRoundKey();
InvMixColumn();
можно заменить на
InvMixColumn()
AddRoundKey(InvRoundKey); Здесь InvRoundKey обозначает результат применения операции InvMixColumn() к ключу. Это следует из линейности операций. Тогда мы получим следующую структуру для двухраундового обратного алгоритма:
AddRoundKey();
InvByteSub();
InvShiftRow();
InvMixColumn();
AddRoundKey(Inv);
InvByteSub();
InvShiftRow();
AddRoundKey();

Таким образом, мы получили структуру прямого двухраундового алгоритма. Для большего числа раундов получаем такой же результат. Таким образом, обратный алгоритм имеет ту же структуру.

Перед первым раундом расшифрования выполняется операция AddRoundKey (которая является обратной самой себе), выполняющая наложение на шифртекст четырех последних слов расширенного ключа, т.е. $\mathbf{W_{4R}…W_{4R+3}}$.

Затем выполняется **R** раундов расшифрования, каждый из которых выполняет следующие преобразования (см. рис. 7):

Операция InvShiftRows выполняет циклический сдвиг вправо трех последних строк массива данных на то же количество байт, на которое выполнялся сдвиг операцией ShiftRows при зашифровании.

Операция InvSubBytes выполняет побайтно обратную табличную замену, которая определена следующей таблицей:

Таблица 2.4. Таблица обратной замены для стандарта AES

52	09	6A	D5	30	36	A5	38	BF	40	A3	9E	81	F3	D7	FB
7C	E3	39	82	9B	2F	FF	87	34	8E	43	44	C4	DE	E9	CB
54	7B	94	32	A6	C2	23	3D	EE	4C	95	0B	42	FA	C3	4E
08	2E	A1	66	28	D9	24	B2	76	5B	A2	49	6D	8B	D1	25
72	F8	F6	64	86	68	98	16	D4	A4	5C	CC	5D	65	B6	92
6C	70	48	50	FD	ED	B9	DA	5E	15	46	57	A7	8D	9D	84
90	D8	AB	00	8C	BC	D3	0A	F7	E4	58	05	B8	B3	45	06
D0	2C	1E	8F	CA	3F	0F	02	C1	AF	BD	03	01	13	8A	6B
3A	91	11	41	4F	67	DC	EA	97	F2	CF	CE	F0	B4	E6	73
96	AC	74	22	E7	AD	35	85	E2	F9	37	E8	1C	75	DF	6E
47	F1	1A	71	1D	29	C5	89	6F	B7	62	0E	AA	18	BE	1B
FC	56	3E	4B	C6	D2	79	20	9A	DB	C0	FE	78	CD	5A	F4
1F	DD	A8	33	88	07	C7	31	B1	12	10	59	27	80	EC	5F
60	51	7F	A9	19	B5	4A	0D	2D	E5	7A	9F	93	C9	9C	EF
A0	E0	3B	4D	AE	2A	F5	B0	C8	EB	BB	3C	83	53	99	61
17	2B	04	7E	BA	77	D6	26	E1	69	14	63	55	21	0C	7D

Данную табличную замену можно выполнить, применив к входному байту преобразование, обратное операции 1.2 (см. описание операции SubBytes), после чего вычислить мультипликативную обратную величину от результата предыдущей операции в конечном поле $GF(2^8)$.

Операция AddRoundKey, как и при зашифровании, выполняет наложение на обрабатываемые данные четырех слов расширенного ключа $\mathbf{W_{4r}…W_{4r+3}}$. Однако, нумерация раундов **r** при расшифровании производится в обратную сторону – от **R**-1 до 0.

Операция InvMixColumns выполняет умножение каждого столбца массива данных аналогично прямой операции MixColumns, однако, умножение производится на полином $\mathbf{a^{-1}(x)}$, определенный следующим образом:

$$\mathbf{a^{-1}(x) = Bx^3 + Dx^2 + 9x + E.}$$

Аналогично зашифрованию, последний раунд расшифрования не содержит операцию InvMixColumns.

Отличия AES от исходного алгоритма Rijndael

Алгоритм Rindael позволяет шифровать данные не только 128-битными блоками, но и блоками по 192 или 256 бит. Таким образом, AES, фактически, имеет лишь одно принципиальное отличие от Rijndael: он предусматривает использование только 128-битных блоков данных. Рассмотрим изменения в приведенном выше описании алгоритма AES, связанные с другими размерами блоков:

Обрабатываемые данные могут представляться не только в виде массива размером 4 X 4, но и 4 X 6 или 4 X 8 для 192- и 256-битных блоков соответственно.

Количество раундов **R** алгоритма Rijndael определяется следующей таблицей в зависимости не только от размера ключа, но и от размера блока:

Размер ключа, бит	*Размер блока, бит*		
	128	*192*	*256*
128	10	12	14
192	12	12	14
256	14	14	14

Количество бит сдвига строк таблицы также зависит от размера блока:

Номер строки	*Размер блока, бит*		
	128	*192*	*256*
1	1	1	1
2	2	2	3
3	3	3	4

Поскольку для 192- и 256-битного блоков увеличивается количество столбцов массива данных до 6 и 8 соответственно, в операции AddRoundKey участвуют уже 6 или 8 слов расширенного ключа вместо четырех. Следовательно, в **r**-м раунде алгоритма выполняется наложение слов расширенного ключа $\mathbf{W_{Nb*r}…W_{Nb*r+3}}$, где **Nb** – количество столбцов массива данных.

В связи с вышесказанным, изменяется и процедура расширения ключа, однако, изменение состоит лишь в том, что данная процедура должна выработать **Nb***(**R**+1)-1 слов расширенного ключа, а не 4*(**R**+1)-1 (что, впрочем, остается справедливым для 128-битного блока).

Реализация алгоритма

Простая структура операций алгоритма обеспечивает легкость реализации и быстроту исполнения. Основные операции, применяемы при этом- это EXOR, применение S-box, и сдвиг. При этом особенно легко реализовать данный алгоритм на процессорах с длиной слова 32 бит и более. При этом для быстроты реализации в памяти создается таблица, содержащая значения S(a), а также еще 4 таблицы, определяемые через S(a) (всего около 4 кбайт памяти), после чего все преобразования сводятся к циклическим сдвигам и операциям XOR с этими таблицами и ключом. В силу того, что структура обратного алгоритма совпадает со структурой прямого, схема реализации не изменится, но значения элементов в таблицах будут другие, и к расширенному ключу необходимо применить операцию обратного смешивания столбцов при его формировании.

Таблица 2.4. Скорость алгоритма, при реализации на разных платформах

Длина (блока, ключа)	Ansi C, Mbit/sec	VisualC++, Mbit/sec
(128,128)	27.0	70.5
(192,128)	22.8	59.3
(256,128)	19.8	51.2

Режимы шифрования

Для различных ситуаций, встречающихся на практике, разработано значительное количество режимов шифрования.

Наиболее очевидное решение задачи закрытия сообщений, состоящих из нескольких блоков, заключается в независимом шифровании каждого блока на одном и том же ключе $\mathbf{k_{AB}}$. Данная классическая схема блочного шифрования (рисунок 2.12) известна под названием

режима *электронной кодовой книги* (**Electronic Code Book** (**ECB**)).

Уравнения зашифрования и расшифрования в режиме **ECB** имеют вид:

$\mathbf{c_i = E_{AB}(p_i)}$,

$\mathbf{p_i = D_{AB}(c_i)}$,

$i = \overline{1,m}$

Режим имеет три существенных недостатка. Так как блоки шифруются независимо друг от друга, при зашифровании двух или более одинаковых блоков получаются одинаковые блоки шифротекста и наоборот. Данное свойство режима ECB позволяет противнику делать выводы о тождественности тех блоков открытого текста, которым соответствуют одинаковые блоки шифротекста. В тех случаях, когда длина исходного сообщения не кратна **n**, где **n** - разрядность блоков, возникает проблема дополнения последнего блока до нужного размера. Дополнение последнего неполного блока некоей фиксированной комбинацией битов в некоторых случаях может позволить противнику методом перебора определить этот неполный блок. И наконец, данный режим нечувствителен к выпадению или вставке целого числа блоков шифротекста.

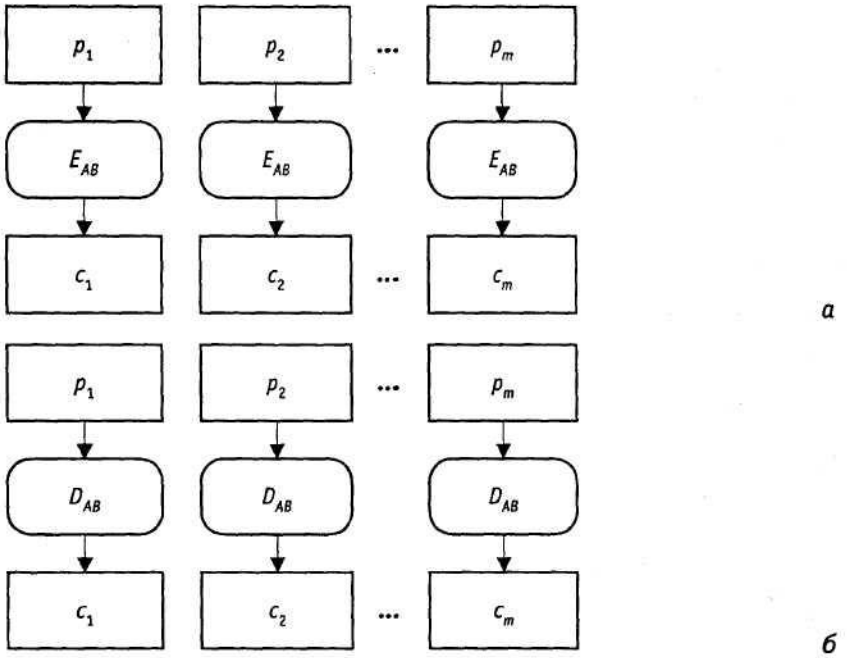


Рисунок 2.22. Режим шифрования ECB: а - зашифрование, 6 - расшифрование

Отмеченные недостатки ограничивают область использования режима **ECB** только шифрованием ключевой информации, объем которой обычно кратен **n**, при этом качественные ключи не могут содержать повторяющихся блоков. Применение режима **ECB** оправдано также в базах данных, когда требуется произвольный доступ для чтения/записи к различным полям.

Все остальные режимы реализуют комбинированные схемы шифрования и обеспечивают зависимость каждого блока шифротекста не только от соответствующего блока открытого текста, но и от его номера. На рисунке 2.13 показана схема шифрования в режиме *сцепления блоков шифротекста* (**Ciphertext Block Chaining** (**CBC**)). Уравнения зашифрования и расшифрования в режиме **CBC** имеют вид:

$\mathbf{c_i = E_{AB}\,(p_i \oplus c_{i-1})}$,

$\mathbf{p_i = D_{AB}\,(c_i) \oplus c_{i-1}}$,

$i = \overline{1,m}$

где секретность **n**-разрядного блока $\mathbf{c_0}$ (синхропосылки или вектора инициализации) не является обязательной.

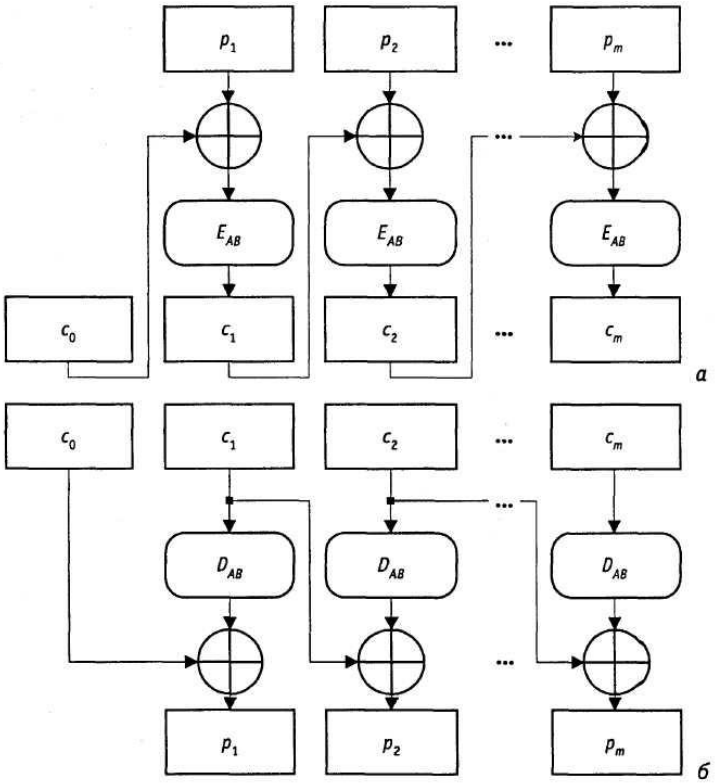


Рисунок 2.23. Режим шифрования CBC: а - зашифрование, 6 - расшифрование

Отличительными особенностями режима **CBC** являются зависимость при зашифровании i-го блока шифротекста от всех предшествующих блоков открытого текста и зависимость при расшифровании каждого блока открытого текста p_i, только от двух блоков c_{i-1} и c_i шифротекста. Первое свойство делает пригодным испол ьзование режима для решения задач контроля целостности информации. Второе свойство делает режим самосинхронизирующимся: одиночная ошибка при передаче (ошибка при передаче одного блока) может привести к неправильному расшифрованию только двух блоков.

Схема режима *обратная связь по шифротексту* (**Ciphertext Feedback** (**CFB**)) показана на рисунке 2.14. Уравнения зашифрования и расшифрования имеют вид:

$$c_i = p_i \oplus E_{AB}^{(t)}(s_{i-1}),$$

$$p_i = c_i \oplus E_{AB}^{(t)}\left(s_{i-1}\right),$$

$$s_i = \left(2^t \cdot s_{i-1} + c_i\right) \bmod 2^n,$$

$$i = \overline{1,m}$$

где

n - разрядность регистра сдвига,

t - разрядность шифруемых блоков данных **(1≤t≤n),**

s_0 - начальное состояние регистра сдвига (синхропосылка/вектор инициализации),

$E_{AB}^{(t)}(s_{i-1})$ - **t** старших битов **n**-разрядной шифрограммы $\mathbf{E_{AB}(s_{i-1})}$.

Схема шифрование в режиме **CFB** при **t = n** показана на рисунке 2.15. Уравнения зашифрования и расшифрования принимают вид:

$$\mathbf{c_i = p_i \oplus E_{AB}(c_{i-1})}$$

$$\mathbf{p_i = c_i \oplus D_{AB}(c_{i-1})}$$

$i = \overline{1, m}$

Свойства данной схемы шифрования аналогичны режиму CBC: при зашифровании каждый блок шифротекста зависит от всего предшествующего ему открытого текста, при расшифровании отсутствует эффект "размножения" ошибок.

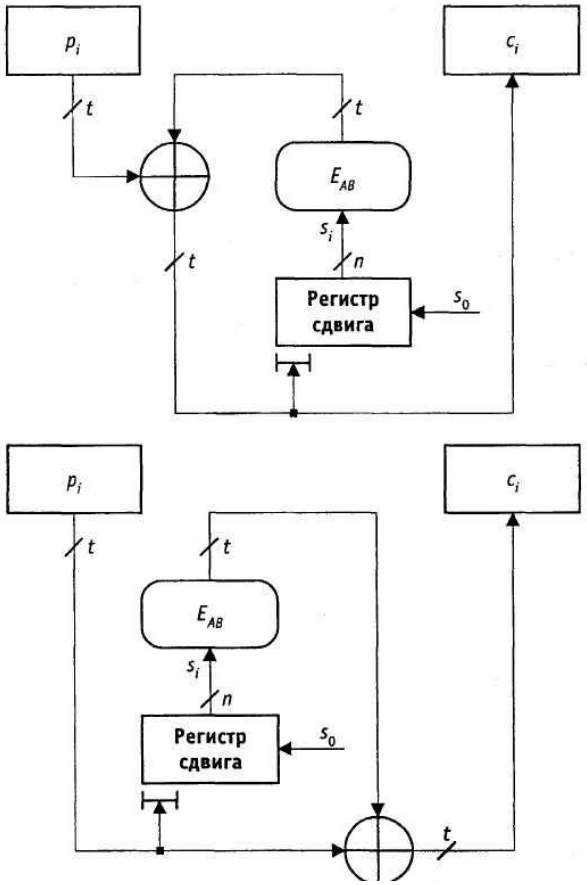


Рисунок 2.24. Режим шифрования CFB: а - зашифрование, б - расшифрование

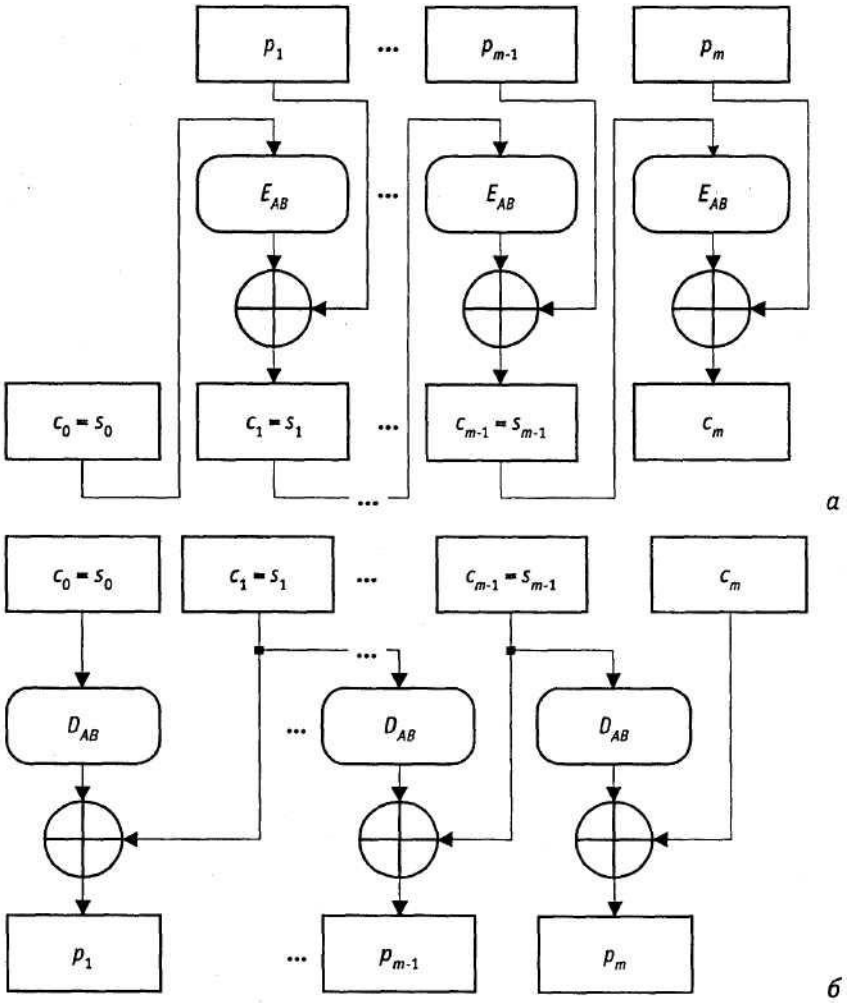


Рисунок 2.25 - Режим шифрования CFB (частный случай t = n):
а - зашифрование; 6 – расшифрование

Схема шифрования в режиме *обратной связи по выходу* (**Output Feedback** (**OFB**)) показана на рисунке 2.16. Гамма шифра снимается с выходного генератора псевдослучайных кодов, реализованного на основе n- разрядного регистра сдвига, в цепи обратной связи которого используется функция зашифрования E_{AB}.

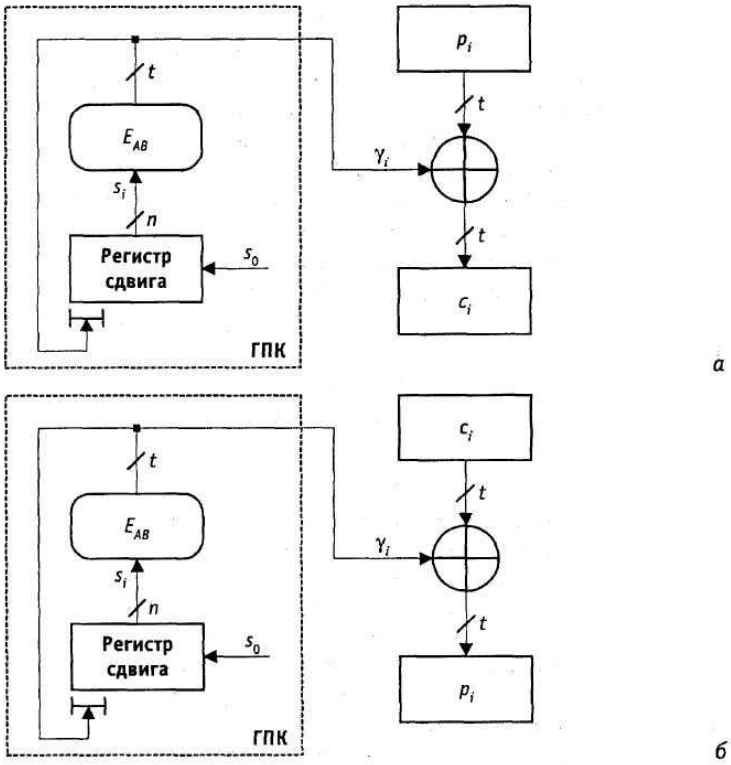


Рисунок 2.26 - Режим шифрования OFB: а – зашифрование, 6 - расшифрование

Уравнения зашифрования и расшифрования имеют вид:

$\mathbf{c_i = p_i \oplus \gamma_i,}$

$\mathbf{p_i = c_i \oplus \gamma i,}$

$\gamma_i = E_{AB}^{(t)}(s_{i-1}),$

$s_i = \left(2^t \cdot s_{i-1} + c_i\right) \bmod 2^n,$

$i = \overline{1,m}$

где

γ_i – очередной элемент гаммирующей последовательности,

n – разрядность регистра сдвига,

t – разрядность шифруемых блоков данных **(1≤t≤n)**,

$\mathbf{s_0}$ – начальное состояние регистра сдвига (синхропосылка/вектор инициализации),

$E_{AB}^{(t)}(s_{i-1})$ - **t** старших битов **n**-разрядной шифрограммы $\mathbf{E_{AB}(s_{i-1})}$.

Последовательность $\gamma=\gamma_1\gamma_2\ldots\gamma_i\ldots\gamma_m$ не зависит от открытого текста и поэтому всякий раз при фиксированных k_{AB} и s_0 будет вырабатываться одна и та же гамма. Данный факт требует при шифровании на одном ключе двух различных массивов данных использовать различные синхропосылки.

Схема шифрования в режиме OFB при t = n показана на рисунке 2.17. Уравнения зашифрования и расшифрования принимают вид:

$\mathbf{c_i = p_i \oplus E_{AB}(s_{i-1}),}$

$\mathbf{p_i = c_i \oplus E_{AB}(s_{i-1}),}$

$\mathbf{s_i = E_{AB}(s_{i-1}),}$

$i = \overline{1,m}$

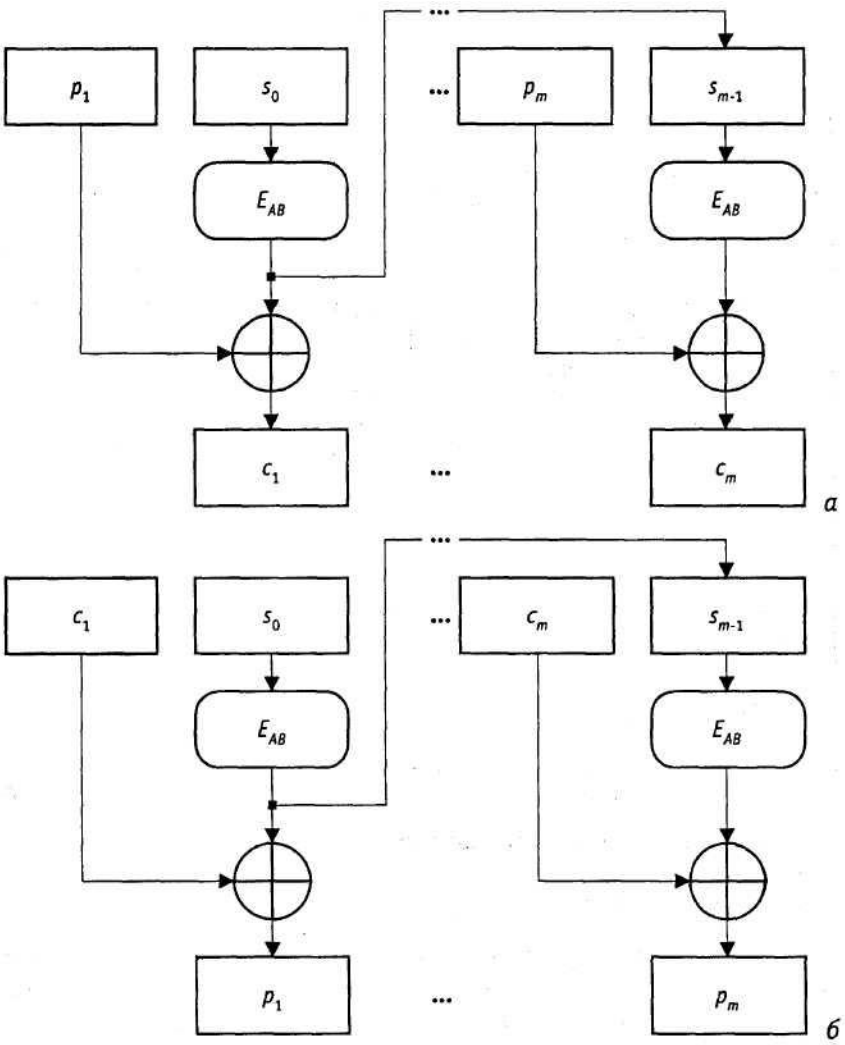


Рисунок 2.27 - Режим шифрования OFB (частный случай t = n):
а - зашифрование, 6 - расшифрование

Под *режимом шифрования* понимается такой алгоритм применения блочного шифра, который при отправке сообщения позволяет преобразовывать открытый текст в шифротекст и, после передачи этого шифротекста по открытому каналу однозначно восстановить первоначальный открытый текст. Как видно из определения сам блочный шифр теперь является лишь частью другого алгоритма – алгоритма режима шифрования. Это обусловлено тем, что блочный шифр работает только с отдельным *блоком* данных, в то время как алгоритм *режима шифрования* имеет дело уже с целым *сообщением*, которое может состоять из некоторого числа *n* блоков. Более того, сообщение вообще не обязано состоять из блоков, в том смысле, что это сообщение не всегда можно разбить на *целое* число *n* блоков. В этом случае в разных режимах шифрования приходиться дополнять сообщение различным количеством бит. Такое дополнение почти неизбежно, но минимальная величина, к которой нужно "подтянуть" длину сообщения различна для разных режимов шифрования и напрямую зависит от длины порции сообщения с которой работает каждая итерация алгоритма данного режима.

Сравнение алгоритмов шифрования ГОСТ 28147-89 и AES

Сравнительные характеристики алгоритмов ГОСТ и Rijndael приведены в следующей ниже таблице.

Таблица 2.5. Сравнительные характеристики алгоритмов ГОСТ28147-89 и Rijndael

Показатель	ГОСТ28147-89	Rijndael
Размер блока, бит	64	128, 192, 256[1]
Размер ключа, бит	256	128, 192, 256
Архитектура	Однородная сбаланси-рованная сеть Файстеля	«Квадрат» (Square)
Число раундов	32	10, 12, 14[2]

Показатель	ГОСТ28147-89	Rijndael
Часть блока, шифруемая за один раунд, бит	32 (полблока)	128, 192, 256 (полный блок)
Размер раундового ключевого элемента, бит	32 (половина размера блока)	128, 192, 256 (равен размеру блока)
Структура раунда	Простая	Более сложная
Используемые на раунде операции	Только аддитивные операции, подстановки и сдвиги	Широкое использование операций над конечными полями
Эквивалентность прямого и обратного преобразований.	С точностью до порядка следования ключевых элементов	С точностью до вектора ключевых элементов, узла замен и прочих констант алгоритма

В отличие от ГОСТа, размер шифруемого блока и размер ключа в алгоритме Rijndael могут изменяться, что допускается использованной в нем архитектурой «квадрат». Данное свойство позволяет варьировать стойкость и быстродействие алгоритма в зависимости от внешних требований к реализации в некоторых пределах, –однако, не очень широких, – число раундов, а вместе с ним и быстродействие, в крайних случаях различаются в 1.4 раза.

Сравнение общих архитектурных принципов

Криптоалгоритм ГОСТ 28147-89, как и большинство шифров «первого поколения», разрабатывавшихся в 70-е годы и в первой половине 80-х, базируется на архитектуре «сбалансированная сеть Файстеля» (balanced Feistel network). Основным принципом этой архитектуры является то, что весь процесс шифрования состоит из серии однотипных раундов. На каждом раунде шифруемый блок $\boldsymbol{T}$ делится на две части ($\boldsymbol{T}0,\boldsymbol{T}1$), одна из которых модифицируется путем побитового сложения по модулю 2 со значением, вырабатываемом из другой части и ключевого элемента раунда с помощью функции шифрования. Между раундами части блока меняются местами, и, таким образом, на следующем раунде текущий измененный блок станет неизменным и наоборот. Схема алгоритма шифрования по ГОСТ 28147-89 приведена на рисунке 1(а). Подобная архитектура позволяет легко получить обратимое криптографическое преобразование из сложной и, возможно необратимой, функции шифрования. Важной особенностью этого подхода является то, что за раунд шифруется ровно половина блока.

Шифр Rijndael имеет принципиально другую архитектуру, получившую название

«квадрат» (Square) по имени первого выполненного в ней шифра,– он был разработан теми же специалистами несколькими годами раньше. Эта архитектура базируется на прямых преобразованиях шифруемого блока, который представляется в форме матрицы байтов.

Зашифрование также состоит из серии однотипных шагов, раундов, однако на каждом раунде блок преобразуется как единое целое и не остается неизменных частей блока. Таким образом, за раунд шифруется полный блок, следовательно, для обеспечения сопоставимой сложности и нелинейности преобразования таких шагов требуется вдвое меньше по сравнению с сетью Файстеля. Каждый раунд заключается в побитовом сложении по модулю 2 текущего состояния шифруемого блока и ключевого элемента раунда, за которым следует сложное нелинейное преобразование блока, сконструированное из трех более простых преобразований, подробно рассмотренных в следующем разделе. Схема алгоритма Rijndael приведена ниже на рисунке.

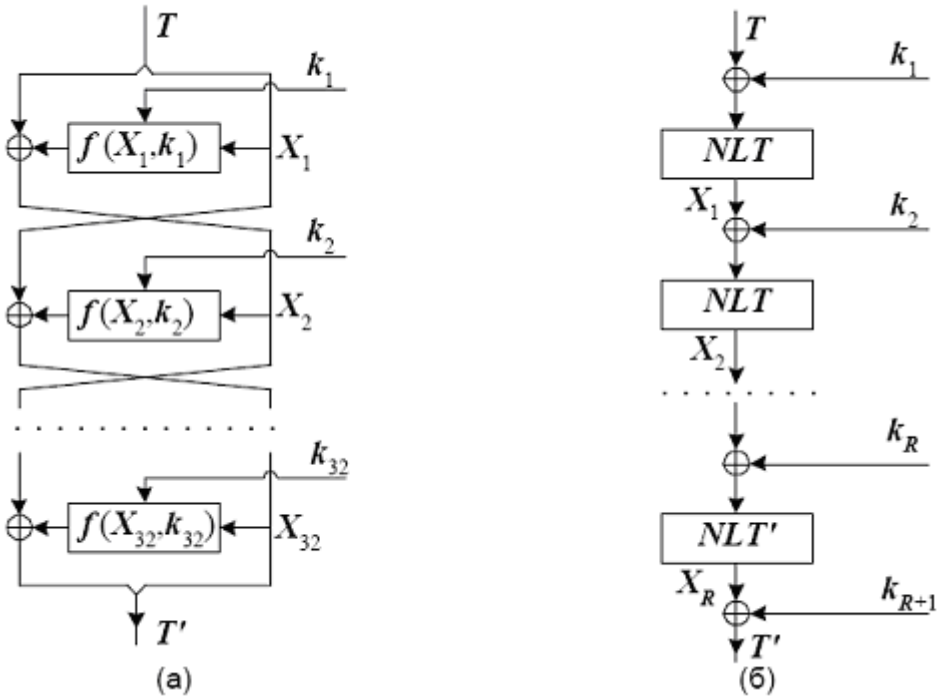


Рисунок 2.28. Схема преобразования данных при шифровании данных по алгоритмам ГОСТ28147-89 (а) и Rijndael (б)

На рисунке 2.18 использованны следующие обозначения:

T,T' – исходный и зашифрованный блоки соответственно;
k_i – ключевой элемент раунда;
X_i – состояние процесса шифрования после i-того раунда;
$f(X,k)$ – функция шифрования алгоритма ГОСТ28147-89;
NLT,NLT' – регулярное нелинейное преобразование и нелинейное преобразование последнего раунда алгоритма Rijndael соответственно;
R – число раундов в алгоритме Rijndael (10, 12 или 14).

Сравнение раундов шифрования

В алгоритме ГОСТ28147-89 используется сравнительно несложная функция шифрования, состоящая из аддитивной операции комбинирования входного полублока с ключевым элементом раунда – сложения их по модулю 232, подстановки, выполняемой независимо в восьми 4-битовых группах, и битовой перестановки – вращения на 11 бит в

сторону старших разрядов. Схема раунда шифрования по ГОСТ изображена на рисунке 2(а).

В Rijndael шифруемый блок и его промежуточные состояния в ходе преобразования представляются в виде матрицы байтов 4 _ ***n***, где ***n*** = 4,6,8 в зависимости от размера блока.

Функция нелинейного преобразования в алгоритме Rijndael состоит из трех следующих
элементарных преобразований, выполняемых последовательно:

байтовая подстановка – каждый байт преобразуемого блока заменяется новым значением, извлекаемым из общего для всех байтов матрицы вектора замены;

побайтовый циклический сдвиг в строках матрицы: первая строка остается неизменной,
вторая строка циклически сдвигается влево на один байт, третья и четвертая строка циклически сдвигаются влево соответственно на 2 и 3 байта для ***n*** = 4 или 6, и на 3 и 4 байта для ***n*** = 8;

матричное умножение – полученная на предыдущем шаге матрица умножается слева на следующую матрицу–циркулянт размера 4x4:

$$M = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix}.$$

При этом операции с элементами матриц (сложение и умножение) выполняются в конечном поле GF(28), порождаемом неприводимым над GF(2) полиномом ***m***(***x***) = ***x***8 + ***x***4 + ***x***3 + ***x*** + 1. В этом конечном поле сложение байтов выполняется как побитовое суммирование по модулю 2, а умножение – несколько более сложным способом. Схема раунда алгоритма Rijndael изображена на рисунке.

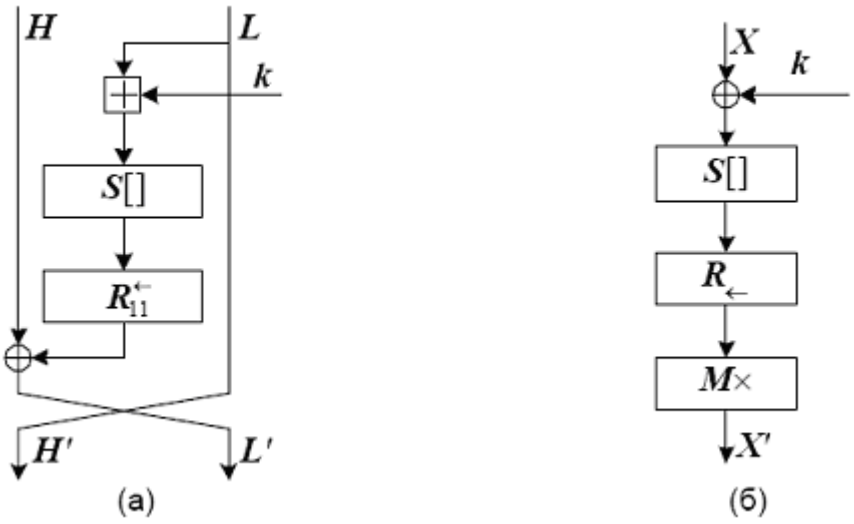


Рисунок 2.29. Схема преобразования данных для одного раунда шифрования по алгоритмам ГОСТ28147-89 (а) и Rijndael (б) соответственно

На рисунке 2.29 использованны следующие обозначения:

$X(H,L), X'(H',L')$ – преобразуемый блок (или его старшая и младшая части соответственно) на входе и на выходе раунда;

k – ключевой элемент раунда;

$S[]$ – функция подстановки, группами по 4 бита для ГОСТа и байтами для алгоритма Rijndael;

$R_{11}^{\leftarrow}$ – операция циклического сдвига (вращения) 32-битового слова на 11 бит в сторону старших разрядов;

$R_{\leftarrow}$ – операция построчного вращения матрицы алгоритма Rijndael;

$M\times$ – умножение матрицы данных слева на матрицу M в алгоритме Rijndael.

Показатели стойкости алгоритмов

Рассмотрим устойчивость обоих алгоритмов к известным видам криптоанализа. Наиболее универсальными и эффективными для алгоритмов широкого класса являются дифференциальный и линейный виды криптоанализа.

Дать оценку устойчивости алгоритма ГОСТ28147-89 к конкретным видам криптоанализа невозможно без спецификации узлов замен, так как качество этого шифра существенным образом зависит от качества использованных узлов. Однако исследования близких по архитектуре шифров с заданными таблицами подстановок (DES) показали, что криптоанализ шифра с 16 раундами в принципе осуществим, однако требует очень большого числа исходных данных, а при 20-24 раундах становится теоретически бесполезным. ГОСТ предусматривает 32 раунда шифрования, и этого количества хватает с запасом, чтобы успешно противостоять указанным видам криптоанализа. В открытой печати отсутствуют сообщения об успешном вскрытии ГОСТа с какими-либо узлами замен, – как с тестовыми, специфицированными в стандарте ГОСТ Р34.11-94, так и с теми, с которыми реализации ГОСТа поставлялись в коммерческие организации.

По оценкам разработчиков шифра Rijndael, уже на четырех раундах шифрования этот алгоритм приобретает достаточную устойчивость к указанным видам криптоанализа. Теоретической границей, за которой линейный и дифференциальный виды криптоанализа теряют смысл, является рубеж в 6-8 раундов в зависимости от размера блока. Согласно спецификации, в шифре предусмотрено 10-14 раундов. Следовательно, шифр Rijndael также устойчив к указанным видам криптоанализа с определенным запасом.

Таким образом, оба сравниваемых шифра обладают достаточной стойкостью к известным видам криптоанализа. В печати отсутствуют какие-либо сведения об успешных случаях вскрытия указанных шифров, а также описания процедур, которые теоретически позволили бы дешифровать сообщение с меньшими вычислительными затратами, чем полный перебор по всему ключевому пространству.

Производительность и удобство реализации

При оценке достижимой эффективности аппаратной реализации шифров главным критерием является количество и сложность элементарных операций, которые необходимо выполнить в цикле шифрования, а также возможность их параллельного выполнения. При оценке эффективности возможных программных реализаций главный интерес представляет реализация на 32-битовых платформах, так как 32-разрядные машины составляют в настоящее время большинство компьютерного парка человечества. Также представляет интерес реализация шифров на 8-битовых микроконтроллерах, являющихся основой технологии интеллектуальных карт. Подобные устройства могут использоваться в различных системах безналичных расчетов, становящихся все более популярными в мире, – число

пользователей таких систем в последнее время растет весьма быстрыми темпами.

Российский стандарт шифрования ГОСТ 28147-89 удобен как для аппаратной, так и для программной реализации. При размере блока данных 64 бита, основная работа ведется с половинками этого блока – 32-битовыми словами, что позволяет эффективно реализовать российский стандарт шифрования на большинстве современных компьютеров.

При реализации на 32-битовых машинах наиболее трудоемкой операцией является замена. Предусмотренные ГОСТом подстановки в 4-битовых группах при программной реализации удобно попарно объединить и выполнять замену в 8-битовых группах, что существенно эффективнее. Надлежащая организация замены позволяет также избежать выполнения вращения слова на выходе функции шифрования, – если хранить узлы замены как массивы 4-байтовых слов, в которых уже выполнены необходимые сдвиги. Такая «раздутая» таблица замен потребует для своего хранения 4 _ 28 _4 = 212 байт или 4K оперативной памяти. Одна замена реализуется за три однотактовые машинные команды: загрузка байта в индексный регистр, загрузка заменяющего значения в регистр, использование загруженного значения в операции побитового суммирования. В итоге перечисленные шаги оптимизации позволяют реализовать раунд шифрования по ГОСТ за 15 однотактовых машинных команд. С учетом возможности процессоров Intel Pentium по параллельному выполнению команд, раунд ГОСТа может быть реализован за 8 тактов работы процессора, а весь процесс шифрования – за 32 _ 8 = 256 тактов. На процессоре Intel Pentium 200 это позволит достичь предела быстродействия шифрования примерно 6.0 Мбайт/с, в реальности эта величина будет меньше.

ГОСТ может быть также эффективно реализован на 8-битовых микроконтроллерах, поскольку составляющие его элементарные операции входят в систему команд большинства наиболее распространенных контроллеров. При этом суммирование по модулю 232 придется разделить на одну операцию сложения без переноса, и три операции сложения с переносом, выполняемые каскадно. Все остальные операции также легко могут быть представлены в терминах 8-байтовых операндов.

При аппаратной реализации ГОСТа один раунд предполагает последовательное выполнение трех операций над 32-битовыми аргументами: суммирование, выполняемая одновременно замена во всех восьми 4-битовых группах и побитовое суммирование по модулю 2. Циклический сдвиг не является отдельной операцией, т.к. обеспечивается простой коммутацией проводников. Таким образом, при аппаратной реализации цикл шифрования требует выполнения ста шести элементарных операций, и эта работа не может быть распараллелена.

Теперь рассмотрим особенности реализации алгоритма Rijndael. Этот алгоритм является байт-ориентированным, т.е. полностью может быть сформулирован в терминах операций с байтами. В алгоритме широко используются алгебраические операции в конечных полях, наиболее сложно реализуемой из которых является умножение в GF(28). Непосредственное выполнение этих операций привело бы к крайне неэффективной реализации алгоритма. Однако байтовая структура шифра открывает широкие возможности по оптимизации программной реализации. Замена байта по таблице с последующим умножением на константу в конечном поле GF(28) может быть представлена как одна замена по таблице. В прямом шифре используются три константы (01, 02, 03), и, следовательно, понадобятся три таких таблицы, в обратном – четыре (0E, 0D, 0B, 09). При надлежащей организации процесса шифрования построчный байтовый сдвиг матрицы данных можно не выполнять. При реализации на 32-битовых платформах возможно реализовать байтовую замену и умножение элемента матрицы данных на столбец матрицы $\boldsymbol{M}$ как одну замену 8 бит на 32 бита. Таким образом, преобразование одного 32-битового слова данных включает четыре байтовые замены, каждая из которых, как было отмечено выше, требует трех однотактовых машинных команд. В итоге часть раунда для одного 32-битового слова может быть реализована на процессорах Intel Pentium за 14 команд или за 7 тактов, что при 14 раундах шифрования позволяет на процессорах Intel Pentium 200 достичь теоретического

предела быстродействия примерно 7.8 Мбайт/с вне зависимости от размера блока данных и ключа. Для меньшего числа раундов скорость пропорционально возрастет.

Указанная выше оптимизация потребует, однако, определенных расходов оперативной памяти. Для каждого столбца матрицы ***M*** строится свой вектор замены одного байта на 4-байтовое слово, получаем точно такую же по размеру, как и в случае ГОСТ, таблицу замен, ее размер равен 4 _ 28 _4 = 212 байт или 4K. Далее, таблицы, используемые при зашифровании и расшифровании, различны, – это удваивает требования к оперативной памяти. Кроме того для выполнения последнего раунда расшифрования нужен отдельный узел замен, его размер равен 256 байт или 0.25K. В итоге получаем, что для 32-битовых программных реализаций шифра Rijndael необходимо 8.25 Кбайт оперативной памяти для хранения узлов замен. Для современных компьютеров на базе Intel Pentium под управлением ОС Windows 9x/NT/2000 это не выглядит чрезмерным требованием.

Байт-ориентированная архитектура алгоритма Rijndael позволяет чрезвычайно эффективно реализовать его на 8-битовых микроконтроллерах, используя только операции загрузки-выгрузки регистров, индексированного извлечения байта из памяти и побитового суммирования по модулю два. Также указанная особенность позволит выполнить эффективную программную реализацию алгоритма. Раунд шифрования требует выполнения 16 байтовых замен плюс четыре операции побитового исключающего или над 128-битовыми блоками, которые могут быть выполнены в три этапа. В итоге получаем 4 операции на раунд или 57 операций на 14-раундовый цикл шифрования с учетом «лишней» операции побитового прибавления ключа по модулю два – это примерно вдвое меньше, чем в ГОСТе.

Так как Rijndael обладает вдвое большим размером блока, это приводит к примерно четырехкратному преимуществу в скорости при условии аппаратной реализации на базе одной и той же технологии. Необходимо заметить, что указанная выше оценка является очень грубой.

Таблица 2.6. Показатели быстродействия реализаций сравниваемых алгоритмов на языке Си

	ГОСТ 28147-89	**Rijndael, 14 раундов**
Pentium 166	2.04 Мбайт/с	2.46 Мбайт/с
Pentium III 500	8.30 Мбайт/с	9.36 Мбайт/с

Что касается аппаратной реализации, то в отличие от ГОСТа, Rijnael позволяет достичь высокой степени параллелизма при выполнении шифрования, оперирует блоками меньшего размера и содержит меньшее число раундов, в силу чего его аппаратное воплощение может оказаться существенно более быстрым. Если судить по длине наибольшего пути в сетевом представлении обоих алгоритмов, его преимущество примерно четырехкратное.

Описание аппаратно-программного комплекса

Описание ADSP-TS101 – TigerSHARC

Цифровой Сигнальный Процессор ADSP-TS0101 - TigerSHARC™ является первым DSP компании Analog Devices, построенным по новой статической суперскалярной архитектуре. Процессор TigerSHARC™ создан для применения в оборудовании телекоммуникационной инфраструктуры и предлагает новый высочайший уровень интеграции и уникальную возможность обрабатывать 8-, 16-, 32-разрядные типы данных с фиксированной и плавающей точкой, используя одну микросхему. Каждый из этих типов

данных является важным для следующего поколения телекоммуникационных протоколов, находящихся в разработке, включая IMT-2000 (также известного под названием радиопротокола третьего поколения) и xDSL (цифровая абонентская линия). В отличии от всех других DSP, процессор ADSP-TS101 имеет уникальную способность увеличивать скорость обработки в зависимости от типа данных. Более того, кристалл обеспечивает высочайший уровень производительности при обработке данных с плавающей точкой.

В оборудовании телекоммуникационной инфраструктуры протоколы вокодера и канального кодера разработаны для 16-разрядного типа данных. Для улучшения качества сигнала многие телекоммуникационные приложения используют линейную коррекцию и технологию подавления эхо-сигналов, что существенно улучшает качество сигнала и характеристики системы. Эти алгоритмы выигрывают, благодаря увеличению точности обработки при применении 32-разрядных данных и данных с плавающей точкой. Поддержка 8-ми разрядного формата данных удобна при реализации часто используемого алгоритма декодера Витерби и при обработке изображений, где RGB сигналы, представляющие основные цвета, принято представлять 8-разрядными данными. Многие из этих приложений требуют высокого уровня производительности и могут предполагать использование алгоритмов, работающих последовательно или даже одновременно. Точные требования определяются конкретными приложениями. Гибкость архитектуры процессора TigerSHARC позволяет разработчикам программного обеспечения выполнять требования по точности, необходимые в том или ином приложении, без каких-либо потерь эффективности работы системы в целом. При использовании процессоров TigerSHARC производительность системы определяется применяемым форматом данных.

Архитектура процессоров TigerSHARC охватывает ключевые элементы целого ряда различных видов микропроцессоров. Это RISC (Reduced Instruction Set Computer), VLIW (Very Long Instruction Word) и DSP для получения наиболее эффективного цифрового сигнального процессора. Новая архитектура поддерживает на высоком уровне такие параметры, присущие DSP процессорам, как короткий машинный цикл с детерминированной длительностью, быстрая реакция на прерывания и отличный интерфейс с периферийными устройствами для поддержки высокой производительности вычислений и высокой скорости ввода и вывода данных. Чтобы достичь наиболее высоких результатов в работе ядра процессора, предусмотрены такие свойства RISC-архитектуры, как операции одновременной загрузки и сохранения данных, устройство управления выполнением команд с глубоким конвейером и предсказанием переходов, большой регистровый файл для передачи данных между вычислительными блоками. Кроме того, использование особенностей архитектуры VLIW позволяет более эффективно использовать программную память, особенно при реализации алгоритмов, характерных для задач управления.

Основные особенности архитектуры процессора TigerSHARC®

Ядро

1200 MMAC/c на частоте 150 МГц -16 бит
с фиксированной точкой

300 MMAC/c на частоте 150 МГц - 32 бита
с плавающей точкой

900 MFLOPS - 32 бита с плавающей точкой

Память

6 Мбит встроенной SRAM, организованные как единая память
в отличие от традиционной Гарвардской архитектуры

Средства ввода-вывода, периферийные устройства и корпус

Скорость передачи данных через внешнюю шину 600 Мбайт/с

Суммарная скорость передачи данных через 4 порта связи 600
Мбайт/с

Поддержка многопроцессорной кластерной системы до

8 процессоров ADSP-TS101 без дополнительных микросхем

4 порта ввода/вывода общего применения

Контроллер динамической памяти SDRAM

Чтобы обеспечить все функциональные блоки командами, необходимо эффективно использовать доступную ширину слова команды. Иначе говоря, многофункциональные команды должны подаваться на вычислительные блоки одновременно и параллелизм выполнения операций должен планироваться заранее, до непосредственного выполнения программы.

Архитектура ядра процессора Tiger SHARC показана на рисунке. Ядро включает несколько функциональных блоков: вычислительные блоки, память, АЛУ для операций с целыми числами и устройство для управления выполнением команд. В архитектуре процессора Tiger SHARC предусмотрены вычислительные блоки X и Y, каждый из которых содержит умножитель, АЛУ и 64-разрядное устройство сдвига. Благодаря ресурсам этих блоков, процессор может выполнять восемь 40-разрядных операций умножения с последующим суммированием 16-разрядных данных, две 40-разрядных операции умножения с последующим суммированием 16-разрядных комплексных чисел или две 80-разрядные операции умножения с последующим суммированием 32-разрядных даннымх. Все перечисленные операции выполняются в одном цикле. Процессор TigerSHARC реализует архитектуру, использующую полностью ортогональный регистровый файл длиной в 32 слова, допускающий чтение и запись в одном машинном цикле.

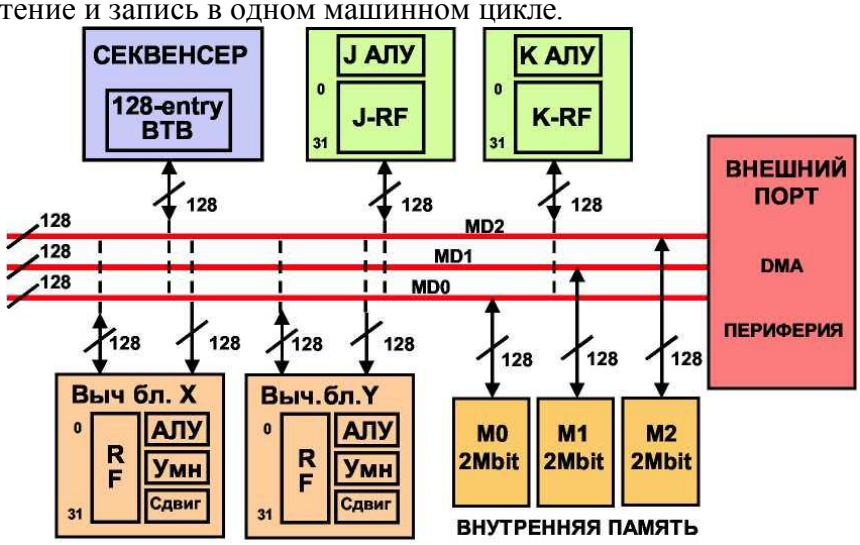


Рисунок 2.30. Структурная схема архитектуры процессора ADSP-TS101 TIGERSHARC

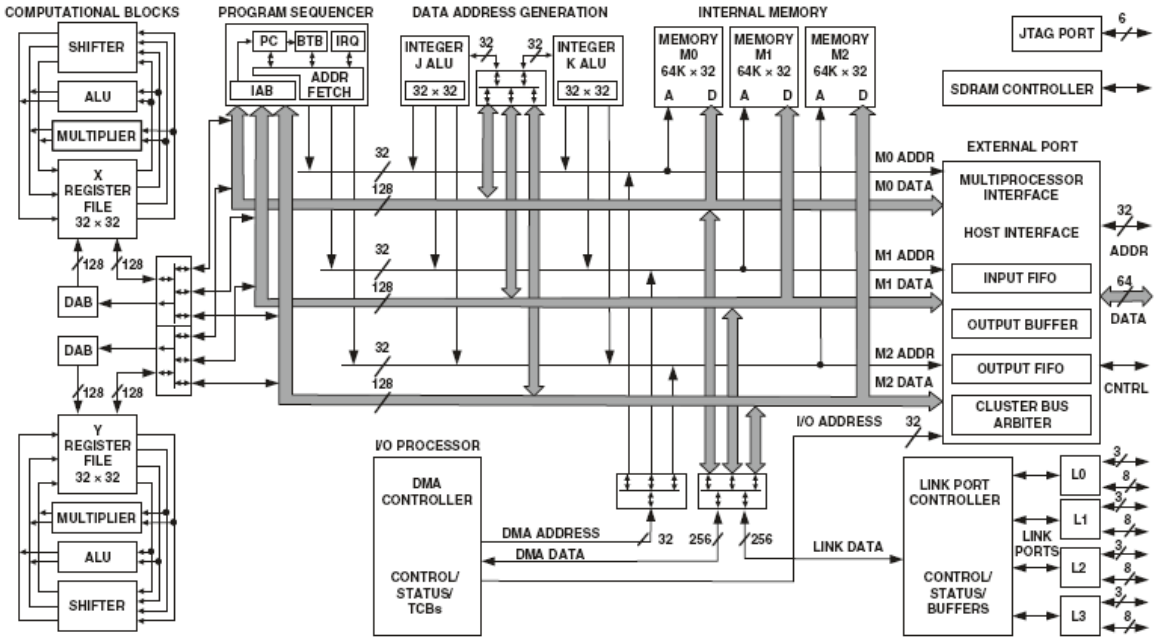


Рисунок 2.31. Функциональная схема архитектуры процессора ADSP-TS101 TIGERSHARC

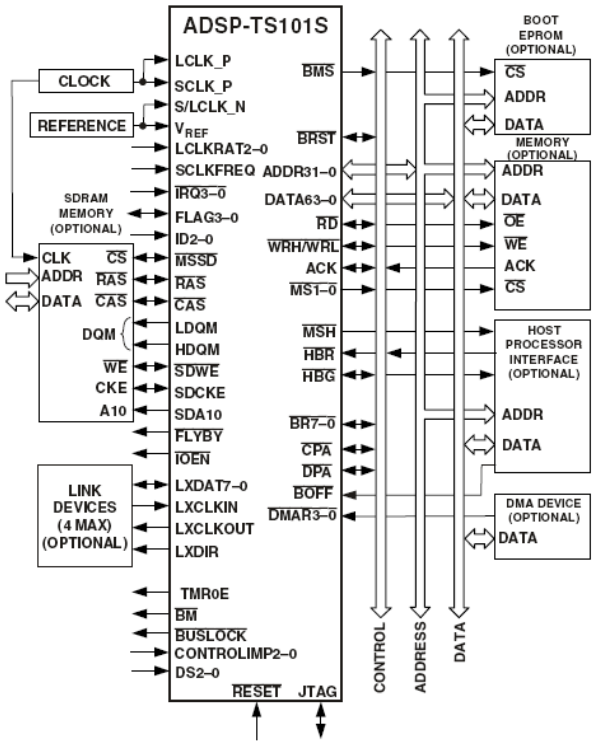


Рисунок 2.32. Однопроцессорная система с внешней памятью SDRAM

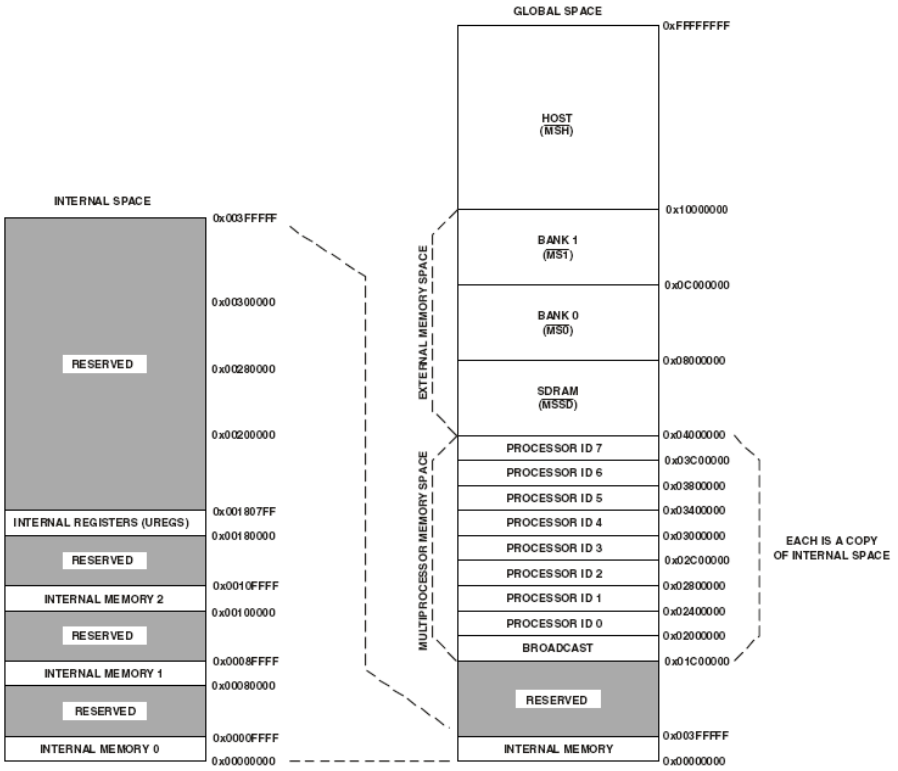


Рисунок 2.33. Организация памяти процессора ADSP-TS101

В архитектуре процессора TigerSHARC векторная организация памяти представлена в виде трех 128 разрядных блоков. При обращении к памяти из нее могут читаться учетверенные, длинные и нормальные слова, которые заносятся затем в регистровый файл для обработки. В каждом цикле может выполняться выборка четырех 32-разрядных команд. Одновременно могут быть загружены в регистровые файлы или записаны в память 256 битов данных. Данные с длиной слова 8, 16 или 32 разряда могут записываться в память последовательно в упакованном виде. Внутренняя и внешняя память организованы в виде единого адресного пространства, которое оставляет полную свободу программисту для распределения памяти. При работе на тактовой частоте 150 МГц скорость обмена с внутренней памятью для данных и команд составляет 7,2 Гбит/с.

Два АЛУ, выполняющие операции с целыми числами, используются для адресации данных и вычисления значений указателей. Они поддерживают циклические буферы и бит-реверсивную адресацию, причем каждое имеет свой регистровый файл длиной 32 слова. Рассматриваемые АЛУ не просто являются блоками, генерирующими адреса данных, но и могут совместно осуществлять вычисления с целыми числами. Наличие АЛУ такого вида позволяет существенно улучшить эффективность компилятора, разрабатываемого для данного процессора, а также повысить гибкость программирования.

Архитектура процессоров TigerSHARC называется *статической суперскалярной архитектурой,* т.к. она предполагает выполнение до четырех 32-разрядных команд за один цикл, и программист имеет возможность независимо задавать команды для всех вычислительных блоков. Устройство управления выполнением команд (program sequencer) поддерживает последовательное исполнение команд, при котором каждая очередная инструкция выполняется в соответствии с результатом предварительно заданного условия. Кроме того, одна и та же команда может быть выполнена двумя вычислительными блоками одновременно с использованием различных значений данных (это называется SIMD - одна инструкция - двойной набор данных).

Архитектура процессоров TigerSHARC позволяет выполнять операции над 8-, 16- и 32-разрядными данными. Производительность процессора повышается по мере уменьшения

разрядности обрабатываемых данных.

Добавление буфера адресов перехода (Branch Target Buffer, BTB) и логики статического предсказания перехода делает ненужным заполнение конвейера команд после перехода. Как отмечалось раньше, переход осуществляется за один цикл.

Три внутренних 128-разрядных шины образуют быстродействующий канал обмена данными между внутренними функциональными блоками и внешними периферийными устройствами. Трехшинная структура отвечает типовым математическим командам, требующим наличия двух исходных данных и на выходе выдают один результат. Процессор имеет ортогональную программную модель и обеспечивает детерминированную реакцию на прерывания.

Архитектура процессора TigerSHARC основана на различных режимах работы аппаратуры. Это позволяет избежать потери циклов и упрощает работу компилятора. Система команд непосредственно поддерживает все числовые форматы, применяемые в ЦОС и в обработке изображений и видеосигналов, включая знаковый и беззнаковый, дробный и целочисленный. Во всех случаях существует возможность ограничения или усечения результатов вычислений.

Работая на тактовой частоте 150 МГц, процессор ADSP-TS101 обеспечивает наилучшую производительность среди процессоров семейства SHARC как при обработке данных с фиксированной точкой, так и при работе с данными в формате с плавающей точкой. Кроме того, разместив на кристалле 6 Мбит статической памяти, компания Analog Devices увеличила степень интеграции памяти на 50% по сравнению с предыдущими членами семейства SHARC. При переходе к меньшим проектным нормам при производстве кристаллов, компания Analog Devices планирует увеличить тактовую частоту работы процессора и объем памяти на кристалле для новых представителей семейства TigerSHARC.

Основные свойства TigerSHARC

Выполнение от 1 до 4 32-разрядных операций за цикл

Принцип "Одна инструкция, много данных" (SIMD) поддерживается двумя вычислительными блоками

Поддержка разных форматов данных вычислительными блоками

В каждом имеется регистровый файл, MAC, АЛУ, устройство сдвига

Работа с 32/40-разрядными данными с плавающей точкой

и с 32-разрядными данными с фиксированной точкой (6 операций за один такт)

16-битные операции (24 за цикл) или 8-битные операции (32 за цикл)

Логика статического предсказания переходов, с целевым буфером перехода (BTB), поддерживающим до 128 входов

Внутренняя пропускная способность 7.2 Гбайт/с

Простая программная модель с гибкой системой прерываний

Применение процессоров ADSP-TS101 уменьшает общую стоимость материалов при проектировании системы, благодаря наличию интегрированных функций ввода-вывода набора периферийных устройств, которые уменьшают или вообще ликвидируют потребность в применении вспомогательных и дополнительных аппаратных средств. Работая на тактовой частоте 150 МГц, процессор ADSP-TS101 объединяет четыре порта связи со скоростью передачи 600 Мбит/с, средства поддержки мультипроцессорного кластера с возможностью подключения до восьми процессоров ADSP-TS101, контроллер динамической памяти и интерфейс JTAG. Данная, не имеющая аналогов комбинация возможностей реализована в 35x35 мм корпусе SBGA с 360 выводами.

При программировании цифровых сигнальных процессоров приходится работать как

на языке высокого уровня, так и на языке низкого уровня, то есть на ассемблере. Выбор языка зависит от целого ряда факторов, включающих требуемую скорость выполнения программы, размер используемой памяти и время, затрачиваемое на разработку программного обеспечения. Таким образом, система, предназначенная для цифровой обработки сигналов, должна давать пользователю возможность программировать как на языках высокого, так и на языках низкого уровня. Архитектура процессора TigerSHARC в точности отвечает этим требованиям.

Действительно, ядро процессора TigerSHARC включает 128 32-разрядных регистров общего назначения. Такое большое число регистров обеспечивает С-компилятору высокую степень гибкости при максимальном использовании в работе всего потенциала архитектуры. Для обеспечения целостности данных все регистры полностью синхронизированы, вследствии чего программисту не требуется контролировать детали, связанные с движением данных. Корректность использования данных при вычислениях контролируется аппаратно. Кроме того, доступ ко всем регистрам может осуществляться с использованием всех возможных режимов адресации (ортогональность), и все вычислительные команды имеют детерминированную задержку выполнения (2 цикла). Помимо прочего, архитектура процессора TigerSHARC включает буфер адресов перехода, в котором сохраняется эффективный адрес последних 128 переходов. Данный буфер облегчает программирование при заполнении конвейера команд после перехода. Как было показано раньше, архитектура позволяет осуществлять переход к следующей команде в одном цикле.

ОСНОВНЫЕ СВОЙСТВА ПРОЦЕССОРОВ TigerSHARC

128 регистров общего назначения

Все регистры полностью синхронизированы

Для адресации можно использовать целочисленное АЛУ общего применения

Предсказание переходов

Нет необходимости переключать аппаратные режимы

Ортогональные режимы адресации

Поддержка языка ассемблера

На рисунке представлена одна из возможных мультипроцессорных систем, построенная на процессорах TigerSHARC. До восьми процессоров ADSP-TS101 могут взаимодействовать напрямую через высокоскоростной 64-разрядный интерфейс внешней шины. При таком взаимодействии широко используемый протокол, построенный по принципу "ведущий - ведомый" (master-slave), позволяет любым двум процессорам непосредственно взаимодействовать в любой момент времени.

В дополнение к внешней шине, неограниченное число процессоров может взаимодействовать между собой через порты связи, которыми оснащен процессор ADSP-TS101. Взаимодействие через порты связи предоставляет большую гибкость при меньшей пропускной способности, чем при обмене через интерфейс внешней параллельной шины.

Следует еще раз упомянуть, что передача данных через порты связи выполняется отдельным процессором ввода-вывода и не требует вмешательства ЦПУ.

Если сложить пропускную способность портов связи (600 Мбит/с) и внешнего порта (600 Мбит/с), то получится суммарная пропускная способность процессора, составляющая 1200 Мбит/с при работе на тактовой частоте 150 МГц. К тому же следует отметить, что интерфейс, основанный на портах связи, как и параллельный интерфейс, не требует для своей реализации никаких дополнительных аппаратных средств.

Процессор ADSP-TS101 является первым представителем планируемого семейства продуктов, основанных на технологии TigerSHARC. Последующие представители семейства TigerSHARC будут характеризоваться оптимальным соотношением объемов встроенной памяти и периферийных устройств с точки зрения наиболее полного удовлетворения

требованиям специализированных рынков. Эти рынки включают базовые станции сотовых сетей третьего поколения, приложения VoIP (голос по протоколу Интернет), серверы и сетевые концентраторы. Ожидаемые усовершенствования в технологии и архитектуре процессора должны привести к двукратному улучшению базовых характеристик процессоров семейства TigerSHARC.

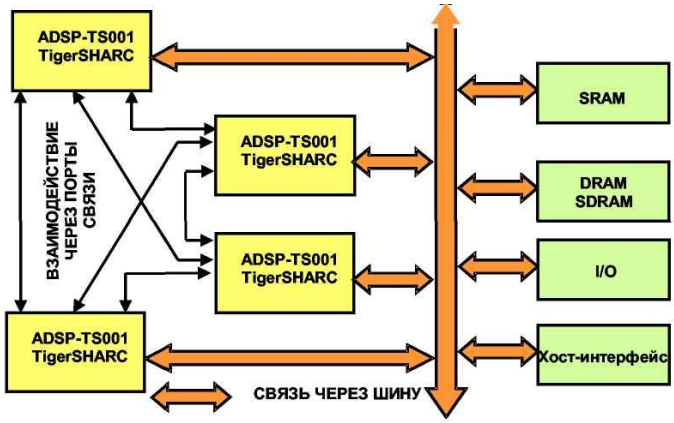


Рисунок 2.34 - Межпроцессорные коммуникации через порты чвязи и параллельную шину в многопроцессорной системе

Сравнение цифровых сигнальных процессоров, основанное только на таких характеристиках как MIPS, MOPS или MFLOPS, не дает полного представления о вычислительных возможностях процессоров. Полезнее сравнить работу ЦСП применительно к реализации специфических алгоритмов. БПФ и КИХ-фильтр, например, являются популярными эталонными тестами, также как и БИХ-фильтр, умножение матриц, деление и вычисление квадратного корня.

В таблицах показаны результаты тестов процессора ADSP-TS101 TigerSHARC, работающего с 16-разрядными данными с фиксированной точкой. На следующем рисунке представлены результаты обработки 32-разрядных данных с плавающей точкой.

Таблица 2.7. Производительность процессора ADSP-TS101 с тактовой частотой 150 МГц при работе с 16 – разрядными данными. (Пиковая производительность 1200 ММАС)

Алгоритм	Время исполнения	Необходимо циклов
256-точечное комплексное БПФ (по основанию 2)	7.3 мкс	1100
КИХ-фильтр с 50 коэффициентами при 1024 входных отсчетах	48 мкс	7200
Одно умножение с накоплением (MAC) в КИХ-фильтре	0.93 нс	0.14
Одно умножение с накоплением (MAC) комплексных чисел в КИХ-фильтре	3.80 нс	0.57
Одна операция "бабочка" при выполнении БПФ	6.7 нс	1.0

Таблица 2.8. Производительность процессора ADSP-TS101 с тактовой частотой 150 МГц при работе с 32 – разрядными данными. (Пиковая производительность 300 ММАС)

Алгоритм	Время исполнения	Необходимо циклов
1024-точечное комплексное БПФ (по основанию 2)	69 мкс	10300
КИХ-фильтр с 50 коэффициентами при 1024 входных отсчетах	184 мкс	27500
Одно умножение с накоплением (MAC) в КИХ-фильтре	3.7 нс	0.55
Одна операция "бабочка" при выполнении БПФ	13.3 нс	2.0
Одно умножение с накоплением (MAC) комплексных чисел в КИХ-фильтре	13.3 нс	2.0
Деление	20 нс	3.0
Квадратный корень	33.3 нс	5.0
Один шаг декодера Витерби (сложить/сравнить/выбрать)	3.3 нс	0.5

Аппаратная часть шифратора

Аппаратная часть шифропроцессора обычно представляет собой либо плату расширения для ПЭВМ (для шин ISA, PCI), либо отдельный автономный блок. В данной дипломной работе в качестве аппаратной части используется плата производства Analog Devices - ADSP-TS101S EZ-KIT Lite (Evaluation Kit for the TigerSHARC Processor)**.** Данная плата обрабатывать информацию может как автономно, так и с использованием для управления ПЭВМ. Данная плата является универсальным устройством позволяющим реализовывать различные устройства, например: цифровые фильтры, спектрографы, шифраторы и т.д.. Для этого в ее составе, помимо цифрового сигнального процессора, так же имеется: аналогово-цифровой преобразователь, цифро-аналоговый преобразователь, два вида памяти – SDRAM и Flash Memory (последняя имеет меньший размер и используется для хранения различных загрузочных модулей), различные разъемы – USB, Stereo Jack, JTAG Interface (с помощью него можно отлаживать работу платы через VisualDSP, установленной на компьютере), некоторое количество сигнальных светодиодов и переключателей и др.

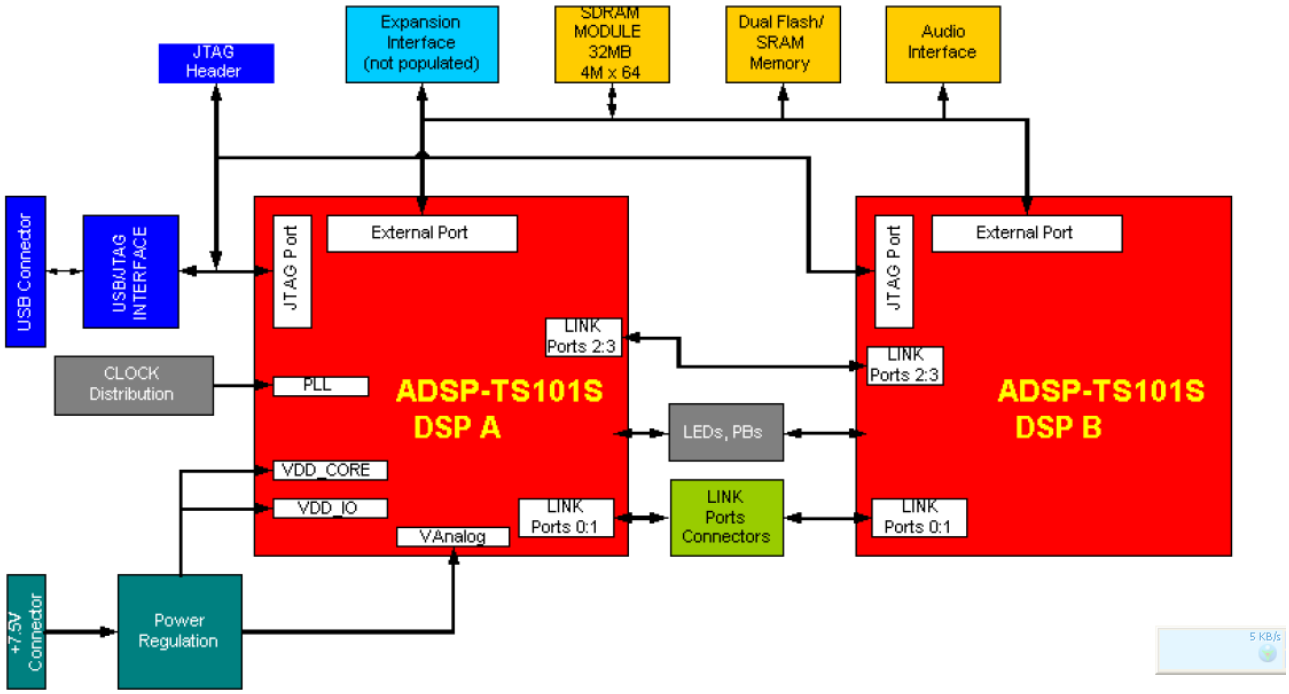


Рисунок 2.35. Архитектура платы EZ-KIT Lite

Но эта плата скорее должна использоваться только для моделирования шифраторов и изучения возможности конкретных алгоритмов шифрования. Аппаратный же шифратор - это аппаратное устройство с предустановленным микроядром ОС и ПО, существляющим базовый набор криптографических примитивов шифрование/дешифрование/ генерация ключевой пары и хеш функции) и процедуры более высокого уровня с их использованием, доступ к которым определятся стандартным интерфейсом. Кроме того реальный аппаратный шифратор отличается от данной платы тем, что имеет аппаратный датчик случайных чисел, что очень важно для любого алгоритма шифрования. В данной работе (с использованием платы Ezkit, которая не имеет аппаратного ДСЧ) такой датчик является псевдослучайным и эмулируется программно.

Физически, представляет собой внешнее или внутреннее устройство в защищенном от разрушения и схемотехнического копирования варианте. Оно имеет пользовательский и программный интерфейс.

Алгоритм использования ключей
Двухключевая схема шифрования

В данном алгоритме использования ключей для шифрования используется не один ключ, а два. Один из ключей (файловый) в этом случае используется для шифрования открытого файла, а другой (долговременный ключ пользователя) для шифрования файлового ключа.

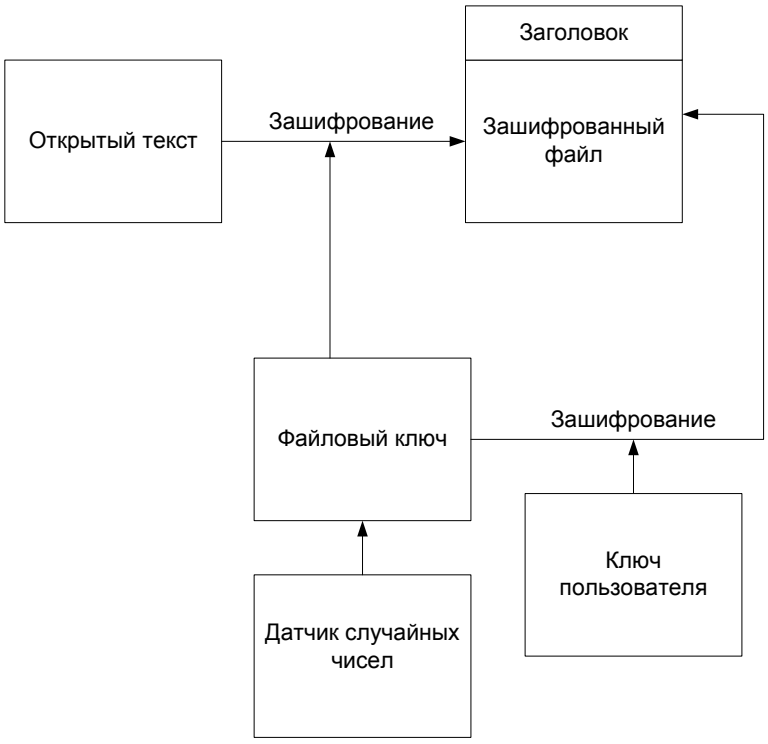


Рисунок 2.36. Двухключевая схема

Может показаться, что в данном случае нет логики в использовании файлового ключа: почему бы не шифровать файл непосредственно на долговременном ключе, не затрачивая время и ресурсы на генерацию, шифрование и передачу файлового? Однако использование файлового ключа преследует иные цели.

Во-первых, уменьшается статистическая нагрузка на долговременный ключ (т. е. долговременным ключом шифруются только короткие файловые ключи, а файловые ключи каждый раз разные) - это существенно снижает вероятность успеха тех атак на долговременный ключ, которые используют большие объемы зашифрованной на конкретном ключе информации.

Во-вторых, при перешифровании (плановом или при компрометации ключа) зашифрованного объекта с одного долговременного ключа на другой достаточно лишь перешифровать короткий файловый ключ, хранящийся в заголовке. Сам же объект может быть сколь угодно большим - например, весь логический диск компьютера. Не стоит пугаться сложности схем многоключевого шифрования - приведенные на них операции выполняются программами шифрования автоматически. Пользователь лишь указывает защищаемый файл и задает дополнительные параметры, например, на каком ключе или для какого пользователя нужно его шифровать.

Трехключевая схема шифрования

Аппаратные шифраторы должны поддерживать несколько уровней ключей шифрования. Обычно реализуется трехуровневая иерархия ключей: большее количество уровней, как правило, уже не дает заметного улучшения качества защиты, а меньшего может не хватить для ряда ключевых схем. Трехуровневая иерархия предусматривает использование сеансовых или пакетных ключей (1-й уровень), долговременных пользовательских или сетевых ключей (2-й уровень) и главных ключей (3-й уровень).

Каждому уровню ключей соответствует ключевая ячейка памяти шифропроцессора. При этом подразумевается, что шифрование данных выполняется только на ключах первого уровня (сеансовых или пакетных), остальные же предназначены для шифрования самих ключей при построении различных ключевых схем.

Трехуровневую схему лучше всего иллюстрирует упрощенный пример процесса шифрования файла (рис. 4). На этапе начальной загрузки в ключевую ячейку № 3 заносится главный ключ. Но для трехуровневого шифрования необходимо получить еще два. Сеансовый ключ генерируется в результате запроса к ДСЧ шифратора на получение случайного числа, которое загружается в ключевую ячейку № 1, соответствующую сеансовому ключу. С его помощью шифруется содержимое файла и создается новый файл, хранящий зашифрованную информацию.

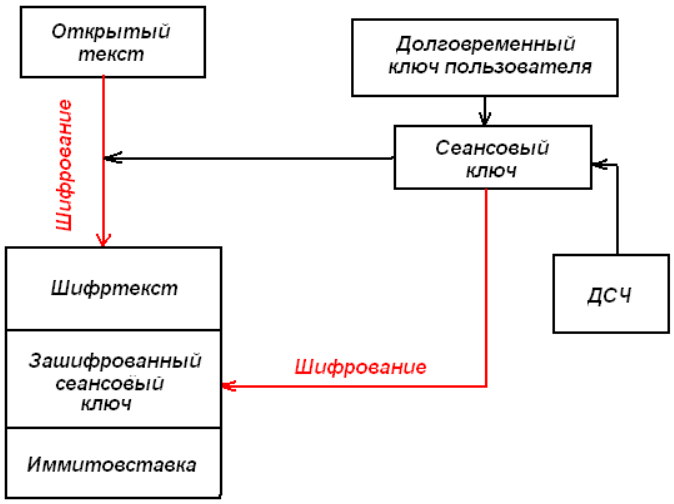


Рисунок 2.37. Шифрование файла по трехключевой схеме

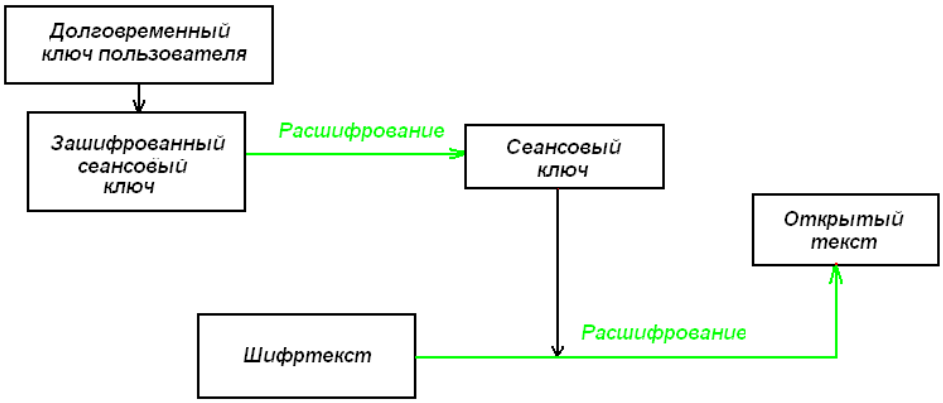


Рисунок 2.38. Дешифрование файла по трехключевой схеме

Далее у пользователя запрашивается долговременный ключ, который загружается в ключевую ячейку № 2 с расшифровкой посредством главного ключа, находящегося в ячейке № 3. Кстати, "серьезный" шифратор должен иметь режим расшифровки одного ключа с помощью другого внутри шифропроцессора; в этом случае ключ в открытом виде вообще никогда "не покидает" шифратора. И, наконец, сеансовый ключ зашифровывается при помощи долговременного ключа, находящегося в ячейке № 2, выгружается из шифратора и записывается в заголовок зашифрованного файла.

При расшифровке файла сначала с помощью долговременного ключа пользователя расшифровывается сеансовый ключ, а затем с его помощью восстанавливается информация.

В принципе можно использовать для шифрования и один ключ, но многоключевая схема имеет серьезные преимущества. Во-первых, снижается нагрузка на долговременный ключ - он используется только для шифрования коротких сеансовых ключей. А это усложняет потенциальному злоумышленнику криптоанализ зашифрованной информации с целью

получения долговременного ключа. Во-вторых, при смене долговременного ключа можно очень быстро перешифровать файл: достаточно перешифровать сеансовый ключ со старого долговременного на новый. И в-третьих, разгружается ключевой носитель - на нем хранится только главный ключ, а все долговременные ключи (а их может быть сколько угодно - для различных целей) могут храниться в зашифрованном с помощью главного ключа виде даже на жестком диске ПК.

Электронный замок

Чтобы улучшить соотношение функциональность/цена, аппаратные шифраторы оснащают различными дополнительными защитными функциями. Из них наиболее полезная и часто применяемая - функция "электронного замка", обеспечивающая ПК защиту от несанкционированного доступа и позволяющая контролировать целостность файлов операционной системы и используемых приложений.

Память каждого шифратора, работающего в режиме электронного замка, должна содержать следующую информацию, которая формируется администратором безопасности или аналогичным по функциям должностным лицом:

список пользователей, которым разрешен вход на защищаемый данным шифратором компьютер, и данные, необходимые для их аутентификации;

список контролируемых файлов с рассчитанным для каждого из них хэш-значением (кроме файлов операционной системы, в этот список могут входить любые другие файлы, например, шаблон Normal.dot, используемый по умолчанию текстовым процессором Microsoft Word);

журнал, содержащий список попыток входа на компьютер, как успешных, так и нет; в последнем случае - с указанием причины отказа в доступе.

В режиме начальной загрузки электронный замок шифратора прежде всего запрашивает у пользователя аутентификационную информацию. Обычно она хранится на том же ключевом носителе, что и главный ключ, и вводится в шифратор напрямую. В случае успешной аутентификации выполняется анализ целостности файлов согласно списку, хранимому в памяти шифратора (путем расчета хэш-значений файлов и сравнения их с эталонными). При нарушении целостности хотя бы одного из контролируемых файлов загрузка компьютера блокируется, а шифратор переходит в специальный режим работы - впредь вход на компьютер будет разрешен только администратору по безопасности, а обычным пользователям вход до "разбора полетов" и устранения несоответствия будет закрыт. Зафиксировав попытку входа в собственном журнале, шифратор возвращает компьютеру управление, что позволяет продолжить загрузку ОС. Однако электронный замок продолжает контролировать процесс загрузки, в частности, блокируя попытки загрузки с альтернативных носителей - дискеты или компакт-диска.

Формат зашифрованного объекта

Осталось сказать несколько слов о заголовке зашифрованного объекта. Очевидно, что необходим некий элемент, контролирующий правильность расшифрования объекта. Иначе при какой-либо ошибке расшифрования (например, при несовпадении параметров алгоритма, использовании неверного долговременного ключа и т. д.) невозможно будет понять, правильно ли расшифрованы данные (конечно, это не относится к случаю банального обмена зашифрованными текстовыми сообщениями, где корректность расшифрования можно проверить визуально). Такой элемент размещается в заголовке объекта, и обычно его роль выполняет имитоприставка (или любая другая контрольная сумма) исходных данных, вычисляемая на файловом ключе.

Имитоприставка вычисляется перед зашифрованием, записывается в заголовок, а после

расшифрования ее значение вычисляется повторно и сравнивается с хранящимся в заголовке. Кроме того, чтобы не расшифровывать весь объект, в его заголовке хранится и другая имитоприставка - файлового ключа, которая вычисляется на долговременном ключе перед зашифрованием файлового и проверяется после его /расшифрования, но (!) до расшифрования всего объекта. С помощью этой второй имитоприставки можно легко диагностировать большинство ошибок расшифрования на ранней стадии.

Итак, зашифрованный объект обычно содержит как минимум следующие данные:

собственно информация, зашифрованная на файловом ключе;
файловый ключ, зашифрованный на долговременном ключе;
имитоприставка файлового ключа на долговременном ключе;
имитоприставка исходных данных на файловом ключе.

Таким образом, трехключевая схема организации памяти представляет собой следующее:

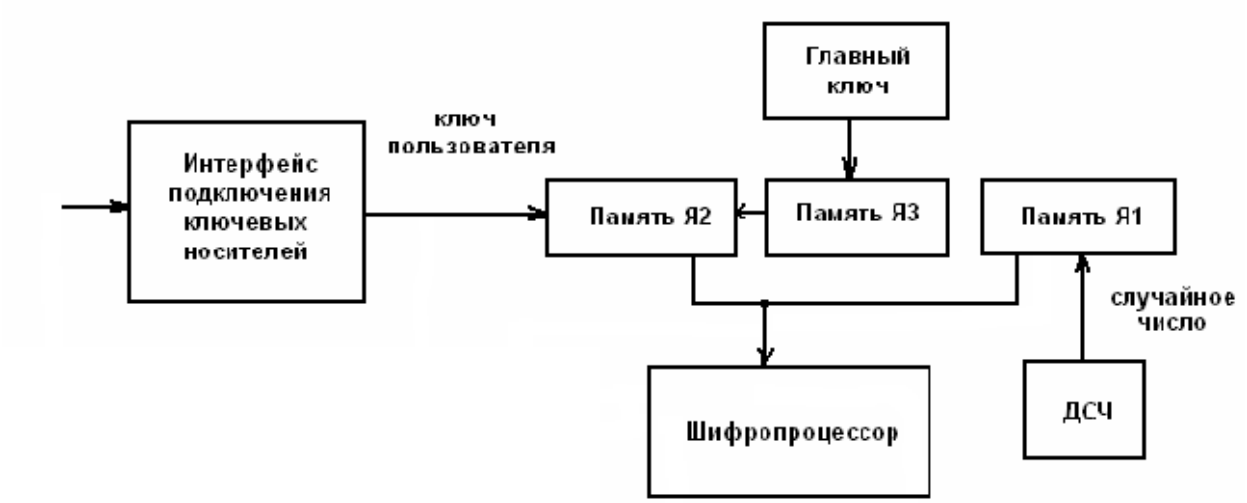


Рисунок 2.39. Трехключевая схема организации памяти

Требования к качеству ключевой информации и источники ключей

Не все ключи и таблицы замен обеспечивают максимальную стойкость шифра. Для каждого алгоритма шифрования существуют свои критерии оценки ключевой информации. Так, для алгоритма DES известно существование так называемых « ***слабых ключей*** », при использовании которых связь между открытыми и зашифрованными данными не маскируется достаточным образом, и шифр сравнительно просто вскрывается.

Исчерпывающий ответ на вопрос о критериях качества ключей и таблиц замен AES если и можно вообще где-либо получить, то только у разработчиков алгоритма. Соответствующие данные не были опубликованы в открытой печати. Однако согласно установленному порядку, для шифрования информации, имеющей гриф, должны быть использованы ключевые данные, полученные от уполномоченной организации. Косвенным образом это может свидетельствовать о наличии методик проверки ключевых данных на «вшивость». Если наличие слабых ключей в AES– дискуссионный вопрос, то наличие слабых узлов замены не вызывает сомнения. Очевидно, что «тривиальная» таблица замен, по которой любое значение заменяется им же самим, является настолько слабой, что при ее использовании шифр взламывается элементарно, каков бы ни был ключ.

Как уже было отмечено выше, критерии оценки ключевой информации недоступны, однако на их счет все же можно высказать некоторые общие соображения.

Ключ должен являться массивом статистически независимых битов, принимающих с равной вероятностью значения 0 и 1. Нельзя полностью исключить при этом, что некоторые конкретные значения ключа могут оказаться «слабыми», то есть шифр может не обеспечивать

заданный уровень стойкости в случае их использования. Однако, предположительно, доля таких значений в общей массе всех возможных ключей ничтожно мала. По крайней мере, интенсивные исследования шифра до сих пор не выявили ни одного такого ключа ни для одной из известных таблиц замен. Поэтому ключи, выработанные с помощью некоторого датчика истинно случайных чисел, будут качественными с вероятностью, отличающейся от единицы на ничтожно малую величину. Если же ключи вырабатываются с помощью генератора псевдослучайных чисел, то используемый генератор должен обеспечивать указанные выше статистические характеристики, и, кроме того, обладать высокой криптостойкостью, – не меньшей, чем у самого алгоритма шифрования. Иными словами, задача определения отсутствующих членов вырабатываемой генератором последовательности элементов не должна быть проще, чем задача вскрытия шифра. Кроме того, для отбраковки ключей с плохими статистическими характеристиками могут быть использованы различные статистические критерии. На практике обычно хватает двух критериев, – для проверки равновероятного распределения битов ключа между значениями 0 и 1 обычно используется критерий Пирсона, а для проверки независимости битов ключа – критерий серий. Об упомянутых критериях можно прочитать в учебниках или справочниках по математической статистике.

В случае же, когда необходимо выработать большой по объему массив ключевой информации, возможно и очень широко распространено использование различных программных датчиков псевдослучайных чисел.

Наилучшим же подходом для выработки ключей использование аппаратных датчиков СЧ.

Таблица замен является долговременным ключевым элементом, то есть действует в течение гораздо более длительного срока, чем отдельный ключ. Предполагается, что она является общей для всех узлов шифрования в рамках одной системы криптографической защиты. Даже при нарушении конфиденциальности таблицы замен стойкость шифра остается чрезвычайно высокой и не снижается ниже допустимого предела. Поэтому нет особой нужды держать таблицу в секрете, и в большинстве коммерческих применений так оно и делается. С другой стороны, таблица замен является критически важным элементом для обеспечения стойкости всего шифра. Выбор ненадлежащей таблицы может привести к тому, что шифр будет легко вскрываться известными методами криптоанализа. Критерии выработки узлов замен – тайна за семью печатями и ФАПСИ вряд ли ей поделится с общественностью в ближайшем обозримом будущем. В конечном итоге, для того, чтобы сказать, является ли данная конкретная таблица замен хорошей или плохой, необходимо провести огромный объем работ – многие тысячи человеко- и машино-часов. Единожды выбранная и используемая таблица подлежит замене в том и только в том случае, если шифр с ее использованием оказался уязвимым к тому или иному виду криптоанализа. Поэтому лучшим выбором для рядового пользователя шифра будет взять одну из нескольких таблиц, ставших достоянием гласности.

Криптографическая стойкость

При выборе криптографического алгоритма для использования в конкретной разработке одним из определяющих факторов является его стойкость, то есть устойчивость к попыткам противника его раскрыть. Вопрос о стойкости шифра при ближайшем рассмотрении сводится к двум взаимосвязанным вопросам:

можно ли вообще раскрыть данный шифр;

если да, то насколько это трудно сделать практически;

Шифры, которые вообще невозможно раскрыть, называются абсолютно или теоретически стойкими. Существование подобных шифров доказывается теоремой Шеннона, однако ценой этой стойкости является необходимость использования для шифрования каждого сообщения ключа, не меньшего по размеру самого сообщения. Во всех случаях за

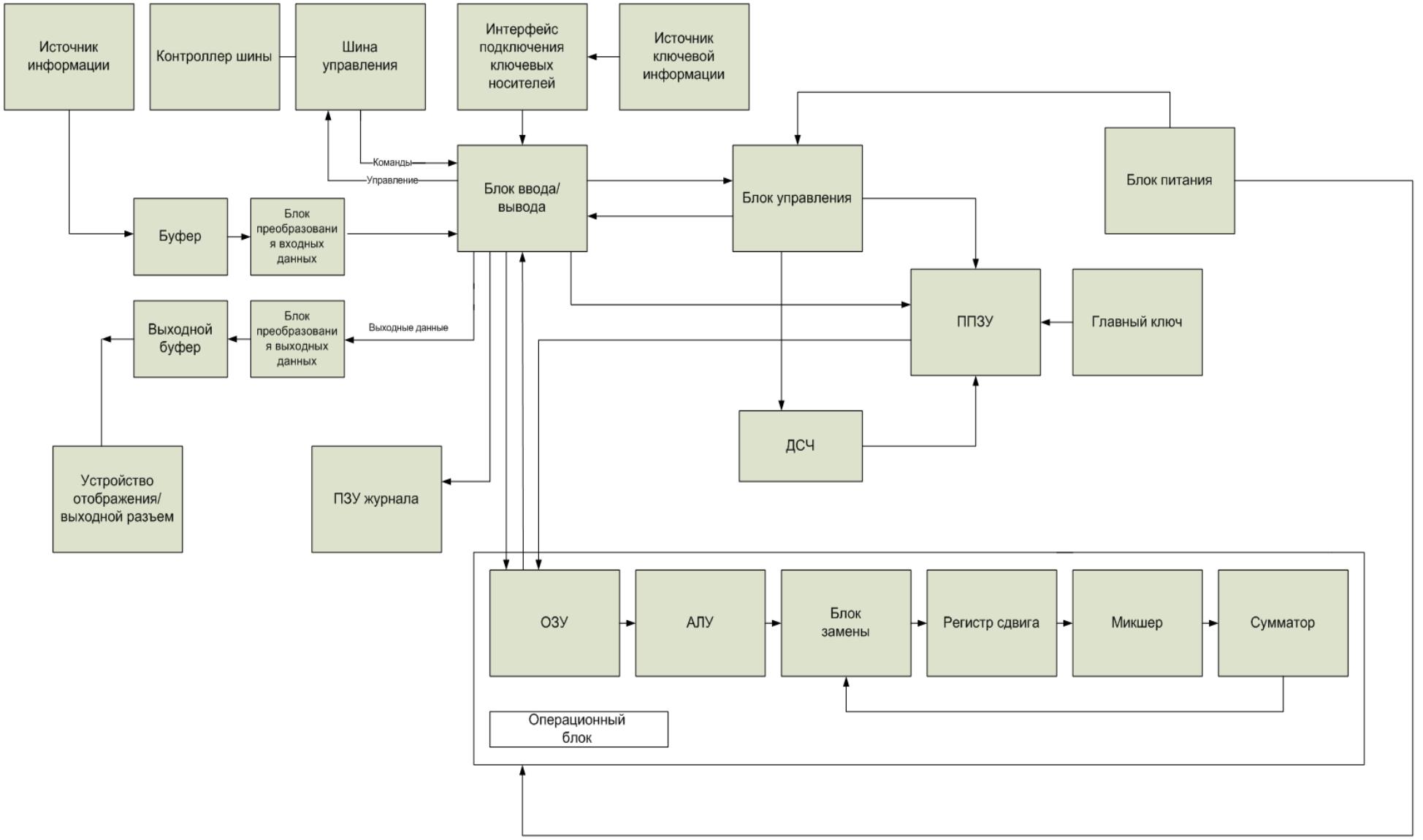
исключением ряда особых эта цена чрезмерна, поэтому на практике в основном используются шифры, не обладающие абсолютной стойкостью. Таким образом, наиболее употребительные схемы шифрования могут быть раскрыты за конечное время или, что точнее, за конечное число шагов, каждый из которых является некоторой операцией над числами. Для них наиважнейшее значение имеет понятие практической стойкости, выражающее практическую трудность их раскрытия. Количественной мерой этой трудности может служить число элементарных арифметических и логических операций, которые необходимо выполнить, чтобы раскрыть шифр, то есть, чтобы для заданного шифртекста с вероятностью, не меньшей заданной величины, определить соответствующий открытый текст. При этом в дополнении к дешифруемому массиву данных криптоаналитик может располагать блоками открытых данных и соответствующих им зашифрованных данных или даже возможностью получить для любых выбранных им открытых данных соответствующие зашифрованные данные – в зависимости от перечисленных и многих других неуказанных условий различают отдельные виды криптоанализа.

Все современные криптосистемы построены по принципу Кирхгоффа, то есть секретность зашифрованных сообщений определяется секретностью ключа. Это значит, что даже если сам алгоритм шифрования известен криптоаналитику, тот, тем не менее, не в состоянии расшифровать сообщение, если не располагает соответствующим ключом. Шифр считается хорошо спроектированным, если нет способа вскрыть его более эффективным способом, чем полным перебором по всему ключевому пространству, т.е. по всем возможным значениям ключа. AES, вероятно, соответствует этому принципу – за годы интенсивных исследований не было предложено ни одного результативного способа его криптоанализа. В плане стойкости он на много порядков превосходит прежний американский стандарт шифрования, DES.

Структурная схема шифратора

В состав шифратора входят:

Блок управления, как следует из его названия, служит для управления работой всего шифратора. Обычно он реализован на базе микроконтроллера. Шифропроцессор представляет собой специализированную микросхему или как в нашем случае DSP, который выполняет шифрование данных. Вообще говоря, УКЗД может иметь несколько шифропроцессоров, например, для взаимного контроля (путем сравнения "на лету" получаемых зашифрованных или открытых данных) и/или распараллеливания процесса шифрования. Для генерации ключей шифрования в устройстве предусмотрен аппаратный датчик случайных чисел (ДСЧ), вырабатывающий статистически случайный и непредсказуемый сигнал, преобразуемый затем в цифровую форму. Обмен командами и данными между шифратором и компьютером обеспечивается контроллером, обычно PCI (или другой системной шины в зависимости от интерфейса шифратора). Взаимодействие шифратора с системной платой ПК осуществляется через контроллер УКЗД. Для хранения ПО микроконтроллера необходима энергонезависимая память, реализованная на одной или нескольких микросхемах. Это же внутреннее ПЗУ используется для записи журнала операций и других целей.


Источник информации
Контроллер шины
Шина управления
Интерфейс подключения ключевых носителей
Источник ключевой информации
Команды
Управление
Блок ввода/ вывода
Блок управления
Блок питания
Буфер
Блок преобразования входных данных
Выходной буфер
Блок преобразования выходных данных
Выходные данные
ППЗУ
Главный ключ
ДСЧ
Устройство отображения/ выходной разъем
ПЗУ журнала
ОЗУ
АЛУ
Блок замены
Регистр сдвига
Микшер
Сумматор
Операционный блок

В состав операционного блока входят: ОЗУ – оперативное запоминающее устройство, которое хранит значение информационного блока открытого текта и шифртекста и ключевого блока для каждого раунда шифрования, блок замены, регистр сдвига, микшер, сумматор – это блоки отвечающие за соответствующие операции алгоритма шифрования.

Кроме того в состав входят блок преобразования входных и выходных данных, который служит для того чтобы из простой последовательности бит формировать блоки размером 128, 192 или 256 бит, которые заполняются данными сверху - вниз и слева – на право.

Программная часть шифратора

Еще три-четыре года назад реализовать свой алгоритм на DSP вы могли, лишь досконально изучив язык ассемблера конкретного процессора. Однако, развитие программных средств в последние годы привело к тому, что в настоящее время достаточно сложные задачи можно программировать на языках высокого уровня – на Си и даже на C++. Современные компиляторы и компоновщики генерируют код для DSP, достаточно эффективный в большинстве случаев. Использование языков программирования высокого уровня позволяет инженеру сосредоточиться на содержательной части алгоритма, существенно уменьшает время создания приложений.

Однако, гораздо более простой и быстрый путь для проверки эффективности разработанного алгоритма заключается в использовании для моделирования системы Matlab. Во всем мире Matlab является стандартом де-факто при экспериментах с алгоритмами ЦОС. Она включает в себя богатейшие библиотеки готовых функций и процедур, в том числе и для обработки сигналов, изображений. В последней версии этой системы (на момент написания книги это V.6.1) имеется даже библиотека написания приложений для ЦПОС фирмы Texas Inst.. Входной язык программирования этой среды во многом похож на Си. Кроме того, в состав Matlab входит Simulink, в котором реализована концепция графического программирования, позволяющая создавать программы путем рисования блок-схем алгоритмов. Классический путь создания новых устройств такой: Matlab -> C -> ассемблер DSP.

Процесс отладки проекта после написания кода программы и успешной компиляции включает три основных этапа: моделирование (Simulation), оценка (Evaluation) и эмуляция (Emulation). На этапе моделирования работает моделирующая программа (симулятор), которая имитирует работу процессора.

Симулятор используется для проверки и отладки программного кода до того, как будет изготовлена плата с процессором. На втором этапе используется оценочная плата EZ-KIT для того, чтобы определить, какой процессор наилучшим образом подходит для решения вашей задачи. Плата подключается к компьютеру с помощью кабеля через параллельный, последовательный или USB-порт. К настоящему времени оценочные платы существуют для всех типов процессоров, начиная с ADSP-2181 и заканчивая новейшим процессором BlackFin.

На третьем этапе, когда устройство уже изготовлено, можно выполнить тестирование платы с помощью специального аппаратно-программного модуля — эмулятора. Этот модуль управляет цифровым сигнальным процессором через JTAG-интерфейс и позволяет подробно отследить выполнение программного кода.

Еще одной важной особенностью, на которую следует обратить внимание, является то, что интерфейс пакета VisualDSP++ единый для всех серий сигнальных процессоров, включая 16-, 32-битные, а также TigerSHARC и BlackFin. Отличия касаются лишь набора установленных компиляторов и имеющейся лицензии.

В итоге всех этих трех этапов получаем программу которую непосредственно и использует DSP. Программа, исполняемая цифровым сигнальным процессором, представляет собой набор команд, которые процессор должен последовательно выполнять. Команды

представляют 48 – битные слова которые могут быть записаны во внутреннюю память процессора. В каждую ячейку памяти процессора может быть записана только одна команда. После загрузки в процессор программа представляет собой последовательность 48 – разрядных слов хранящихся во внутренней памяти процессора. У каждой ячейки памяти процессора имеется адрес, обращаясь по которому, процессор может считать, а затем и выполнить команду. Работа программы начинается с того, что процессор обращается к начальному адресу, в котором лежит первая команда программы. Оканчивается работа программы исполнением последней команды и переходом процессора в режим пониженного потребления питания.

VisualDSP «умеет» работать с двумя языками программирования: ассемблер и Си. Так как в конечном итоге генерируется код для самого DSP, то нет разницы на каком из языков работать внутри VisualDSP.

Функция зашифрования

Шифрование AES состоит:

- из начального добавления раундового ключа;
- N_r - 1 раундов;
- заключительного раунда, в котором отсутствует операция MixColumns.

На вход алгоритма подаются блоки входных данных, в ходе преобразований содержимое блока изменяется, посредством соответствующих операций (описаны выше) и на выходе образуется шифротекст, организованный опять же в виде блоков состояния.

Перед началом первого раунда происходит суммирование по модулю 2 с начальным ключом шифрования, затем - преобразование массива байтов в течение 10, 12 или 14 раундов в зависимости от длины ключа. Последний раунд несколько отличается от предыдущих тем, что не задействует функцию перемешивания байт в столбцах MixColumns.

Кроме того в алгоритм работы шифратора используется ряд проверок, направленных на корректную работу алгоритма шифрования. Одной из проверок является проверка длины ключа шифрования – если длина ключа шифрования составляет меньше или больше длины определенной алгоритмом, то выводится сообщение о неправильной длине ключа и необходимо ввести ключ верной длинны, в противном случае ситуация повторяется.

Вторая проверка заключается в сравнении длины ключа блока шифрования и длины шифруемого блока, если длины блоков равны или длина ключа меньше, то производится следующая по списку операция. В противном случае возврат на несколько шагов назад. Кроме того, если длина ключа блока шифрования и длина шифруемого блока равны то выдается рекомендация выбрать меньшую длину ключа. Это сделано с целью использования алгоритма расширения ключа (ключ задается не прямым образом, что положительно сказывается на криптостойкости).

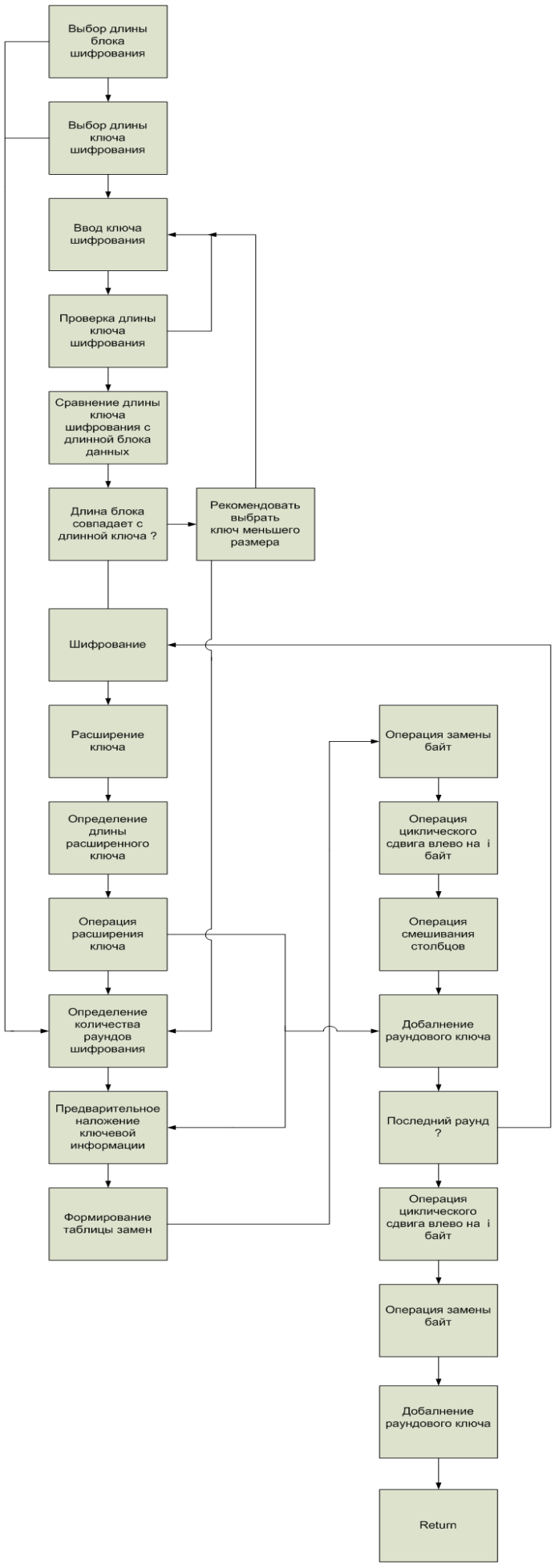

Выбор длины блока шифрования
Выбор длины ключа шифрования
Ввод ключа шифрования
Проверка длины ключа шифрования
Сравнение длины ключа шифрования с длинной блока данных
Длина блока совпадает с длинной ключа ?
Рекомендовать выбрать ключ меньшего размера
Шифрование
Расширение ключа
Определение длины расширенного ключа
Операция расширения ключа
Определение количества раундов шифрования
Предварительное наложение ключевой информации
Формирование таблицы замен
Операция замены байт
Операция циклического сдвига влево на i байт
Операция смешивания столбцов
Добалнение раундового ключа
Последний раунд ?
Операция циклического сдвига влево на i байт
Операция замены байт
Добалнение раундового ключа
Return

Рисунок 2.40. Процесс шифрования/дешифрования файла

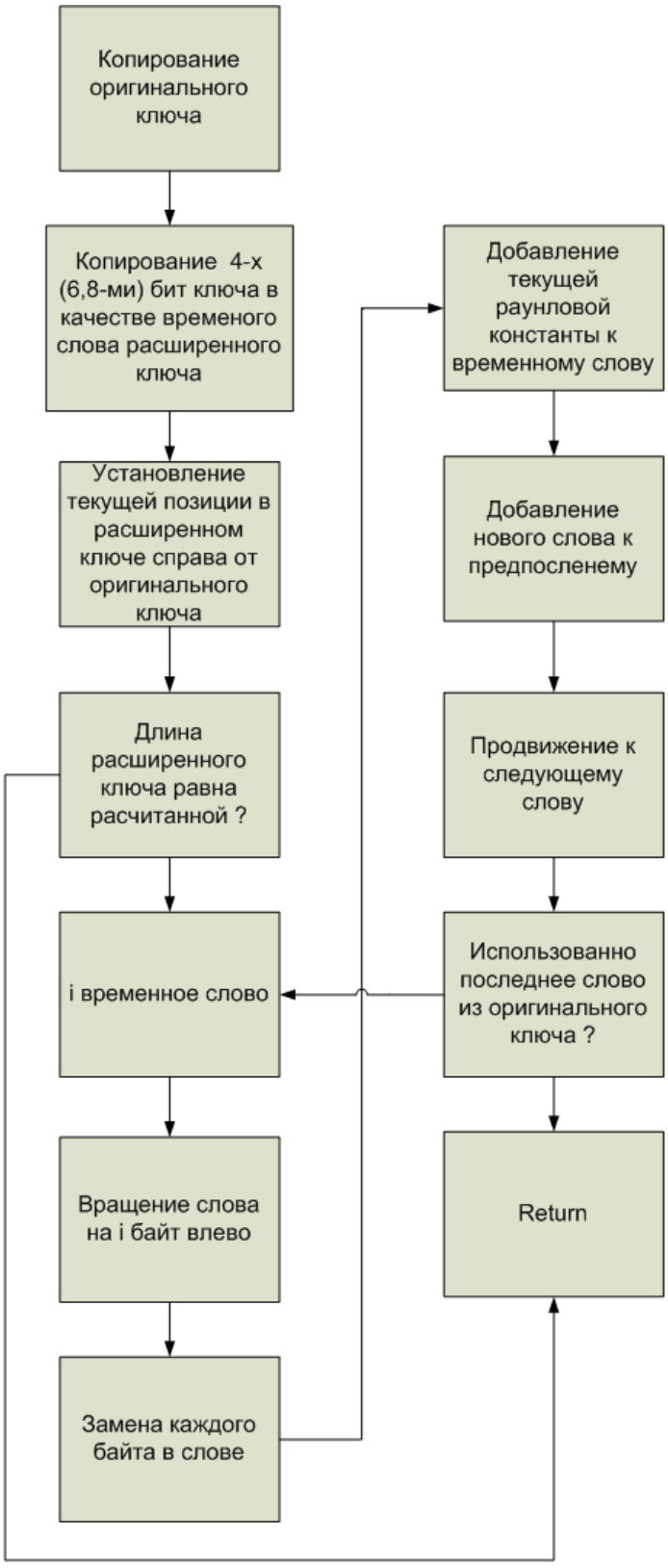


Рисунок 2.41. Процесс расширения оригинального ключа

Алгоритм выработки ключей (Key Schedule)

Раундовые ключи получаются из ключа шифрования посредством алгоритма выработки ключей. Он содержит два компонента: расширение ключа (Key Expansion) и выбор раундового ключа (Round Key Selection). Основополагающие принципы алгоритма выглядят следующим образом:

- общее число битов раундовых ключей равно длине блока, умноженной на число раундов, плюс 1 (например, для длины блока 128 бит и 10 раундов требуется 1408 бит раундовых ключей);
- ключ шифрования расширяется в расширенный ключ (Expanded Key);
- раундовые ключи берутся из расширенного ключа следующим образом: первый раундовый ключ содержит первые N_b слов, второй - следующие N_b слов и т. д.

Расширение ключа (Key Expansion). Расширенный ключ представляет собой линейный массив w[i] из $N_b(N_r+ 1)$ 4-байтовых слов, $i = 0,1…N_b(N_r + 1)$. В AES массив w[i] состоит из $4(N_r +1)$ 4-байтовых слов, $i = 0,1…4(N_r + 1)$.

Первые N_k слов содержат ключ шифрования. Все остальные слова определяются рекурсивно из слов с меньшими индексами. Алгоритм выработки ключей зависит от величины N_k.

Как можно заметить (рисунка , а), первые N_k слов заполняются ключом шифрования. Каждое последующее слово w[i] получается посредством XOR предыдущего слова w[i-l] и слова на N_k позиций ранее w[i - Nk]'.

$w[i] = w[i - 1] \oplus w[i -N_k]$.

Для слов, позиция которых кратна N_k, перед XOR применяется преобразование к w[i-1], а затем еще прибавляется раундовая константа Rcon. Преобразование реализуется с помощью двух дополнительных функций:

RotWord(), осуществляющей побайтовый сдвиг 32-разрядного слова по формуле $\{a_0\ a_1\ a_2\ a_3\} \rightarrow \{a_1\ a_2\ a_3\ a_0\}$ и

SubWord(), осуществляющей побайтовую замену с использованием S-блока функции SubBytes(). Значение Rcon[j] равно 2^{j-l}.

Значение w[i] в этом случае равно

$w[i] - SubWord(RotWord(w[i - 1])) \oplus Rcon[i/N_k] \oplus w[i - N_k]$.

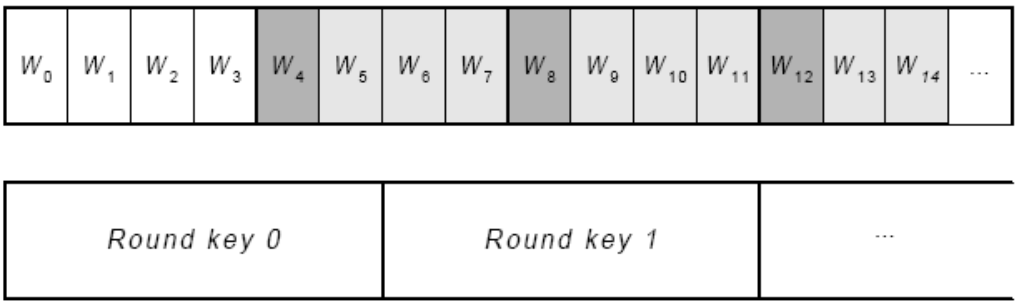


Рисунок 2.42. Процедуры:

а - расширения ключа (светло-серым цветом выделены слова расширенного ключа, которые формируются без использования функций SubWord() и RotWordQ; темно-серым цветом выделены слова расширенного ключа, при вычислении которых используются преобразования SubWordQ и RotWordQ);

б - выбора раундового ключа для Nk – 4.

Выбор раундового ключа (Round Key Selection). Раундовый ключ i получается из слов массива раундового ключа от W[Nb i] и до $W[N_b (i + 1)]$, как показано на рисунке 3.8.

Примечание. Алгоритм выработки ключей можно осуществлять и без использования массива w[i]. Для реализаций, в которых существенно требование к занимаемой памяти, раундовые ключи могут вычисляться "на лету" посредством использования буфера из N_k слов.

Расширенный ключ должен всегда получаться из ключа шифрования и никогда не указывается напрямую. Нет никаких ограничений на выбор ключа шифрования.

Запуск шифратора

По большому счету у аппаратных шифраторов существует два основных режима работы: начальной загрузки и выполнения операций.

Первый начинается при загрузке компьютера, в тот момент, когда BIOS ПК опрашивает все подключенные к нему внутренние и внешние устройства. В этот момент шифратор перехватывает управление и выполняет последовательность команд, "зашитую" в его память, предлагая пользователю прежде всего ввести главный ключ шифрования (т. е. вставить соответствующий ключевой носитель), который будет использоваться в дальнейшем. После завершения начальной загрузки шифратор ожидает от ПК команд и данных на исполнение операций шифрования.

Кстати, помимо собственно функций шифрования, каждый шифратор в этом режиме должен "уметь" как минимум:

выполнять различные операции с ключами шифрования: их загрузку в шифропроцессор и выгрузку из него, а также взаимное шифрование ключей;

рассчитывать имитоприставки для данных и ключей (имитоприставка представляет собой криптографическую контрольную сумму, вычисленную на определенном ключе);

генерировать случайные числа по запросу.

Рассмотрим работу шифратора в операционных системах семейства Microsoft Windows. В общем случае шифратор может получать команды сразу от нескольких программ. Например, это могут быть команды программы шифрования файлов; команды шифрования данных и вычисления имитоприставок от драйвера, выполняющего прозрачное (автоматическое) шифрование сетевых пакетов (скажем, реализующего механизмы виртуальных частных сетей); запросы на генерацию случайных чисел от программы-генератора криптографических ключей.

Во избежание возникновения коллизий программы не имеют прямого доступа к шифратору и управляют им с помощью специальных программных приложений.

Ввод ключа шифрования

Пользовательский ключ шифрования можно вводить посредством либо клавиатуры, либо с помощью сменного носителя (например с помощью смарт-карты). Второй способ является наиболее предпочтительным, так как существуют способы удаленного считывания информации с клавиатуры, либо возможны программные закладки. Ввод ключа шифрования с клавиатуры осуществляется при соответствующем программном запросе. Ввод ключа шифрования с помощью сменного носителя осуществляется при включении компьютера, после того как BIOS опросит все подключенные устройства и аппаратный шифратор включается в работу.

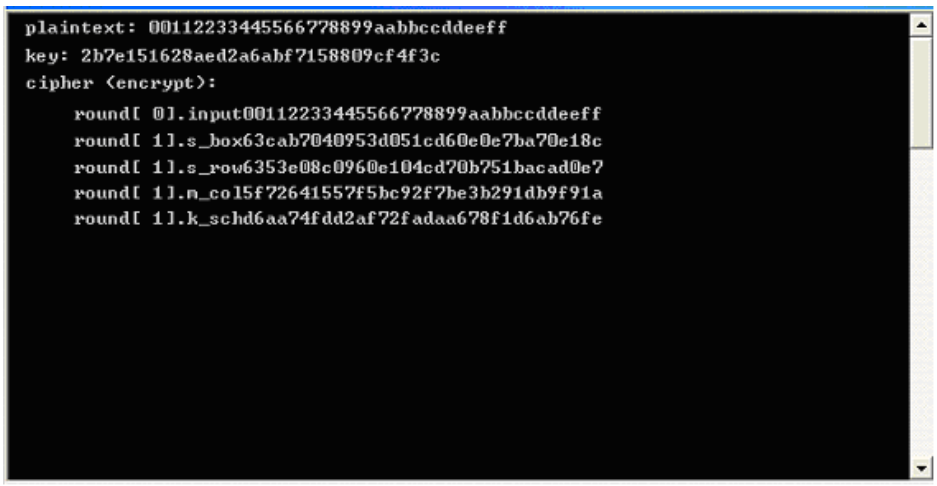


Рисунок 2.43. Ввод ключа шифрования с клавиатуры и отображение результатов преобразования в каждом раунде

Текст для шифратора можно также вводить непосредственно с клавиатуры, либо шифровать информации содержащуюся в каком – либо файле. Для шифрования информации содержащейся в файле необходимо при соответствующем запросе указать путь к папке где расположен требуемый файл.

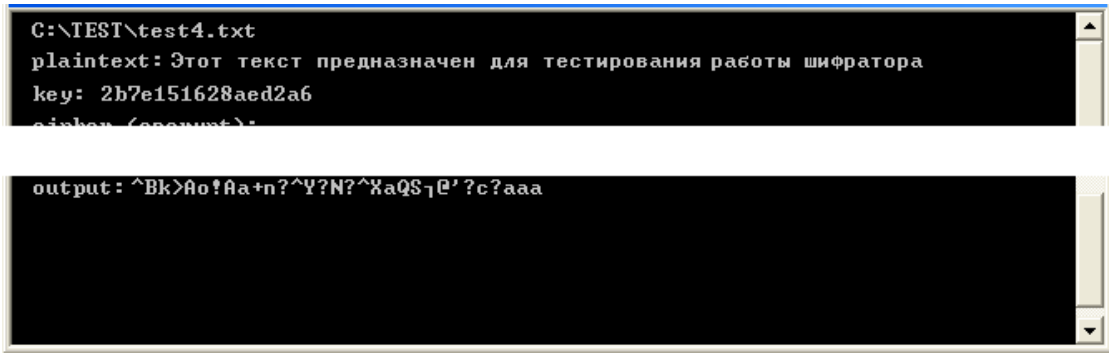


Рисунок 2.44. Открытие текстового документа для шифрования

3. Порядок выполнения работы

Методика создания и испытания AES шифратора на DSP.

Практическая инструкция

Для создания AES-шифратора на основе DSP, потребуется отладочная плата Ezkit Lite, программные оболочки: VisualDSP++ версии 3.5 или выше и Borland C++ 6.0.

Основной код программы создается на C++, так как данный алгоритм позволяет более гибко реализовывать задуманное. Использование языков программирования высокого уровня позволяет инженеру сосредоточиться на содержательной части алгоритма, существенно уменьшает время создания приложений.

В качестве исходного материала для написания программного обеспечения шифратора необходимо использовать официальные документы НИСТ такие как: FIPS Publication 197. Specification for the Advanced Encryption Standard. //http://csrc.nist.gov – November 26, 2001 и AES Round 1 Information. // http://csrc.nist.gov – January 26, 2001, кроме них можно воспользоваться описанием и рекомендациями которые дают сами разработчики алгоритма - Joan Daemen and Vincent Rijmen, The Design of Rijndael, AES - The Advanced Encryption Standard, Springer-Verlag 2002. В данных публикациях довольно подробно описано как

работает алгоритм шифрования, даны некоторые рекомендации по реализации этого алгоритма.

По окончанию изучения материалов необходимо разработать общую структуру, определится с последовательностью выполняемых модулей.

После этого можно приступать непосредственно к написанию кода.

Первое что следует начать реализовывать после описания основных частей (переменных, входных данных), это алгоритм расширения ключа.

Следующий шаг это создание блока шифрования и расшифрования, хотя эти блоки по алгоритму и различаются только константами, на языке программирования это все же будет иметь значение.

Так же необходимо выделить необходимое время на доводку и отладку проекта.

После создания программного кода на C++, можно преступать к работе с VisualDSP++. Данный продукт как раз и предназначен для непосредственной работы с цифровыми сигнальными процессорами, кроме всего прочего он эмулирует выбранный цифровой сигнальный процессор и позволяет посмотреть результат работы программы без непосредственного подключения аппаратной части.

Установка VisualDSP производится так же как и установка других программных продуктов. После запуска выбирается тот цифровой сигнальный процессор, который будет эмулироваться. Создаем новый проект. На данном этапе проект «FirstProject» включает в себя три пустые папки. Первая из них «Source Files» предназначена для файлов исходного кода проекта (.asm, .cpp, .c). Вторая «Linker Files» предназначена для хранения файла карты памяти (.ldf). Третья «Header Files» содержит заголовочные файлы проекта. В заголовочных фалах обычно хранятся описания констант, стандартных обозначений, переменных, классов.

Чтобы проект можно было скомпилировать и превратить в рабочую программу, необходимо создать файл «CodeFirst.cpp», который будет содержать исходный код и добавить его к проекту. Для создания файла необходимо выбрать пункт меню «File->New». В результате на экране монитора появится окно нового документа.

. Далее в проект добавляется код написанный на C++, компилируется и на выходе получаем исполняемый модуль. Если имеют место какие-либо ошибки, то необходимо воспользоваться пошаговым выполнением программы (Shift+F5), локализовать и исправить ошибку.

. Процесс отладки проекта после написания кода программы и успешной компиляции включает три основных этапа: моделирование (Simulation), оценка (Evaluation) и эмуляция (Emulation). На этапе моделирования работает моделирующая программа (симулятор), которая имитирует работу процессора.

. Симулятор используется для проверки и отладки программного кода до того, как будет изготовлена плата с процессором. На втором этапе используется оценочная плата EZ-KIT для того, чтобы определить, какой процессор наилучшим образом подходит для решения вашей задачи. Плата подключается к компьютеру с помощью кабеля через параллельный, последовательный или USB-порт. К настоящему времени оценочные платы существуют для всех типов процессоров, начиная с ADSP-2181 и заканчивая новейшим процессором BlackFin.

. На третьем этапе, когда устройство уже изготовлено, можно выполнить тестирование платы с помощью специального аппаратно-программного модуля — эмулятора. Этот модуль управляет цифровым сигнальным процессором через JTAG-интерфейс и позволяет подробно отследить выполнение программного кода.

. В итоге всех этих трех этапов получаем программу которую непосредственно и использует DSP . Программа, исполняемая цифровым сигнальным процессором, представляет собой набор команд, которые процессор должен последовательно выполнять. Команды представляют 48 – битные слова которые могут быть записаны во внутреннюю память процессора. В каждую ячейку памяти процессора может быть записана только одна команда. После загрузки в процессор программа представляет собой последовательность 48 – разрядных слов хранящихся во внутренней памяти процессора. У каждой ячейки памяти

процессора имеется адрес, обращаясь по которому, процессор может считать, а затем и выполнить команду. Работа программы начинается с того, что процессор обращается к начальному адресу, в котором лежит первая команда программы. Оканчивается работа программы исполнением последней команды и переходом процессора в режим пониженного потребления питания.

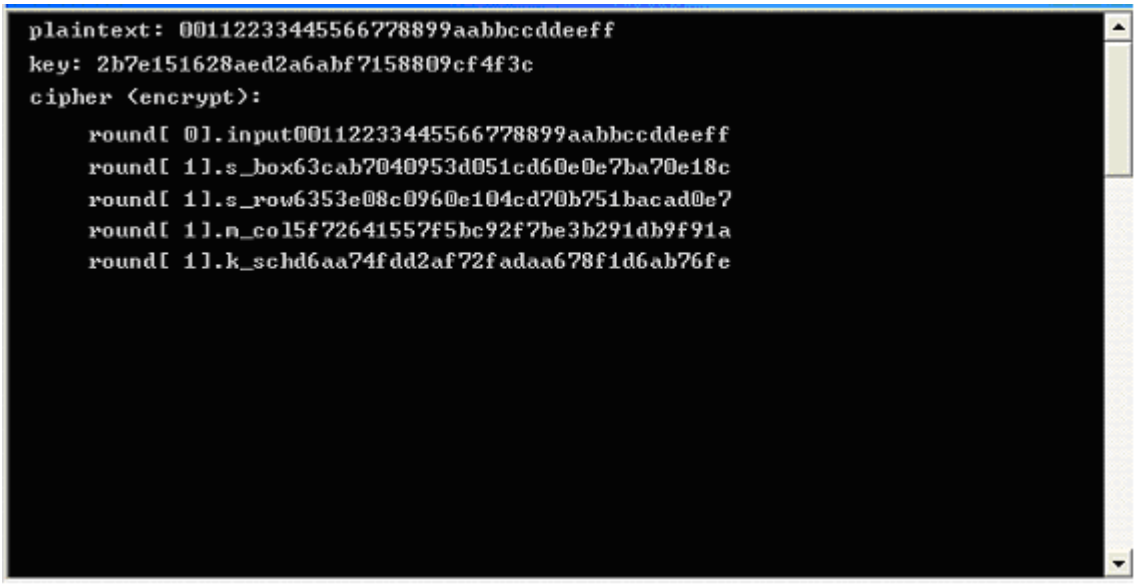
Методика испытания AES шифратора на DSP

Задавая различные значения входных блоков и ключей пронаблюдать каждый этап шифрования.

В качестве входных блоков при расшифровании указать результаты шифрования предыдущего пункта. Ключ использовать такой же как и в предыдущем пункте. На выходе должен получится блок той длины и содержания что и в пункте 1.

Задавая различные значения и размеры входного блока и ключей замерить время шифрования и дешифрования.

Результаты испытания AES шифратора на DSP



PLAINTEXT (Входной блок): 00112233445566778899aabbccddeeff
KEY (Ключ шифрования): 2b7e151628aed2a6abf7158809cf4f3c
Операция шифрования CIPHER (ENCRYPT):

round[0].input 00112233445566778899aabbccddeeff
round[0].k_sch 000102030405060708090a0b0c0d0e0f
round[1].s_box 63cab7040953d051cd60e0e7ba70e18c
round[1].s_row 6353e08c0960e104cd70b751bacad0e7
round[1].m_col 5f72641557f5bc92f7be3b291db9f91a
round[1].k_sch d6aa74fdd2af72fadaa678f1d6ab76fe
round[2].start 89d810e8855ace682d1843d8cb128fe4
round[2].s_box a761ca9b97be8b45d8ad1a611fc97369
round[2].s_row a7be1a6997ad739bd8c9ca451f618b61
round[2].m_col ff87968431d86a51645151fa773ad009
round[2].k_sch b692cf0b643dbdf1be9bc5006830b3fe
round[3].start 4915598f55e5d7a0daca94fa1f0a63f7
round[3].s_box 3b59cb73fcd90ee05774222dc067fb68

round[3].s_row 3bd92268fc74fb735767cbe0c0590e2d
round[3].m_col 4c9c1e66f771f0762c3f868e534df256
round[3].k_sch b6ff744ed2c2c9bf6c590cbf0469bf41
round[4].start fa636a2825b339c940668a3157244d17
round[4].s_box 2dfb02343f6d12dd09337ec75b36e3f0
round[4].s_row 2d6d7ef03f33e334093602dd5bfb12c7
round[4].m_col 6385b79ffc538df997be478e7547d691
round[4].k_sch 47f7f7bc95353e03f96c32bcfd058dfd
round[5].start 247240236966b3fa6ed2753288425b6c
round[5].s_box 36400926f9336d2d9fb59d23c42c3950
round[5].s_row 36339d50f9b539269f2c092dc4406d23
round[5].m_col f4bcd45432e554d075f1d6c51dd03b3c
round[5].k_sch 3caaa3e8a99f9deb50f3af57adf622aa
round[6].start c81677bc9b7ac93b25027992b0261996
round[6].s_box e847f56514dadde23f77b64fe7f7d490
round[6].s_row e8dab6901477d4653ff7f5e2e747dd4f
round[6].m_col 9816ee7400f87f556b2c049c8e5ad036
round[6].k_sch 5e390f7df7a69296a7553dc10aa31f6b
round[7].start c62fe109f75eedc3cc79395d84f9cf5d
round[7].s_box b415f8016858552e4bb6124c5f998a4c
round[7].s_row b458124c68b68a014b99f82e5f15554c
round[7].m_col c57e1c159a9bd286f05f4be098c63439
round[7].k_sch 14f9701ae35fe28c440adf4d4ea9c026
round[8].start d1876c0f79c4300ab45594add66ff41f
round[8].s_box 3e175076b61c04678dfc2295f6a8bfc0
round[8].s_row 3e1c22c0b6fcbf768da85067f6170495
round[8].m_col baa03de7a1f9b56ed5512cba5f414d23
round[8].k_sch 47438735a41c65b9e016baf4aebf7ad2
round[9].start fde3bad205e5d0d73547964ef1fe37f1
round[9].s_box 5411f4b56bd9700e96a0902fa1bb9aa1
round[9].s_row 54d990a16ba09ab596bbf40ea111702f
round[9].m_col e9f74eec023020f61bf2ccf2353c21c7
round[9].k_sch 549932d1f08557681093ed9cbe2c974e
round[10].start bd6e7c3df2b5779e0b61216e8b10b689
round[10].s_box 7a9f102789d5f50b2beffd9f3dca4ea7
round[10].s_row 7ad5fda789ef4e272bca100b3d9ff59f
round[10].k_sch 13111d7fe3944a17f307a78b4d2b30c5
round[10].output 69c4e0d86a7b0430d8cdb78070b4c55a

Операция дешифрования INVERSE CIPHER (DECRYPT):

round[0].iinput 69c4e0d86a7b0430d8cdb78070b4c55a
round[0].ik_sch 13111d7fe3944a17f307a78b4d2b30c5
round[1].istart 7ad5fda789ef4e272bca100b3d9ff59f
round[1].is_row 7a9f102789d5f50b2beffd9f3dca4ea7
round[1].is_box bd6e7c3df2b5779e0b61216e8b10b689
round[1].ik_sch 549932d1f08557681093ed9cbe2c974e
round[1].ik_add e9f74eec023020f61bf2ccf2353c21c7
round[2].istart 54d990a16ba09ab596bbf40ea111702f
round[2].is_row 5411f4b56bd9700e96a0902fa1bb9aa1
round[2].is_box fde3bad205e5d0d73547964ef1fe37f1
round[2].ik_sch 47438735a41c65b9e016baf4aebf7ad2

round[2].ik_add baa03de7a1f9b56ed5512cba5f414d23
round[3].istart 3e1c22c0b6fcbf768da85067f6170495
round[3].is_row 3e175076b61c04678dfc2295f6a8bfc0
round[3].is_box d1876c0f79c4300ab45594add66ff41f
round[3].ik_sch 14f9701ae35fe28c440adf4d4ea9c026
round[3].ik_add c57e1c159a9bd286f05f4be098c63439
round[4].istart b458124c68b68a014b99f82e5f15554c
round[4].is_row b415f8016858552e4bb6124c5f998a4c
round[4].is_box c62fe109f75eedc3cc79395d84f9cf5d
round[4].ik_sch 5e390f7df7a69296a7553dc10aa31f6b
round[4].ik_add 9816ee7400f87f556b2c049c8e5ad036
round[5].istart e8dab6901477d4653ff7f5e2e747dd4f
round[5].is_row e847f56514dadde23f77b64fe7f7d490
round[5].is_box c81677bc9b7ac93b25027992b0261996
round[5].ik_sch 3caaa3e8a99f9deb50f3af57adf622aa
round[5].ik_add f4bcd45432e554d075f1d6c51dd03b3c
round[6].istart 36339d50f9b539269f2c092dc4406d23
round[6].is_row 36400926f9336d2d9fb59d23c42c3950
round[6].is_box 247240236966b3fa6ed2753288425b6c
round[6].ik_sch 47f7f7bc95353e03f96c32bcfd058dfd
round[6].ik_add 6385b79ffc538df997be478e7547d691
round[7].istart 2d6d7ef03f33e334093602dd5bfb12c7
round[7].is_row 2dfb02343f6d12dd09337ec75b36e3f0
round[7].is_box fa636a2825b339c940668a3157244d17
round[7].ik_sch b6ff744ed2c2c9bf6c590cbf0469bf41
round[7].ik_add 4c9c1e66f771f0762c3f868e534df256
round[8].istart 3bd92268fc74fb735767cbe0c0590e2d
round[8].is_row 3b59cb73fcd90ee05774222dc067fb68
round[8].is_box 4915598f55e5d7a0daca94fa1f0a63f7
round[8].ik_sch b692cf0b643dbdf1be9bc5006830b3fe
round[8].ik_add ff87968431d86a51645151fa773ad009
round[9].istart a7be1a6997ad739bd8c9ca451f618b61
round[9].is_row a761ca9b97be8b45d8ad1a611fc97369
round[9].is_box 89d810e8855ace682d1843d8cb128fe4
round[9].ik_sch d6aa74fdd2af72fadaa678f1d6ab76fe
round[9].ik_add 5f72641557f5bc92f7be3b291db9f91a
round[10].istart 6353e08c0960e104cd70b751bacad0e7
round[10].is_row 63cab7040953d051cd60e0e7ba70e18c
round[10].is_box 00102030405060708090a0b0c0d0e0f0
round[10].ioutput 00112233445566778899aabbccddeeff

Примечание:
input: блок входных данных
s_box: состояние блока после SubBytes()
s_row: состояние блока после ShiftRows()
m_col: состояние блока после MixColumns()
k_sch: значение ключа
output: блок выходных данных
iinput: блок входных данных
is_box: состояние блока после SubBytes()
is_row: состояние блока после ShiftRows()
ik_sch: состояние блока после MixColumns()

ik_add: значение ключа
ioutput: блок выходных данных

Как можно видеть при зашифровании и расшифровании результат зашифрования получаем один и тот же блок, что соответствует о правильности шифрования.

4. Рекомендуемая литература

1. FIPS Publication 197. Specification for the Advanced Encryption Standard. //http://csrc.nist.gov – November 26, 2001.
2. AES Round 1 Information. // http://csrc.nist.gov – January 26, 2001.
3. Joan Daemen and Vincent Rijmen, The Design of Rijndael, AES - The Advanced Encryption Standard, Springer-Verlag 2002 (238 pp.)
4. VisualDSP 3.5 + User Guide.
5. Справочное руководстве по архитектуре процессора Analog Devices ADSP TS101 - http://www.analog.com/en/prod/0,2877,ADSP%252DTS101S,00.html
6. Винокуров Андрей, Применко Эдуард. Сравнение стандарта шифрования РФ и нового стандарта шифрования США - http://www.enlight.ru/crypto/frame.htm
7. Алгоритм шифрования AES и его криптоанализ - http://www.cio-world.ru/bsolutions/e-safety/320670/
8. ***Современные методы вскрытия алгоритмов шифрования*** - http://www.cio-world.ru/weekly/300850/
9. ***Стандарт криптографической защиты AES - http://winaes.narod.ru/***
10. Аппаратные шифраторы - http://www.osp.ru/pcworld/2002/08/163808/
11. Программно-аппаратные средства шифрования - http://www.zinfo.ru/srubrpodr/67/
12. Брассар Ж. Современная криптология. – Пер. с англ.: - М.: Полимед. 1999 – 176 с.
13. Nechvatal J., Barker E., Dodson D., Dworkin M., Foti J., Roback E. Status report on the first round of the development of the advanced encryption standard. // http://csrc.nist.gov – National Institute of Standards and Technology.
14. AES Round 1 Information. // http://csrc.nist.gov – January 26, 2001.
15. Романец Ю. В., Тимофеев П. А., Шаньгин В. Ф. "Защита информации в современных компьютерных системах" – М.: ТРИУМФ, 2002 – 816 с.
16. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. – М.: ТРИУМФ, 2002 – 816 с.

Компьютерный практикум 3. Исследование методов автоматизированного проектирования сетей и систем радиосвязи

1. Цель работы

Исследование методов и средств автоматизированного проектирования сетей радиосвязи, включая методы управления радиочастотным спектром, оценку электромагнитной обстановки (ЭМО) в местах предполагаемого размещения радиоэлектронных средств (РЭС) для обоснования решений о выделении полос, назначении радиочастот и принятия мер по повышению эффективности использования радиочастот, на основе оптимизации частотных присвоений, прогнозирования и измерения границ зон уверенного приема и анализ электромагнитной совместимости (ЭМС) РЭС.

2. Краткие теоретические сведения

Цифровые радиорелейные станции

Современная цифровая РРС - сложный технический комплекс, в который входит приемопередатчик, модем, мультиплексор, приемопередающие антенны, система автоматического резервирования, система телеуправления и телесигнализации, контрольно-измерительная аппаратура, устройства служебной связи, система электропитания. Рассмотрим функции основных устройств: приемопередатчика, модема и мультиплексора.

Приемопередатчик РРС – устройство, которое выполняет функции приема и передачи модулированных электрических колебаний заданных частот. Приемник выделяет электрический сигнал заданной частоты из сигналов, принятых приемной антенной. С выхода приемника сигнал поступает на модулятор. Передатчик вырабатывает модулированный электрический сигнал заданной частоты для последующего его излучения передающей антенной. На вход передатчика сигнал поступает из модулятора.

Один комплект приемопередающей аппаратуры, установленный на РРС, образует ствол. Для увеличения пропускной способности на РРС устанавливают несколько комплектов такой аппаратуры – создают несколько стволов.

Модем РРС – оконечное устройство, служащее для модуляции/демодуляции сигнала. Поступающий из мультиплексора дискретный сигнал модем преобразует в аналоговый (непрерывный) сигнал некоторой промежуточной частоты и передает его в приемопередатчик, а при приеме поступающий из приемопередатчика аналоговый сигнал преобразуется в дискретный. Таким образом, в составе цифрового радиорелейного тракта модем выполняет функции цифрового стыка, который должен соответствовать рекомендациям G.703 MKKTT.

Как правило, в модеме РРС дополнительно создаются:

• речевой канал, позволяющий организовывать служебную телефонную связь;

• канал RS-232 (9600 Бит/с), который может быть использован как дополнительный сервисный канал связи, так и для дистанционного контроля параметров.

В многопролетных системах связи программное обеспечение позволяет проводить дистанционное управление и диагностику модемов.

Для преобразования сигнала в модемах РРС чаще всего применяются следующие методы модуляции:

• FSK (Frequency Shift Keying) – частотная модуляция (ЧМ), сущность которой заключается в том, что дискретные сигналы 0, 1 передаются гармоническими сигналами (синусоидами), имеющими различные частоты;

• PSK (Phase Shift Keying) – фазовая модуляция, при которой дискретные сигналы 1 и 0 передаются путем переключения двух несущих, сдвинутых на полпериода относительно друг друга. Другой вариант PSK – изменение фазы на 900 в каждом такте при передаче нуля и на 2700 при передаче единицы.

Мультиплексор РРС предназначен для асинхронного объединения нескольких цифровых потоков в один, например Е1 (2048 Мбит/с), Е2 (8448 Мбит/с) в сигнал Е2
(8448 Мбит/с) или сигнал Е3 (34368 Мбит/с) в соответствии с рекомендацией G.742 (G.751) МККТТ.

В зависимости от места, которое занимает РРС в радиорелейной линии, различают оконечные, промежуточные и узловые РРС. Оконечными называют РРС, расположенные на концах радиорелейной линии; размещенные между оконечными РРС носят название промежуточных. Промежуточные станции, на которых предусмотрено выделение каналов, называют главными. Если на главной станции предусмотрено ответвление на другую радиорелейную линию, то такую РРС называют узловой. Главные и узловые РРС имеют специальное оборудование выделения каналов или ответвления. Как правило, оконечные и главные станции обслуживаются специалистами, а обычные промежуточные – дистанционно контролируются с оконечных и/или главных станций и персонала не имеют.
Наличие этих, так называемых необслуживаемых РРС, позволяет строить не только радиорелейные линии большой протяженности, но и разветвленные радиорелейные сети.

Радиорелейные линии на основе цифровых РРС стали важной составной частью цифровых сетей электросвязи – ведомственных, корпоративных, региональных, национальных и даже международных.
РРЛ классифицируют по следующим взаимосвязанным признакам:
• скорость передачи данных (цифрового потока) – пропускная способность, в зависимости от которой различают РРЛ:
• высокоскоростные (скорость передачи свыше 140 Мбит/с);
• среднескоростные
(до 52 Мбит/с);
• низкоскоростные
(до 8 Мбит/с);
• емкость радиорелейной линии (количество стволов и каналов в них), в зависимости от которой различают РРЛ:
• большой емкости;
• средней емкости;
• малоканальные.
• количество пролетов в радиорелейной линии, по которому различаются РРЛ:
• однопролетные;
• многопролетные.

Высокоскоростные большой емкости радиорелейные линии применяются в глобальных сетях передачи данных и называются магистральными. Среднескоростные средней емкости радиорелейные линии – для создания региональных, зоновых сетей передачи данных и называются зоновыми. Наконец, малоканальные широко используются для организации связи на железнодорожном транспорте, газопроводах, нефтепроводах, линиях электропередачи и т. п. Малоканальные радиорелейные линии с подвижными РРС применяются в военных целях.
Полосы радиочастот РРЛ расположены в диапазоне от 2 до 50 ГГц и жестко регламентируются внутри каждой полосы как рекомендациями ITU (Международного союза электросвязи), так и Радиорегламентом Российской Федерации.
При организации связи по цифровой радиорелейной линии должна быть решена проблема выделения частот приема и передачи. Ее решение относится к компетенции ГКРЧ России, и для РЭС всех назначений эта процедура осуществляется в соответствии с «Положением о порядке выделения полос (номиналов) радиочастот...» и результатами рассмотрения в установленном порядке радиочастотных заявок, поступающих от заявителей.
В ряде случаев, например в условиях больших городов, получение свободных радиочастот на некоторых направлениях затруднительно, что связано с проблемой электромагнитной совместимости с другими радиотехническими системами (РТС). Решение этих проблем – тема отдельного разговора.

Построение цифровых радиорелейных линий

Спектр применения современных цифровых радиолиний достаточно широк, это объясняется тем, что они позволяют:

• оперативно наращивать возможности системы связи путем установки оборудования РРС в помещениях узлов связи, используя антенно-мачтовые устройства и другие сооружения, что уменьшает капитальные затраты на создание радиорелейных линий связи;

• организовать многоканальную связь в регионах со слабо развитой (или с отсутствующей) инфраструктурой связи, а также на участках местности со сложным рельефом;

• развертывать разветвленные цифровые сети в регионах, больших городах и индустриальных зонах, где прокладка новых кабелей слишком дорога или невозможна;

• восстанавливать связь в районах стихийных бедствий или при спасательных операциях и др.

Сеть РРС может строиться как однопролетная линия, многопролетная линия и радиорелейная сеть.

Однопролетная РРЛ состоит из двух территориально разнесенных РРС. Такие радиолинии могут создаваться для соединения базовых центров сотовой связи, АТС и других аналогичных объектов. Примерами такой структуры могут служить радиолинии, разработанные фирмой Nera (Норвегия). Радиолиния с пропускной способностью 140 Мбит/с для российского телевидения соединила телецентр на Ямском поле с земной станцией спутниковой связи в Клину, обеспечив одновременную передачу 17 телевизионных каналов. РРЛ с пропускной способностью 155 Мбит/с и емкостью 1920 цифровых каналов РФ связала Центробанк с его подразделением, удаленным на 140 км.

Примером радиорелейной сети может служить созданная в Киргизской Республике в качестве первичной сети цифровая радиорелейная магистраль из 16 РРС, замкнутых в кольцо, от узловых станций которой отведены три радиолинии с семью другими РТС. Горный рельеф позволил увеличить некоторые пролеты между РРС до 165 км. Сеть охватывает все регионы республики и имеет выходы на наземную станцию спутниковой связи COMSTAT (США) с антенной, направленной на искусственный спутник Intelsat 630, что обеспечивает прямой выход сети связи республики на национальные сети связи многих стран Азии и Европы.

Широкое применение получили малогабаритные, быстро разворачиваемые РРС диапазонов 18, 23 и 36 ГГц, которые способны передавать на расстояние до 25 км как аналоговую (телевизионную), так и цифровую информацию (со скоростью до 34 Мбит/с). Типичное применение цифровых РРС данных диапазонов – организация сетей местной связи, сетей сотовой и транковой связи. В последнем случае, как правило, применяются однопролетные РРЛ «базовая станция» – «базовая станция» и «базовая станция» – «коммуникационная станция».

РТС могут быть использованы также вместо широкополосных оптоволоконных линий, создаваемых в городских условиях для связи между узловыми АТС и другими объектами связи. Такие РРС могут быть встроены в телекоммуникационные сети, отвечающие стандартам SDH/SONET.

Основными направлениями применения радиолиний в этом случае могут быть:

• магистраль. РРЛ вписывается в городские сети SDH/SONET и служит для замыкания колец, для соединения между кольцами и для подключения удаленных узлов доступа. Линия может использоваться как транспортная альтернатива оптоволокну или для его резервирования;

• организация доступа к сети АТМ. РРЛ соединяется с оконечным сетевым устройством АТМ и концентратором доступа АТМ;

• сопряжение между собой сетей АТМ, FAST ETHERNET и других.

В настоящее время появилось большое количество РТС этих диапазонов, которые выпускаются зарубежными и отечественными производителями. На мировом рынке представлены РТС около 15 фирм, в том числе Microwave Network (США), Ceragon Networks.

Предлагают свои малогабаритные РТС и отечественные производители. С 1993–1994 гг. начали выпускаться РРС серии «Радан-МС», «Радан-МГ», семейство станций «Эриком», «Пихта-2», «Радиус-15», «Комплекс-15» и ряд других. В тот период эти РРС по техническому уровню и надежности не могли сравниться с зарубежными аналогами. В дальнейшем положение изменилось,

и были разработаны РТС нового поколения – серия станций «Просвет», станции «Радиус-ДС», «Радиус-15М», «Звезда-11», «Радиус-18» и ряд других.

Общие принципы построения ЦРРЛ и особенности современной аппаратуры

Радиорелейные линии связи основываются на принципах многократной ретрансляции сигнала, что иллюстрируется упрощенной структурной схемой, показанной на рис.3.1. Различаются оконечные, промежуточные и узловые станции.

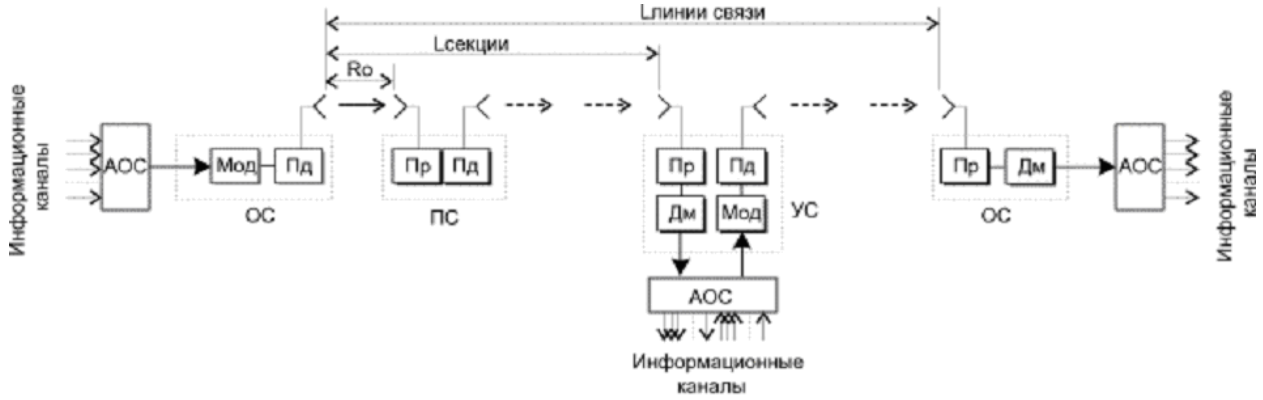


Рисунок 3.1. Структурная Схема одного направления РРЛ

Оконечные станции устанавливаются в крайних пунктах линии связи и содержат модуляторы и передатчики в направлении передачи сигналов и приемники с демодуляторами в направлении приема. Для приема и передачи применяется одна антенна, соединенная с трактами приема и передачи при помощи антенного разветвителя (дуплексера). Модуляция и демодуляция сигналов проводится на одной из стандартных промежуточных частот (70 - 1000 МГц). При этом модемы могут работать с приемопередатчиками, использующими различные частотные диапазоны. Передатчики предназначены для преобразования сигналов промежуточной частоты в рабочий диапазон СВЧ, а приемники - для обратного преобразования и усиления сигналов промежуточной частоты. Существуют системы РРЛ с непосредственной модуляцией сигналов СВЧ (например, аппаратура Эриком-11), но они имеют ограниченное распространение.

Упрощенная структурная схема оконечной станции показана на рис. 3.2.

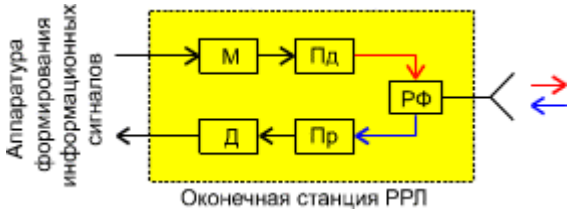


Рисунок 3.2. Оконечная станция

Промежуточные станции располагаются на расстоянии прямой видимости и предназначаются для приема сигналов, усиления их и дальнейшей передаче по линии связи. Прием и передача сигналов на промежуточных станциях должна проводится на разных частотах для устранения паразитных связей в приемопередатчиках за счет влияния обратного излучения близко расположенных антенн. Разница между частотами приема и передачи называется частотой сдвига (***f*сдв**). На рис. 3.3 показана структурная схема промежуточной станции.

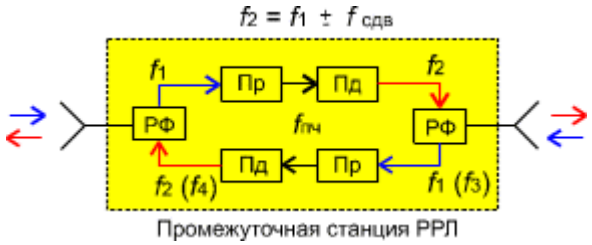


Рисунок 3.3. Промежуточная станция

Узловые станции (рис. 3.4) выполняют как функции промежуточных станций, так и функции ввода и вывода информации. Поэтому они устанавливаются в крупных населенных пунктах или в точках пересечения (ответвления) линий связи.

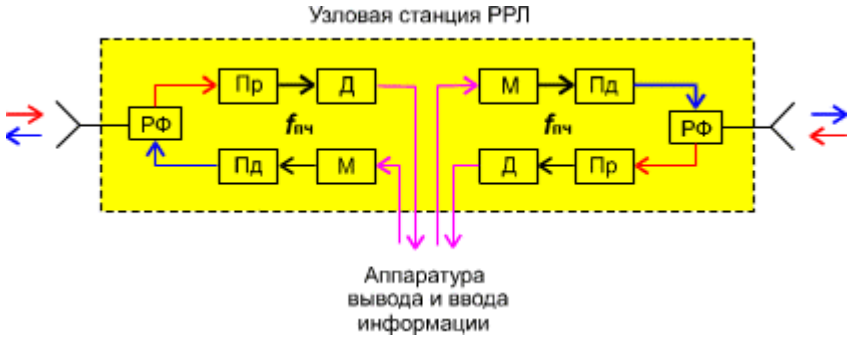


Рисунок 3.4. Узловая станция

Промежуток между ближайшими станциями называется пролетом (или интервалом) РРЛ. Протяженность пролета зависит от многих причин и, в среднем, достигает 50 - 60 км в диапазонах частот до 6 - 8 ГГц и нескольких км в диапазонах 30 - 50 ГГц.

Промежуток между оконечной станцией и ближайшей узловой или между узловыми станциями называется секцией РРЛ, а совокупность приемопередающего оборудования образует ствол РРЛ. Различаются однонаправленные стволы и двунаправленные (для дуплексной связи).

При передачи сигналов в прямом и обратном направлениях применяются 2-частотные и 4-частотные системы.

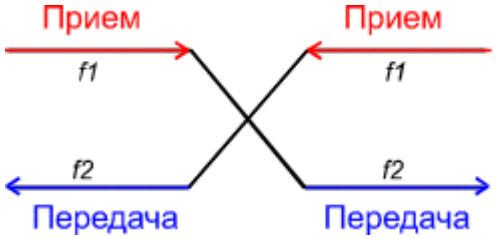


Рисунок 3.5.

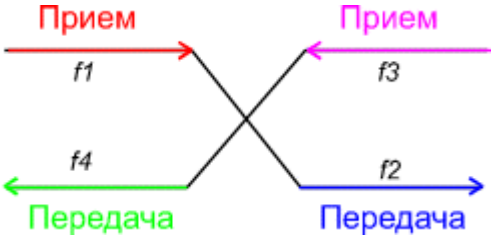


Рисунок 3.6.

2-частотная система (рис. 3.5) экономична с точки зрения использования полосы частот, выделенной для организации радиорелейной связи, но требует применения антенн с хорошими защитными свойствами от приема и передачи сигналов с боковых и обратных направлений. В диапазонах частот выше 10 ГГц широко применяются параболические антенны улучщенного исполнения с дополнительными экранами (воротниками), позволяющими достичь требуемых показателей.

4-частотная система (рис. 3.6) допускает применение более простых и дешевых антенн и позволяет улучшить защищенность линии связи от взаимных помех, но используется достаточно редко. Как правило, четырехчастотную систему можно рекомендовать для организации линий связи при очень сложной электромагнитной обстановке.

Для повышения экономической эффективности и пропускной способности радиорелейные системы часто делают многоствольными, в которых на каждой станции работают с различными частотами несколько приемопередатчиков через общие антенно-фидерные устройства.

С целью увеличения надежности работы линии связи применяются различные способы резервирования. В диапазонах частот выше 10 ГГц в ЦРРЛ наибольшее распространение получают системы резервирования 1 + 1, когда на один рабочий ствол приходится один резервный. В сложных условиях распространения радиоволн, оба ствола могут быть использованы для организации разнесенного приема, существенно улучшающего устойчивость работы системы связи. Зачастую строятся простые одноствольные системы связи без резервирования, учитывая высокую надежность современной аппаратуры. К примеру, время наработки на отказ аппаратуры ЦРРЛ типа MINI - LINK E шведской фирмы ERICSSON достигает (согласно рекламе) 20 - 30 лет.

Широкое развитие информационных радиосетей заставляет строго регламентировать использование рабочих частот в выделенных диапазонах волн. На рис. 3.7 показан пример плана распределения рабочих частот для системы РРЛ, работающей в диапазоне 11 ГГц в соответствии с Рекомендациями 387-2 МСЭ-Р.

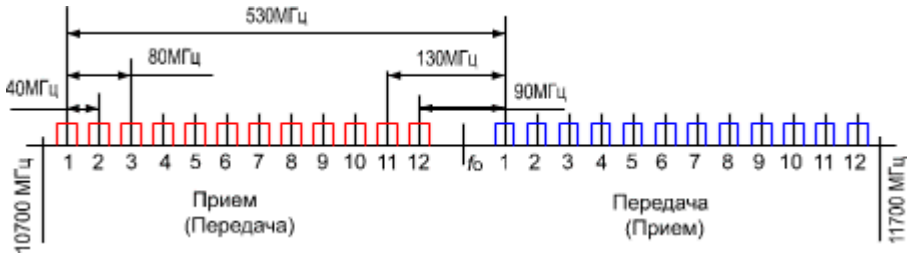


Рисунок 3.7. Пример плана распределения рабочих частот

В более высокочастотных диапазонах волн применяются гибкие частотные планы. Разнос частотных каналов в таких случаях определяется пропускной способностью (скоростью работы ЦРРЛ) и видом модуляции. Чаще всего применяется шаг разноса рабочих частот равный 3.5 МГц. Тогда, к примеру, при скорости работы 4 Мбит/с и 4-уровневой модуляции разнос частот можно выбрать равным шагу разноса, а при кратном увеличении скорости разнос также кратно увеличивается и может равняться
7, 14 или 28 МГц.

В последние годы разработаны новые частотные планы с использованием двойной поляризации радиоволн, позволяющие существенно повысить эффективность использования частотного спектра.

Современная аппаратура радиорелейных систем для диапазонов частот выше 10 ГГц имеет определенные особенности в конструктивном выполнении по сравнению с более низкочастотной аппаратурой. В диапазонах частот до 10 ГГц приемопередающая аппаратура, как правило, выполняется в виде достаточно громоздких стоек, располагающихся в аппаратных помещениях. Связь с антеннами осуществляется фидерными волноводами, имеющими значительную длину и, следовательно, вносящими существенные потери. Переход к диапазонам частот выше 10 ГГц существенно изменил конструктивное выполнение аппаратуры. Аппаратура, работающая в диапазоне выше 10 ГГц, имеет небольшие габариты и располагается на вершине антенной опоры, объединенная в единый блок с антенной.

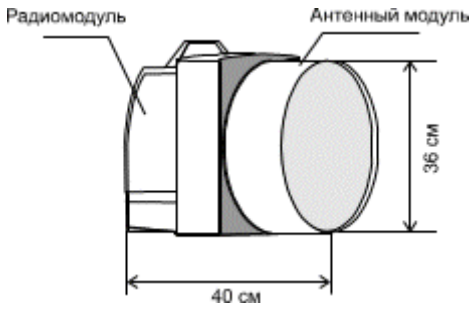


Рисунок 3.8. Приемопередающий блок

На рис. 3.8 показан пример конструктивного выполнения приемопередающего блока цифровой аппаратуры MINI-LINK для диапазона частот 23 - 38 ГГц. Здесь параболическая антенна имеет диаметр 30 см и соединяется с приемопередающим блоком непосредственно без волновода. Элементы для крепления всего модуля к антенной опоре располагаются на антенном блоке и имеют устройства для юстировки в вертикальной и горизонтальной плоскостях. Приемопередающий блок можно легко отсоединить от антенного блока для замены, настройки и профилактики. В таком исполнении вес блока составляет 11-12 кг. Аппаратура позволяет использовать антенны и большего диаметра (0.6 и 1.2 м).

В случае применения антенны диаметром 0.6 м конструктивное выполнение остается таким же, как показано на рис. 3.8, а антенна диаметром 1.2 м соединяется с приемопередатчиком коротким гибким волноводом.

Пример расположения модулей аппаратуры на антенной опоре (отечественная аппаратура БИСТ) показан на рис. 3.9.

Рисунок 3.9. Антенная опора с аппаратурой

Компактная аппаратура с небольшими габаритами и весом, которая применяется в диапазонах частот выше 10 ГГц, допускает использование облегченных антенных мачт, выполненных в виде ферм треугольного сечения или трубчатых конструкций, которые можно установить на высоких зданиях, дымовых трубах или возвышенных местах. Приемопередающие блоки соединяются коаксиальными кабелями с модемным оборудованием, располагающимся в помещении. Современное модемное оборудование - это легко трансформирующийся комплекс, функционирующий под управлением центрального или местного компьютера
. Модемное оборудование может обеспечивать формирование и обработку цифровых потоков на скорости от 1 до 34 Мбит/с, проводить мультиплексирование потоков и функционировать в режимах организации сетей связи любой конфигурации.
. Для примера, на рис. 3.10 показана схема организации системы связи между локальными компьютерными сетями. Подобную схему можно применить и для связи между базовыми станциями подвижной связи.

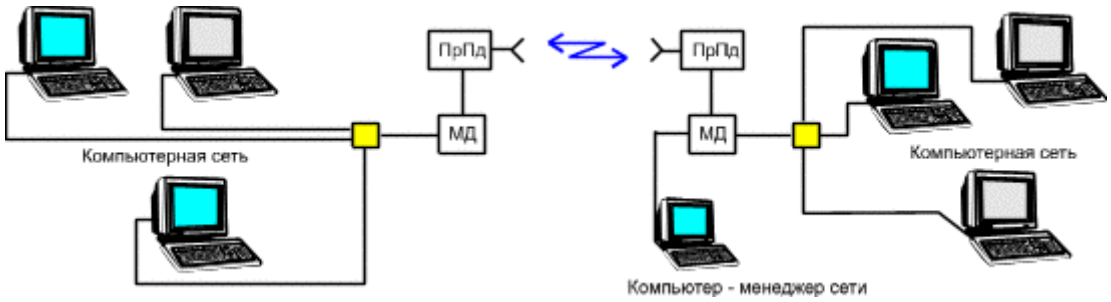


Рисунок 3.10.

Пример типовой конфигурации цифровой сети связи представлен на рис. 3.11. Здесь показаны различные типы станций РРЛ, работающих с разными цифровыми потоками, с резервированием и без резервирования, функционирующие под управлением компьютера - менеджера сети

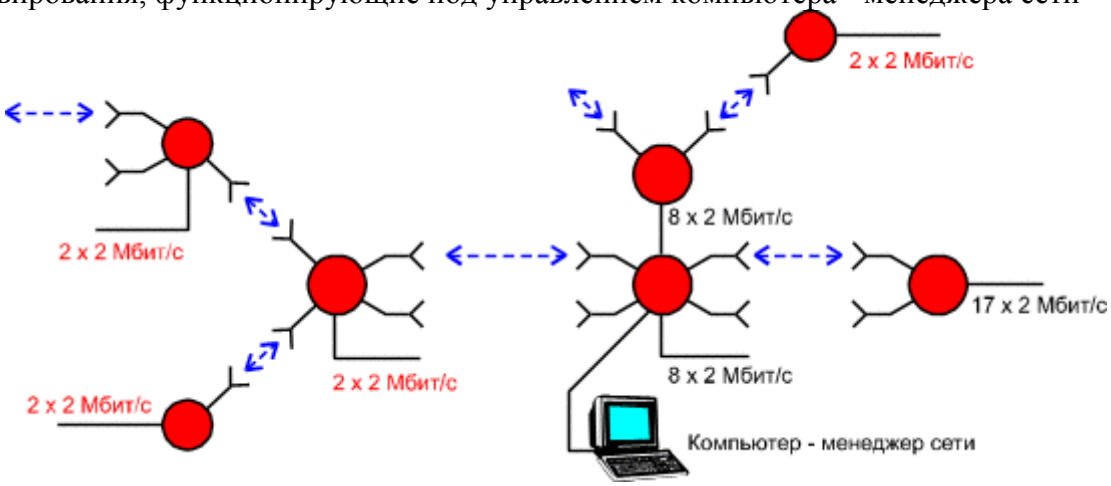


Рисунок 3.11.

В последние годы начинают бурно развиваться микроволновые многоканальные системы распределения информации (MMDS, MVDS, LMDS). Такие системы позволяют организовать распространение телевизионных программ или компьютерной информации для индивидуальных или коллективных абонентов. Системы MMDS представляют собой сеть базовых станций, работающих в диапазоне частот 2.7 ГГц, с антеннами, имеющими круговую диаграмму направленности в горизонтальной плоскости и угол раскрыва порядка 3 - 6 град. в вертикальной плоскости (***G*** = 12-17 дБ).

Множество приемных абонентских устройств (как индивидуального, так и коллективного пользования), с направленными антеннами, имеющими коэффициент усиления 25 - 35 дБ, располагаются в зоне прямой видимости от базовых станций. Обмен информацией между базовыми станциями осуществляется при помощи различных систем связи, в том числе и при помощи РРЛ.

Наиболее перспективны, с точки зрения использования в подобных системах связи, диапазоны частот выше 10 ГГц, так как диапазоны часто ниже 10 ГГц сильно загружены и не позволяют строить компактные приемные устройства. Для локальных систем распределения информации (LMDS) предполагается использовать диапазон частот 27 - 29 ГГц. Применение частот выше 30 ГГц позволяет принимать информацию с высоким качеством только на небольших расстояниях (2 - 7 км) из-за малого коэффициента усиления антенн базовых станций (в случае применения кругового излучения) и значительных потерь при распространении в гидрометеорах и газах атмосферы. Однако габариты пользовательских антенн и ресиверов получаются весьма малыми. Поэтому в Европе выделен диапазон частот 40,5.42,5 ГГц для организации систем распределения видеоинформации (MVDS).

Разница в названиях систем весьма условна, поскольку рекомендации для них разрабатывались

на разных континентах. С технической же точки зрения это одни и те же устройства, изготовленные, как правило, производителями радиорелейного оборудования. Радиотракт такой системы "прозрачен" для передачи различных типов аналоговых или цифровых сигналов, будь то NTSC, PAL, SECAM или DVB. Различия будут лишь в числе каналов.

Для передачи сигналов телевидения вполне может быть использован цифровой стандарт MPEG-2, получивший широкое распространение в спутниковых системах телевизионного вещания и модуляция COFDM, защищенная от интерференционных искажений. Для улучшения энергетических показателей на базовых станциях, возможно применение секторных и многолепестковых антенных систем с коэффициентами усиления до 30 - 40 дБ.

Таким образом, микроволновые многоканальные сети распределения информации могут являться дополнением и конкурентом для систем кабельной, радиорелейной и спутниковой связи.

Нормы на показатели неготовности и на показатели качества по ошибкам

Нормы, по рекомендации МСЭ-Т G. 821, состоят из двух основных компонент: показатели неготовности и показатели качества по ошибкам.

Показатели неготовности (ПНГ)

Неготовность аппаратуры - такое состояние участка ЦРРЛ, при котором в течение десяти секундных интервалов, следующих подряд, имеет место хотя бы одно из событий:

пропадание сигнала (потеря синхронизации);

коэффициент ошибок kош = Nош / N > 10^{-3}, где N - число переданных символов, Nош - число ошибочно принятых символов.

Причины, приводящие к неготовности аппаратуры:

экранирующее влияние препятствия при субрефракции;

влияние гидрометеоров (учитывается при частотах выше 6 ГГц);

влияние промышленных атмосферных метеоров (экологические факторы). Данные для расчетов отсутствуют;

ненадежность аппаратуры;

ошибки обслуживающего персонала.

Таблица 3.1. Зависимость качества линии и ПНГ

Качество линии		**ПНГ, %**
Линии связи высокого качества		**0.3 L / 2500**
Линии связи среднего качества	**1 класс**	**0.033 (L=280 км)**
	2 класс	**0.05 (L=280 км)**
	3 класс	**0.05 (L=50 км)**
	4 класс	**0.1 (L=50 км)**
Линии связи локального качества		**0.01-1**

В ряде случаев принято оценивать состояние оборудования термином "готовность". При этом общее время работы оборудования составляется из периодов готовности и неготовности, а линия находится в состоянии готовности, если оба ее направления "готовы".

Показатели качества по ошибкам (ПКО)

Показатели качества по ошибкам системы связи относятся к тем промежуткам времени, в течение которых система находится в состоянии готовности !

Различаются следующие параметры:

- сильно пораженные секунды (СПС);
- минуты пониженного качества (МПК);
- секунды с ошибками (СО);

- остаточный ***кош*** (ОКО).

Сильно пораженные секунды представляют собой процент времени превышения величины ***кош*** = 10^{-3} за 1 секунду. Минуты пониженного качества - процент времени превышения ***кош*** = 10^{-6} за 1 минуту. Секунды с ошибками - процент времени превышения ***кош*** = 10^{-6} за 1 секунду (эта норма определяет качество работы системы связи при передаче данных). В некоторых источниках имеется определение параметра секунды с ошибками как процентное отношение числа бракованных секунд, в течение которых имеется одна или больше ошибок к общему времени работы системы. Параметр СО определяется любыми причинами (а не только замираниями на трассе линии связи).

Величины всех этих параметров зависят от интерференционных замираний сигнала на интервале ЦРРЛ, которые складываются из гладких и частотно-селективных. К гладким замираниям необходимо относить такие замирания, которые не искажают частотную характеристику системы связи.

Соответственно частотно-селективные замирания влияют на АЧХ ствола РРЛ, т.е. в пределах полосы пропускания линии связи вносят различные ослабления на разных частотах. Эти замирания необходимо учитывать при полосе пропускания ВЧ ствола больше 10-15 МГц.

Таблица 3.2. Показатели качества по ошибкам

Линии связи высокого качества		СПС 0.054% L / 2500 МПК 0.4% L / 2500
Линии связи среднего качества *L*секции = 280 км	**1 класс**	СПС 006% МПК 045%
	2 класс	СПС 0.0075% МПК 0.2%
Линии связи среднего качества *L*секции = 50 км	**3 класс**	СПС 0.002% МПК 0.2%
	4 класс	СПС 0.005% МПК 0.5%
Линии связи локального качества		СПС 0.015% МПК 1.5%

Необходимо иметь ввиду, что для проектирования новых цифровых беспроводных линий связи рекомендуется пользоваться новыми, более жесткими нормами, установленными в соответствии с Рек. G.826, особенно, при проектировании систем связи синхронной транспортной иерархии (SDH).

Рекомендации по выбору рабочих частот

В настоящее время освоен весьма широкий диапазон рабочих частот для целей микроволновой радиосвязи, начиная с диапазона 2 ГГц.

Диапазон 2 ГГц (1.7-2.1 ГГц)

Этот диапазон характеризуется возможностью распространения сигналов на достаточно протяженных пролетах (до 50-80 км). Устойчивость распространения радиоволн в сильной степени зависит от экранирующего действия препятствий на интервалах РРЛ при атмосферной рефракции. В этом диапазоне волн антенны обладают весьма большими габаритами, и поэтому коэффициенты усиления не превышают 35-38 дБ при диаметрах параболических антенн до 5 м. С уменьшением размеров антенн эффективность системы связи резко падает. Диапазон подвержен

влиянию помех от других радиотехнических средств.

Диапазон 4 ГГц (3.4-3.9 ГГц)

Наиболее освоенный и загруженный РРЛ диапазон частот. В этом диапазоне работают многие магистральные системы связи. Характеризуется возможностью получать довольно протяженные пролеты (40-55 км) при хороших качественных показателях. Остронаправленные антенны (с коэффициентами усиления порядка 40 дБ) обладают значительными габаритами и весом (прил.2) и, следовательно, требуют весьма дорогостоящих антенных опор.

На распространение сигналов оказывает существенное воздействие атмосферная рефракция, приводящая к экранированию сигнала препятствиями на пролетах, и интерференция прямых и отраженных волн.

Диапазон сложен с точки зрения электромагнитной совместимости, так как в нем работает множество радиотехнических средств.

Диапазон 6 ГГц (5.6-6.2 ГГц)

Популярный в последние десятилетия диапазон частот, предназначенный для магистральных систем связи. Позволяет получить достаточно эффективные системы РРЛ, передающие большие объемы информации. Средняя протяженность пролета достигает 40-45 км. Размеры антенн не слишком велики (например, антенна с коэффициентом усиления 43 дБ имеет диаметр 3.5 м).

На распространение сигналов оказывает существенное воздействие атмосферная рефракция, приводящая к экранированию сигнала препятствиями на пролетах, и интерференция прямых и отраженных волн.

Диапазон 8 ГГц (7.9-8.4 ГГц)

Диапазон 8 ГГц освоен в настоящее время достаточно хорошо. В нем работает большое количество радиорелейных систем средней емкости (порядка 300-700 ТЛФ каналов в стволе для аналоговых систем и до 55 Мбит/с - для цифровых). Существует и аппаратура большой емкости, предназначенная для передачи потоков STM-1.

В этом диапазоне на распространение сигнала начинают оказывать влияние гидрометеоры (дождь, снег, туман и пр.). Кроме того, влияет атмосферная рефракция, приводящая к закрытию трассы или к интерференции волн.

Средняя протяженность пролета РРЛ составляет 30-40 км. Антенны имеют высокий коэффициент усиления при диаметрах порядка 1.5 - 2.5 м.

Число радиосредств в России, использующих этот диапазон, пока относительно невелико, и, следовательно, электромагнитная обстановка благополучна. Однако необходимо учитывать помехи от соседних радиорелейных линий, работающих в данном диапазоне частот.

В настоящее время диапазон применяется для организации зоновых линий связи и различных ответвлений от магистраль-ных систем. Отечественные и зарубежные фирмы хорошо освоили производство аппаратуры и предлагают на рынке широкий спектр аналоговых и цифровых систем как средней, так и большой емкости.

Диапазоны 11 и 13 ГГц (10.7-11.7, 12.7-13.2 ГГц)

Эти диапазоны перспективны с точки зрения эффективности систем РРЛ. При протяженности пролета 15-30 км, высокоэффективные антенны имеют небольшие габариты и вес, что обеспечивает относительную дешевизну антенных опор.

Доля влияния атмосферной рефракции на устойчивость ра-боты систем уменьшается, но увеличивается влияние гидрометеоров.

В этих диапазонах, в основном, строятся цифровые радиорелейные системы связи на скорости до 55 Мбит/с, хотя, есть примеры передачи цифровых потоков со скоростями до 155 Мбит/с

Аппаратура часто строится в виде моноблоков, т.е. приемопередатчики объединены с

антенной и располагаются на вершине антенной опоры.

Но эти диапазоны используют большое количество радиосредств. Спутниковые системы связи, различные радиолокаторы и пеленгаторы, охранные системы создают неблагоприятную электромагнитную обстановку, что затрудняет работу в данных диапазонах.

Диапазоны 15 и 18 ГГц (14.5-15.35, 17.7-19.7 ГГц)

Интенсивное развитие систем связи привело к бурному освоению этих диапазонов частот. Средняя протяженность пролетов достигает 20 км для зон с умеренным климатом. Аппаратура выполняется в виде моноблока. Типовые параболические антенны имеют диаметры 0.6, 1.2 или 1.8 м при коэффициентах усиления от 38 до 46 дБ.

В ряде регионов России диапазон 15 ГГц уже перегружен радиосредствами. Диапазон 18 ГГц пока более свободен.

На распространение сигналов сильное влияние оказывают гидрометеоры и интерференция прямых и отраженных волн. Ослабление в дожде может составлять 1-12 дБ/км (при интенсивности дождей 20-160 мм/час). Некоторое влияние оказывает и сама атмосфера (атомы кислорода и молекулы воды), ослабление в которой достигает 0.1 дБ/км.

Диапазон 23 ГГц (21.2-23.6 ГГц)

Согласно рекомендациям МСЭ-Р в этом диапазоне разрешено строить системы аналоговой и цифровой связи любой емкости.

Средняя протяженность пролетов меньше 20 км, так как на распространение сигналов сильное влияние оказывают гидрометеофакторы и ослабления в атмосфере. Желательно использовать вертикальную поляризацию радиоволн, хотя разрешено использование любой поляризации. Типовые параболические антенны имеют диаметры 0.3, 0.6 и 1.2 м.

Ослабление в дождях может быть от 2 до 18 дБ/км, а в атмосфере достигает 0.2 дБ/км. Диапазон разрешено использовать в спутниковых системах связи. Поэтому при расчетах необходимо учитывать возможность помех.

Диапазон 27 ГГц (25.25-27.5 ГГц)

Диапазон предназначен для построения систем фиксированного радиообслуживания. Характеризуется несколько меньшим ослаблением (меньше 0.1 дБ/км) сигнала в атмосфере. Средняя протяженность пролета 12 км. Ослабление в дождях 3-24 дБ/км. Антенны имеют диаметр 0.3, 0.6 м.

Диапазон 38 ГГц (37-39.5, 38.6-40 ГГц)

Согласно рекомендациям МСЭ-Р в этом диапазоне разрешено строить системы аналоговой и цифровой связи любой емкости. Протяженность пролета меньше 8 км. В случае если показатель неготовности линии связи соответствует локальному качеству, протяженность интервала можно довести до 15 км.

Аппаратура представляет собой моноблок с антенной диаметром 0.3 м. Используется только вертикальная поляризация, так как, при этом получается лучшая устойчивость системы свя-зи при наличии дождей.

Ослабление в атмосфере составляет порядка 0.12 дБ/км, а в гидрометеорах - от 5 до 32 дБ/км (при интенсивности дождей от 20 до 160 мм/час).

Диапазон 55 ГГц (54.25-57.2 ГГц)

Протяженность пролета составляет несколько километров при антеннах диаметром 15 см. Ослабление сигнала в атмосфере до 5 дБ/км, а в дождях - от 7 до 40 дБ/км.

Диапазон 58 ГГц (57.2-58.2 ГГц)

В этом диапазоне разрешено строить системы аналоговой и цифровой связи любой емкости, но рекомендации также пока отсутствуют. Диапазон можно использовать для создания

пролета РРЛ на расстояние в 1-2 км, используя антенны диаметром меньше 15 см. Ослабление сигнала в атмосфере до 12 дБ/км, а в дождях - от 9 до 45 дБ/км. Сильное влияние дождей приводит к неустойчивости работы системы связи.

Необходимо учитывать, что этот диапазон является почти предельным для создания радиосистем, так как на частотах выше 60 ГГц наблюдается непрозрачность атмосферы для радиоволн из-за поглощения энергии в атомах кислорода (резонансные частоты поглощения равны 60 и 120 ГГц). Однако, в последние годы, появился интерес к этим диапазонам для создания безлицензионных радиосистем с пролетами протяженностью 1-2 км.

В условиях очень сухого климата, при малой вероятности осадков или на коротких пролетах, может использоваться диапазон частот 84-86 ГГц и выше В России имеется аппаратура на диапазон частот 93 ГГц.

Проектирование линий связи

Нормы на показатели качества и готовности

Прежде, чем приступать к расчету параметров радиорелейной линии необходимо определить: по какой методики производить расчеты, а также каким нормам эти расчеты должны соответствовать. Выбор и обоснование методики расчета приведен ниже. А сейчас разберемся с нормами на качественные показатели радиорелейной сети.

Показатели качества и готовности для различных СВЧ систем тесно связаны с характеристиками сетей связи. Эти характеристики рекомендованы МСЭ-Р и МСЭ-Т. Основными рекомендациями являются рекомендации МСЭ-Т G.801, G.821 и G.826.

Характеристики в G.82I рекомендованы для цифровых сетей с интегрированными услугами (ISDN) и относятся к каналам со скоростью передачи 64 кбит/с в обоих направлениях. При измерениях на каналах с более высокой скоростью передачи можно воспользоваться рекомендацией G.821 МСЭ-Т, приложение D. Для проектирования систем со скоростью передачи STM-1 и выше используют рекомендацию G.826 МСЭ-Т «Параметры и нормы показателей качества по ошибкам для международных цифровых трактов с постоянной скоростью передачи, равной или выше первичной скорости».

Гипотетическое цифровое соединение, тракт и участок

В Рекомендации G.801 МСЭ-Т определяются модели цифровой сети как совокупности гипотетических объектов определенной длины и состава.

Цифровое ГЭС — это модель, на основе которой могут проводиться исследования применительно к общим показателям качества, что облегчает формирование соответствующих стандартов и норм. Применительно к показателям качества сети ЦСИС принято рассматривать чисто цифровое соединение со скоростью передачи 64 кбит/с. Поскольку показатели качества полной сети и каждый ее параметр в отдельности должны соответствовать требованиям пользователя, то такие показатели в основном должны быть связаны с моделью сети, представляющей очень длинные соединения. На рисунке 3.13 показано удовлетворяющее этому требованию гипотетическое эталонное соединение протяженностью 27 500 км.

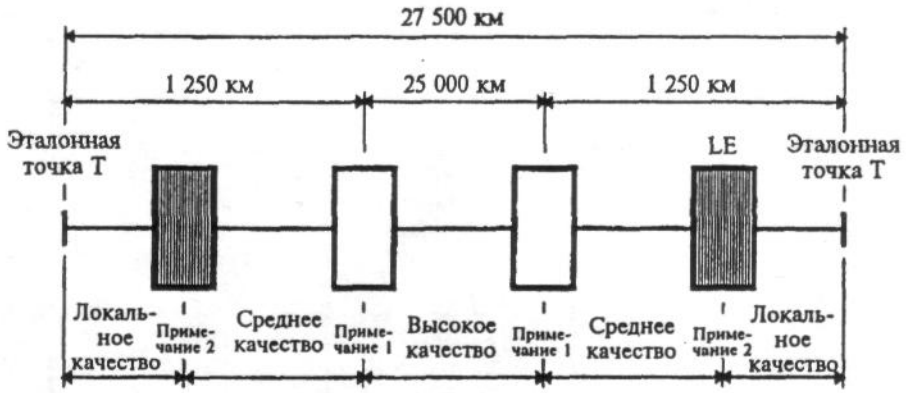


Рисунок 3.13 – Гипотетическое эталонное соединение

Примечание 1.— Невозможно определить, где проходит граница между участками среднего и высокого качества гипотетического эталонного соединения.

Примечание 2.— LE обозначает "местную станцию" или эквивалентную точку схемы.

Для облегчения исследования ухудшений цифровой передачи (например, ошибки в битах, дрожание и дрейф фазы, проскальзывания, время передачи) модель сети должна включать сочетание различных типов элементов передачи (например, системы передачи, мультиплексоры, демультиплексоры, цифровые тракты, транскодеры). Такая модель определяется как ГЭЦЛ. В Рекомендациях МСЭ-Р обычно используется термин ГЭЦТ. Его длина принимается равной 2500 км. Гипотетический эталонный цифровой тракт протяженностью 2500 км для радиорелейных систем состоит из девяти радиоучастков, каждый из которых имеет длину примерно 280 км.

Для того чтобы при расчетах на основе модели могли быть использованы качественные параметры, взятые непосредственно из технических описаний систем передачи, в составе модели используется понятие *гипотетический эталонный цифровой участок* (ГЭЦУ). Входной и выходной порты указанного участка — рекомендуемые интерфейсы, соответствующие Рекомендациям G.703 МСЭ-Т и F.556 МСЭ-Р для различных скоростей цифровой иерархии. Протяженность участков выбрана типичной для цифровых участков, встречающихся в реальных сетях, и достаточно большой, чтобы соответствовать реальным показателям качества цифровых радиосистем. Модель является однородной, то есть она не включает другого цифрового оборудования, такого как мультиплексоры и демультиплексоры. Это позволяет ей быть основой для построения гипотетического эталонного цифрового тракта (ГЭЦТ). В Рекомендации G.921 МСЭ-Т для ГЭЦУ предусмотрена протяженность 50 и 280 км.

Характеристики готовности и качества

МСЭ-Т не устанавливает характеристики готовности для ГЭС. Характеристики готовности для ГЭЦГ установлены в рекомендации 557 МСЭ-Р.

ГЭЦТ считается неготовой, если в течение 10 последовательных секунд возникли следующие условия или одно из них:

- передача цифрового сигнала прервана;
- в каждой секунде BER хуже 10^{-3}.

Неготовность аппаратуры уплотнения исключается. Ее характеристики будут установлены МСЭ-Т позже. Характеристики неготовности делятся на неготовность оборудования и неготовность, вызванную условиями распространения радиоволн. Величина этих долей определяется администрациями или проектировщиками линий, но большинство администраций приняло величину неготовности, вызванную дождем, между 30% - 50% .

Параметры и нормы на показатели качества по ошибкам, согласно G.821

ГЭС, ГЭЦТ и ГЭЦУ служат основой для определения параметров качества по ошибкам и готовности [11, 22].

Рекомендация G.821 МСЭ-Т была разработана 15 лет назад; она была первой Рекомендацией, посвященной показателям качества по ошибкам для международного цифрового соединения. В ней определялись параметры и нормы на показатели качества по ошибкам для канала 64 кбит/с, а в Приложении D содержалась специальная процедура пересчета норм для того случая, если измерения проводились на скорости передачи битов в системе.

На рисунке 4.1 приведена конфигурация полностью цифрового ГЭС с показателями качества по ошибкам соединения по коммутируемому каналу 64 кбит/с и распределением показателей качества по элементам соединения.

Показатели качества по ошибкам должны оцениваться только тогда, когда соединение находится в состоянии готовности.

Параметры показателей качества по ошибкам получаются на основе следующих событий:

- *Секунда с ошибками* (ES): период в 1 секунду, в течение которого наблюдаются ошибки в одном или нескольких битах.
- *Секунда, пораженная ошибками* (SES): период в 1 секунду, в течение которого коэффициент ошибок по битам ≥ 1 x 10^{-3}.

Параметрами являются:

- *Коэффициент секунд с ошибками* (ESR): отношение числа ES к общему числу секунд в период готовности в течение фиксированного интервала измерений;
- *Коэффициент секунд, пораженных ошибками* (SESR): отношение числа SES к общему числу секунд в период готовности в течение фиксированного интервала измерений.

В таблице 3.3 представлены показатели качества по ошибкам для международного соединения сети ЦСИС и его участков в соответствии с Рекомендацией G.821 МСЭ-Т и Рекомендациями F.594, F.634 и F.696 МСЭ-Р.

Таблица 3.3. Показатели качества по ошибкам для международного соединения сети ЦСИС и его участков

Тип участка	**Показатели качества в соответствии с Рек. G.821**		**Показатели качества для ЦРРС**	
	ESR	SESR	ESR	SESR
Локальное качество (значение коэффициента усреднено по	0,012	0,00015	0,012 Рек. F.697 МСЭ-Р	0,00015 Рек. F.697 МСЭ-Р
Среднее качество (значение коэффициента усреднено по блокам)	0,012	0,00015	0,012 Рек. F.696 МСЭ-Р	0,0004 Рек. F.696 МСЭ-Р
Высокое качество 25 000 км, 2500км	0,032 0,0032	0,0004 0,00004	0,0032 Рек. F.594, F.634 МСЭ-Р	0,00054 Рек. F.594, F.634 МСЭ-Р
Международное соединение сети ЦСИС, 27 500 км	<0,08	< 0,002 (0,001+0,001)		

Примечание 1. — К значениям SESR для участков среднего и высокого качества прибавляется поправочная величина 0,001 для учета возникающих время от времени неблагоприятных условий распространения сигнала в сети (имеется в виду худший месяц года). Ввиду случайного характера эффектов, возникающих в худший месяц года в соединениях, которые могут находиться в любой точке

земного шара, принято следующее распределение общей поправочной величины SESR 0,001:

- 0,0005 SESR для ГЭЦТ протяженностью 2500 км радиорелейных систем при использовании в соединении на участке высокого качества;
- 0,0005 SESR для ГЭЦТ протяженностью 2500 км радиорелейных систем при использовании в соединении на участке среднего качества.

Параметры и нормы на показатели качества по ошибкам, согласно G.826

Рекомендация G.826 МСЭ-Т применяется к международным трактам с постоянной скоростью передачи битов, равной или превышающей первичную скорость [23]. Эти тракты могут быть основаны на плезиохронной цифровой иерархии, синхронной цифровой иерархии или быть частью какой-либо другой передающей сети, например, сотовой. Рекомендация является общей в том смысле, что определяет параметры и нормы для трактов независимо от типа сети, частью которой эти тракты являются. Если соединение 64 кбит/с удовлетворяет требованиям этой Рекомендации, можно быть уверенным в том, что оно в большинстве случаев будет удовлетворять и требованиям, содержащимся в Рекомендации G.821 МСЭ-Т. Таким образом, Рекомендация G.826 является единственной Рекомендацией, необходимой для расчетов показателей качества по ошибкам при проектировании сетей с первичной скоростью передачи или выше.

Рекомендация G.826 МСЭ-Т составлена на основе измерения показателей качества по ошибкам в блоках. ***Блоком*** называется набор последовательно передаваемых по данному каналу битов; каждый бит принадлежит одному и только одному блоку. Последовательность битов может не быть непрерывной во времени.

В Рекомендации G.826 МСЭ-Т указываются нормы на показатели качества и готовности, которые сведены в таблицу 3.4.

Таблица 3.4. Нормы на показатели качества и готовности в соответствии с рекомендацией G.826

Участок ВСС России	Длина тракта, км	Показатель SESR, %	Коэффициент неготовности $K_{НГ}$, %	Распределение доли SESR и $K_{НГ}$ для реальных линий связи
Международный участок	12500	0.06	1.5	Пропорционально L для $L \geq 2500$ км
Магистральная сеть (национальный участок)	2500	0.012	0.3	Пропорционально L для $L \geq 50$ км
Внутризоновая сеть	600	0.012	0.05	Пропорционально L для $L > 600$ км; Независимо от длины для $200 < L < 600$ км
	200	0.012	0.05	Пропорционально L для $50 < L < 200$ км
	50	0.003	0.0125	Независимо от длины для

				$L < 50$ км
Местная сеть	100	0.01	0.05	Независимо от длины для $L < 100$ км
Сеть доступа	-	0.015	0.05	Независимо от длины

Таким образом, в нашем случае будем рассчитывать коэффициент неготовности $K_{НГ}$ и количество значительно пораженных секунд SESR, используя нормы из таблицы 3.4.

Выбор методики расчета

В настоящее время существует достаточно большое количество методик расчета радиорелейных трасс. Выбор той или иной методики зависит, как правило, от следующих двух факторов:

1. доступности методики;
2. соответствие методики техническим требованиям на расчет радиорелейной линии.

Мной были найдены следующие методики:

- Методика расчета трасс аналоговых и цифровых РРЛ прямой видимости, Москва, 1987 г., 243 с.;
- Мордухович Л.Г., Степанов А.П. Системы радиосвязи. Курсовое проектирование: Учеб. Пособие для вузов. – М.: Радио и связь, 1987.-192 с.;
- Проектирование радиорелейных линий прямой видимости: Ингвар Хенне, Пер Торвальдсен – Берген: Nera Telecommunications, 1994г. 153с.;
- Справочник по цифровым радиорелейным системам, Международный союз электросвязи, Бюро радиосвязи, г. Женева, 1996 г.

Первые две методики не были взяты для проектирования по следующим причинам:

- методики были составлены в 1987 году и уже морально устарели;
- нет полного представления о методах расчета цифровых РРЛ, хотя относительно аналоговых РРЛ дается вполне достаточно информации;
- в большинстве случаев приводится слишком полный расчет, отсутствие моделей упрощённого расчёта;
- отсутствие экспериментальных данных.

Среди двух оставшихся наиболее приемлемая методика фирмы NERA NETWORKS AS, Норвегия. Автор - Ингвар Хенне, Пер Торвальдсен. Работа довольно подробная, содержащая предварительную и детальную часть расчётов. Учитывает возможность проектирования во всех возможных частотных диапазонах, практически на любой аппаратуре. Последний из перечисленных документов нельзя полностью использовать в расчетах, поскольку, прежде всего, – это справочная литература, хотя некоторые расчеты приводятся достаточно подробно и обоснованно.

Среди частных методик можно выделить две, распространяемые в виде компьютерных вычислительных комплексов:

1. DRRL 4.0;
2. Territories фирмы «Золотая корона».

Обе эти методики используют фирмы, занимающиеся расчетами радиорелейных трасс. Кроме того, Territories имеет хорошую техническую поддержку в виде предоставления цифровых карт при расчете профиля трассы, а также более правильные расчеты в диапазоне меньше 1 ГГц и при передаче потока STM-1.

Таким образом, в качестве основной методики расчетов мной была выбрана методика фирмы NERA NETWORKS, как общедоступная и отвечающая критерию достоверности расчетов. В качестве дополнительной справочной информации было решено использовать Справочник по

цифровым радиорелейным системам международного союза электросвязи.

Расчет качественных показателей радиорелейных линий

Основные положения

Расчет любой радиорелейной линии в первую очередь сводится к выбору трассы и места расположения станций проектируемой сети. Как правило, любой проект по строительству РРЛ подразумевает конкретные места расположения станций. В нашем случае все радиорелейные станции располагаются вблизи газопроводов (основная их задача – обеспечение технологической связи), а также, по возможности, как можно ближе к населенным пунктам и проходящим дорогам, что облегчает обслуживание РРЛ и подвод необходимых коммуникаций. Все внешнее оборудование размещается либо на существующих антенных башнях и опорах, либо на проектируемых. Внутренне оборудование располагается либо в уже существующих старых зданиях на месте демонтируемого оборудования системы «Трал 400/24», либо в специально устанавливаемых контейнерах типа «Север». Все мультиплексорное оборудование и внутренне оборудование радиорелейной связи, а также источники питания устанавливаются в проектируемые 19 дюймовые шкафы связи.

Общая протяженность ЦРРЛ составляет 275.48 км. Средняя длина интервала – 35,435 км. Минимальная длина интервала – 14,75 км. Максимальная длина интервала – 46,15 км. Большая часть площадок проектируемой ЦРРЛ совпадают со станциями существующей РРЛ «Трал-400/24» Нижневартовск – Парабель – Томск. Размещение новых станций будет произведено рядом с н.п. Тунгусово и н.п. Кривошеино, ввиду производственной необходимости ООО «Томсктрансгаз». Нумерация радиорелейных станций ведется от п. Чажемто до г. Томска.

Стоит отметить, что в случае превышения норм на качественные параметры связи РРЛ, применяют следующие технические решения:

1. поднимают антенны станций на большую высоту, что сопряжено с рядом трудностей: как с ограниченностью самой башни (мачты), так и возможной сложной э/м обстановкой с уже имеющимся оборудованием;
2. выбор другого места положения радиорелейной станции;
3. применение другого оборудования (более чувствительный приемник, более мощный передатчик, антенны с большим диаметром);
4. еще один очень часто используемый способ – применение разнесенного приема, который бывает двух видов – пространственный (разнос антенн) и частотный (передача на двух частотах), также может использоваться комбинация этих методов. Частотный метод в терминологии радиорелейной связи более известен как метод выбора «систем резервирования». Поскольку систем резервирования известно несколько, а не все радиорелейное оборудование поддерживает все из них, то наша задача также будет заключаться в выборе наиболее оптимального из этих способов для применения в нашем случае.

Для работы при различных условиях эксплуатации и окружающей среды все активное оборудование может быть использовано в одном из перечисленных ниже режимах:

- 1 + 0 – передача радиосигнала без резервирования;
- 1 + 1 горячий резерв – передача радиосигнала с полным резервированием оборудования.
- 1 + 1 резервирование линии – передача STM – 1 канала через основной и резервный радиоканал, используя два номинала частот с помощью одной антенны.

Режим «горячего резервирования» 1 + 1 представляет собой резервирование оборудования, при котором передается один STM – 1 поток с использованием одного радиочастотного канала. При выходе из строя оборудования, система автоматически переключается на резервный комплект. При этом время переключение настолько мало, что такое пропадание сигнала не превышает нормы по качественным показателям радиорелейной линии, а на практике составляет менее 10 нс. При горячем резервировании необходимо наличие двух комплектов ППУ, которые работают на одну антенну (рисунок 5.1). Существуют еще два режима резервирования «теплый» и «холодный», их основное отличие от «горячего» заключается во времени переключения на

резервный канал. При этом, при «холодном» и «теплом» резервировании можно работать на той же частоте, что и основной канал. Как правило, в последнее время производители современного радиорелейного оборудования стараются использовать только «горячий», и лишь в редких случаях - «теплый».

В некоторых случаях обеспечивают постоянную передачу одной и той же информации по двум независимым каналам, при этом каждый канал имеет свое ППУ и свою антенну. Устройство на приеме производит сравнение сигналов, поступающих на вход приемников и, в зависимости от уровня сигнала, выбирает наилучший. Такой способ позволяет свести потерю информации в связи с замираниями сигнала в атмосфере на нет, но за это надо платить как большим занимаемым частотным ресурсом, так и большей стоимостью оборудования.

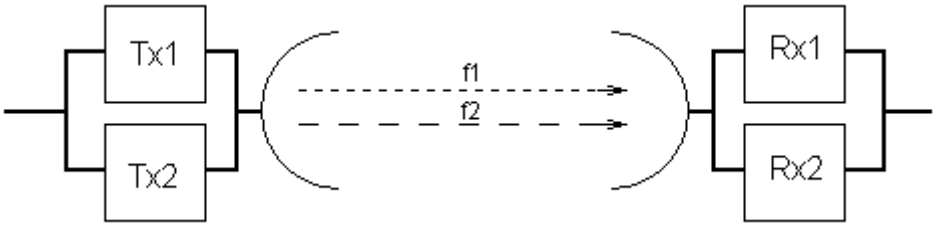


Рисунок 3.14 - Принцип частотного разнесения каналов

Исходные данные для расчетов

Трасса проектируемой ЦРРЛ проходит по климатической зоне Западно-Сибирской низменности через Томский, Шегарский, Кожевниковский, Кривошеинский, Молчановский и Колпашевский район Томской области.

Величина интенсивности дождей составляет 70 мм/ч.

Параметром аппаратуры цифровых РРЛ, характеризующим помехоустойчивость является пороговый уровень сигнала на входе приемника $P_{ПР\,ПОР}$, при котором обеспечивается максимальная нормируемая величина коэффициента ошибок $P_{ОШ\ МАКС}$ (BER). Результаты каждого пролета трассы производились при помощи двух методов. Как основной метод расчета использовалась методика фирмы Nera, для проверки результатов была использована специализированная программа Territories. Нормы на показатели качества приняты как для внутризоновых сетей.

Для расчета статистики глубины сравнительно медленных рефракционных замираний с учетом нелинейного изменения диэлектрической проницаемости воздуха замирания ξ с высотой, вводится понятие эффективного вертикального градиента диэлектрической проницаемости воздуха g. Под величиной g понимают постоянный по высоте градиент $\partial\varepsilon/\partial n$, при котором напряженность поля в точке приема будет такой же, как и в случае реального изменения ξ на трассе. Климатический район проектирования ЦРРЛ характеризуется средним значением градиента диэлектрической проницаемости воздуха $g = -10 \cdot 10^{-8}\ 1/м$ и дисперсией диэлектрической проницаемости воздуха $\sigma = 9 \cdot 10^{-8}\ 1/м$. Рабочая частота аппаратуры составляет $f_P = 7.4\ \ ГГц$.

Расчет качественных показателей пролетов ЦРРЛ

Основные положения

В качестве качественных показателей пролета любой радиорелейной линии используют два параметра, которые мы и будем рассчитывать:

1. Коэффициент неготовности;
2. Коэффициент секунд со значительным количеством ошибок.

Коэффициент неготовности линии $K_{НГ}$ складывается из следующих величин.

$$K_{НГ} = P_{СУМ} + P_{ДОЖ} + P_{ОБОР} \quad , \qquad (3.1)$$

где $P_{СУМ}$ - общая вероятность нарушения радиосвязи, вызванная многолучевым замиранием;

$P_{ДОЖ}$ - вероятность нарушения радиосвязи, вызванная дождем;

$P_{ОБОР}$ - вероятность нарушения радиосвязи, вызванная отказом оборудования.

Прежде, чем приступать к расчету вероятностей нарушения связи, разберемся с таким понятием, как запас на замирание.

Расчет необходимого запаса на замирание

Атмосферные возмущения оказывают влияние на условия передачи на радиорелейных линиях прямой видимости. Уровень принимаемого сигнала изменяется во времени и характеристики системы определяются вероятностью того, что уровень сигнала упадёт ниже порогового значения, или спектр принимаемого сигнала будет сильно искажён.

Рассмотрим упрощенную структурную схему интервала радиолинии и соответствующую диаграмму уровней сигнала (рисунок 5.15). Очевидно, что качество работы линии связи, определяется уровнем сигнала на входе приемника $P_{ПР}$ и возможными отклонениями этого уровня при замираниях.

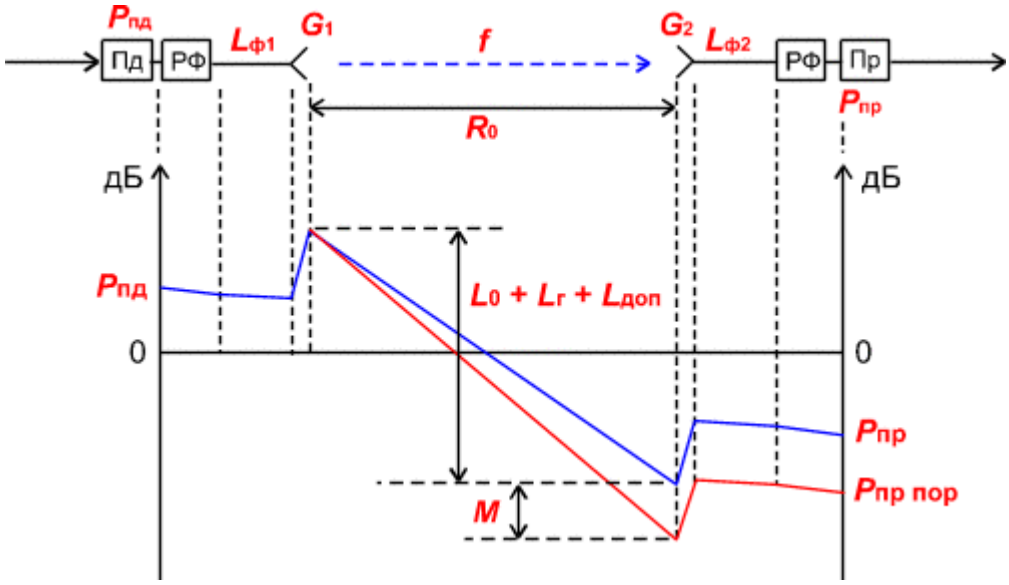


Рисунок 3.15. Диаграмма уровней сигнала на пролете РРЛ

На диаграмме уровней видно, что сигнал излучается передатчиком с уровнем $P_{ПД}$, проходит через разделительный фильтр (РФ), в котором уровень упадет за счет внутренних потерь и поступает через фидерную линию в передающую антенну с коэффициентом усиления G_1. За счет потерь в фидерной линии $L_{ф1}$ уровень сигнала еще уменьшиться, а в передающей антенне увеличится на величину G_1.

При распространении сигнала по интервалу РРЛ (протяженностью R_0, на рабочей частоте f) уровень сигнала упадет за счет ослабления свободного пространства, потерь в газах атмосферы и некоторых дополнительных потерь. Общее ослабление сигнала за счет этих причин может достигнуть 130-140 дБ и больше.

В приемной антенне уровень сигнала увеличится на величину G_2, затем уменьшится в приемной фидерной линии, в разделительном фильтре и поступит на вход приемника с уровнем

$P_{ПР}$. Это значение получается в отсутствии замираний сигнала на пролете РРЛ.

Запас на замирания M является разницей между уровнем сигнала на входе приемника $P_{ПР}$ и его пороговым значением $P_{ПР\,ПОР}$, которое определяется из параметров конкретной аппаратуры цифровых РРЛ для заданной величины $k_{ош}$ (**(**10^{-3} или 10^{-6}).

Уровень сигнала на входе приемника можно определить по следующей формуле:

$$P_{ПР} = P_{ПД} + G_1 + G_2 - L_0 - L_{ф1} - L_{ф2} - L_Г - L_{РФ} - L_{ДОП}\,, \qquad (3.2)$$

где $P_{ПД}$ – уровень мощности передатчика, *дБм*;

G_1, G_2 – коэффициенты усиления передающей и приемной антенн;

$L_{ф1}, L_{ф2}$ – ослабление сигнала в фидерных линиях (Ф1, Ф2), *дБ*;

При отсутствии фидера (когда приемопередатчики объединены с антенной в виде моноблока) необходимо учитывать конструктивные особенности устройства объединения, как правило, в этих случаях потери в фидерах можно принять равными 0 дБ. При больших диаметрах антенн соединение проводится коротким отрезком гибкого волновода, потери в котором $L_{ф1} = L_{ф2} = 0.5\,дБ$;

$L_{РФ}$ – определяется из параметров аппаратуры. Обычно значение ослабления в разделительных фильтрах соответствует сумме потерь в передающем и приемном устройствах. При моноблочной конструкции, данные на уровень мощности передатчика и пороговые значения уровня сигнала на входе приемника, часто относятся к точкам, соответствующим уровням на антенном волноводном соединителе (другими словами, в значения уровней уже заложены потери в разделительных фильтрах). В этих случаях величина потерь $L_{РФ} = 0$. При разнесенной конструкции приемопередатчиков и антенн, потери в РФ составляют 4 - 5 дБ в зависимости от типа и длины фидера.

$L_{ДОП}$ – дополнительные потери, складывающие из потерь в антенных обтекателях $L_{АО}$ и потерь от перепада высот приемной и передающем антенн $L_{ПВ}$ ($L_{ДОП} = 1 - 2\,дБ$);

L_0 – ослабление радио волн при распространении в свободном пространстве рассчитывается по следующей формуле:

$$L_0 = 20 \cdot \lg(4.189 \cdot 10^4 R_0 \cdot f),\, дБ\,, \qquad (3.3)$$

где R_0 – протяженность интервала РРЛ, км;

f – рабочая частота, ГГц.

$L_Г$ – атмосферные потери (потери в газах) рассчитываются по формуле:

$$L_Г = (\gamma_0 + \gamma_H) \cdot R_0 = \gamma_{СУМ} \cdot R_0\,, \qquad (3.4)$$

где γ_0 и γ_H – погонные затухания в водяных парах и атомах кислорода атмосферы, рассчитываемые следующим образом.

Расчет атмосферных потерь

Атмосферные потери, в основном, складываются из потерь в атомах кислорода и в молекулах воды. Практически полная непрозрачность атмосферы для радиоволн наблюдается на частоте 118.74 ГГц (резонансное поглощение в атомах кислорода), а на частотах больше 60 ГГц погонное затухание превышает 15 дБ/км. Ослабление в водяных парах атмосферы зависит от их концентрации и весьма велико во влажном теплом климате и доминирует на частотах ниже 45 ГГц.

Погонные потери в атомах кислорода (дБ/км):

$$\gamma_0 = \left[7.19 \cdot 10^{-3} + \frac{6.09}{f^2 + 0.227} + \frac{4.81}{(f-57)^2 + 1.5} \right] \cdot f^2 \cdot 10^{-3}, \quad (3.5)$$

где f – рабочая частота, ГГц.

Эта формула справедлива для рабочих частот ниже 57 ГГц, при нормальном атмосферном давлении и при температуре воздуха +15 градусов С.

Погонные потери в водяных парах (дБ/км):

$$\gamma_H = \left[0.05 + 0.0021 \cdot \rho + \frac{3.6}{(f-22.2)^2 + 8.5} + \frac{10.6}{(f-183.3)^2 + 9} + \frac{8.9}{(f-325.4)^2 + 26.3} \right] \cdot f^2 \cdot \rho \cdot 1$$

, 3.6)

где ρ – концентрация водяных паров в атмосфере, г/м^3 (обычно $\rho = 7.5\ {}^{г}/_{м^3}$).

Суммарные погонные потери (дБ/км) при температуре, отличной от 15 градусов С:

$$\gamma_{СУМ} = \left[1 - (t-15) \cdot 0.01\right] \cdot \gamma_0 + \left[1 - (t-15) \cdot 0.06\right] \cdot \gamma_H, \quad (3.7)$$

где *t* - температура воздуха в градусах С.

Таким образом, расчет запаса на замирания можно провести по следующей формуле:

$$M = P_{ПР} - P_{ПР\ ПОР}, \quad (3.8)$$

где $P_{ПР\ ПОР}$ – минимально-допустимый уровень мощности сигнала на входе приемника (чувствительность приемника).

Расчет вероятности нарушения связи из-за многолучевого распространения

Метеорологические условия в пространстве, разделяющем передатчик и приёмник, могут иногда оказывать вредное воздействие на принимаемый сигнал. Лучи, которые обычно затухают в тропосфере, могут преломляться и попадать в приёмную антенну и в приёмник, где они суммируются с полезным сигналом. Амплитудно-фазовые соотношения между этими сигналами определяют результирующий сигнал на выходе приёмника.

При этом возникают два эффекта, влияющих на качество передачи сигналов. В одних случаях все компоненты полезного сигнала уменьшаются в равной степени. Это так называемые «плоские» замирания.

В других случаях подавляются только некоторые компоненты спектра, вызывая его искажения. Это так называемые «селективные» замирания. Эти два эффекта проявляются раздельно.

Плоские замирания

В отчёте 338-6 МСЭ-Р и в рекомендации 530 даются два различных метода для расчёта вероятности появления замираний для худшего месяца. Эти методы называются метод 1 и метод 2. Метод 1 используется для проектирования на начальном этапе, метод 2 - для более детального проектирования. Несмотря на то, что профиль нам известен, для пролёта Чажемто -Леботер проведём расчёт первым методом.

Измерения проведённые в различных частях мира (отчёт 336-8 МСЭ-Р и рекомендация 530), показали, что вероятность снижения уровня принимаемого сигнала на M *дБ* по сравнению с уровнем сигнала в свободном пространстве (вероятность нарушения связи), равна:

$$P_{ПЛОСК} = P_0 \cdot 10^{-M/10} \quad \%, \quad (3.9)$$

где M – запас на замирание, *дБм*;

P_0 – вероятность появления замирания, %, которая находится по следующей формуле:

$$P_0 = K \cdot R_0^{3.6} \cdot f_B^{0.89} \cdot (1+|E_h|)^{-1.4}, \% \qquad (3.10)$$

где E_h – наклон пролёта (миллирадиан):

$$E_h = \frac{|h_1 - h_2|}{R_0} \quad \text{мрад}, \qquad (3.11)$$

где h_1, h_2 – абсолютные высоты подвеса антенн, м;

K – геоклиматический коэффициент, его можно оценить по данным замираний для среднего худшего месяца.

При отсутствии таких данных можно использовать следующие эмпирические соотношения для сухопутных трасс:

$$K = 10^{-5.1} \cdot P_L^{1.5} \cdot M \qquad (3.12)$$

где P_L – это процент времени, в течении которого средний коэффициент преломления в самых нижних 100 м атмосферы меньше, чем – 100 N/км. В методике Nera приведены значения P_L для четырёх различных месяцев. Выбирается месяц, имеющий наибольшее значение P_L. По рисункам в находим значение P_L = 5. $M=10^{-0,2}$ этот коэффициент используется при сильно изрезанных профилях пролётов, когда не имеет смысла определять среднее значение угла касания. В нашем случае M=1.

Селективные замирания

Характеристики радиорелейных линий прямой видимости могут быть серьёзно ухудшены селективными замираниями из-за амплитудных и фазовых искажений в полосе сигнала. Эти многолучевые (или селективные) замирания могут появиться в результате отражений от поверхности или аномалий в атмосфере, например, большого градиента в атмосферном волноводе.

При неизменной во времени горизонтально расслоенной атмосфере вертикальный градиент преломления в атмосфере вызывает появление нескольких лучей распространения между передатчиком и приёмником на линии прямой видимости, как показано на рисунке 3.16. Но это лишь упрощенная модель, на самом деле в приемник приходит множество отраженных сигналов на один переданный.

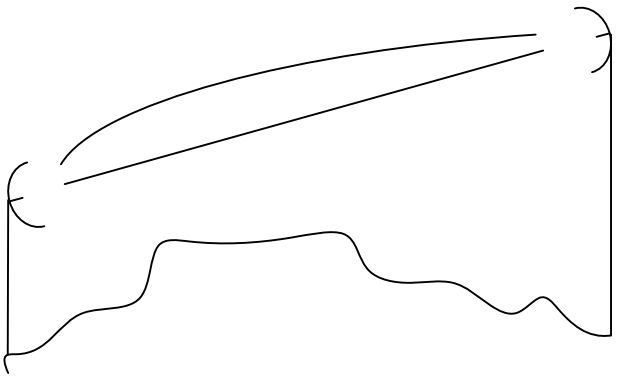


Рисунок 3.16. Упрощённая двулучевая модель селективных замираний

Если через τ обозначить относительное время задержки между двумя путями распространения радиоволн, то относительная фаза между двумя сигналами будет равна $2\pi f \tau$, являясь функцией частоты f. Т.е. амплитуда и фаза принятого сигнала изменяется с частотой. Такое изменение сигнала на радиолинии в зависимости от частоты называется селективным

замиранием.

Влияние селективного замирания на цифровую радиорелейную линию можно кратко описать следующим образом:

- уменьшается отношение сигнал/шум и, следовательно, увеличивается вероятность ошибки (BER);
- искажается форма импульса, увеличивая межсимвольную интерференцию и вероятность ошибки;
- увеличиваются взаимные помехи между ортогональными несущими, потоками I и Q и, следовательно, увеличивается BER.

Имеется целый ряд различных методов прогноза нарушений связи, вызванных селективными замираниями. Фирма “Nera” выбрала использование метода сигнатур, описанных в отчёте 784-3 МСЭ-Р.

Этот метод достаточно хорошо согласуется с результатами измерений и ясно показывает способность радиоаппаратуры противостоять селективным замираниям.

Вероятность появления селективного замирания равна:

$$P_{СЕЛ} = 4.3 \cdot 10^{-1} \cdot \eta \cdot sf \cdot \frac{\tau_m^2}{\tau_0} \quad \%, \tag{3.13}$$

где $sf = 1.8 \cdot 10^{-3}$ – коэффициент сигнатуры оборудования;

τ_m – типовое значение задержки отражённого сигнала на пролёте, *нс,* определяется по следующей формуле: $\tau_m = 0.7 \cdot \left(\frac{R_0}{50} \right)^{1.5}$;

τ_0 – время задержки отражённого сигнала во время измерения кривых сигнатуры; τ_0 = 6,3 нс;

η – коэффициент активности замирания, находится по следующей формуле:

$$\eta = 1 - \exp(-0.2 \cdot \left(\frac{P_0}{100} \right)^{\frac{3}{4}}) \tag{3.14}$$

Общая вероятность нарушения радиосвязи, вызванная многолучевым замиранием, равна сумме вероятностей нарушений, вызванных плоским и селективным замиранием:

$$P_{СУМ} = P_{ПЛОСК} + P_{СЕЛ} \quad \%, \tag{3.15}$$

В методике Nera нет детального расчета параметра SESR. Его значение будем брать из программы Territories. Упрощенно этот расчет можно отобразить следующей формулой:

$$SESR = \left(\frac{K_{ИНТ} - 1}{\phi_{ИНТ}} + 1 \right) \cdot T_{ИНТ} \cdot \varphi_{ИНТ} + T_0 \cdot \varphi_{\tau 0}, \tag{3.16}$$

где $T_{ИНТ}$ – процент времени, в течение которого величина коэффициента ошибок на выходе ЦРРЛ превосходит максимально допустимый коэффициент ошибок из-за многолучевых (интерференционных) замираний на интервале;

T_0 – процент времени, в течение которого величина коэффициента ошибок на выходе цифровой РРЛ превосходит максимально допустимый коэффициент ошибок из-за субрефракционных замираний, происходящих по причине экранирующего влияния препятствий при субрефракции;

$K_{ИНТ}$ – коэффициент интерференции (обычно $K_{ИНТ} = 1$);

$\varphi_{ИНТ}$ – коэффициент готовности в условиях интерференционных замираний;

$\varphi_{\tau 0}$ – коэффициент готовности в условиях субрефракционных замираний.

Расчет вероятности нарушения связи вызванного дождем

Передача СВЧ-сигнала подвержена влиянию осадков. Дождь, снег, частички льда и град ослабляют и рассеивают СВЧ-сигнал, что определяет готовность системы с точки зрения качества передачи. Энергия ослабляется из-за переизлучения (рассеяние) и поглощения (нагревания).

Так как радиоволны представляют собой переменное во времени электромагнитное поле, оно наводит в дождевой капле дипольный момент. Диполь дождевой капли изменяется во времени так же, как и радиоволна и поэтому действует как антенна, переизлучающая энергию. Дождевая капля представляет собой антенну с очень небольшой направленностью и какая-то доля энергии переизлучается по различным направлениям, что приводит к частым потерям энергии. Когда длинна волны меньше размера дождевых капель, большая часть энергии уходит на нагревание капель. Напряжённость поля радиоволны сильно меняется из-за наведения дипольного момента.

Увеличение дождевых капель приводит к изменению их формы, они приобретают форму отличную от сферической. Это отклонение от сферической формы вызывает их растяжение в горизонтальном направлении. Следовательно, капли будут ослаблять горизонтально поляризованную волну больше, чем вертикально поляризованную. Это значит, что вертикальная поляризация предпочтительней на высоких частотах, где доминирует «простой» радиолинии, вызванный дождём.

Поскольку дождь имеет тенденцию идти зарядами (особенно дожди с высокой скоростью), только часть пролёта радиолинии будет подвержена влиянию дождя.

Эффективная длина пролёта, содержащего дождевые заряды, определяется выражением:

$$\psi = \frac{R_0}{1 + \frac{R_0}{35 \cdot \exp(-0.015 \cdot I)}} \quad \text{км}, \tag{3.17}$$

где $I = 70\ {}^{мм}/_{ч}$ – интенсивность дождя (значение было приведено в исходных данных, выбирается в зависимости от региона).

Затухание на пролёте, вызванное дождём, может быть найдено по формуле:

$$A = \psi \cdot k \cdot R^{\alpha}, \quad дБ \tag{3.18}$$

где k = 0.00454, α = 1.327 – коэффициенты регрессии для данного частотного диапазона, как функции частоты и поляризации (взяты из методики фирмы Nera). Расчёт неготовности, вызванной дождём, будет вестись для горизонтальной поляризации, т.к. в этом случае затухание в осадках электромагнитной волны выше.

Неготовность, вызванная дождём, может быть найдена по формуле:

$$P_{ДОЖ} = 10^{11.628 \cdot \left(-0.546 + \sqrt{0.29812 + 0.172 \cdot \log\left(0.12 \cdot \frac{A}{M} \right)} \right)} \tag{3.19}$$

Чтобы избежать мнимых значений, необходимо использовать округленное значение ${A}/{M} = 0.155$, если ${A}/{M} < 0.155$.

Учет рефракции радиоволн

Рефракцией называется искривление траектории волн, обусловленное неоднородным строением тропосферы. Коэффициент преломления в тропосфере:

$$n = \sqrt{\varepsilon} \approx 1 + \frac{\varepsilon + 1}{2}, \tag{3.20}$$

где ε – относительная диэлектрическая проницаемость воздуха, которая находится:

$$\varepsilon = 1 + \left(\frac{1.552 \cdot 10^{-4}}{T}\right) \cdot \left(P + \frac{4810 \cdot e}{T}\right), \tag{3.21}$$

где $T = 273^0 C + t^0 C$ – температура воздуха по абсолютной шкале;

P – общее давление воздуха, ГПа (1Гпа = 1мбар);

e – давление водяного пара, Гпа;

Коэффициент преломления n, также как и ε, в интересующем нас диапазоне частот по величине близок к единице, поэтому чаще пользуются коэффициентом преломления выраженном в «N–единицах»:

$$N = (n-1) \cdot 10^{-6} \approx \left[\frac{\varepsilon - 1}{2}\right] \cdot 10^6, \tag{3.22}$$

Так как $P, e \; и \; T$ являются функциями высоты, N также является функцией высоты. Для нормальной атмосферы (стандартной, хорошо смешанной) изменение N с высотой определяется выражением:

$$N(h) = 315 \cdot e^{-(0.316 \cdot h)}, \tag{3.23}$$

где h – высота над поверхностью Земли, км.

Под величиной $a_э$ понимают такое значение радиуса Земли, при котором траекторию радиоволн можно считать прямолинейной

$$\frac{1}{a_э} = \left(157 + \frac{dN}{dh}\right) \cdot 10^{-6}, \tag{3.24}$$

Для определения кривизны луча на практике используется понятие коэффициента рефракции:

$$K = \frac{1}{\left(1 + R_з \cdot \frac{dN}{dh} \cdot 10^{-6}\right)}, \tag{3.25}$$

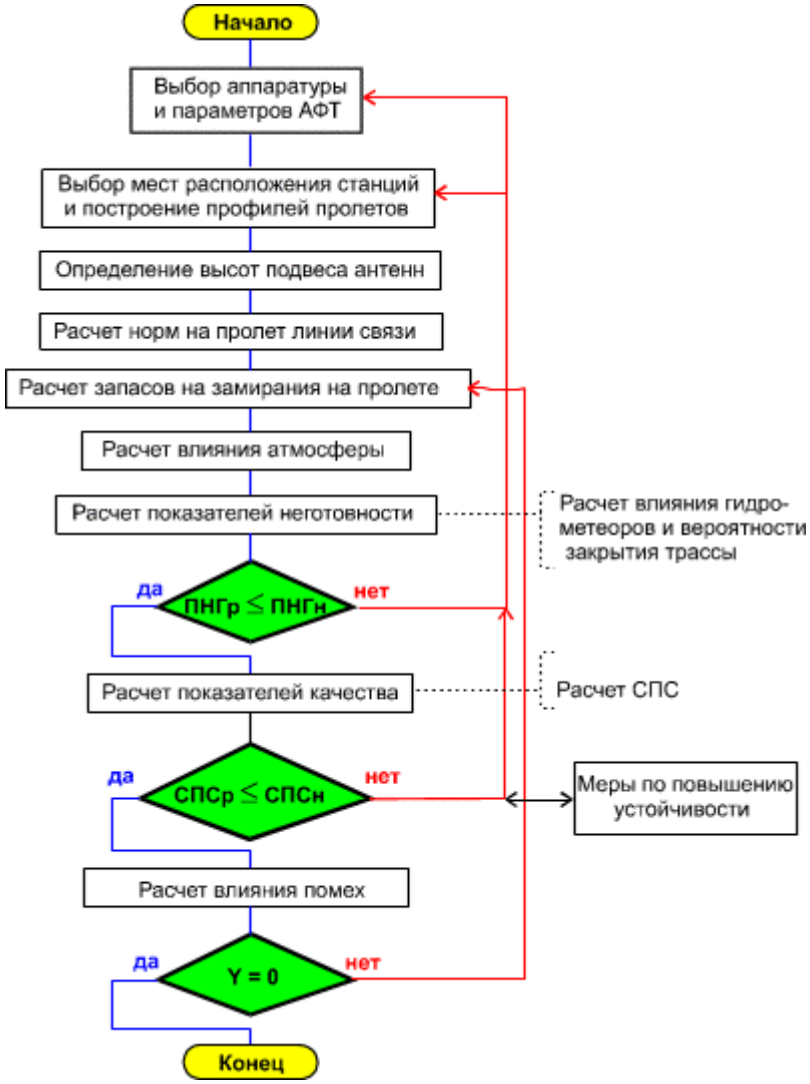
Для нормальной атмосферы $dN/dh = -40$. Соответствующее значение K по формуле 3.25 равно: $K = \frac{1}{\left(1 + 6370 \cdot (-40) \cdot 10^{-6}\right)} = \frac{4}{3}$

Это значение и будем использовать при моделировании распространения радиоволн в дальнейших расчетах.

Алгоритм расчета параметров ЦРРЛ

По материалам предыдущих разделов можно составить общий алгоритм расчетов, который заключается в последовательном подборе параметров аппаратуры и трассы для достижения заданных качественных показателей. На практике встречаются несколько задач при расчетах ЦРРЛ. Перечислим наиболее часто встречающиеся варианты.

1. Рассчитать линию связи при заданных пропускной способности и качественных показателях.
2. Рассчитать линию связи при заданных пропускной способности, диапазоне рабочих частот и качественных показателях.
3. Определить основные параметры линии связи при заданных аппаратуре и конечных пунктах.
4. Провести модернизацию существующей линии связи.
5. Определить возможность построения линии связи между пунктами при наименьшей стоимости системы.



Естественно, алгоритм расчета по разным вариантам необходимо модифицировать для конкретных условий. В большинстве случаев расчет начинается с выбора диапазона рабочих частот, типов аппаратуры и параметров антенн. Аппаратуру желательно выбирать с возможно меньшим значением уровня порогового сигнала на входе приемника при заданной пропускной способности и с возможностью варьирования несколькими значениями уровней мощностей

передающих устройств.

При выборе антенн нужно пользоваться несколькими соображениями. Антенны с большим коэффициентом усиления увеличивают энергетический потенциал сигналов на линии связи, что улучшает качественные показатели. Такие антенны в определенной мере могут улучшить помеховую ситуацию на трассе РРЛ за счет хорошего защитного действия. Однако антенны с большим коэффициентом усиления имеют и большие размеры. Они подвержены сильным ветровым нагрузкам и требуют жесткого крепления и жестких антенных опор, что увеличивает стоимость линии связи. Поэтому нужно выбирать разумный компромисс между стоимостью и качеством.

При выборе мест расположения станций и продольных профилей пролетов можно воспользоваться рекомендациями, приведенными выше. Это очень ответственный этап, во многом определяющий работоспособность линии связи. При этом нужно пользоваться качественным картографическим материалом, а в наиболее критических случаях проводить практическое обследование местности со съемкой основных высотных отметок. Высоты подвеса антенн определяются (в диапазонах частот выше 10 ГГц) по критериям.

После определения мест расположения станций и уточнении протяженностей пролетов РРЛ можно рассчитать нормы, относящиеся к каждому пролету, пользуясь данными, приведенными выше. Необходимо напомнить, что нормы на цифровые РРЛ не установлены окончательно. Поэтому нужно следить за рекомендациями МСЭ-Р по данным вопросам.

На этапе расчета запаса на замирания в пролетах РРЛ можно сделать предварительные выводы о правильности выбора основных параметров пролетов, аппаратуры и антенн. В большинстве случаев запас на замирания не должен быть меньше 26 - 28 дБ. При таком запасе, в определенных условиях, еще возможно выполнение норм на показатели ЦРРЛ. Слишком большие запасы на замирания (50-60 дБ) экономически неоправданны и их нужно избегать.

Перед проведением расчета показателей неготовности требуется определить факторы, приводящие к нарушениям работоспособности линии связи. Как правило в рассматриваемых диапазонах частот работоспособность линии определяется, в основном, влиянием дождей (гидрометеоров). Закрытия трасс маловероятны при малой протяженности пролетов и учитываются в отдельных случаях.

Из всех показателей качества по ошибкам в большинстве случаев определяется процентная величина сильно пораженных секунд, остальные величины рассчитываются по потребности.

Если после выполнения вышеперечисленных действий нормы на неготовность и качественные показатели не выполняются, расчет повторяется с другими данными на аппаратуру, антенны или пролеты до получения удовлетворительных результатов.

Следующий пункт расчетов - учет помеховой ситуации для каждого пролета. Здесь необходимо провести анализ всех источников помех, провести расчеты отношений С/П и определить величины деградации порогов приемных устройств. После этого, пересчитываются запасы на замирания с учетом величин деградации порогов и повторяются все расчеты в целях получения требуемых качественных показателей. При невыполнении норм применяются меры по увеличению энергетических уровней сигналов на пролетах, изменению азимутов пролетов, планов распределения рабочих частот или структуры линии связи в зависимости от конкретной ситуации.

В некоторых сложных случаях приходится применять меры по повышению устойчивости работы системы связи на отдельных пролетах. Но подобные способы нужно использовать только в случаях крайней необходимости, так как они экономически невыгодны.

Автоматизация проектирования цифровых радиорелейных линий

На данный момент существует необходимость быстро и точно рассчитывать качественные показатели цифровых радиорелейных линий в зависимости от окружающей их обстановки – этой цели как раз и служат программные комплексы по автоматизации проектирования РРЛ.

Существует несколько образцов данного ПО:

1. RPS2: Radio Planning System 2

2. Балтика-РРЛ
3. Проектирование и анализ радиосетей (ПИАР)
4. DRRL версия 3.1

RPS2: Radio Planning System 2

Универсальная Система RPS-2 предназначена для автоматизированного проектирования беспроводных сетей различной архитектуры (радиорелейных, транкинговых, сотовых), применяющих различные стандарты передачи данных. Использование системы позволяет в сжатые сроки разработать проект новой сети или расширить уже развернутую сеть, оценить ее достоинства и недостатки, проанализировать показатели электромагнитной совместимости проектируемой сети с другими сетями, работающими в той же местности, и оптимизировать характеристики с учетом конкретных географических условий местности при заданном распределении трафика и источников помех.

По своим функциональным возможностям, точности и полноте расчета характеристик сети, по удобству пользовательского интерфейса, программа RPS-2 не уступает наиболее известным зарубежным аналогам, выгодно отличаясь от них ценой, существенно более низкими требованиями к конфигурации компьютера, русским интерфейсом, доступностью технической поддержки и сопровождения.

Исходными данными являются:

- Цифровые карты местности. Они могут быть представлены в одном из стандартных форматов (“MapInfo”, “Planet” и т.д.) и с помощью прилагаемого конвертора преобразованы во внутренний формат программы, более экономный с точки зрения скорости проведения расчетов. При необходимости, не выходя из программы, картографические данные можно отредактировать, добавив новые объекты – препятствия и типы местности.
- База данных с характеристиками применяемого оборудования (частотный диапазон, диаграммы направленности и усиление антенн, частотные и энергетические характеристики приемопередатчиков, потери в фидерах и т.д.).

Программа позволяет:

- размещать радиостанции в заданном месте рассматриваемой территории, работающие в любом из применяемых в России и за рубежом стандартов (NMT-450, AMPS, D-AMPS, GSM, IS-95, SmarTrunk, TETRA, MPT 1327, EDACS и т.д.). Кроме того, пользователь имеет возможность определить свой стандарт проектируемой сети, введя его основные параметры: частотный диапазон, ширину канала и т.д.;
- определять для радиостанций оптимальный состав оборудования из базы данных, которая может пополняться и редактироваться пользователем;
- задавать и редактировать распределение плотности трафика в рассматриваемом регионе, что позволяет анализировать характеристики сотовых и транкинговых систем в условиях различной загрузки;
- рассчитывать, отображать на экране и выдавать на печать основные характеристики планируемой сети;
- рассчитывать показатели электромагнитной совместимости (уровень взаимных помех) планируемой сети с другими сетями;
- оптимизировать параметры планируемой сети путем изменения местоположения радиостанций, а также варьируя состав и технические характеристики размещаемого на них оборудования (программа снабжена удобным пользовательским интерфейсом, обеспечивающим возможность интерактивно проводить указанные изменения);
- отображать результаты измерений уровня принимаемого сигнала и сравнивать их с результатами расчета с последующей оптимизацией параметров применяемых математических моделей расчета.

Характеристики беспроводной сети, рассчитываемые с помощью программы RPS-2:

- область прямой видимости радиостанции;
- уровень сигнала (покрытие) в заданной окрестности указанной радиостанции с учетом

диаграммы направленности излучающей антенны;

- требуемая мощность излучения абонента, достаточная для надежного приема его сигнала;
- помехи от близлежащих и удаленных радиостанций;
- профиль любой радиолинии;
- потери распространения между передающей и приемной антеннами;
- сигнал на входе приемной антенны абонента;
- отношение сигнал/шум в прямой и обратной линиях с учетом всех видов внутрисистемных и внешних помех;
- зоны, обслуживаемая секторами базовых станций в условиях помех и их реальная загруженность (трафик, приходящийся на каждый сектор);
- зоны, в которых происходит переключение абонентов с одной станции на другую, или с одного на другой их сектор (зоны hand-off);
- сбалансированность прямой и обратной линий базовых станций.

При расчете радиопокрытия пользователь имеет возможность выбрать одну из нескольких моделей распространения радиоволн. Все они рекомендованы к использованию МККР. В программе используются статистические модели распространения Хата и Уолфиш-Икегами, в которых грубо учитывается характер местности (сельская, пригород, городская, плотная городская), модель распространения МККР - рекомендация 370-5, в которой используются статистические данные профиля радиолинии. Кроме того, имеется возможность использовать модель, основанную на строгом анализе профиля радиолинии с выделением препятствий и учетом дифракционных потерь на них, поиском точек отражения и учетом соответствующих потерь. Здесь же имеется возможность учесть дополнительные потери в листве деревьев, эффекты дифракции на крышах и экранировки в городской местности. Имея хорошую цифровую карту, можно с высокой точностью рассчитать покрытие и другие характеристики сети.

Программу RPS-2 можно использовать для планирования как макро-, так и микро-ячеек сотовых сетей, включая микросотовые системы, работающие внутри зданий. При расчете характеристик распространения сигналов внутри зданий использована оригинальная математическая модель.

RPS-2 состоит из следующих программных модулей:

- модуль расчета радиорелейных сетей;
- модуль расчета транкинговых и сотовых сетей всех стандартов;
- модуль расчета сетей в стандарте CDMA;
- модуль расчета сетей, работающих внутри зданий;
- модуль импорта результатов эксперимента, их отображения, сравнения с расчетом и корректировки параметров используемых моделей по результатам этого сравнения;
- модуль расчетов, связанных с разработкой санитарного паспорта места;
- автоматический конвертор цифровой карты из стандартного формата во внутренний формат представления картографических данных.

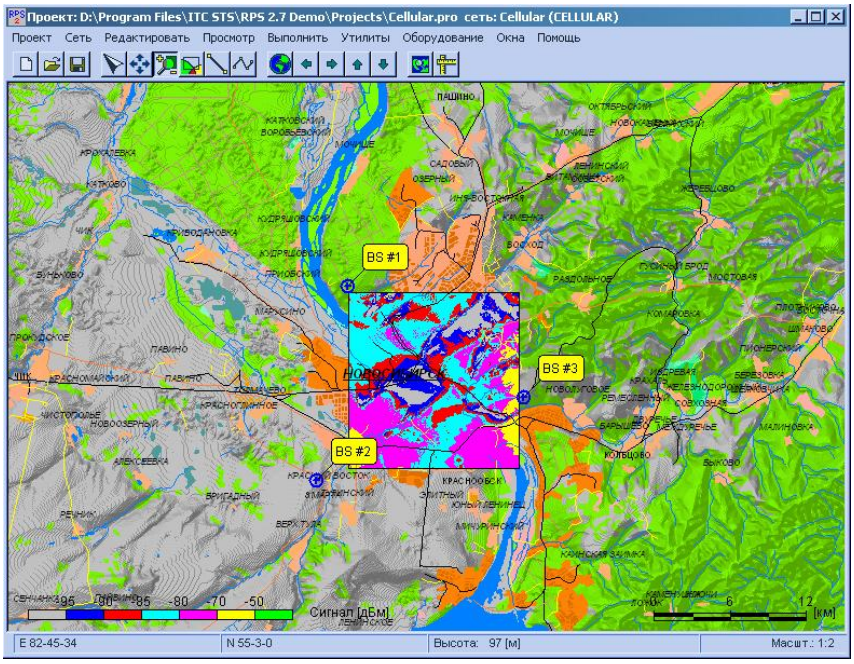
По желанию заказчика возможна поставка программы с любым набором указанных модулей.

Минимальные требования к конфигурации компьютера:

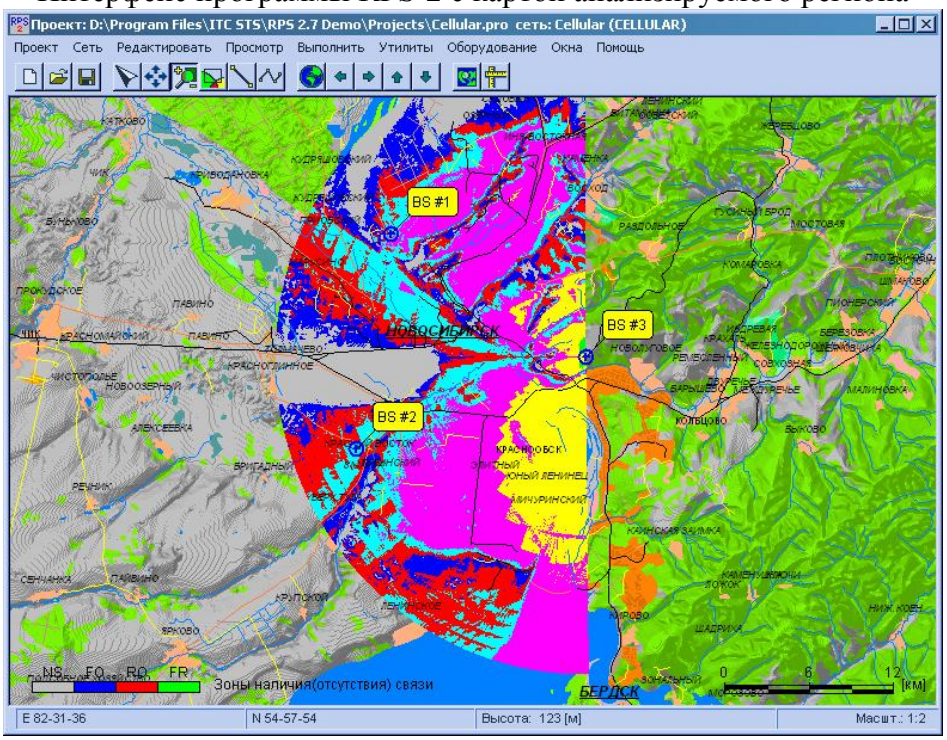
- Процессор Pentium II, 400 МГц или аналогичный;
- MS Windows 9x/Me/NT/2k/XP;
- 32 Мб ОЗУ;
- не менее 120 Мб свободного пространства на жестком диске;
- монитор с разрешением 800x600 High Color.

Оптимальные требования к конфигурации компьютера:

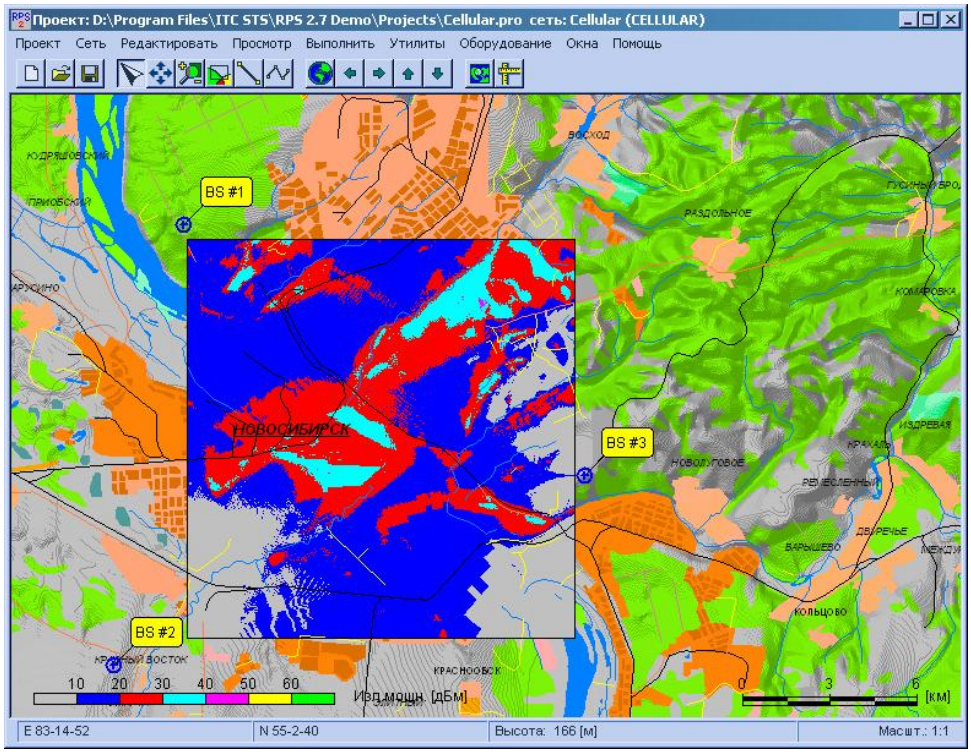
- процессор Pentium 4, 2 ГГц или аналогичный;
- 128 Мб ОЗУ;
- 200 Мб свободного места на жестком диске;
- монитор с разрешением 1280x1024 True Color.



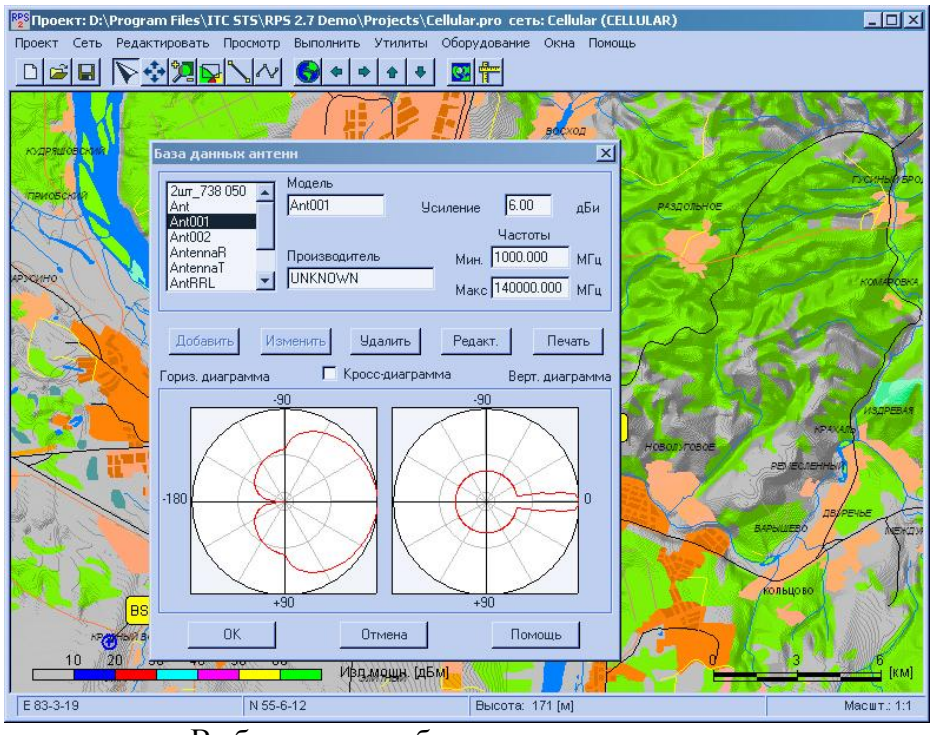
Интерфейс программы RPS-2 с картой анализируемого региона



Покрытие



Необходимая мощность абонентов



Выбор антенн в базе данных программы

Балтика-РРЛ

Решаемые задачи:

- построение профиля трасс РРЛ;
- расчет потерь распространения радиоволн;
- расчет устойчивости связи;
- оптимизация высоты подвеса антенн.

Пользовательский интерфейс обеспечивает:

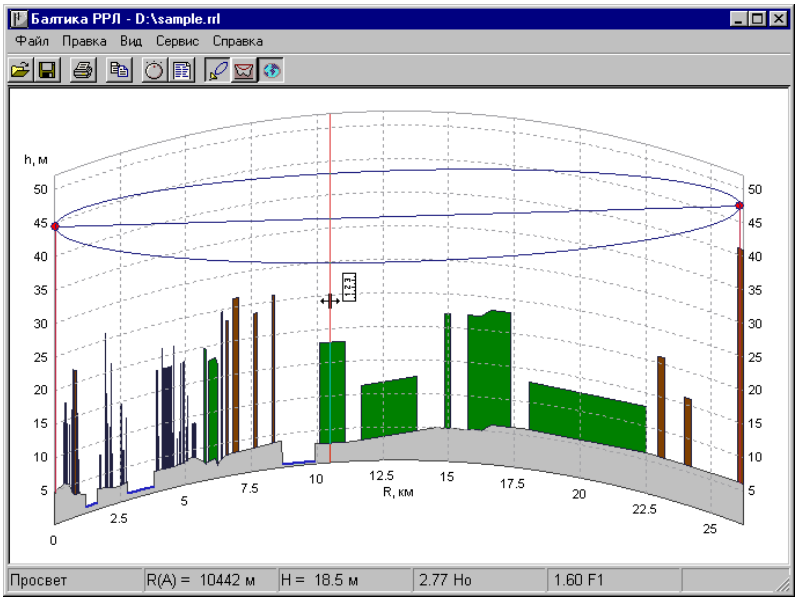
- ввод данных для построения профилей интервалов;
- ввод и редактирование исходных данных для расчетов;
- сохранение всех данных с целью их повторного использования;
- формирование и печать отчета.

При проведении расчетов учитывается:

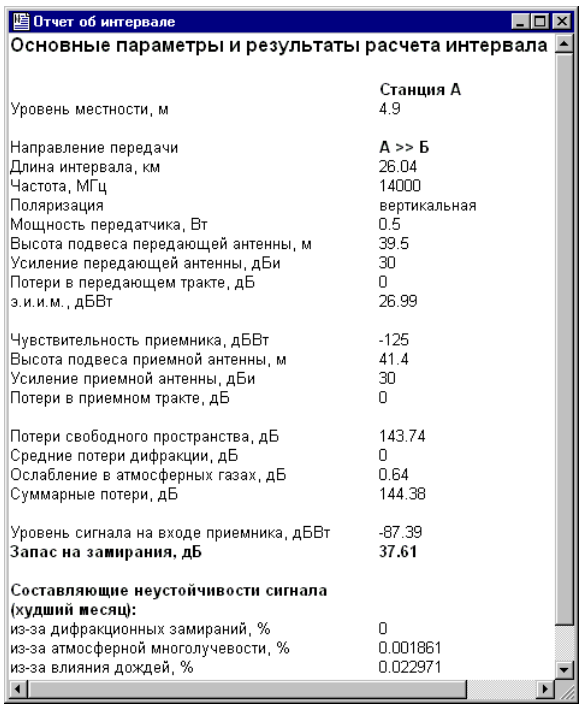
- частота сигнала;
- поляризация;
- мощность передатчика;
- чувствительность приемника;
- потери в антенно-фидерных трактах передатчика и приемника;
- высоты подвеса и коэффициенты усиления антенн;
- параметры распределения градиента индекса рефракции;
- концентрация водяного пара в атмосфере;
- интенсивность выпадения осадков;
- профиль рельефа местности;
- характер местности.

Расчеты:

- потерь распространения с учетом дифракции на основе анализа профиля местности;
- ослабления в атмосферных газах;
- запаса на замирания;
- неустойчивости связи на интервале в условиях наихудшего месяца, в том числе:
    - составляющей неустойчивости связи при субрефракции;
    - составляющей неустойчивости связи, обусловленной влиянием дождей;
    - составляющей неустойчивости связи, обусловленной многолучевым распространением в атмосфере.



Интерфейс программы


Отчет об интервале

Основные параметры и результаты расчета интервала

	Станция А
Уровень местности, м	4.9
Направление передачи	**А >> Б**
Длина интервала, км	26.04
Частота, МГц	14000
Поляризация	вертикальная
Мощность передатчика, Вт	0.5
Высота подвеса передающей антенны, м	39.5
Усиление передающей антенны, дБи	30
Потери в передающем тракте, дБ	0
э.и.и.м., дБВт	26.99
Чувствительность приемника, дБВт	-125
Высота подвеса приемной антенны, м	41.4
Усиление приемной антенны, дБи	30
Потери в приемном тракте, дБ	0
Потери свободного пространства, дБ	143.74
Средние потери дифракции, дБ	0
Ослабление в атмосферных газах, дБ	0.64
Суммарные потери, дБ	144.38
Уровень сигнала на входе приемника, дБВт	-87.39
Запас на замирания, дБ	**37.61**
Составляющие неустойчивости сигнала (худший месяц):	
из-за дифракционных замираний, %	0
из-за атмосферной многолучевости, %	0.001861
из-за влияния дождей, %	0.022971

Результаты расчетов

Расчеты основаны на рекомендациях МСЭ Р.530-7, Р.526-4, Р.676-3, Р.838 и "Методике расчета трасс аналоговых и цифровых РРЛ прямой видимости" (НИИР).

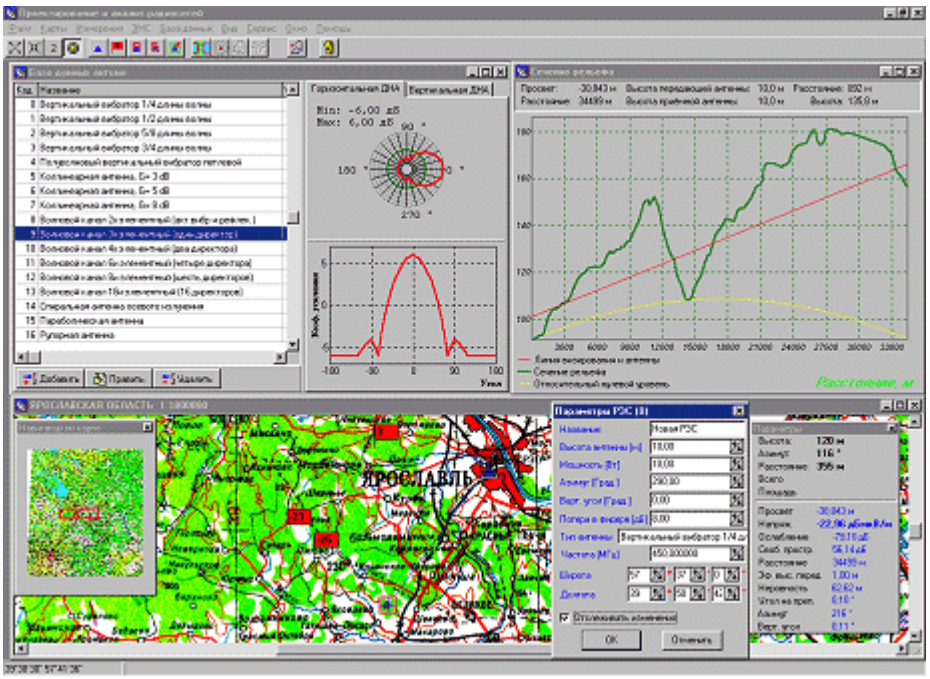
3. Порядок выполнения работы

Система ПИАР
Проектирование и анализ радиосетей (ПИАР)
версия 4.53

Технологии управления радиочастотным спектром включают в числе прочих следующие задачи:

- оценка электромагнитной обстановки (ЭМО) в местах предполагаемого размещения РЭС для обоснования решений о выделении полос, назначении радиочастот и принятия мер по повышению эффективности использования радиочастот, на основе оптимизации частотных присвоений, прогнозирования и измерения границ зон уверенного приема;
- анализ электромагнитной совместимости ЭМС РЭС (ВЧ устройств).

Для решения указанных задач в НПФ «ЯР» разработана система «Проектирование и анализа радиосетей» (ПИАР). Исходные данные для расчета ЭМО и ЭМС измеряются и прогнозируются по верифицированной методике, метрологически аттестованной в соответствии с ГОСТ Р8.563-96 (Свидетельство N 32/037-2002 от 19.03.2002 года), в связи с чем их достоверность гарантируется. В настоящее время Геоинформационная система (ГИС) ПИАР версии 4.53 находится в эксплуатации в 52 регионах России.

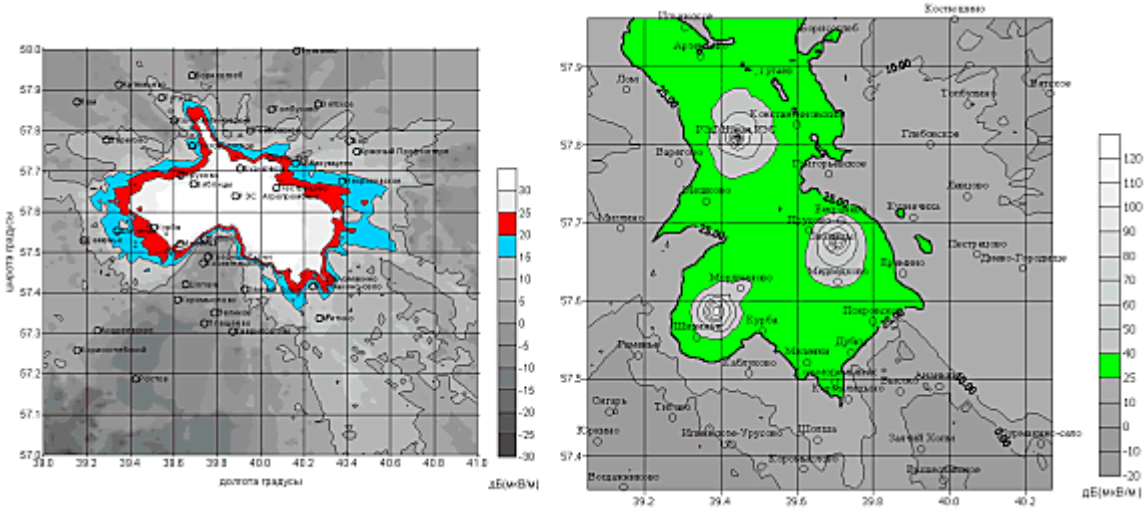


Интерфейс программы ПИАР 4.53

ГИС ПИАР позволяет решать следующие основные задачи:

- производить анализ напряженности электромагнитных полей передатчиков,
- выполнять расчет карт напряженности поля,
- строить зоны уверенного радиоприема и радиосвязи,
- рассчитывать количество населения в зоне уверенного приема,
- анализировать ЭМС РЭС.

В пакет поставки входит утилита для математической обработки множества зон покрытия, позволяющая, например, строить пересечения, объединения зон и многое другое. Кроме того, Заказчику поставляются заполненные справочники типов РЭС (более тысячи наименований), антенн и классов излучений. Данные справочники постоянно пополняются фильтруемыми из множества источников достоверными сведениями.



Хочется отметить тот факт, что это единственный производитель который предоставил демо – версию своей программы для ознакомления. Программа обладает удобным и понятным интерфейсом и позволяет выполнять все заявленные действия, в пределах доступных в демонстрационной версии.

4. Рекомендуемая литература

1. Евсеенко Г. Н. Цифровые системы передачи: Учебное пособие. — Ростов-на-Дону: РКСИ, 2005. — 100 с.;
2. Маковеева М. М., Шинаков Ю. С., Системы связи с подвижными объектами: Учеб. Пособие для вузов – М.: Радио и связь, 2002 – 440 с., ил;
3. Мордухович Л.Г., Степанов А.П. Системы радиосвязи. Курсовое проектирование: Учеб. пособие для вузов. – М.: Радио и связь, 1987. – 192с.: ил;
4. М. А. Баркун, О. Р. Ходасевич - Цифровые системы синхронной коммутации. -М.: Эко-Трендз, 2001.;
5. Проектирование радиорелейных линий прямой видимости: Ингвар Хенне, Пер Торвальдсен – Берген: Nera Telecommunications, 1994г. 153с.;
6. Система сигнализации ОКС №7 – М.: Радио и связь. 2002. 368 с.;
7. Справочник по радиорелейным системам; Международный союз электросвязи, - Бюро радиосвязи, 1996 г., Женева;
8. Телекоммуникационные системы и сети. Т1: Учеб. Пособие/ Крук Б. И., Попантонопуло В. Н., Шувалов В. П., - Изд. 2-е, испр и доп., - Новосибирск: Сиб. предприятие «Наука» РАН, 1998 г.;
9. http://www.kunegin.narod.ru;
10. http://www.micran.ru;
11. http://www.morion.ru;
12. http://www.nec.ru;
13. http://www.nera.com.ru;
14. www.rps2.ru - RPS2: Radio Planning System 2
15. www.loniir.ru – Байкал РРЛ
16. dsplab.uniyar.ac.ru – ПИАР 4.53
17. www.ctt-group.ru – DRRL 3.1

Компьютерный практикум 4. 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 NETGEAR.

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

Проведение картирования дает достоверную информацию о размерах зон покрытия каждой из точек. При развертывании радиоканла для подключения удаленного офиса был учтен тот факт, что в здании фирмы уже развернута беспроводная сеть, были приняты меры

по снижению взаимного влияния. В сети применяется взаимная ориентированная на пользователя аутентификация EAP-PEAP-MSCHAP v2. Для шифрования передаваемой по радиоканалу информации применяется алгоритм шифрования AES. Система реализована на базе оборудования производимого фирмой NETGEAR, оборудование полностью соответствует стандарту 802.11g и обладает достаточной для реализации проекта функциональностью.

2. Краткие теоретические сведения

Беспроводные сети стандарта 802.11 или Wi-Fi, приобретают все большую популярность. В качестве среды передачи используется радиофир. 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).

Данная работа посвящена вопросам проектирования беспроводной высокозащищенной локальной сети передачи данных фирмы «Стек», в задачи которой входят:

- Обеспечение доступа сотрудников организации к ресурсам ЛВС
- Организация связи с удаленным офисом
- Обеспечение доступа к сети Internet

Для того чтобы начать проектирование такой сети, необходимо представить ее структуру, зафиксировать основные функции, рассмотреть существующие на сегодняшний день стандарты передачи данных. Выполнить их сравнительный анализ, который позволит определить, какая из радиотехнологий позволит построить данную систему оптимальным образом. Для этого необходимо будет задаться некими качественными требованиями к системе. Это позволит нам на основе сформулированных критериев качества выбрать программно-аппаратный комплекс. На базе которого будет развернута радиосеть. Необходимо произвести планирование размещения компонентов системы, с последующей их установкой, а также анализ защищенности и производительности сети, с проведением испытаний системы. В результате проектирования мы получим беспроводную сеть передачи данных удовлетворяющую условиям ТЗ.

Назначение и область применения системы

Проектируемая сеть стандарта 802.11g относится к классу беспроводных сетей, т.е. в качестве среды передачи используется радиоэфир. 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 к Интернет. Не мало важными характеристиками сети являются

скорость передачи и задержки при передачи пакетов. Беспроводные сети не могут похвастаться высокими скоростями передачи. 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

Перед началом проектирования следует четко определить функции проектируемой сети. В дальнейшем это позволит построить оптимальную, с точки зрения производительности и безопасности систему, удовлетворяющую потребностям организации. Главной функцией проектируемой сети является предоставление сотрудникам фирмы доступа к ресурсам локальной вычислительной сети. В корпоративной сети циркулирует конфиденциальная информация, нуждающаяся в защите, поэтому второй немаловажной задачей является обеспечение ее конфиденциальности. Конфиденциальность достигается применением шифрования и надежной, желательно двухсторонней аутентификацией. В рамках данного проекта не требуется подсчет трафика потребленного пользователем, так как это будет делать шлюз проводной LAN. Итак сформулируем 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. 4.1).

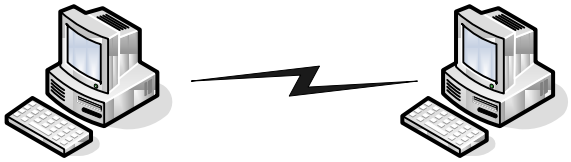


Рисунок 4.1. Структура IBSS

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. 4.2).

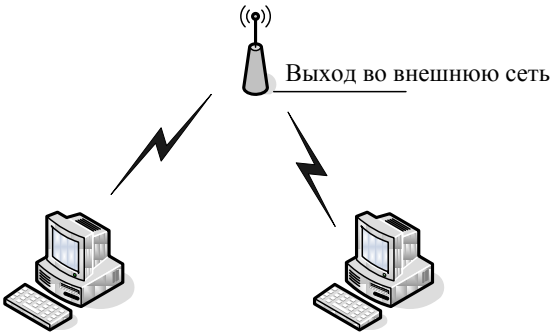


Рисунок 4.2. Структура BSS

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.

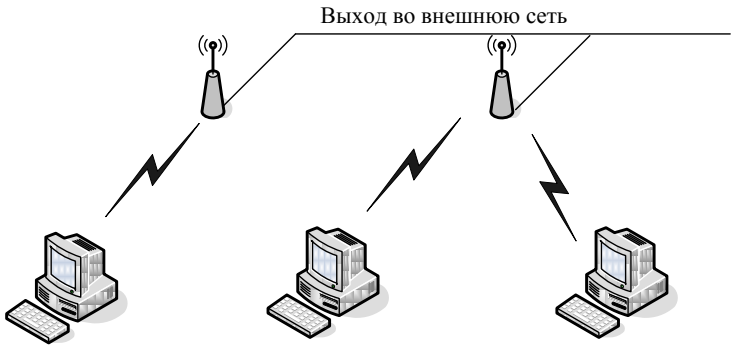


Рисунок 4.3. Структура ESS

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. 4.4).

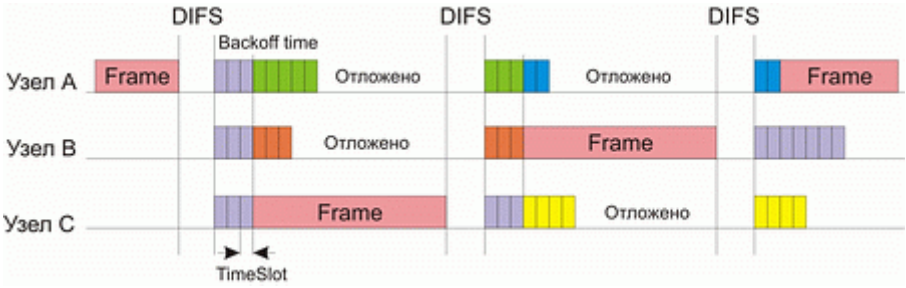


Рисунок 4.4. Реализация равноправного доступа к среде передачи данных в методе DCF

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. 4.5). 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.

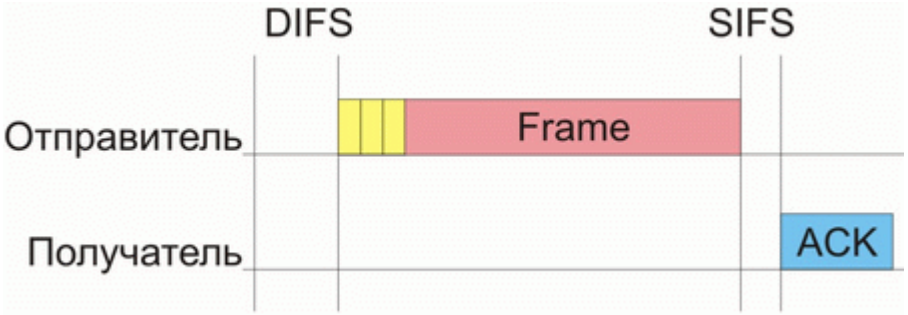


Рисунок 4.5. Кадры квитанции, отсылаемые в случае успешной передачи данных

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 рисунке 4.6.

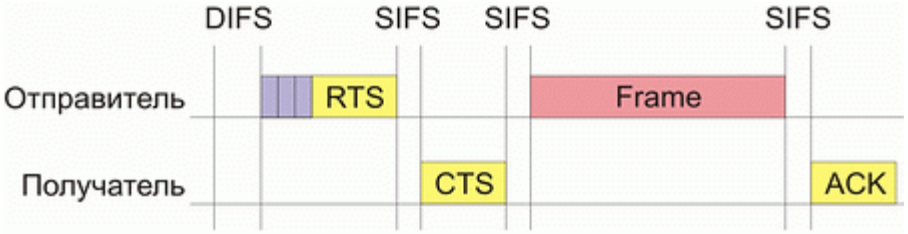


Рисунок 4.6. Взаимодействие между двумя узлами сети в соответствии с алгоритмом RTS/CTS

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.

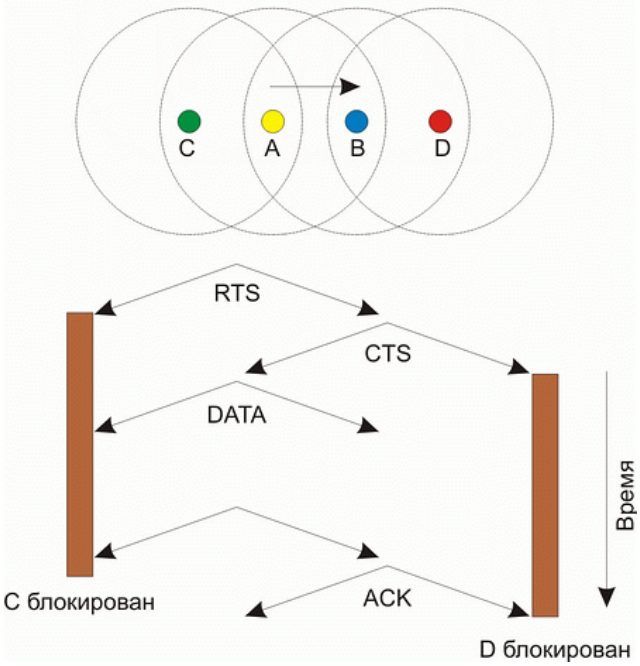


Рисунок 4.7. Решение проблемы скрытых узлов в алгоритме RTS/CTS

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.

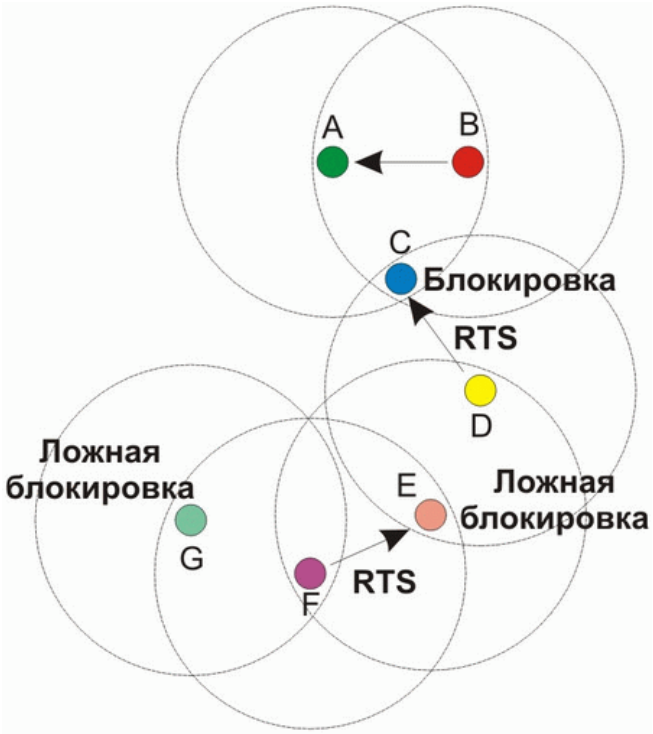


Рисунок 4.7 - Возникновение ложных блокировок узлов сети

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, назаначение 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. 4.8).

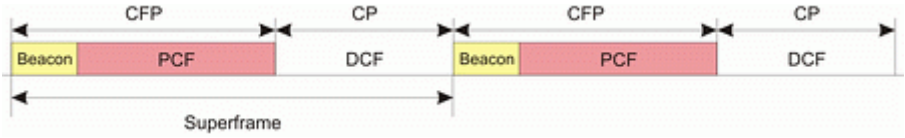


Рисунок 4.8. Объединение режимов PCF и DCF в одном суперфрейме

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

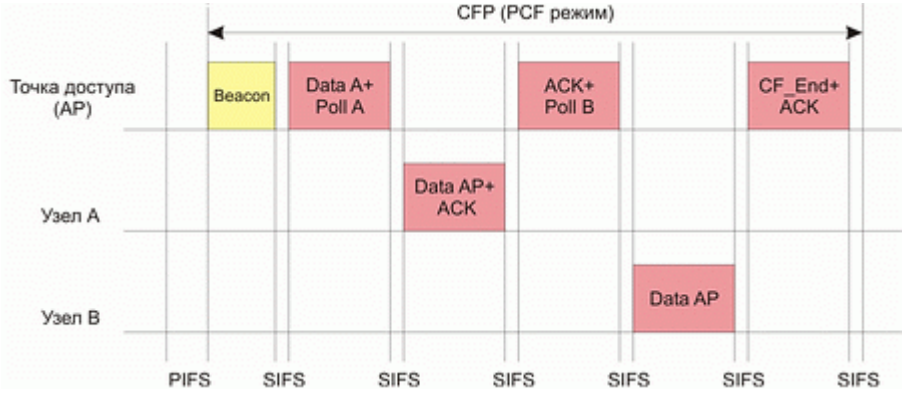


Рисунок 4.9. Организация передачи данных между узлами сети в режиме PCF

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 рисунке 4.10 показана как эти уровни соотносятся между собой и вышестоящими уровнями.

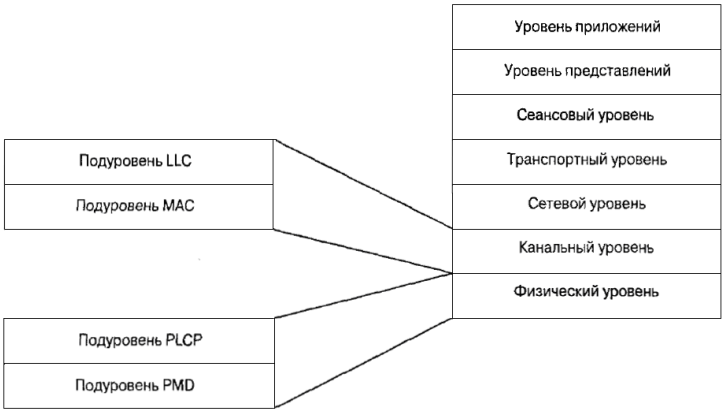


Рисунок 4.10. Подуровни уровня PHY модели взаимодействия открытых систем (OSI)

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. 4.11. 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.

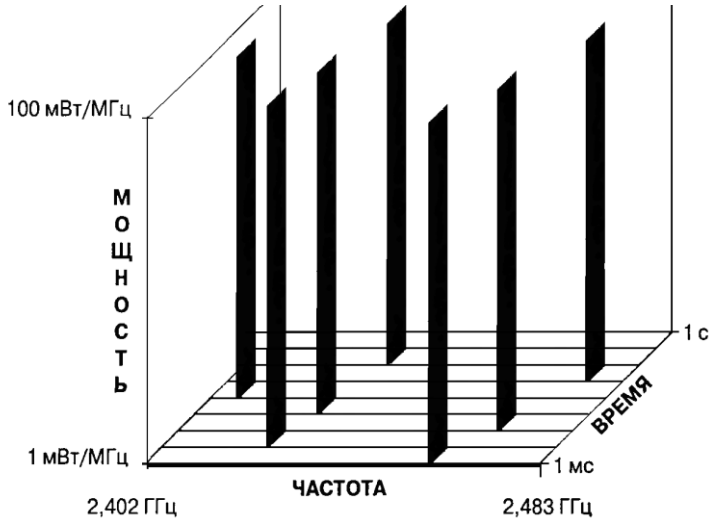


Рисунок 4.11. Пример скачкообразной перестройки частоты

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 4.1. Схемы скачкообразной перестройки частоты

Набор частот	Схема скачкообразной перестройки частоты
1	0,3,6,9,12,15,18,21,24,27,30,33,36,39,42,45,48,51,54,57,60,63,66,69,72,75
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 рисунке 4.12 представлен формат фрейма FHSS подуровня PLCP.

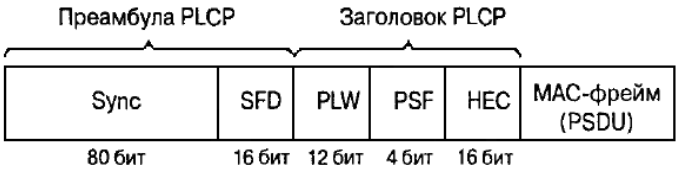


Рисунок 4.12. Формат фрейма FHSS подуровня PLCP

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.

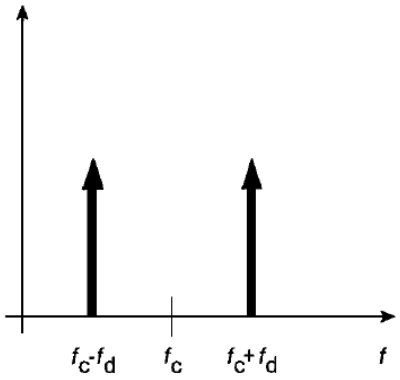


Рисунок 4.13. Модуляция GFSK

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 4.2. 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 ошутимы

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 рисунке 4.14.

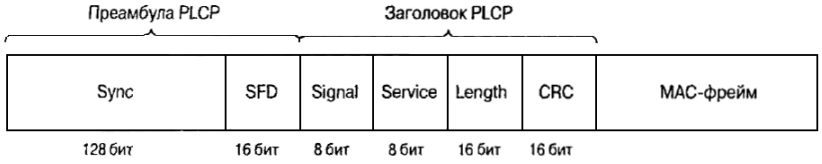


Рисунок 4.14. Формат фрейма DSSS PPDU стандарта 802.11

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.

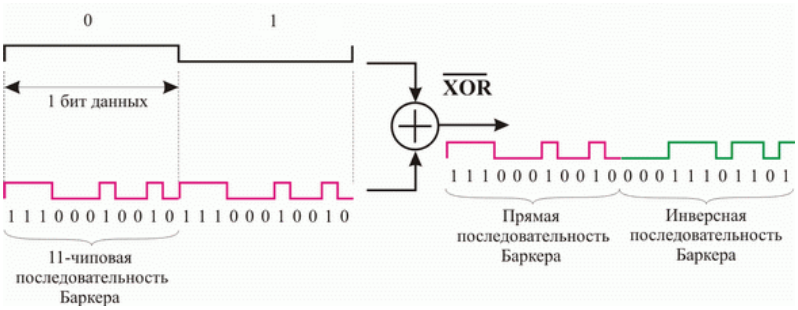


Рисунок 4.15 Расширение спектра по технологии DSSS

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

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

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

Физический уровень сетей стандарта 802.11b

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

Подуровень PLCP технологии HR-DSSS стандарта 802.11b

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

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

Подполе Service определяет ранее зарезервированные биты (Таблица 43)

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

Таблица 4.3. Определение битов подполя Service

Бит	Наименование	Значение
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)

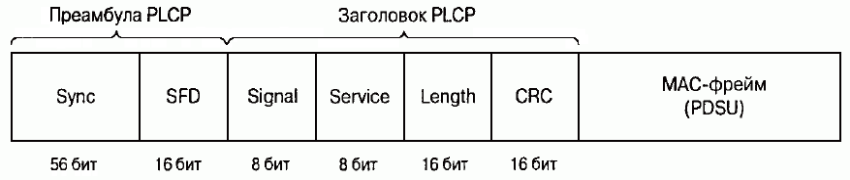


Рисунок 4.16 Короткий PPDU технологии HR-DSSS

Модуляция CCK 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 4.4. 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 4.5. 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.

В заключение обсуждения протокола 802.11b/b+ приведем таблицу соответствия между скоростями передачи и типом кодирования (табл. 4.2).

Таблица 4.6. 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	Количество 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. 4.17).

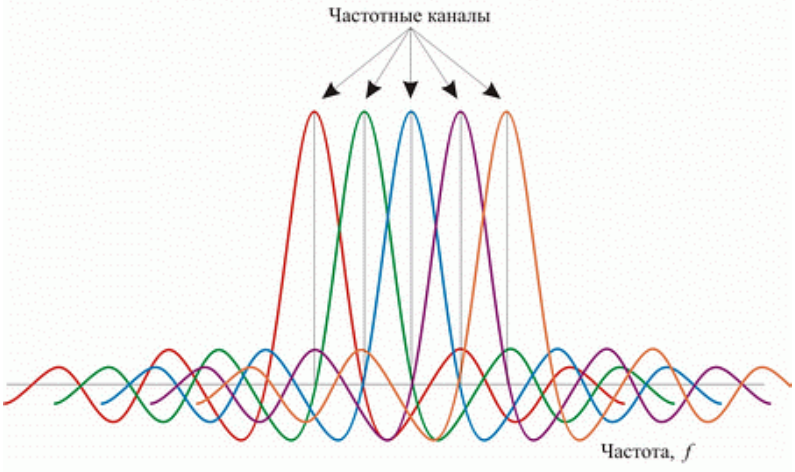


Рисунок 4.17. Пример перекрывающихся частотных каналов с ортогональными несущими

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. 4.18).

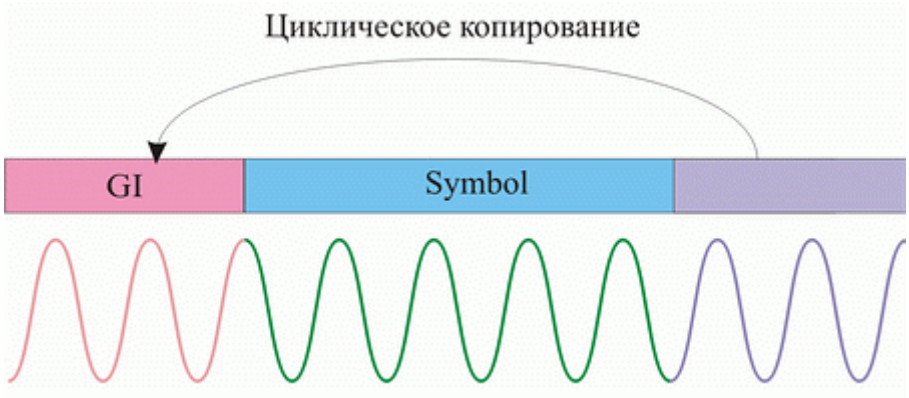


Рисунок 4.18. Охранный интервал GI

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. 4.19).

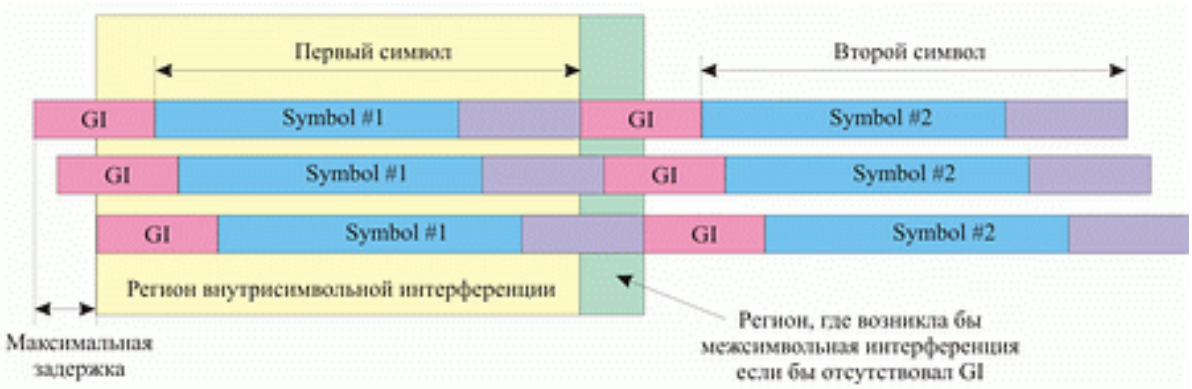


Рисунок 4.19. Избежание межсимвольной интерференции за счет использования охранных интервалов

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. 5.7.

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.

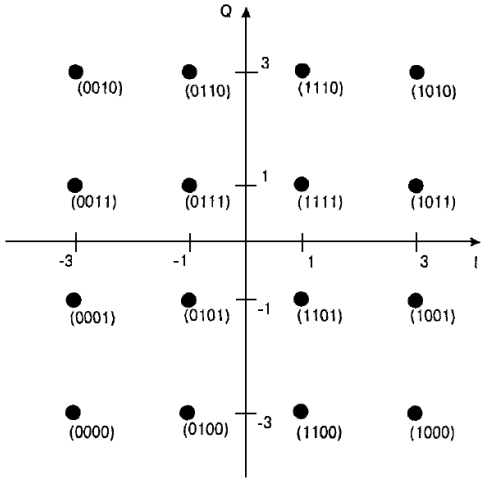


Рисунок 4.20. Представление сигнала при QAM-16

Из таблицы 4.7 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 4.7. Соотношение между скоростями передачи и типом кодирования в стандарте 802.11g

Скорость передачи (Мбит/с)		Метод кодирования	Модуляция
1	(опционально)	Код Баркера	DBPSK
2	(опционально)	Код Баркера	DQPSK
5.5	(обязательно)	CCK	DQPSK
	(опционально)	PBCC	DBPSK
6	(обязательно)	OFDM	BPSK
	(опционально)	CCK-OFDM	BPSK
9	(опционально)	OFDM, CCK-OFDM	BPSK
11	(обязательно)	CCK	DQPSK
	(опционально)	PBCC	DQPSK
12	(обязательно)	OFDM	QPSK
	(опционально)	CCK-OFDM	QPSK

18	(обязательно)	OFDM, CCK-OFDM	QPSK
22	(опционально)	PBCC	DQPSK
24	(обязательно)	OFDM	16-QAM
	(опционально)	CCK-OFDM	
33	(опционально)	PBCC	
36	(опционально)	OFDM, CCK-OFDM	16-QAM
48	(опционально)	OFDM, CCK-OFDM	16-QAM
54	(опционально)	OFDM, CCK-OFDM	16-QAM

Стандарт также предусматривает применение гибридного кодирования. Для того чтобы понять сущность этого термина, вспомним, что любой передаваемый пакет данных содержит заголовок/преамбулу со служебный информацией и поле данных. Когда речь идет о пакете в формате CCK, имеется в виду, что заголовок и данные кадра передаются в формате CCK. Аналогично при использовании технологии OFDM заголовок кадра и данные передаются посредством OFDM-кодирования. При применении технологии CCK-OFDM заголовок кадра кодируется с помощью CCK-кодов, но сами данные кадра передаются посредством многочастотного OFDM-кодирования. Таким образом, технология CCK-OFDM является своеобразным гибридом CCK и OFDM. Технология CCK-OFDM — не единственная гибридная технология: при использовании пакетного кодирования PBCC заголовок кадра передается с помощью CCK-кодов и только данные кадра кодируются посредством PBCC.

Безопасность беспроводных LAN

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

В таблице приведены основные подходы к обеспечению безопасности беспроводных сетей.

Таблица 4.8. Сравнение подходов к обеспечению безопасности беспроводных сетей

Характеристики	**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	Да[3]	Да[3]	Нет	Да[4]	Нет

устройствах					
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.

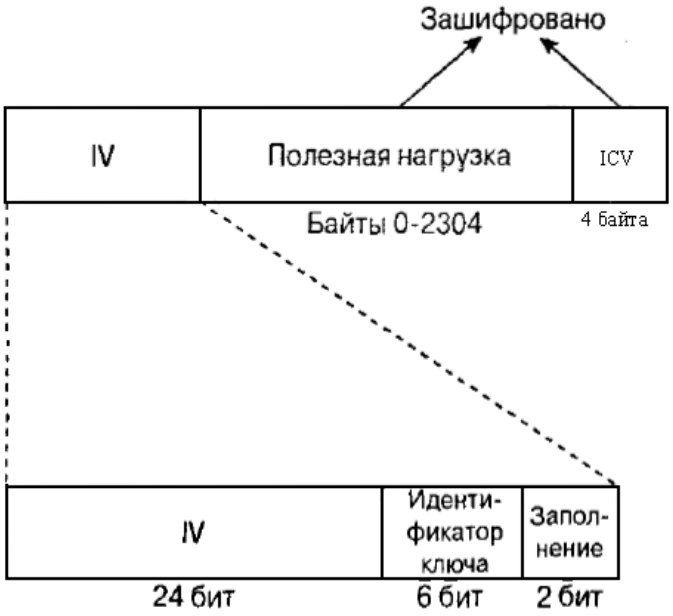


Рисунок 4.21. Фрейм, зашифрованный алгоритмом WEP

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 рисунке 4.22 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 рисунках 4.22 и 4.23 показан процесс дешифрования фреймов и вычисления контрольного признака целостности.

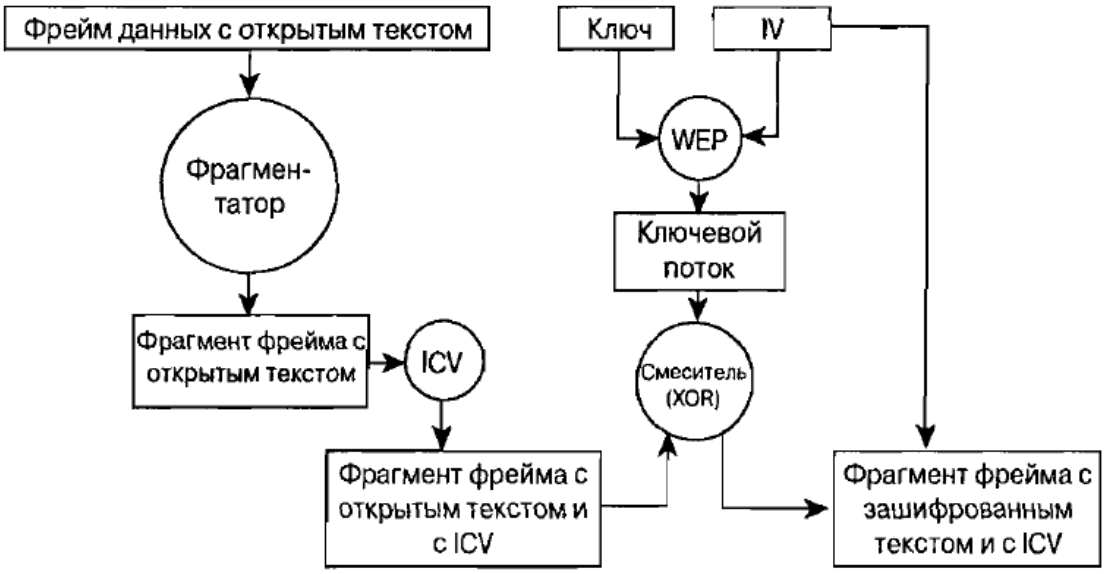


Рисунок 4.22. Шифрование по алгоритму WEP

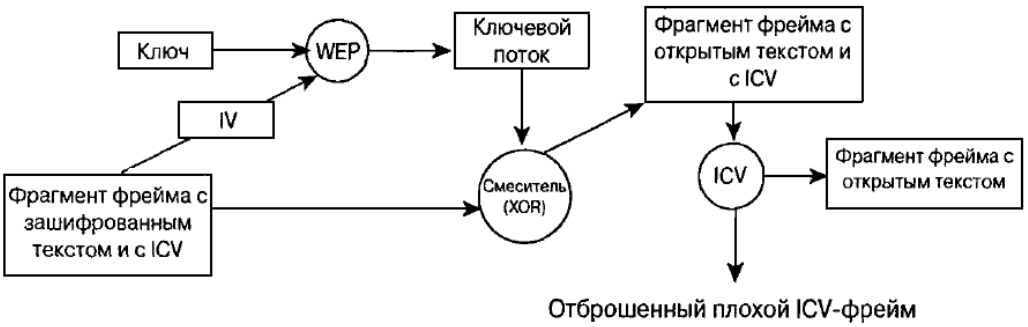


Рисунок 4.23. Дешифрование по алгоритму WEP

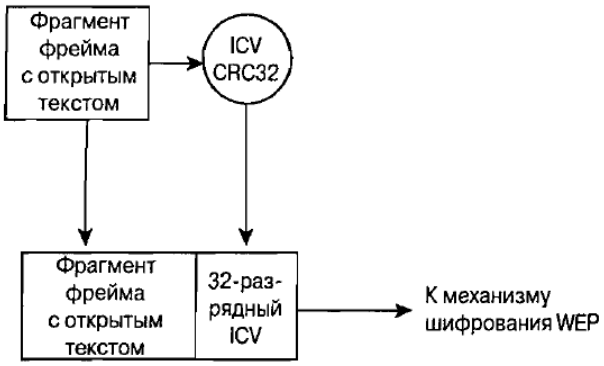


Рисунок 4.24. Диаграмма функционирования механизма ICV

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.

иент посылает точке доступа запрос на аутентификацию с совместно используемым ключом.

чка доступа отвечает фреймом вызова (challenge frame), содержащим открытый текст.

иент шифрует вызов и посылает его обратно точке доступа.

ли точка доступа может правильно расшифровать этот фрейм и получить свой исходный вызов, клиенту посылается сообщение об успешной аутентификации.

иент получает доступ WLAN.

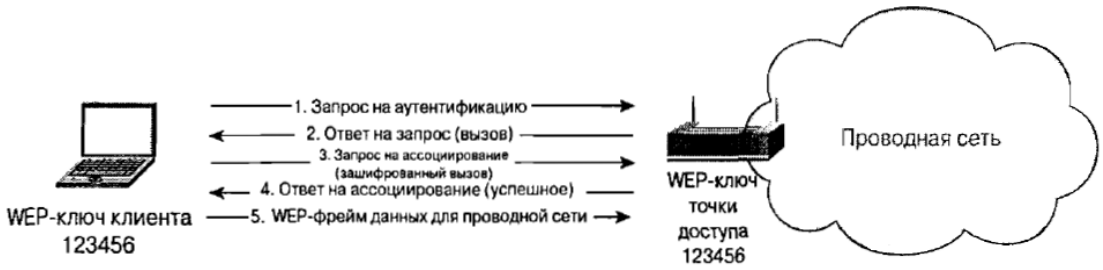


Рисунок 4.25. Процесс аутентификации с совместно используемым ключом

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.

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.

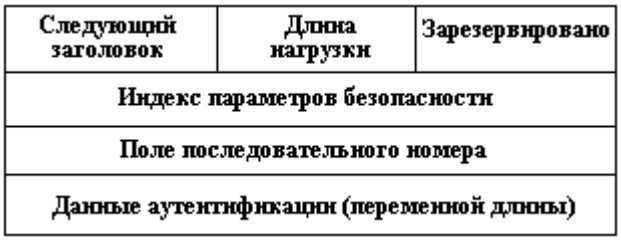


Рисунок 4.26. Формат заголовка AH

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.

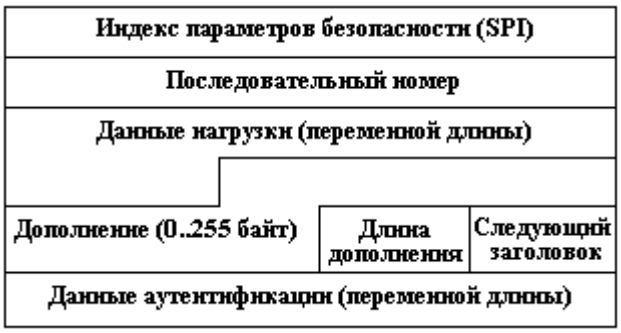


Рисунок 4.27. Формат заголовка ESP

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”.

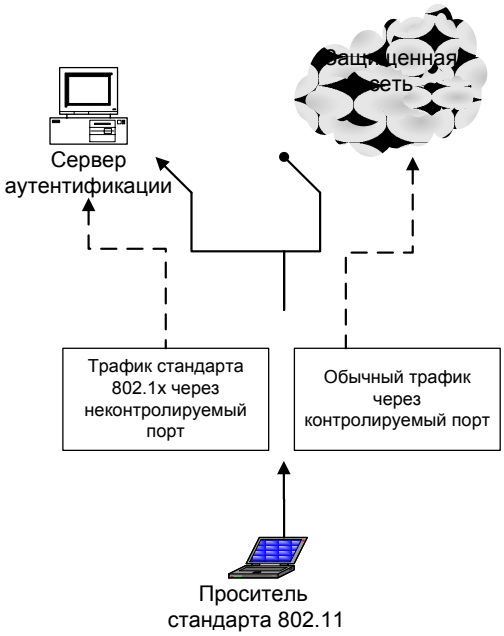


Рисунок 4.28. Логические порты аутентификатора стандарта 802.1X

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 сапликанта 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 сапликантом 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, таковы:

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 (рисунок 4.29)

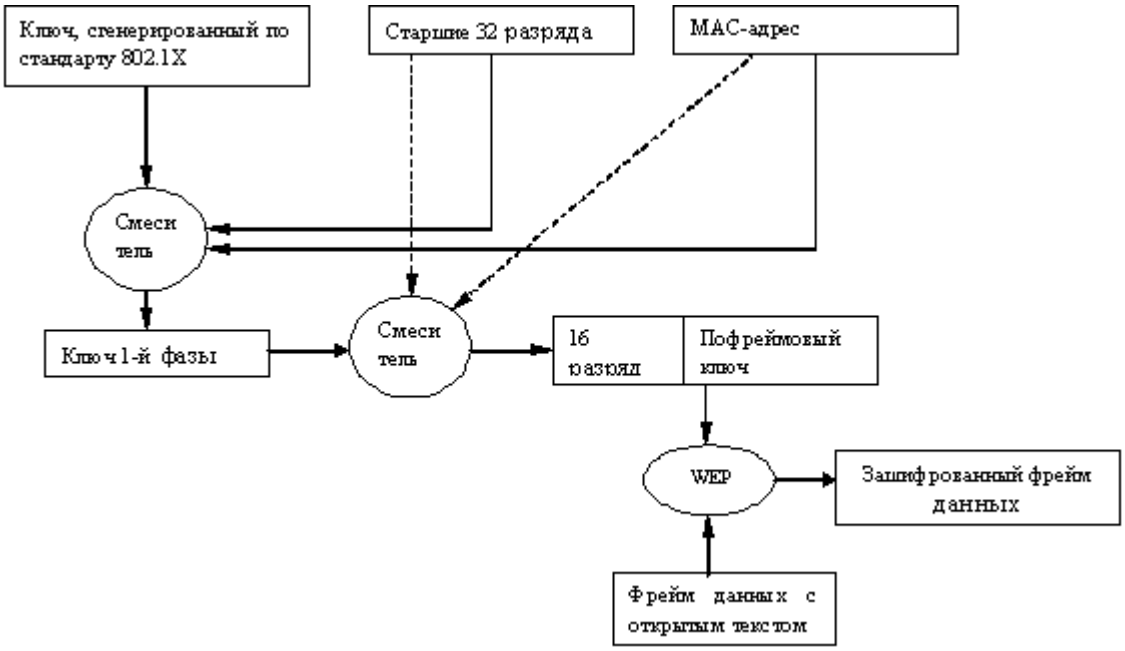


Рисунок 4.29. Пофреймовое изменение ключей

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 рисунке 4.30 показан механизм работы алгоритма MIC.

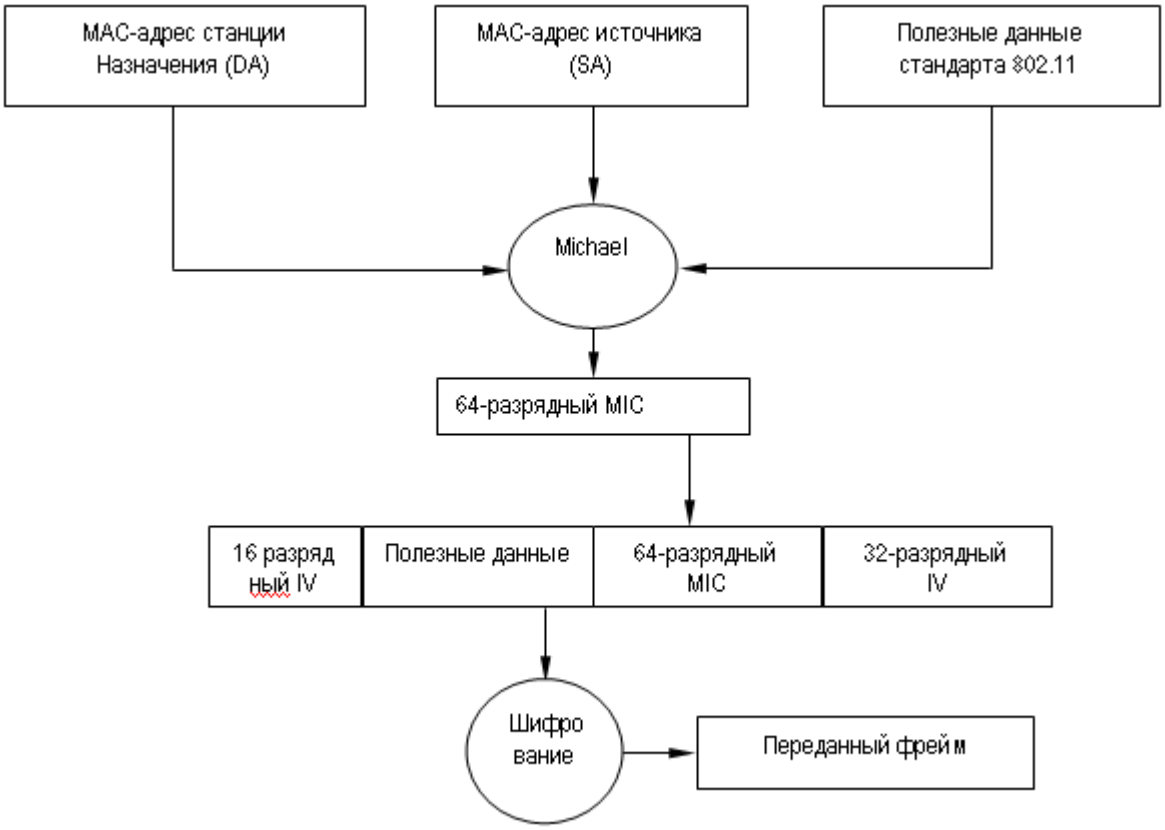


Рисунок 4.30. Работа алгоритма MIC

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. 4.31)

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.

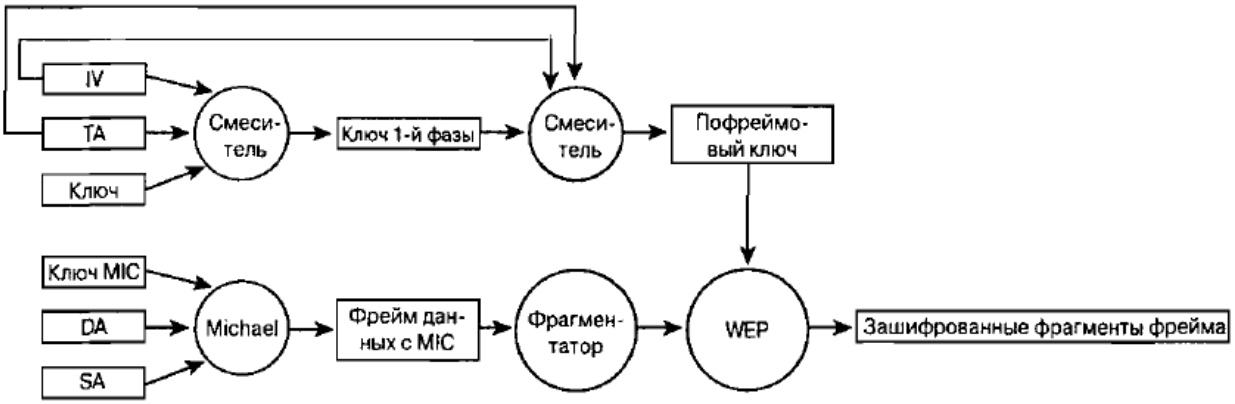


Рисунок 4.31 – Алгоритм шифрования TKIP

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.

Структура алгоритма шифрования RIJNDAEL

RIJNDAEL – это итерационный блочный шифр, имеющий архитектуру «квадрат». Шифр имеет переменную длину блоков и различные длинны ключей. Длина ключа и длина блока независимо друг от друга могут составлять 128, 192 и 256 бит. В стандарте AES определена длина блока данных равняя 128 битам.

Промежуточные результаты преобразований, выполняемые алгоритмом, называются состояниями (State). Состояния можно представить в виде прямоугольного массива байтов. При размере блока данных равном 128 битам, этот 16 – байтовый массив имеет 4 строки и 4 столбца (каждый столбец и каждая строка при этом могут рассматриваться как 32 – разрядные слова). Входные данные для шифра обозначаются как байты состояния в порядке s_{00}, s_{10}, s_{20}, s_{30},… После завершения действия шифра выходные данные получаются из байтов состояния в том же порядке. В общем случае число столбцов N_b равно длине блока, деленной на 32.

s_{00}	s_{01}	s_{02}	s_{03}
s_{10}	s_{11}	s_{12}	s_{13}
s_{20}	s_{21}	s_{22}	s_{23}
s_{30}	s_{31}	s_{32}	s_{33}

а

k_{00}	k_{01}	k_{02}	k_{03}
k_{10}	k_{11}	k_{12}	k_{13}
k_{20}	k_{21}	k_{22}	k_{23}
k_{30}	k_{31}	k_{32}	k_{33}

б

Рисунок 4.32. Форматы данных: а – пример представление блока (N_b=4)
б – ключа шифрования (N_k=4), где s_{ij} и k_{ij} соответственно байты массива state и ключа, находящиеся на пересечении i–го и j–го столбца.

Ключ шифрования также представлен в виде прямоугольного массива с четырьмя строками (рис 4.32). Число столбцов этого массива равно длине ключа деленной на 32. В стандарте AES определены длины всех трех размеров – 128, 192 и 256 бит, то есть соответственно 4, 6 и 8 32-разрядных слова. Число раундов в алгоритме зависит от значений N_k и N_b, как показано в таблице 4.9. В стандарте AES определено соответствие между размером ключа, размером блока данных и числа раундов шифрования, как показано в таблице 4.10

Таблица 4.9 - Число раундов N_r как функция от длины ключа и размера блока

N_r	$N_b = 4$	$N_b = 6$	$N_b = 8$
$N_k = 4$	10	12	14
$N_k = 6$	12	12	14
$N_k = 8$	14	14	14

Таблица 4.10 Соответствие между размером ключа, размером блока данных и числа раундов шифрования

Стандарт	Длина ключа	Размер блока данных	Число раундов
AES-128	10	12	14
AES-192	12	12	14
AES-256	14	14	14

В спецификации стандарта 802.11i регламентировано использование AES-128.

Раундовое преобразования

Раунд состоит из четырех преобразований:

Замена байтов SubBytes() – побайтовая подстановка в S-блоках с фиксированной таблицей замен размерностью 8×256;

Сдвига строк ShiftRows() – побайтового сдвига строк массива Sate на различное количество байт;

Перемешивания столбцов MixColumns() – умножение столбцов состояния, рассматриваемых как многочлены над $GF(2^8)$, на многочлен третьей степени g(x) по модулю x^4+1;

Сложение с раундовым ключом AddRoundKey() – поразрядного XOR с текущим моментом развернутого ключа.

Замена байтов

Преобразование SubBytes представляет собой нелинейную замену байтов, выполняемую независимо с каждым байтом состояния. Таблицы замены S-блоков являются инвертируемыми и построены из композиции следующих двух преобразований входного байта:

получение обратного элемента умножения в поле $GF(2^8)$, нулевой элемент 00 переходит сам в себя

применение преобразования над GF(2), определенного следующим образом:

$$\begin{bmatrix} b'_0 \\ b'_1 \\ b'_2 \\ b'_3 \\ b'_4 \\ b'_5 \\ b'_6 \\ b'_7 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{bmatrix} \cdot \begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \\ b_4 \\ b_5 \\ b_6 \\ b_7 \end{bmatrix} + \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix}$$

Логика работы S-блока при преобразовании байта {xy} отражена в таблице 4.. Например, результат {ed} преобразования байта {53} находится на пересечении 5-й строки и

3-го строка.

Таблица 4.11 - Таблица замен S-блока.

x	y															
	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	63	7c	77	7b	f2	6b	6f	c5	30	01	67	2b	fe	d7	ab	76
1	ca	82	c9	7d	fa	59	47	fo	ad	d4	a2	af	9c	a4	72	c0
2	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
3	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
4	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
5	53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
6	d0	ef	aa	fb	43	4d	33	85	45	f9	02	7f	50	3c	9f	a8
7	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
8	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
9	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
a	e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	e4	79
b	e7	c8	37	6d	8d	d5	4e	a9	6c	56	14	ea	65	7a	ae	08
c	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
d	70	3e	B5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e
e	e1	f8	98	11	69	d6	8e	94	9b	1e	87	e9	ce	55	28	df
f	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

Преобразование сдвига строки (ShiftRows)

Последние три строки циклически сдвигаются влево на различное число байт. Строка 1 сдвигается на c_1 байт, строка 2 на c_2 байт, строка три на c_3 байт. Значение сдвигов c_1, c_2, c_3 зависят от длины блока N_b. Для стандарта AES-128 сдвиги имеют следующие значения $c_1 = 1$, $c_2 = 2$, $c_3 = 3$.

Операция сдвига последних трех бит, ShiftRows, показана на рис))))

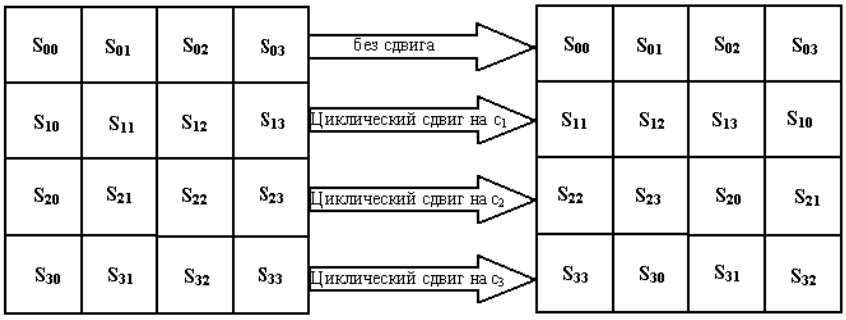


Рисунок 4.33. - Действие ShiftRows на строки состояния

Преобразование перемешивания столбцов MixColumns()

В этом преобразовании столбцы состояния рассматриваются как многочлены над $GF(2^8)$ и умножаются по модулю $x^4 + 1$на многочлен $g(x)=\{03\}x^3 + \{01\}x^2 + \{01\}x + 1$. Это преобразование также может быть представлено в матричном виде:

$$\begin{bmatrix} s'_{0c} \\ s'_{1c} \\ s'_{2c} \\ s'_{3c} \end{bmatrix} = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \cdot \begin{bmatrix} s_{0c} \\ s_{1c} \\ s_{2c} \\ s_{3c} \end{bmatrix}, 0 \le c \le 3$$

Где c – номер столбца массива State.
Применение этой операции ко всем четырем столбцам состояния обозначено как MixColumns(State)

Добавление раундового ключа

В операции раундовый ключ добавляется к состоянию по средствам простого поразрядного XOR. Раундовый ключ вырабатывается из ключа шифрования посредством алгоритма выработки ключей (key schedule). Длина раундового ключа (в 32-разрядных словах) равна длине блока N_b. Преобразование, содержащее добавление посредством XOR раундового ключа к состоянию (рисунок 4.34), обозначено как AddRoundKey()

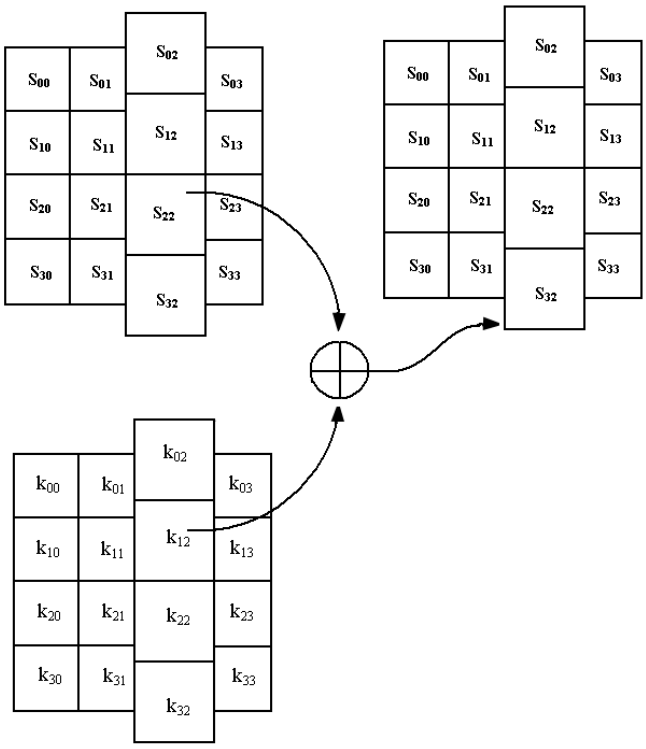


Рисунок 4.34. Операция AddRoundKey

Алгоритм выработки ключей

Раундовые ключи получаются из ключа шифрования по средствам алгоритма выработки ключей. Он содержит два компонента: расширение ключа (Key Expansion) и выбор раундового ключа (Round Key Selection). Основополагающие принципы алгоритма выглядят следующим образом:

общее число битов раундовых ключей равно длине блока, умноженной на число раундов, плюс 1 (например, для длины блока 128 бит и 10 раундов требуется 1408 бит раундовых ключей)

ключ шифрования расширяется в расширенный ключ

раундовые ключи берутся из расширенного следующим образом: первый раундовый клич содержит первые N_b слов, второй последующие N_b, и т. д.

Первые N_k слов содержат ключ шифрования, каждое последующее слово w[i] получается посредствам XOR предыдущего слова w[i-1] и слова на N_k позиции ранее w[i-N_k]:

$$w[i] = w[i-1] \oplus w[i-N_k]$$

Для слов позиция которых кратна N_k, перед XOR применяется преобразование к w[i-1], а затем еще прибавляется раундовая константа Rcon. Преобразование реализуется с помощью двух дополнительных функций: RotWord() – осуществляет побайтовый сдвиг по формуле { a_0, a_1, a_2, a_3}> { a_1, a_2, a_3, a_0}, и Subword() – осуществляет побайтную замену с использованием S – блока функции SubByte(). Значение Rcon[j] равно 2^{j-1}. Значение w[i] в этом случае равно:

$$w[i] = SubWord(RotWord(w[i-1])) \oplus Rcon[\,i/N_k\,] \oplus w[i-N_k]$$

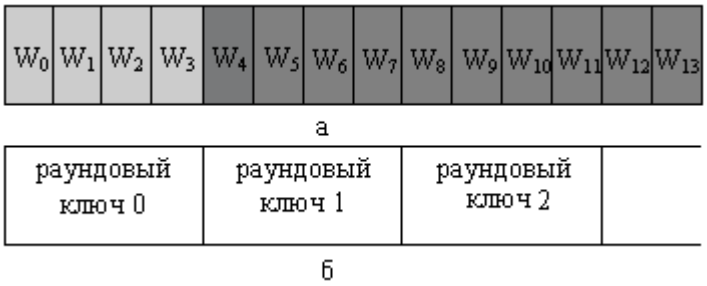


Рисунок 4.34. Процедуры: а – расширения ключа (светло-серым цветом выделено слова расширенного ключа, которые формируются без использования функции RotWord и Subword, серым цветом обозначены слова формируемые с использованием этих функций) б – выбор раундового ключа для $N_k = 4$

Функции зашифрования

Шифр Rijndael состоит (рисунок 4.35):

Из начального добавления раундового ключа;

N_r-1 раундов

Заключительного раунда, в котором отсутствует операция MixColumns()

На вход алгоритма подаются блоки данных State, в ходе преобразований содержимое блока изменяется и на входе образуется шифротекст, организованный в виде блоков State.

Для получения исходного текста необходимо выполнить обратную последовательность действий. При этом необходимо помнить что порядок раундовых ключей является обратным тому который использовался при шифровании.

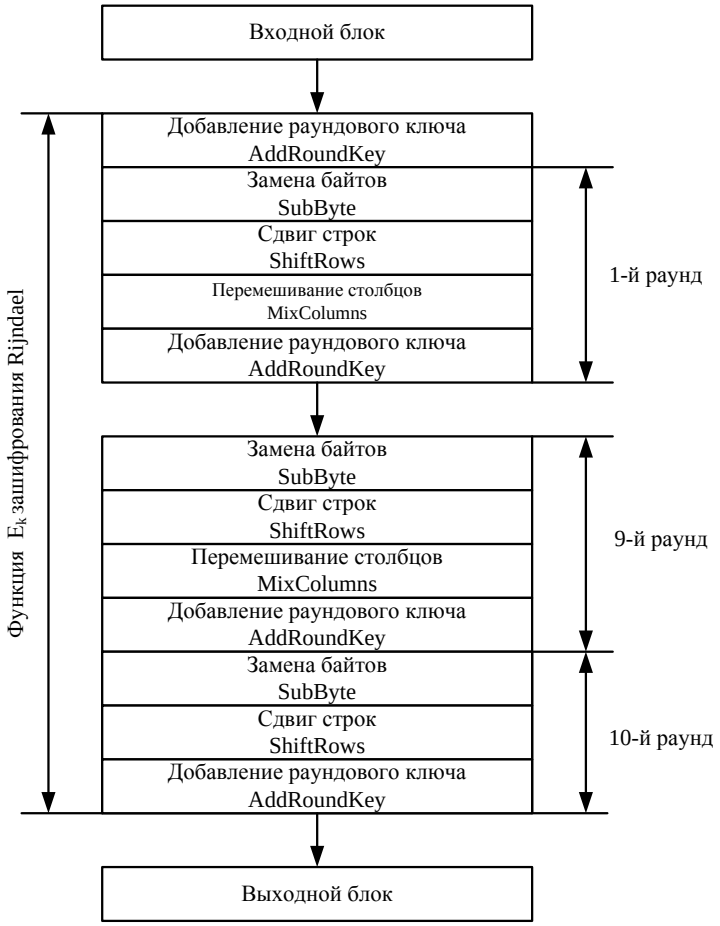


Рисунок 4.35. Схема функции зашифрования криптоалгоритма Rijndael при $N_k = N_b = 4$

Режим сцепления блоков

Как уже отмечалось выше в стандарте wpa2, определено использование алгоритма шифрования AES в режиме сцепления блоков шифротекста (Ciphertext Block Chaining).

Данный режим обеспечивает зависимость зашифрованного блока не только от открытого текста но и от его номера в последовательности. На рисунке показана схема иллюстрирующая работу алгоритма в режиме CBC.

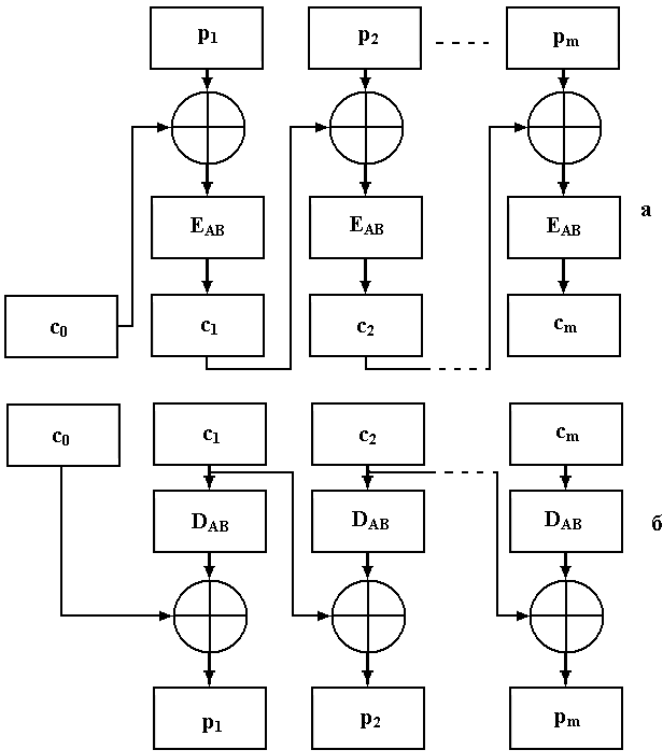


Рисунок 4.36. Режим шифрования CBC: а – зашифрование; б – расшифрование

Уравнения зашифрования и расшифрования имеют следующий вид:

$$c_i = E_{AB}(p_i \oplus c_{i-1})$$

$$p_i = D_{AB}(c_i) \oplus c_{i-1}; i = 1,..m$$

Где, E_{AB} и D_{AB} – функции зашифрования и расшифрования соответственно.
c_i и p_i - зашифрованное и открытое сообщения

Отличительной особенностью режима CBC является зависимость при зашифровании i-го блока шифротекста от всех предыдущих блоков открытого текста и зависимость открытого текста p_i только от двух блоков c_{i-1} и c_i. Первое свойство делает пригодным использование режима для решения задач контроля целостности информации. Второе свойство делает режим самосинхронизирующимся: одиночная ошибка при передаче (ошибка при передачи одного блока) может привести к неправильному расшифрованию только двух блоков.

На сегодняшний день нет данных о успешных атаках на рассмотренный алгоритм, по этому его использование гарантирует высокий уровень зашиты передаваемой информации.

Выбор стандарта зашиты

Для построения подсистемы защиты в данной работе будет использоваться стандарт 802.1i. Он сочетает в себе надежные методы аутентификации и стойкий алгоритм шифрования. Перед тем как переходить к выбору метода аутентификации, сформулируем несколько критериев:

Аутентификация должна быть взаимной (в процессе аутентификации обе стороны подтверждают свою подлинность)

Аутентификация должна быть централизованной и ориентированной на пользователя

Должны использоваться динамично шифруемые ключи

При использовании централизованной и ориентированной на пользователя аутентификации неавторизованный злоумышленник не сможет воспользоваться авторизованным устройствам для доступа к ресурсам сети, можно также запретить отдельным пользователям доступ к ресурсам сети. Взаимная аутентификация препятствует атакам в ходе которых злоумышленник выдавая свою точку за «законную» получает «секрет» пользователя.

Наиболее подходящим из представленных в пункте 6.5.3 методов аутентификации является EAP-PEAP (Protected EAP - защищенный EAP), перед аутентификацией устанавливается TLS – туннель, а внутри этого туннеля осуществляется сама аутентификация с использованием стандартного EAP - MSCHAP V2 (аутентификация на основе логина и пароля пользователя). Пользователи которые будут использовать беспроводную сеть не должны иметь слишком простой пароль. Администратором сети будет создано правило, в соответствии с которым пользователи должны будут иметь пароль удовлетворяющий требованиям сложности (длина не менее 8 символов, использование заглавных и прописных букв, цифр и знаков).

Рассмотрим схему работы протокола EAP-PEAP-MSCHAP V2. При этом можно выделить следующие основные режимы работы:

Клиент получая доступ к среде посылает точке доступа сообщение EAP – Start инкапсулированное по стандарту 802.1x

Точка доступа передает сообщение EAP – Start беспроводному коммутатору

Коммутатор блокирует порт позволяя передавать только данный стандарта 802.1x и посылает сообщение EAP – запросом на аутентификацию

Точка доступа пересылает сообщение с EAP – запросом на аутентификацию

Клиент отвечает EAP – ответов содержащим идентификатор (имя пользователя)

Точка доступа передает полученное сообщение беспроводному коммутатору, а он в свою очередь переправляет полученное сообщение, инкапсулированное в пакет запроса к серверу RADIUS, серверу аутентификации.

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

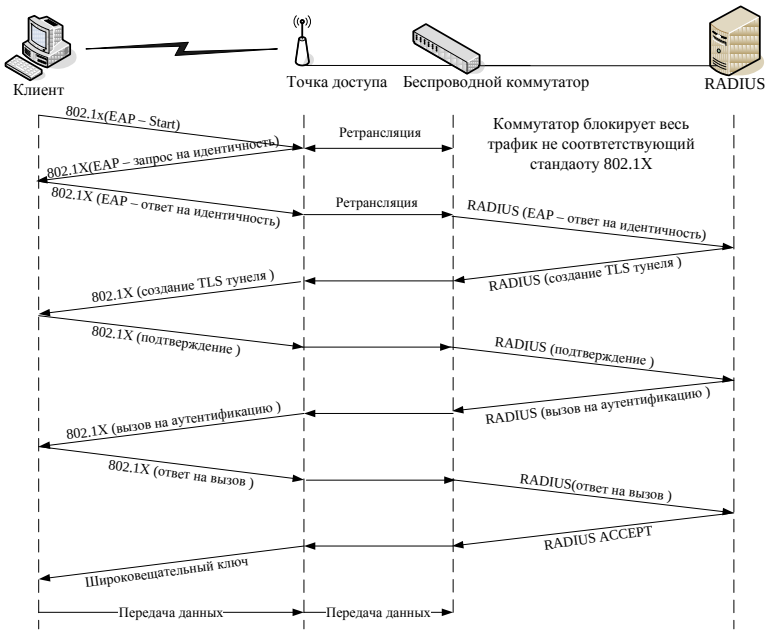


Рисунок 4.37. Процедура прохождения аутентификации EAP-PEAP-MSCHAP V2

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.

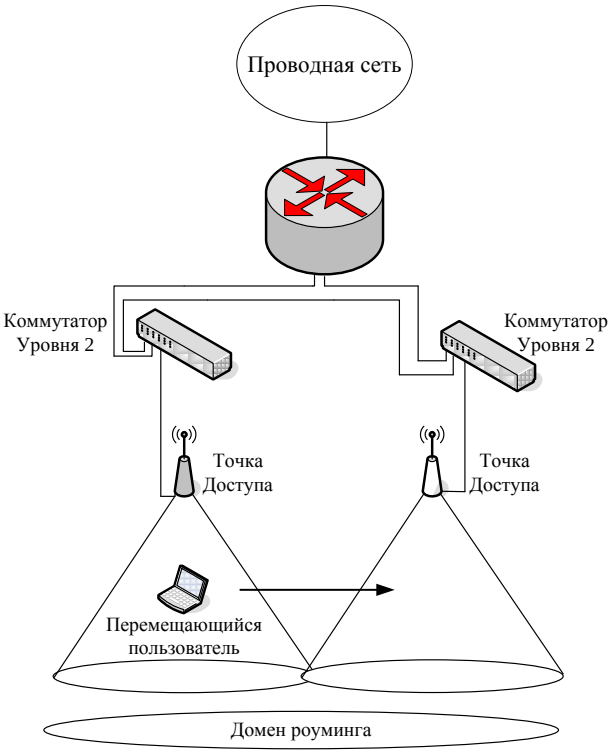


Рисунок 4.38. Домен роуминга уровня два

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 ро-уминга.

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.

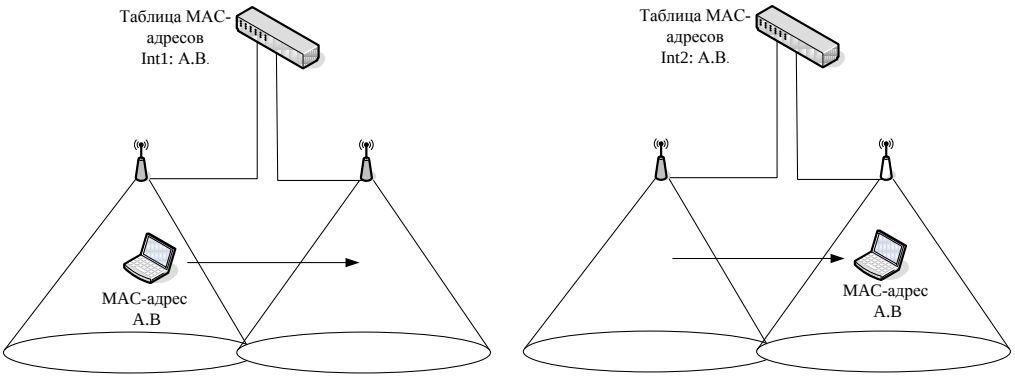


Рисунок 4.39. Процесс роуминга с использованием беспроводного коммутатора

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 параметрам

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.

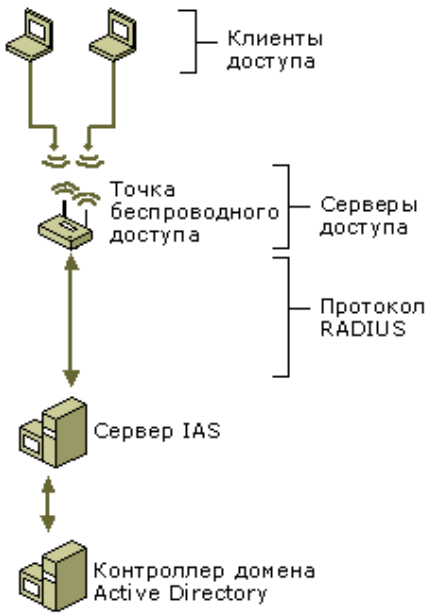


Рисунок 4.39. Использование IAS в качестве RADIUS-сервера

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.

Таблица 4.12 Характеристики коммутатора Netgear ProSafe Smart WFS709TP

Тип оборудования	Беспроводной коммутатор
Физические характеристики	
Габаритные размеры	4.45 x 44.2 x 33 см
Вес	4.5 кг
Энергопотребление	200 Вт
Питающее напряжение	180 – 246 В AC; 47-63 Гц
Производительность и емкость беспроводного коммутатора	
Управление точками доступа	До 16 точек
Пользователей	256
MAC-адресов	4096
IP-интерфейсов VLAN	128
Порты Fast Ethernet	8 портов 10/100Base-T PoE
Порты Gigabit Ethernet	1 порт uplink
Последовательные порты	1 для подключения кончоли
Общая пропускная способность	1 Gbps

Пропускная способность с шифрованием (AES-CCM)	200 Mbps
Безопасность беспроводных LAN и функции управления	
Безопасность 802.11i	сертифицирован WFA по WPA2 и WPA
Аутентификация пользователей и устройств 802.1x	есть
Поддержка EAP-PEAP, EAP-TLS и EAP-TTLS	есть
Кэширование 802.11i PMK для приложений роуминга	есть
Аутентификация Stateful 802.1x для отдельной AP	есть
Аутентификация на базе MAC-адресов, SSID и месторасположения	есть
Поддержка Multi-SSID для работы нескольких WLAN	есть
Выбор сервера RADIUS на базе SSID	есть
Безопасное управление и контроль AP через IPSEC или GRE	есть
Функции управления радиоканалом IntellWiFi	
Автоматическая настройка каналов и мощности для управляемых точек доступа	есть
Одновременный мониторинг радиоканалов и сервисы для конечных пользователей	есть
Автоматическая подстройка покрытия на основе изменения условий для передачи радиосигнала	есть
Балансировка нагрузки точек доступа на основе числа пользователей	есть
Обнаружение мертвых зон и наложений радиосигналов	есть
Функции защиты от взлома беспроводной сети	
Интеграция с беспроводной инфраструктурой	есть
Функции мониторинга	есть
Обнаружение и встроенная визуализация месторасположения фальшивых точек доступа	есть
Сетевые функции и расширенные сервисы	
Коммутация L2 и L3 для радиоканала и проводной сети	есть
Пулы VLAN для легкого и масштабируемого построения сети	есть
Мобильность VLAN для роуминга L2	есть
Прокси мобильных IP и прокси роуминга DHCP L3	есть
Функции администрирования беспроводного коммутатора	
Доступ с помощью Web-интерфейса пользователя по HTTP и HTTPS	есть
Экраны Quickstart для упрощения конфигурирования контроллера	есть
Ограниченный доступ CLI с	есть

использованием консоли, заблокированный по умолчанию доступ CLI, консоль SSH и telnet	
Ролевой контроль доступа для ограничения доступа admin	есть
Аутентификация доступа с помощью RADIUS, LDAP или внутренней базы данных	есть
SNMPv3 и SNMPv2 для мониторинга контроллера	есть
Сертификаты соответствия стандартам и правилам безопасности	есть Маркировка CE (для внешнего источника питания AC/DC) Маркировка PSE (для внешнего источника питания AC/DC) Underwriters Laboratories (UL) 60950 Canadian Standards Association CAN/CSA) C22.2 No. 60950 EN 60950 / IEC 60950 CB Scheme FCC Part 15 Class A VCCI Class A AS/NZS CISPR 22 Class A AS/NZS4771 (C-Tick)
Условия эксплуатации	
Температура	0 – 40°C
Влажност	10% - 70%

Таблица 4.13 - Характеристики точки доступа NETGEAR WG102

Общие характеристики	
Тип оборудования	точка доступа
Серия	ProSafe
Соответствие стандартам	соответствует IEEE 802.11g, обратная совметимость с 802.11b
Диапазон рабочих частот	2.4 - 2.4835 ГГц
Режимы работы	
Режим точки доступа	Есть
Режим моста	Есть
Интерфейсы ввода/вывода	
LAN порт	1 порт 10/100 Base-T Ethernet (RJ - 45) с поддержкой POE и MDI-X
Антенна	одна, съемная, всенаправленная коэффициент усиления 5 dBi
Индикаторы	4 светодиода: Power, LAN, WLAN, TEST
Разъем для подключения БП	есть, 12 В 1,2 А
Мониторинг и конфигурирование	
Веб – интерфейс	есть
Telnet	есть
Поддержка SNMP	есть
Безопасность	

Wi-Fi Protected Access (WPA)	есть
Wi-Fi Protected Access 2(WPA2)	есть
Block SSID Broadcast	есть
Фильтрация MAC – адресов	есть
Аутентификация	по стандарту 802.1X, поддержка EAP, PEAP
Поддерживаемые скорости передачи и чувствительность приемника	
802.11b	2 Mbps – 93 dBm
	5.5 Mbps – 91 dBm
	11 Mbps – 89 dBm
802.11g	6 Mbps – 91 dBm
	9 Mbps – 90 dBm
	12 Mbps – 89 dBm
	18 Mbps – 87 dBm
	24 Mbps – 84 dBm
	36 Mbps – 81 dBm
	48 Mbps – 77 dBm
	54 Mbps – 75 dBm
	108 Mbps – 71 dBm
Потребляемая мощность	4,3 Вт
Максимальная излучаемая мощность	
802.11b	+19 dBm
802.11g mode 6 to 24 Mbps	+18 dBm
802.11g mode 36, 48, 54 Mbps	+17/16/16 dBm
Физические характеристики	
Габаритные размеры	14.1×10×2.7 см
Вес	386 гр.
Условия эксплуатации	
Диапазон рабочих температур	от 0 до +40 ^{0}C
Влажность	относительная влажность не более 90%, без конденсата
Совместимость с ОС	Windows 98/2000/XP/Vista

Таблица 4.14 - Характеристики точки доступа NETGEAR WAG102

Общие характеристики	
Тип оборудования	точка доступа
Серия	ProSafe
Соответствие стандартам	соответствует IEEE 802.11g, обратная совметимость с 802.11b
Диапазон рабочих частот	2.4 - 2.4835 ГГц
Режимы работы	
Режим точки доступа	Есть
Режим моста	Есть
Интерфейсы ввода/вывода	
LAN порт	1 порт 10/100 Base-T Ethernet (RJ - 45) с поддержкой MDI-X
Антенна	две, съемные, всенаправленная коэффициент усиления 5 dBi
Индикаторы	4 светодиода: Power, LAN, WLAN, TEST
Разъем для подключения БП	есть, 12 В 1,2 А

Мониторинг и конфигурирование	
Веб – интерфейс	есть
Telnet	есть
Поддержка SNMP	есть
Безопасность	
Wi-Fi Protected Access (WPA)	есть
Wi-Fi Protected Access 2(WPA2)	есть
Block SSID Broadcast	есть
Фильтрация MAC – адресов	есть
Аутентификация	по стандарту 802.1X, поддержка EAP, PEAP
Поддерживаемые скорости передачи и чувствительность приемника	
802.11b	2 Mbps – 93 dBm
	5.5 Mbps – 92 dBm
	11 Mbps – 89 dBm
802.11g	6 Mbps – 90 dBm
	9 Mbps – 90 dBm
	12 Mbps – 89 dBm
	18 Mbps – 87 dBm
	24 Mbps – 85 dBm
	36 Mbps – 80 dBm
	48 Mbps – 75 dBm
	54 Mbps – 70 dBm
Потребляемая мощность	4,3 Вт
Максимальная излучаемая мощность	
802.11b	+19 dBm
802.11g mode 6 to 24 Mbps	+18 dBm
802.11g mode 36, 48, 54 Mbps	+17/16/16 dBm
Физические характеристики	
Габаритные размеры	32×190.5×122 мм
Вес	620 гр.
Условия эксплуатации	
Диапазон рабочих температур	от 0 до +40 ^{0}C
Влажность	относительная влажность не более 90%, без конденсата
Совместимость с ОС	Windows 98/2000/XP/Vista

Выбор антенн для подключения к удаленному офису

Для организации беспроводного канала между зданиями предприятия. Предположим, что здания удалены друг от друга на расстояние 400 метров, трасса распространения сигнала частично перекрывается вершинами деревьев. Для организации беспроводного канала будут использоваться офисные беспроводные точки доступа NETGEAR WG102, с внешними направленными антеннами. Необходимо обеспечить скорость передачи не ниже 54 Мбит/с.

Прежде чем переходить к выбору антенно-фидерного оборудования следует определить суммарное усиление тракта, необходимое для передачи сигнала на расстояние 400 метров. По графику приведенному на рисунке 4.40 следует определить суммарное усиление тракта соответствующее заданному расстоянию. Данный график не учитывает влияние атмосферных осадков, а также различных шумов и помех на распространение сигнала. По этому стоит выбрать значение суммарного усиления тракта с запасом. Итак для того чтобы организовать беспроводной канал между зданиями удаленными на расстояние 400

метров, суммарное усиление тракта должно составлять не менее 105 дБ.

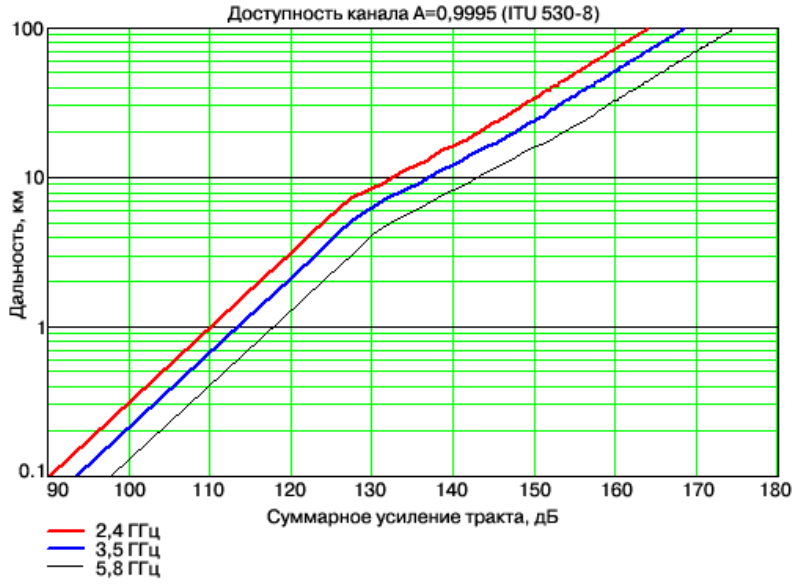


Рисунок 4.40. Зависимость дальности радиосвязи при прямой видимости от суммарного усиления тракта радиосигнала

Согласно суммарное усиление тракта рассчитывается по формуле:

$$Y_{дБ} = P_{t\,дБ} + G_{t\,дБ} + G_{r\,дБ} - P_{\min\,дБ} - L_{t\,дБ} - L_{r\,дБ} \qquad (4.1)$$

, где:

$P_{t,дб}$ – мощность передатчика;

$G_{t,дб}$ – коэффициент усиления передающей антенны;

$G_{r,дб}$ – коэффициент усиления приемной антенны;

$P_{min,дб}$ – чувствительность приемника;

$L_{t,дб}$ – потери сигнала в коаксиальном кабеле и разъемах передающего тракта;

$L_{r,дб}$ – потери сигнала в коаксиальном кабеле и разъемах приемного тракта.

Более подробно рассмотрим каждый параметр:

1. Мощность передатчика - мощность беспроводной точки доступа или адаптера в dBm. Эту информацию можно найти в спецификации на оборудование таблица 4.13. Для точки доступа NETGEAR WG102, ***16 dBm, для скорости 54 Мбит/с.***

2. Чувствительность приемника, которую также можно найти в спецификации на оборудование. Чувствительность приемника зависит от скорости на котором работает оборудование и задается со знаком "минус". Значение чувствительности приёмника для скорости 54 Мбит/с составляет – 75 дБм.

5. Потери в коаксиальном кабеле и разъёмах. Точка доступа будет соединена с антенной кабелем ANT24-ODU(LMR-200) длинной 2 метра, с затуханием 0.6 дБ/м.

Для зашиты точек будет применятся модуль грозозащиты ANT24-SP, вносимое модулем затухание составляет 0.5 дБ. Потери в разъемах не менее 0.3 дБ. Суммарное затухание вносимое кабелями и разъемами составляет 2.3 дБ. Т.к. конфигурации приемного и передающего трактов одинаковы вносимые потери также одинаковы.

Теперь подставив в формулу 4.1 все известные величины, определим коэффициенты усиления приемной и передающей антенн.

$$G_{t.дБ} + G_{г.д.} = 105 - 16 - 75 + 2.3 + 2.3 = 18.6 \text{ дБ}$$

Предполагается что будут использоваться одинаковые антенна, согласно расчетам коэффициент усиления каждой из них должен составлять не менее 10 дБ.

Перед выбором антенн определим некоторые требования:

- Антенны должны работать вне помещения

-Антенны должны быть направленными

-Дальность распространения сигналов должна быть больше дальности до оборудования удаленного офиса, потому как в различных метеоусловиях, а также в черте города данные характеристики могут меняться

-Антенны должны подключаться к внутренним точкам доступа

-Антенны должны иметь приемлемую стоимость

Исходя из последнего условия, остановимся на антеннах производимых фирмой D-link, они имеют достаточную функциональность при достаточно низкой цене. Коэффициент усиления антенн должен быть не много больше рассчитанного порядка 12 -14 дБ.

D-Link ANT 24-1400

Антенна работает в диапазоне частот 2,3 –2,5 ГГц, что позволяет ее использовать совместно с аппаратурой, выпускаемой для медицины и науки. Антенна ANT24-1400 подключается к беспроводным устройствам, имеющим реверсный SMA-разъем и предоставляет возможность расширить площадь покрытия существующей беспроводной сети, работающей в диапазоне 2,4 ГГц. Корпус антенны сделан устойчивым к погодным явлениям, что позволяет использовать ее не только внутри помещений. В комплект поставки антенны включен модуль грозозащиты и кабель-переходник для разъема SMA

Рисунок 4.41. Направленная антенна ANT24-1400

Таблица 4.15 - Технические характеристики антенны ANT24-1400

Диапазон частот От 2.3ГГц до 2.5ГГц	**Поляризация** Линейная, вертикальная
Сопротивление 50 Ом	**Диаграмма направленности** по вертикали 15 град по горизонтали 15 град

Максимальное усиление (без затухания в кабеле) 14 dBi	**Подводимая мощность** 50 Вт
Теоретическое расстояние передачи при скорости 1 Мбит/с/11 Мбит/с (при работе с внутренними точками доступа)* До 2,5км/900м	**Теоретическое расстояние передачи при скорости 1 Мбит/с / 11 Мбит/с (при работе с внешними точками доступа)** До 4км/1,5км

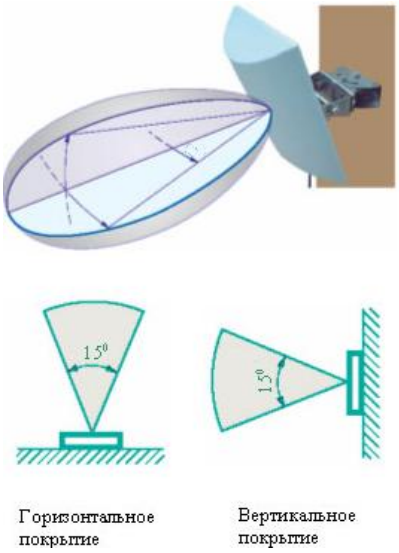


Рисунок 4.42. Диаграммы направленности для антенны ANT24-1400

D-Link ANT24-1201

Направленная внешняя антенна типа Яги D-Link ANT24-1201 подключается к беспроводным устройствам, работающим в частотном диапазоне 2,4 ГГц для увеличения площади покрытия беспроводной сети. Корпус антенны сделан из устойчивого к погодным явлениям материала. Антенна поставляется с кабелем – переходником, позволяющим подключать антенну к беспроводным устройствам с реверсным разъемом SMA.

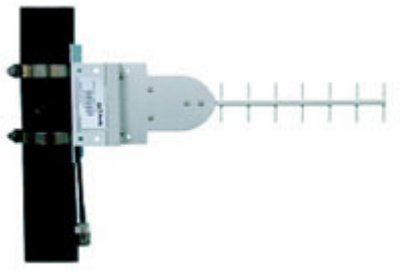


Рисунок 4.43. Направленная внешняя антенна ANT24-1201

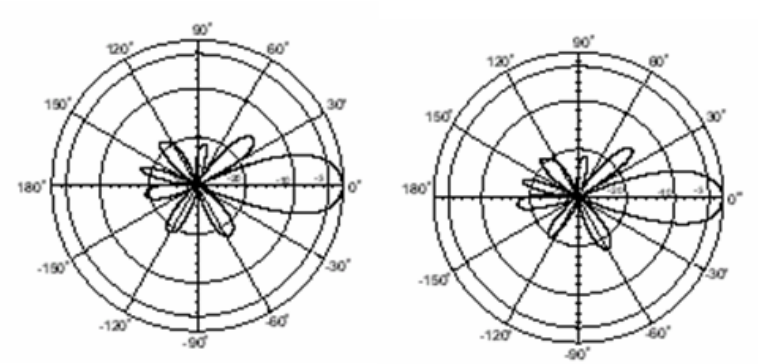


Рисунок 4.44. Диаграммы направленностей в вертикальной и горизонтальной плоскостях антенны ANT24-1201

Таблица 4.16. Технические характеристики антенны ANT24-1201

Диапазон частот От 2.4ГГц до 2.5ГГц	Поляризация Линейная вертикальная
Сопротивление 50 Ом	Диаграмма направленности по вертикали 50 град по горизонтали 50 град
Максимальное усиление (без затухания в кабеле) 12 dBi	Подводимая мощность 50 Вт
Теоретическое расстояние передачи при скорости 1 Мбит/с/11 Мбит/с (при работе с внутренними точками доступа)* До 1,5км/500м	Теоретическое расстояние передачи при скорости 1 Мбит/с / 11 Мбит/с (при работе с внешними точками доступа) 2,5км/1км

D-Link ANT24-1800

Антенна работает в диапазоне частот 2,4 –2,5 ГГц, что позволяет использовать ее совместно с аппаратурой, выпускаемой для медицины и науки. Антенна ANT24-1800 подключается к беспроводным устройствам, имеющим реверсный SMA-разъем и предоставляет возможность расширить площадь покрытия существующей беспроводной сети, работающей в диапазоне 2,4 ГГц.

Корпус антенны сделан устойчивым к погодным явлениям, что позволяет использовать ее не только внутри помещений. В комплект поставки антенны входит крепеж для монтажа и кабель-переходник для разъема RP-SMA.

Рисунок 4.45. Направленная антенна ANT24-1800

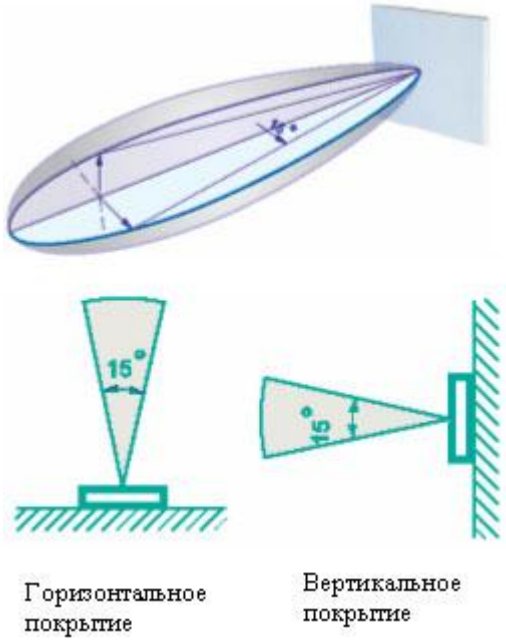


Рисунок 4.46. Диаграммы покрытия для антенны ANT24-1800

Таблица 4.17. Технические характеристики антенны ANT24-1800

Диапазон частот От 2.4ГГц до 2.5ГГц	**Поляризация** Линейная, вертикальная
Сопротивление 50 Ом	Диаграмма направленности по вертикали 15 град по горизонтали 15 град
Максимальное усиление (без затухания в кабеле) 18 dBi	Подводимая мощность 50 Вт
Теоретическое расстояние передачи при скорости 1 Мбит/с/11 Мбит/с (при работе с внутренними точками доступа)* До 5км/2км	Теоретическое расстояние передачи при скорости 1 Мбит/с / 11 Мбит/с (при работе с внешними точками доступа) 8км/3км

D-Link ANT24-1801

Направленная антенна типа Яги. Антенна работает в диапазоне частот 2,4 –2,5 ГГц, что позволяет ее использовать совместно с аппаратурой, выпускаемой для медицины и науки. Антенна ANT24-1801 подключается к беспроводным устройствам, имеющим реверсный SMA-разъем и предоставляет возможность расширения площади покрытия существующей беспроводной сети, работающей в диапазоне 2,4 ГГц.

Рисунок 4.47. Направленая антенна типа волновой канал ANT24-1801

Рисунок 4.48. Диаграммы направленностей антенны ANT24-1801

Таблица 4.18 - Технические характеристики антенны ANT24-1801

Диапазон частот От 2.4ГГц до 2.5ГГц	**Поляризация** Линейная вертикальная
Сопротивление 50 Ом	**Диаграмма направленности** по вертикали 15 град по горизонтали 15 град
Максимальное усиление (без затухания в кабеле) 18 dBi	**Подводимая мощность** 50 Вт
Теоретическое расстояние передачи при скорости 1 Мбит/с/11 Мбит/с (при работе с внутренними точками доступа)* До 5км/2км	**Теоретическое расстояние передачи при скорости 1 Мбит/с / 11 Мбит/с (при работе с внешними точками доступа)** 8км/3км

D-Link ANT24-2100

D-Link ANT24-2100 подключается к беспроводным устройствам D-Link стандартов 802.11b и 802.11g (2.4 ГГц) и имеет коэффициент усиления 21 dBi. Антенна также может быть

подключена к беспроводному оборудованию 802.11b и 802.11g других производителей. D-Link ANT24-2100 предоставляет возможность существенно расширить площадь покрытия существующей беспроводной сети и/или создать беспроводной мост для передачи данных на большие расстояния.

Через кабель-переходник SMA N-типа, входящий в комплект поставки антенны, ANT24-2100 легко подключается к любым внутриофисным точкам доступа и беспроводным адаптерам, со съемными штатными антеннами. Сама антенна имеет разъем для подключения N-типа (N-type-female), что позволяет подключать её к внешним точкам доступа. Высокий коэффициент направленности антенны (21 dBi) позволяет строить радиомосты на большие расстояния. Теоретическая дальность передачи при использовании ANT24-2100 совместно с активным оборудованием 2,4ГГц мощностью 35mW* на обоих концах беспроводного канала связи (без использования дополнительных кабельных сборок) для скорости 1 Мбит/с составляет около 10 км.

В комплект поставки ANT24-2100 входит модуль грозозащиты (surge protector), являющийся важным аксессуаром для внешних антенн. Даже при наличии на крыше мачт громоотводов, которые исключают прямое попадание молнии в антенну, мощный грозовой разряд в непосредственной близости от внешней антенны может полностью вывести из строя всё приёмо-передающее оборудование. Модуль грозозащиты включается в антенно-фидерный тракт и заземляется.

Рисунок 4.49. Параболическая направленная антенна ANT24-2100

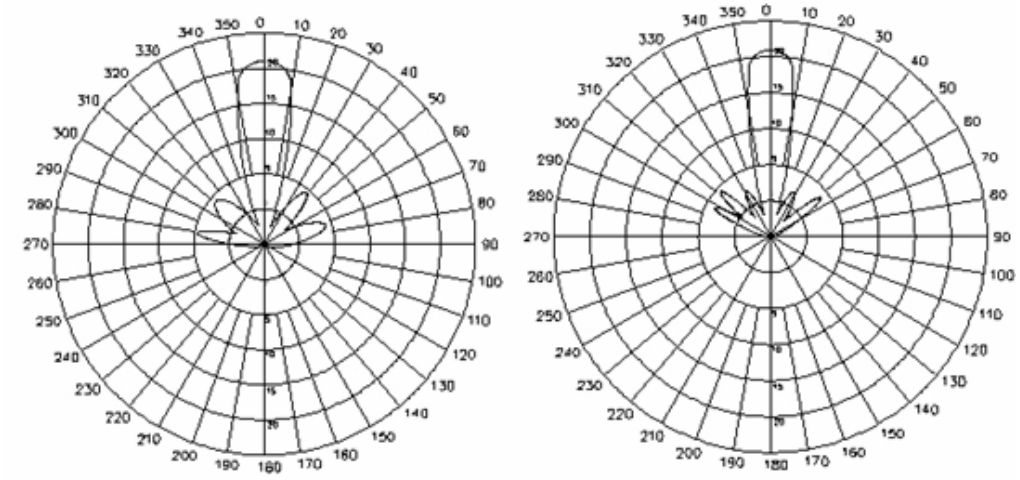


Рисунок 4.50. Диаграммы направленностей в горизонтальной и вертикальной плоскостях антенны ANT24-2100

Таблица 4.19 Технические характеристики антенны ANT24-2100

Диапазон частот От 2.4ГГц до 2.5ГГц	**Поляризация** Линейная, вертикальная
Сопротивление 50 Ом	**Диаграмма направленности** по вертикали 8 град по горизонтали 5 град
Максимальное усиление (без затухания в кабеле) 21 dBi	**Подводимая мощность** 50 Вт
Теоретическое расстояние передачи при скорости 1 Мбит/с/11 Мбит/с (при работе с внутренними точками доступа)* До 8км/3км	**Теоретическое расстояние передачи при скорости 1 Мбит/с / 11 Мбит/с (при работе с внешними точками доступа)** 10км/4,5км

Из рассмотренных антенн наиболее подходящей является D-Link ANT 24-1400, она имеет более чем достаточный коэффициент усиления и узкую диаграмму направленности.

3. Порядок выполнения работы

Настройка оборудования

Конфигурирование RADIUS сервера

Для конфигурирования службы IAS необходимо открыть панель управление и дважды щелкнуть значок «Администрирование», затем в открывшемся списке выбрать компонент «Службы проверки подлинности в интернет».

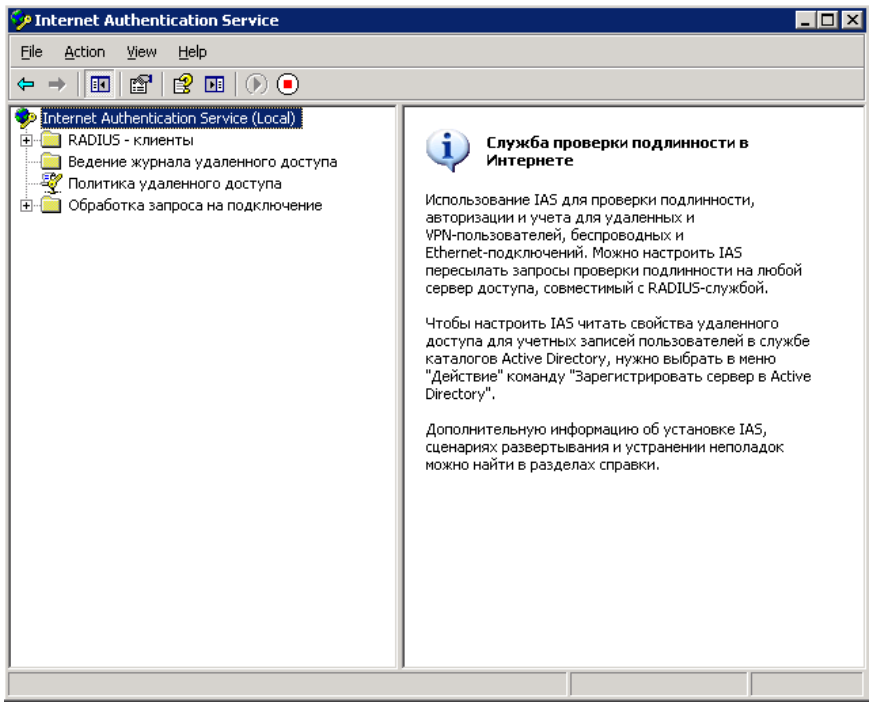


Рисунок 4.53. Консоль управления службой IAS

Настройка службы достаточно проста. Прежде всего необходимо добавить клиентов RADIUS (все имеющиеся точки доступа), для этого необходимо щелкнуть правой кнопкой мыши узел «RADIUS-клиенты» и выбрать команду «Новый RAS-клиент» рисунок 4.54.

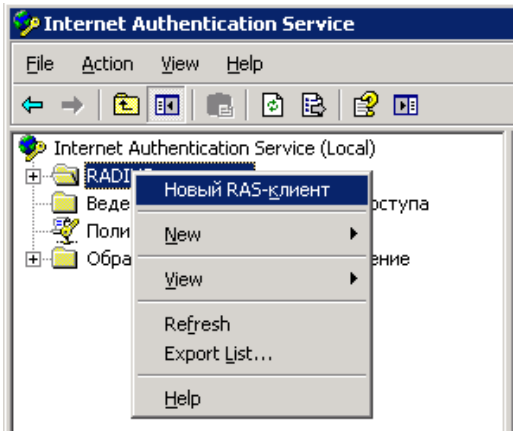


Рисунок 4.54. Добавление RAS-клиента

Далее в открывшемся окне, предлагается ввести понятное имя в качестве такового будем использовать IP – адреса точек доступа.

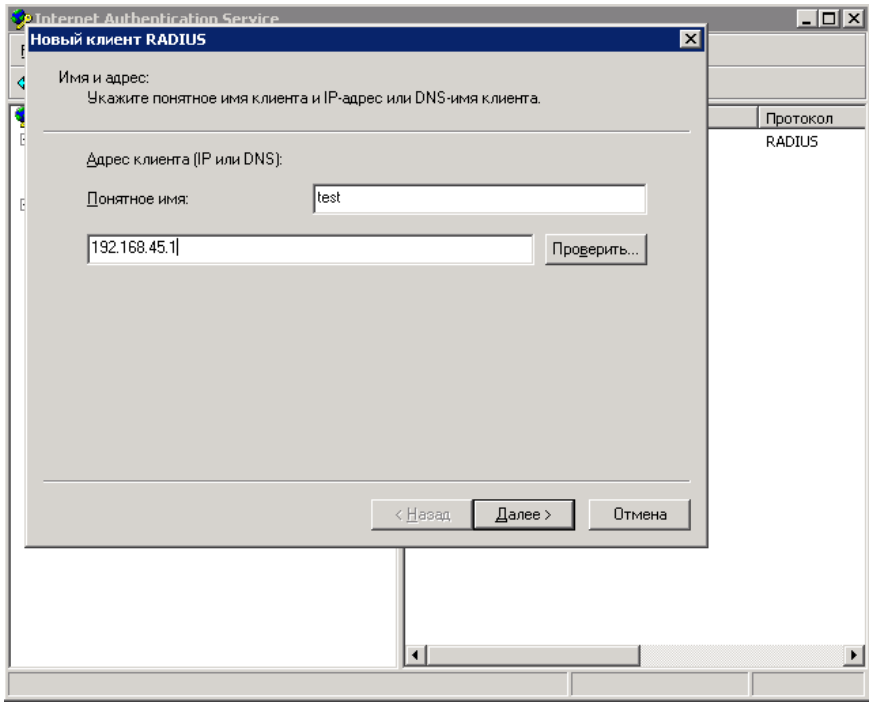


Рисунок 4.55. Настройка параметров клиента

В следующем окне предлагается выбрать поставщика оборудования, так как используемое оборудование не включено в список, в пункте клиент – вендор указываем RADIUS Standard. Далее следует указать общий секрет на основе которого точка доступа и сервер RADIUS будут идентифицировать друг друга. Секрет задается для каждого нового RAS-клиента индивидуально и может содержать до 64 символов (исходя из соображений безопасности общий секрет должен содержать цифра, заглавные и строчные буквы и символы, также имеет смысл периодически менять общий секрет). Если атрибут проверки подлинности сообщения включен, все сообщение RADIUS зашифровано, а общий секрет

используется в качестве ключа.

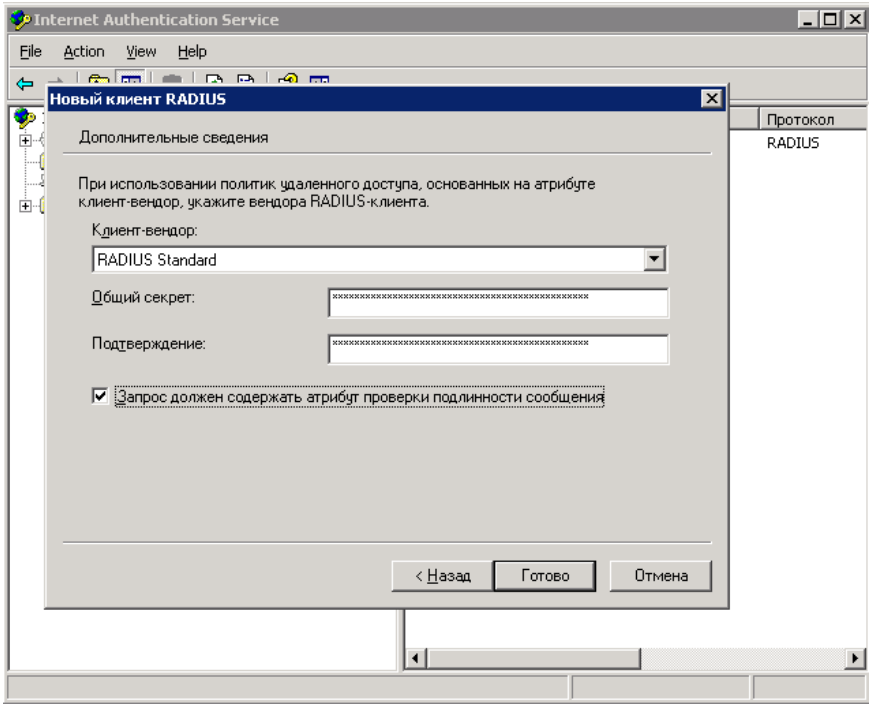


Рисунок 4.56.

После того как все точки доступа добавлены, перейдем к настройке журнала удаленного доступа. В журнале по желанию администратора могут фиксируются запросы учеты, запросы проверки подлинности, промежуточные состояния.

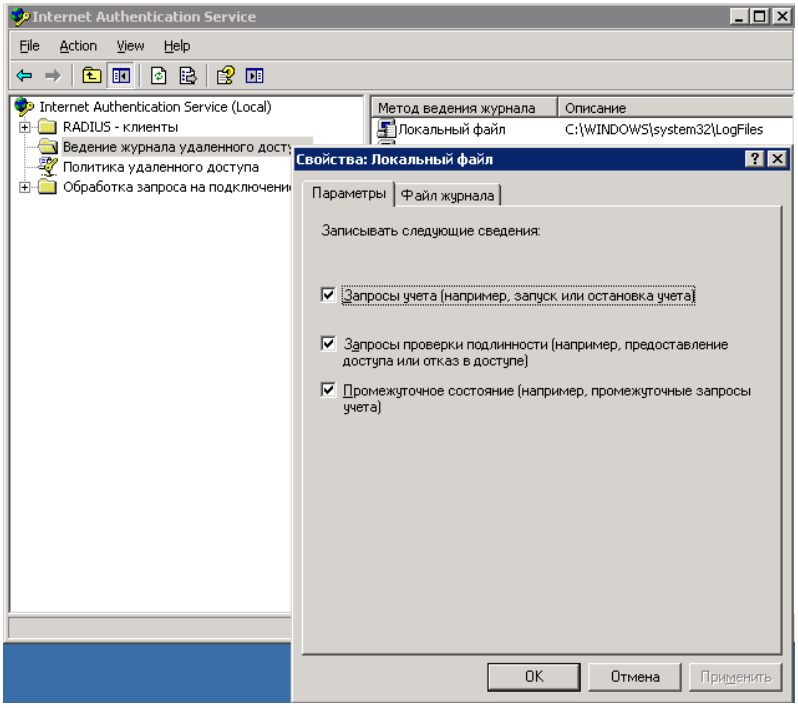


Рисунок 4.57. Настройка журнала удаленного доступа

Далее необходимо определить политики удаленного доступа, для создания политики в дереве консоли нужно щелкнуть правой кнопкой мыши «Политика удаленного доступа» и

выбрать из контекстного меню команду «Создать политику удаленного доступа».

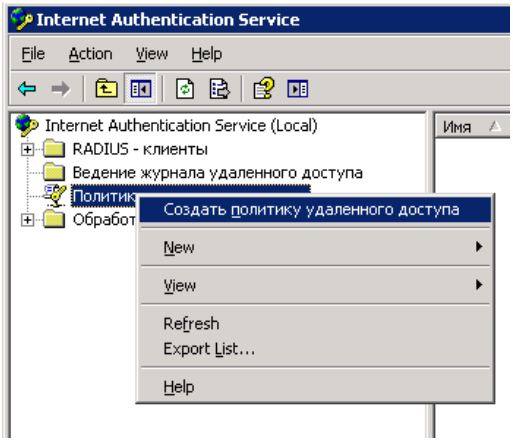


Рисунок 4.58. Создание политики удаленного доступа

Для создания политики будем использовать мастера создания политики удаленного доступа. После запуска мастера предлагается выбрать способ доступа к сети, из предложенного списка выбираем «Беспроводной доступ»

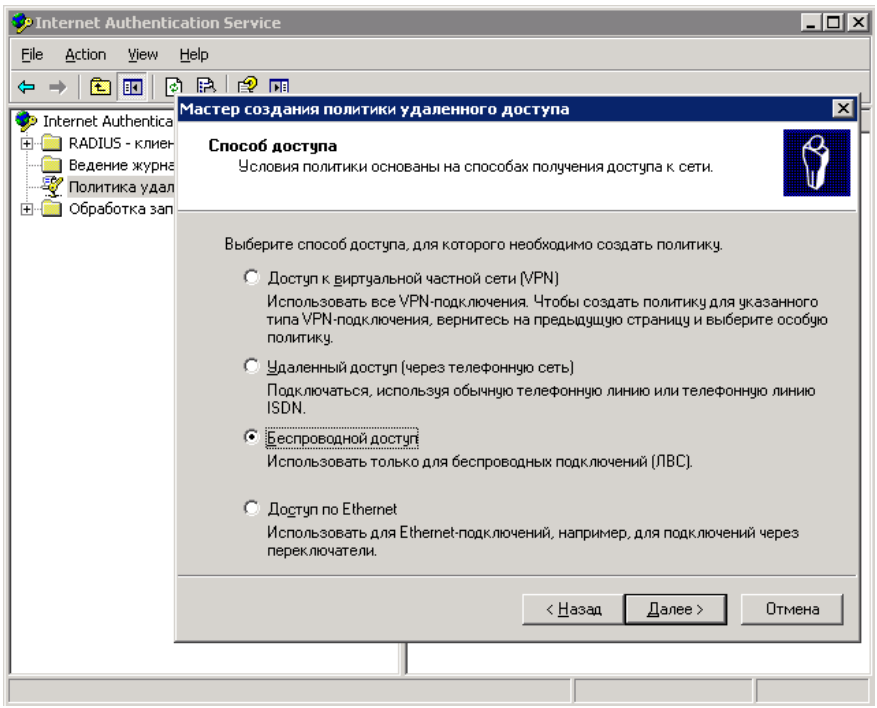


Рисунок 4.59. Мастер создания политики

Далее следует выбрать пользователей или группы пользователей которым разрешено использовать беспроводной доступ (в моем случае в Active Directory создана группа, куда внесены все пользователи, которые будут пользоваться беспроводной связью, ее мы и добавляем).

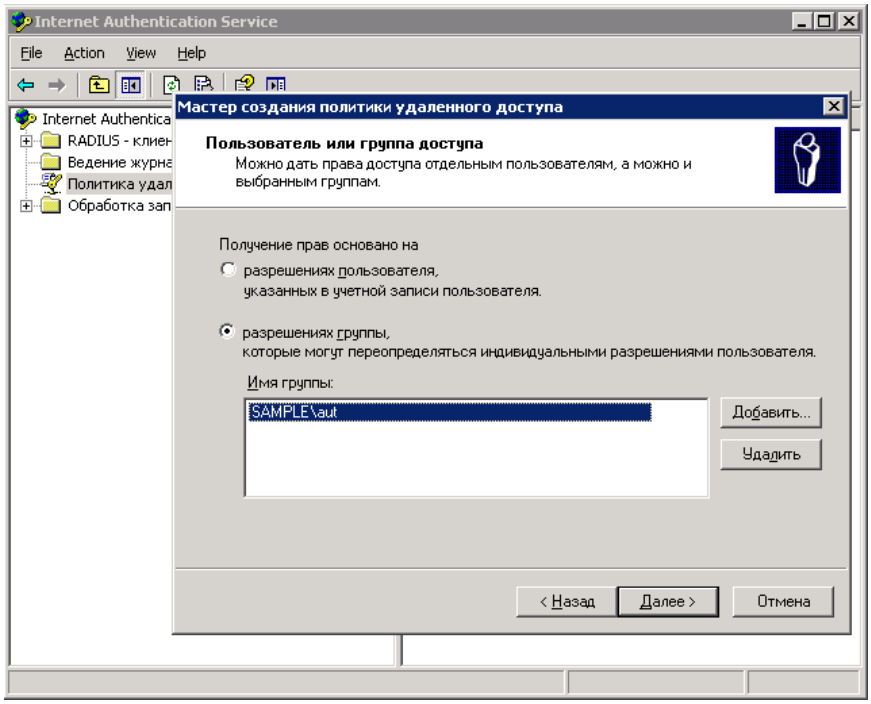


Рисунок 4.60. Создание политики удаленного доступа

Следующим шагом необходимо определить методы проверки подлинности, как было описано в пункте 6.7, в данной работе будет использоваться защищенный протокол расширенной проверки подлинности (Protected Extensible Authentication Protocol, PEAP). Выбираем PEAP, жмем кнопку настроить, в появившемся окне «защищенные свойства EAP» необходимо выбрать методы проверки подлинности, выбираем EAP – MSCHAP v2 (Microsoft Challenge Handshake Authentication Protocol, версия 2).

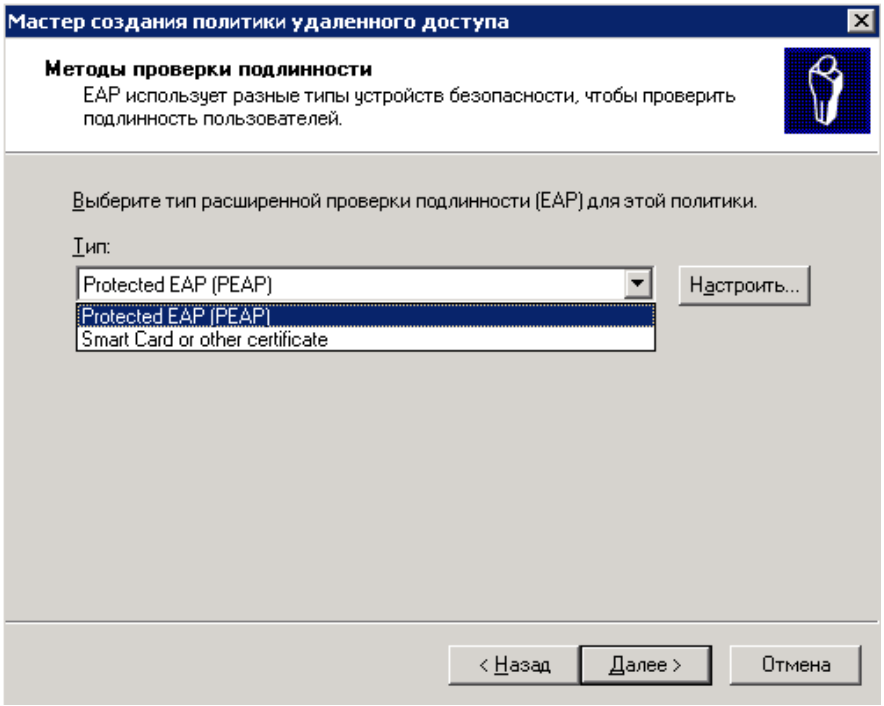


Рисунок 4.61. Настройка аутентификации

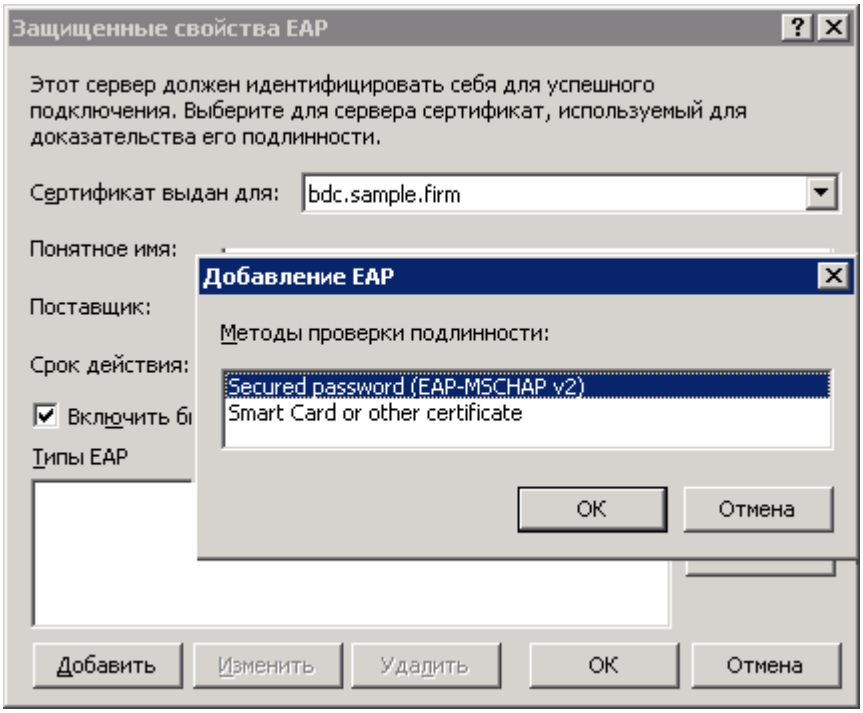


Рисунок 4.62. Выбор метода аутентификации

После того как политика создана произведем ее окончательное редактирование. Для этого нужно в области сведений дважды щелкните политику, которую требуется изменить, в открывшемся окне следует выбрать действие которое необходимо выполнить если запрос удовлетворяет заданным в политике условиям. Выбираем предоставить право удаленного доступа, так как в данном проекте реализуется политика «запрещено все, что в явном виде не разрешено», т.е. только пользователи, входящие в группу aut, смогут авторизоваться на сервере.

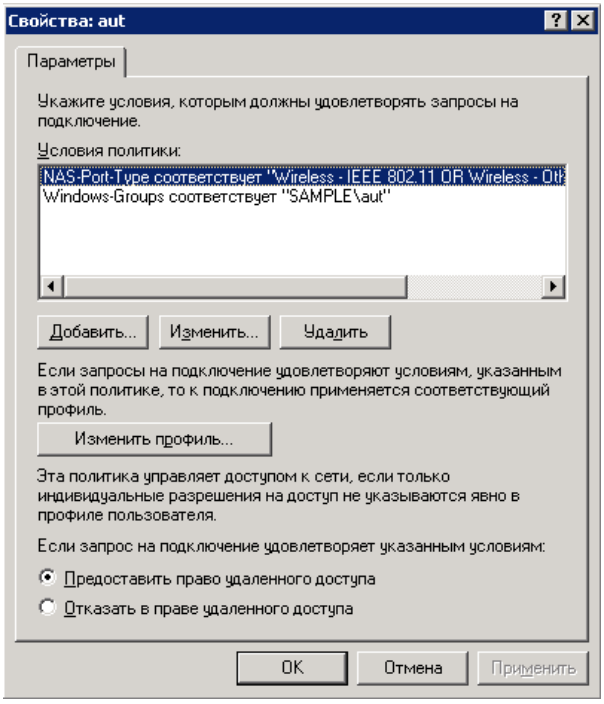


Рисунок 4.63. Выбор действия при прохождении аутентификации

Перейдем к настройке профиля политики удаленного доступа, на вкладке ограничение по входящим звонкам разрешим доступ только в определенное время (ежедневно с 7.00 до 22.00). В пункте тип порта NAS указываем Wireless – IEEE 802.11.

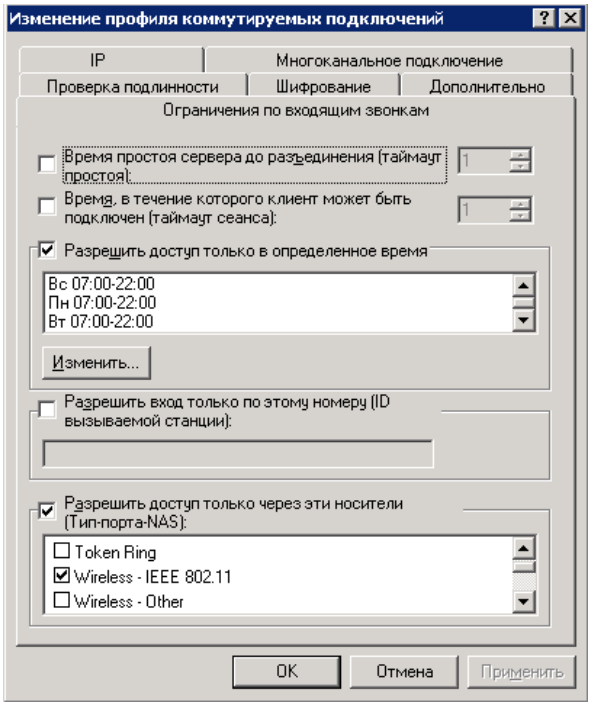


Рисунок 4.64. Изменение профиля коммутируемых подключений

На вкладке IP необходимо указать, что IP адрес клиента должен быть назначен сервером. На вкладке проверка подлинности нужно открыть окно выбор поставщиков EAP и добавить тип EAP Protected EAP, щелкнуть кнопку изменить и указать, что используется шифрованная проверка подлинности MSCHAP v2.

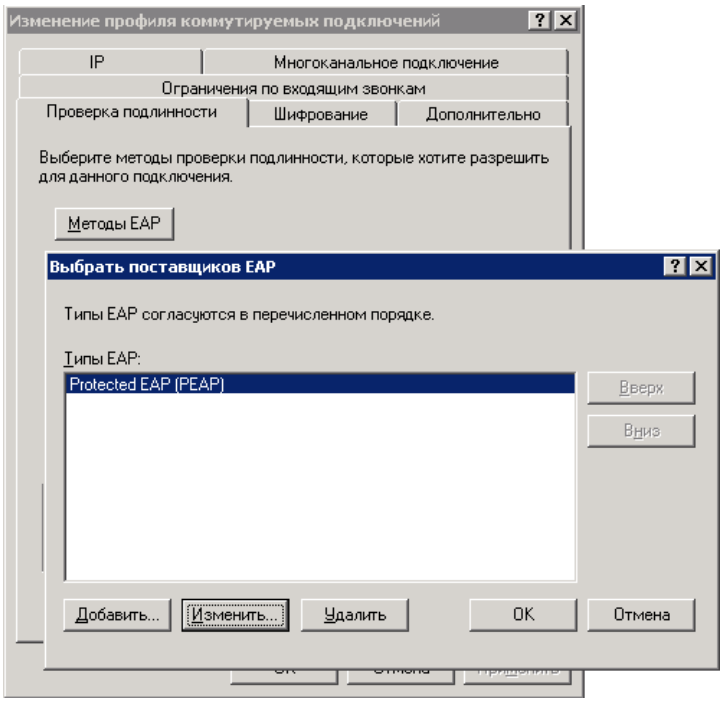


Рисунок 4.65. Проверка подлинности

Настройка точек доступа

Для того чтобы перейти к настройке точки доступа необходимо подключить ее к ПК по средствам Ethernet и подключится к ней, используя telnet или WEB – интерфейс. Мы буду использовать WEB – интерфейс, он более прост и нагляден. По умолчанию точки доступа NETGEAR WG102, имеют IP – адрес 192.168.0.229, имя пользователя “admin” и пароль “password”.

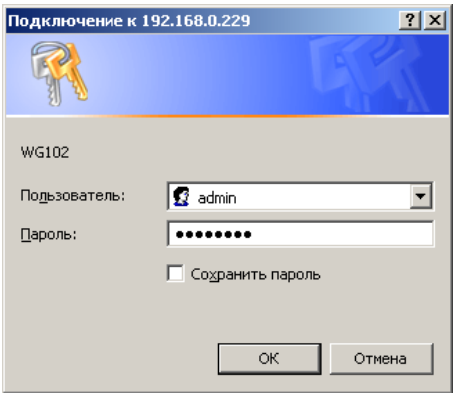


Рисунок 4.66. Подключение к беспроводной точке доступа

Прежде всего, необходимо выбрать канал на котором будет работать точка. В пункте 12.2. для каждой точки были определены соответствующие каналы а также уровень выходной мощности. Для их настройки необходимо перейти на вкладку Wireless Settings, в поле Channel/Frequency устанавливается нужный канала (1, 6, 11); Чтобы сохранить совместимость со стандартном 802.11b в поле Operating Mode следует выбрать «Auto(802.11g/802.11b)».

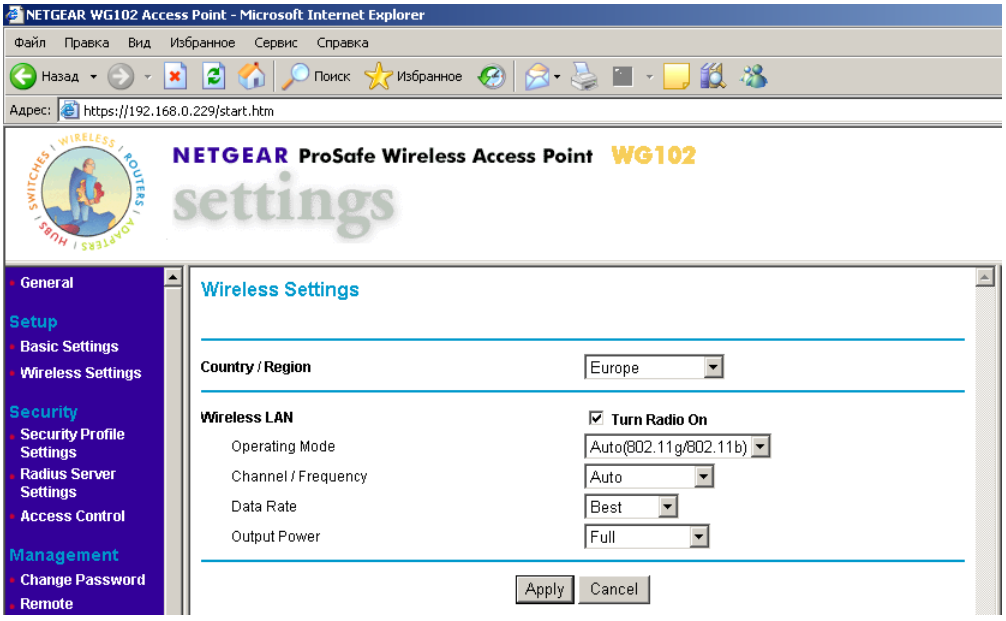


Рисунок 4.67. Выбор частотного канала

На следующем этапе необходимо присвоить точке идентификатор зоны обслуживания (SSID) и установить параметры зашиты, для этого переходим на вкладку Security Profile Setting рисунок 4.68. Для обеспечения роумнга требуется чтобы все точки имели одинаковый SSID.

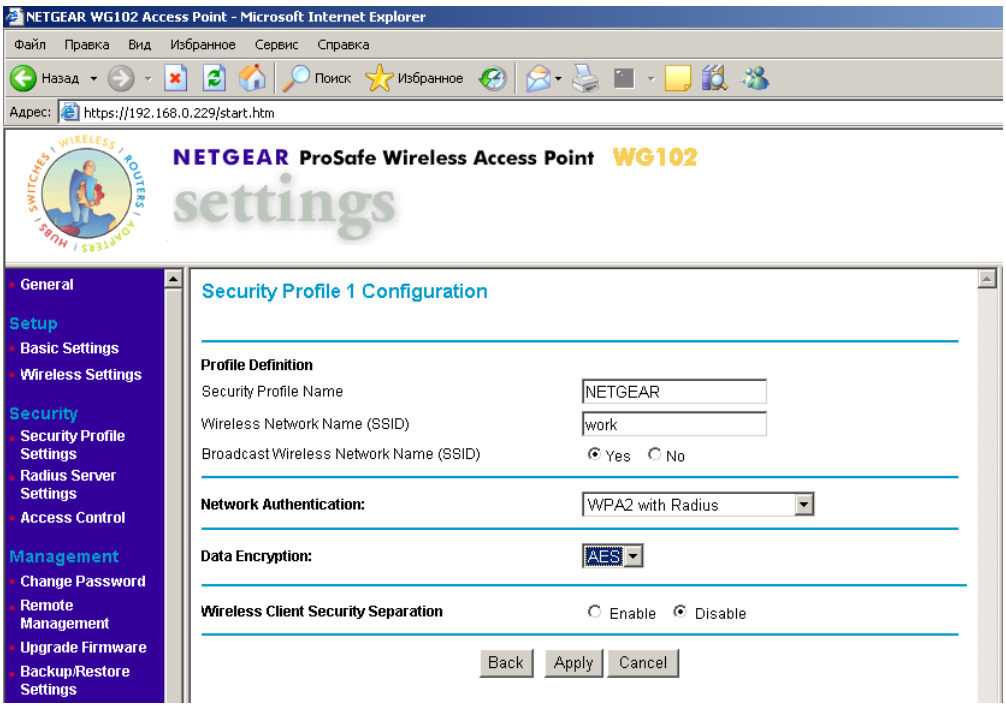


Рисунок 4.68. Настройка параметров безопасности

Так как для аутентификации в сети используется RADIUS сервер, в пункте Network Authentication следует указать “WPA2 with Radius”. В качестве алгоритма шифрования следует выбрать AES. Параметры RADIUS сервера задаются в пункте Radius Server Settings. Следует указать IP адрес сервера, порт, и общий секрет рис. 4.69.

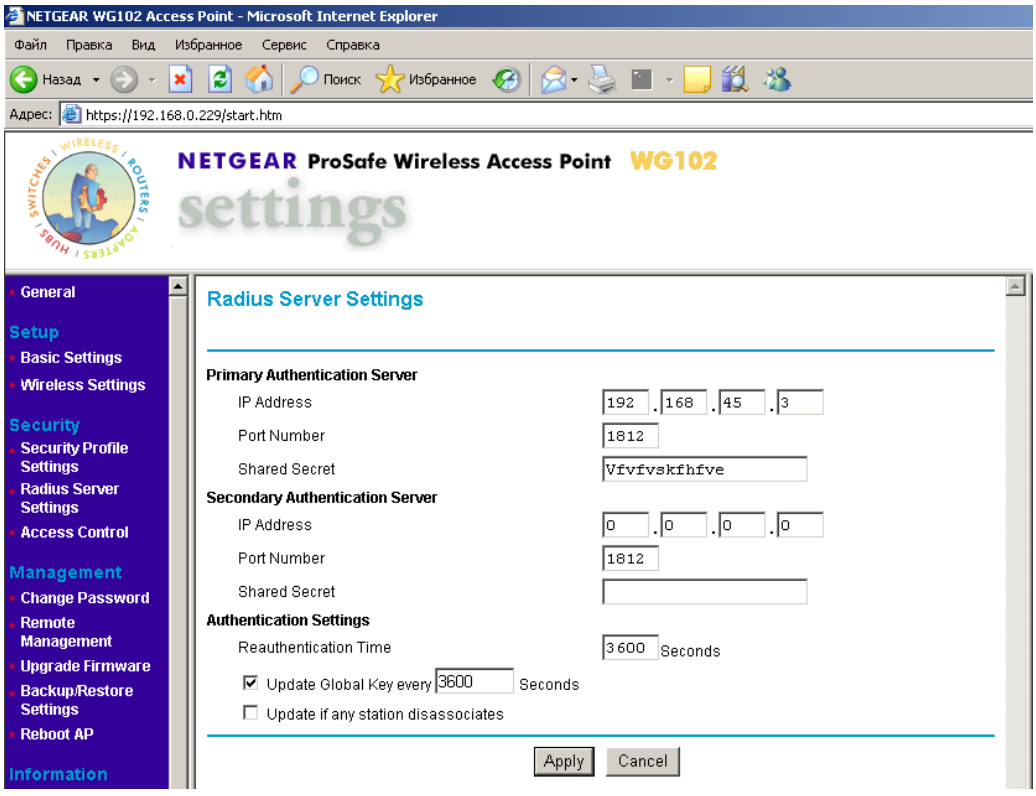


Рисунок 4.69. Настройки параметров RADIUS сервера

В проектируемой сети точки доступа будут иметь фиксированные IP адреса, по этому

их нужно прописать на каждой точке, также стоит указать DNS и Шлюз рисунок 4.70.

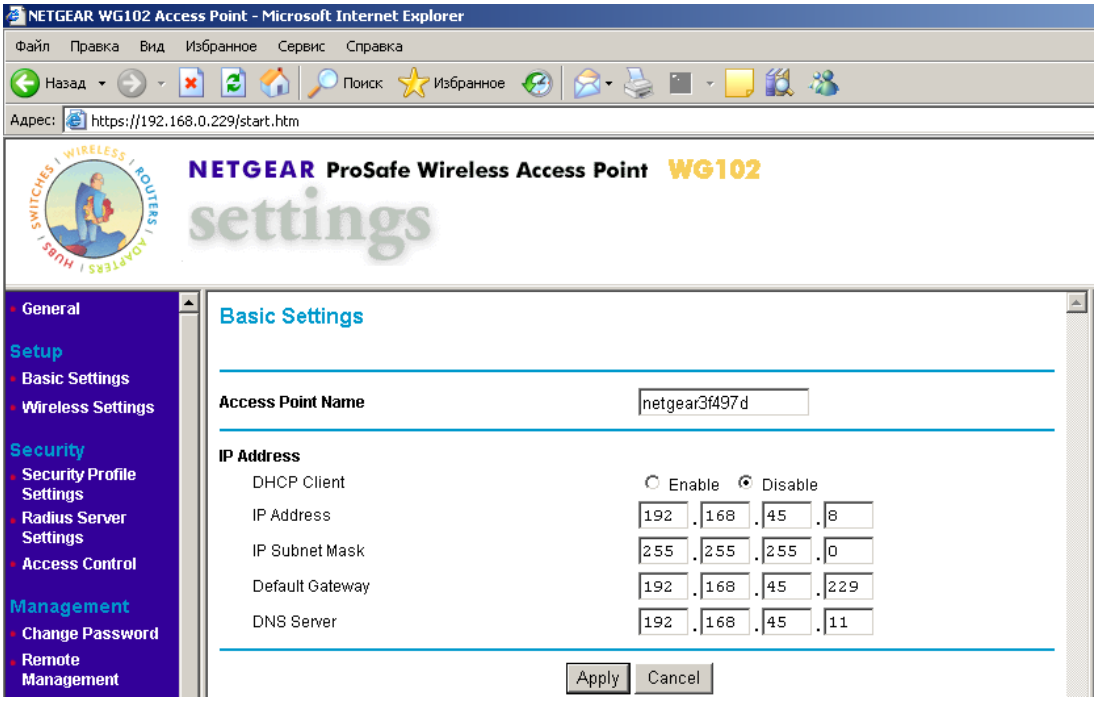


Рисунок 4.70. Сетевые настройки точки

В целях безопасности следует сменить стандартный пароль, для этого переходим на вкладку Change Password, вначале указывается старый пароль затем новый и подтверждение (желательно чтобы пароль удовлетворял требованиям сложности).

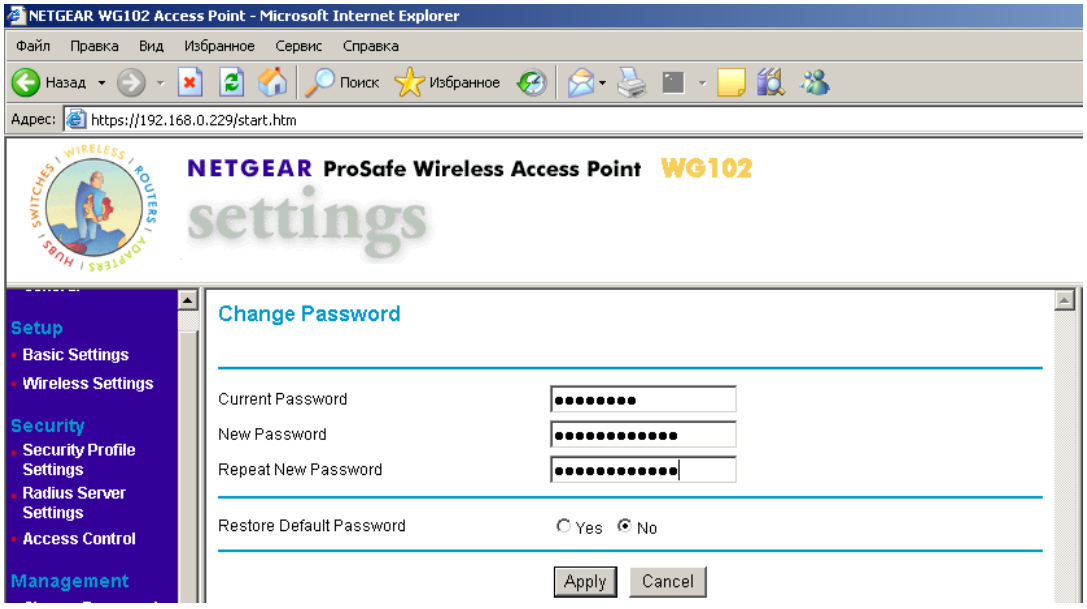


Рисунок 4.71. Изменение пароля администратора

Для вступления настроек в силу необходимо перезагрузить точку доступа для этого переходим на вкладку Rebut AP.

Настройка клиенткой системы

На всех компьютерах пользователей установлена операционная система Windows XP SP2. Для того чтобы клиент смог проверить подлинность сервера и организовать с ним шифрованное соединение – клиенту нужно иметь сертификат сервера. Это можно сделать несколькими способами. Открыть internet explorer и в поле адреса написать http://CA_адрес/certsrv, на открывшейся странице выбрать пункт установка сертификата и следовать указаниям мастера. Более подходящий в моем случае вариант (компьютеры пользователей еще не имеют подключения к сети предприятия), скопировать сертификат выданный серверу RADIUS корневым центром сертификации на съемный носитель и произвести установку на машины клиентов с этого носителя. При двойном щелчке по файлу сертификата на экране появляется окно изображенное на рис. 4.72.

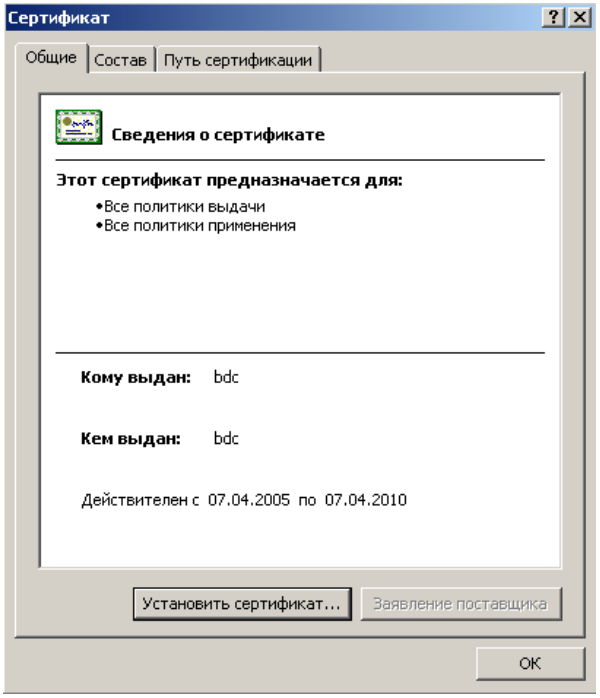


Рисунок 4.72. Установка сертификата

На вкладке состав можно просмотреть характеристики сертификата (алгоритм цифровой подписи, серийный номер сертификата, кем и когда выдан, дата окончания срока действия, алгоритм и длина открытого ключа). Чтобы установить сертификат необходимо кликнуть кнопку установить сертификат и следовать указаниям мастера установки сертификатов.

Далее следует выбрать режим, в котором будет работать сетевая карта (рис. 4.73). В операционной системе Windows предлагается 3 основные настройки. Это подсоединение к любой существующей сети, подключение к точке доступа AP и режим работы Ad-Hoc (соединение между двумя компьютерами). В нашем случае, во избежание конфликтов сети, следует выбрать режим Access Point network only (режим обмена данными только с точками доступа).

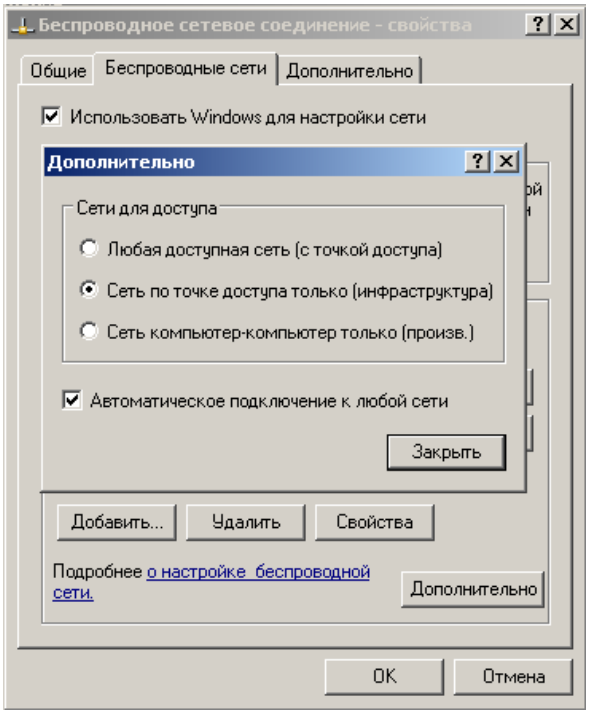


Рисунок 4.73. Выбор режима работы сетевой карты

Следующий шаг, настройка беспроводных адаптеров пользовательских компьютеров, для этого необходимо открыть папку сетевые подключения и перейти в свойства беспроводного адаптера, на вкладку беспроводные сети. Далее необходимо добавить точку доступа, с которой будет работать пользователь, для этого в поле «предпочитаемые беспроводные сети» нужно нажать кнопку добавить. В появившемся окне свойства беспроводной сети необходимо указать SSID сети в моем случае «test», проверка подлинности WPA, шифрование данных AES. Далее переходим на вкладку проверка подлинности.

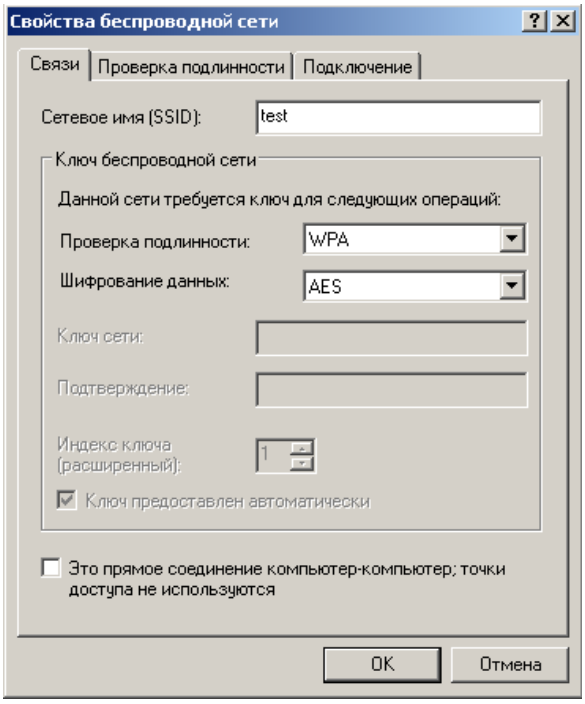


Рисунок 4.74. Выбор метода аутентификации

В поле тип EAP указываем Защищенный EAP (PEAP), далее нажав кнопку свойства переходим в окно защищенные свойства EAP (рисунок 4.75), устанавливаем галочку в поле проверять сертификат сервера и выбираем доверенные корневые центры сертификации выбираем наш центр сертификации. В поле выбор метода проверки подлинности указываем безопасный пароль (EAP-MSCHAP v2).

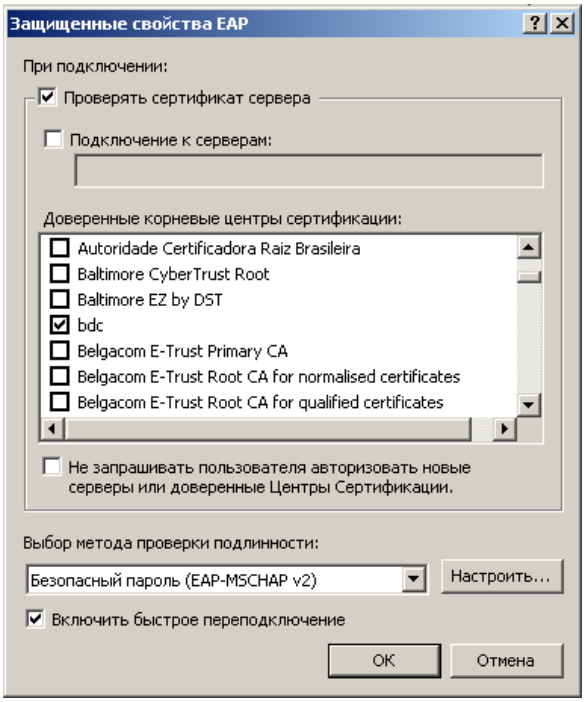


Рисунок 4.75. Защищенные свойства EAP

Пробуем подключиться к беспроводной сети попытка оказывается удачной. В журнале событий отображается уведомление, сгенерированное службой IAS, о том что пользователю test1 входящему в группу aut, предоставлен доступ, клиент также получил ip адрес и к ниму применилась групповая политика.

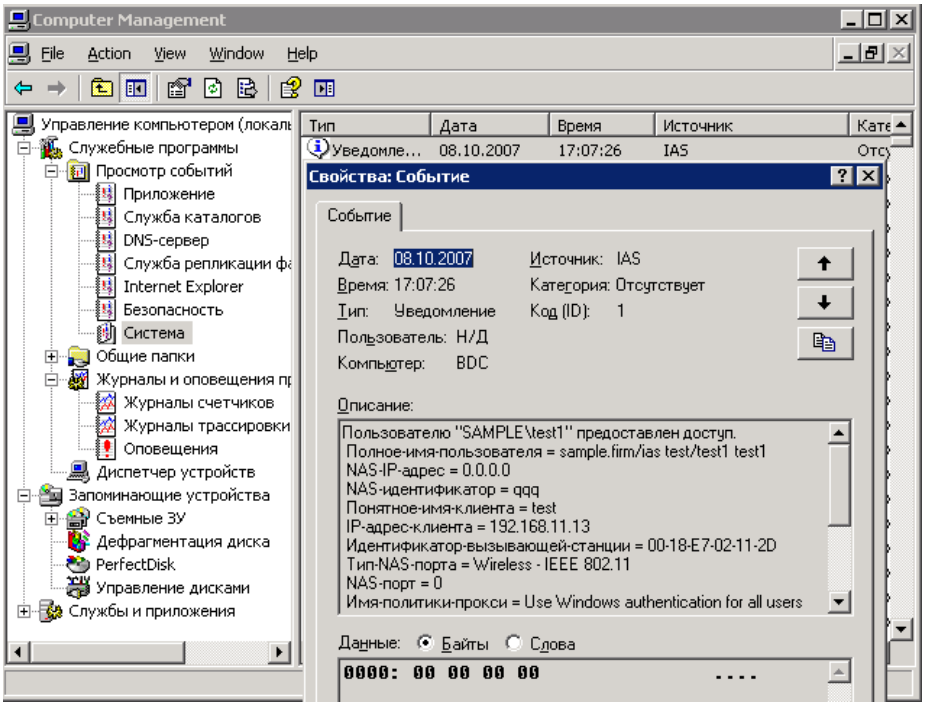


Рисунок 4.76. Просмотр событий

Настройка оборудования для подключения удаленного офиса

Для организации беспроводного канала необходимо что бы точки работали в режиме моста. Для этого необходимо войти в меню настройки точки доступа. В меню Access Point Settings выбираем пункт Wireless Point – to- Point Bridge и вводим MAC-адрес второй точки доступа. На второй точке доступа следует сделать аналогичные настройки, и ввести MAC-адрес первой точки.

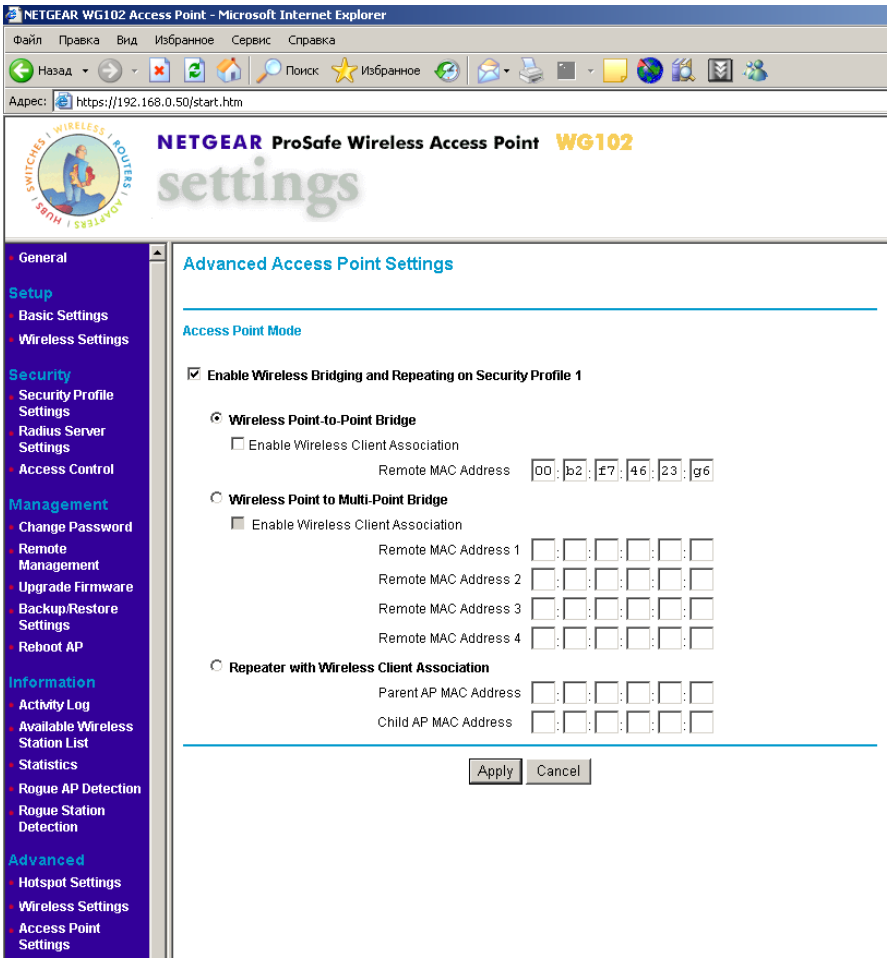


Рисунок 4.77. Перевод точки доступа в режим моста

Затем следует выбрать метод аутентификации и защиты передаваемого трафика, для этого переходим в меню Security Profile Settings. Из возможных вариантов самым надежным является WPA2-PSK, аутентификация на основе общего секрета, для шифрования трафика применяется AES. Секрет задается в пункте WPA Passphrase, максимальная длинна для данной модели составляет 63 символа. Также полезно отключить передачу SIDD в широковещательных пакетах это можно сделать в пункте Broadcast Wireless Network Name (SSID).

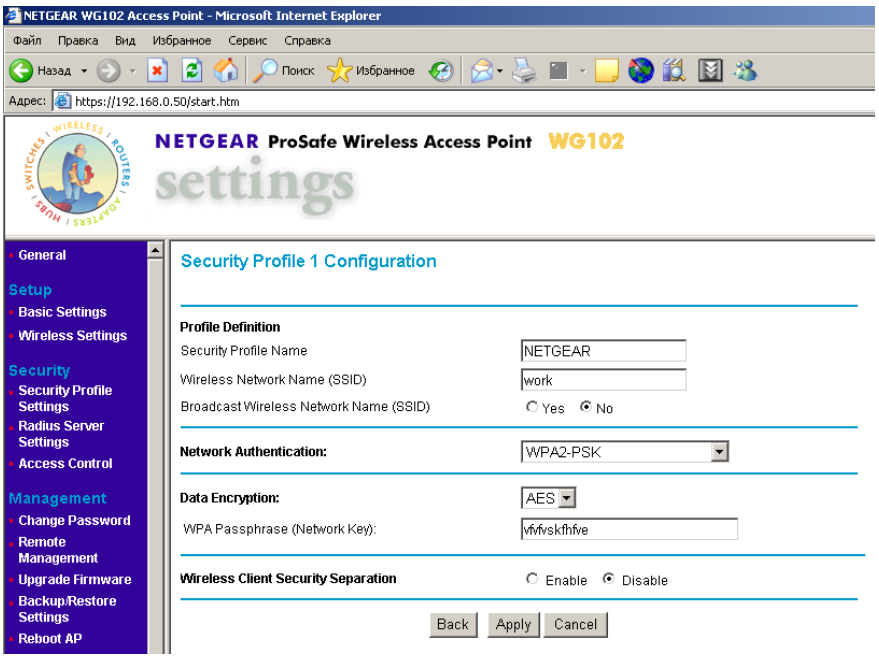


Рисунок 4.78. Настройка параметров аутентификации и шифрования передаваемого трафика

Следует также определить частотный канал, скорость передачи, и уровень выходной мощности, в соответствии с пунктом 11 точки доступа должны работать на первом канале, скорость передачи данных 54 Мбит/с. Для установки этих параметров нужно перейти в меню Wireless Settings, рисунок 4.78.

Тестирование точек доступа

В ходе проведения тестирования будут определены возможности выбранного для реализации данного проекта оборудования (точек доступа).

Оценка производительности точек доступа

Данный тест направлен на оценку производительности используемых в работе точек доступа Netgear WG102. 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 SP2. Схема тестирования приведена на рисунке 15.1. В помещении, где проводится тестирование, нет оборудования работающего в диапазоне 2.4 ГГц. Точки разнесены на 3 метра, работают в режиме моста.

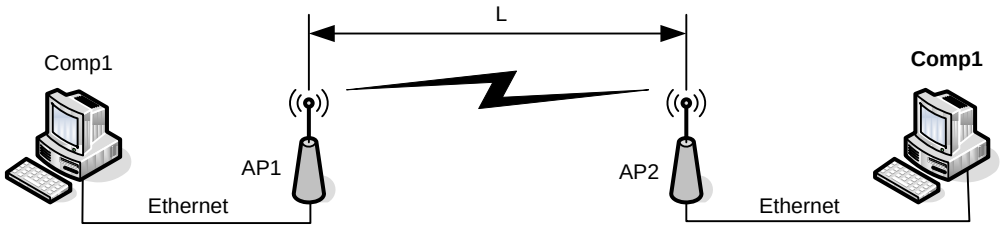


Рисунок 4.79. Тестовый стенд для определения максимальной пропускной способности точек доступа

Методика тестирования:

Осуществляется передача трафика, сгенерированного программой NetIQ Chariot, между узлами Comp1 и Comp2. В ходе тестирования направление передачи и количество потоков трафика будет меняться:

Передача трафика от узла Comp1 к узлу Comp2 с длинной пакета:

Пакеты максимального размера (1500 байт);

Пакеты размера 512 байт;

Пакеты размера 64 байта;

Передача трафика с максимальной длиной пакета в обоих направлениях

Передача трафика с максимальной длиной пакета в 16 потоков (8 в направлении Comp1, 8 – в направлении Comp2)

Для каждого случая измеряется скорость передачи и средняя величина времени отклика. Измерение скорости производится в течении 5-ти минут.

Описание тестового стенда:

Точки доступа: Netgear WG102

Конфигурация ПК: Конфигурация обоих ПК одинакова:

Таблица 4.20. Конфигурация ПК

Материнская плата	Gigabyte GA-945P-DS3
Процессор	DualCore Intel Pentium E2140
Память	2 × 512 Kingston DDR2
Видеокарта	NVIDIA GeForce 8400 GS (512 Мб)
HDD	Seagate Barracuda ST380811AS
OS	Windows XP SP2

Настройка программного обеспечения:

На обоих ПК устанавливаются «конечные точки» (сенсоры). На один из компьютеров (на comp1) устанавливается консоль управления. ПК назначаются адреса из одной подсети (в нашем случае comp1 имеет IP: 192.168.0.1; comp2: 192.168.0.2). Точки доступа переводятся в режим моста, для этого, переходим на вкладку настройки режима точки доступа «AP mode» и выбираем Wireless Point to Point Bridge, далее следует ввести MAC – адрес второй точки доступа в поле «Remote Bridge MAC». Вторая точка настраивается аналогично, в поле «Remote Bridge MAC» указывается MAC – адрес первой точки.

Далее следует перейти в главное окно консоли управления IxChariot и сконфигурировать тест. В меню Edit выбираем команду Add Pair, в открывшемся окне вводим адреса хостов. Далее следует выбрать скрипт на основе которого будет генерироваться трафик, я использую скрипт throughput.scr (TCP трафик без ограничений (циклическая пересылка файлов со случайно-сгенерированным содержанием)). Для каждого из вариантов тестирования следует изменять размер генерируемого файла. По умолчанию

генерируется блоки данных размером 100000 бит. В этом случае большая часть пакетов, проходящих через точку, будет максимально возможного размера. Изменить размер генерируемого файла можно перейдя в окно Script Editor рисунок 4.80.

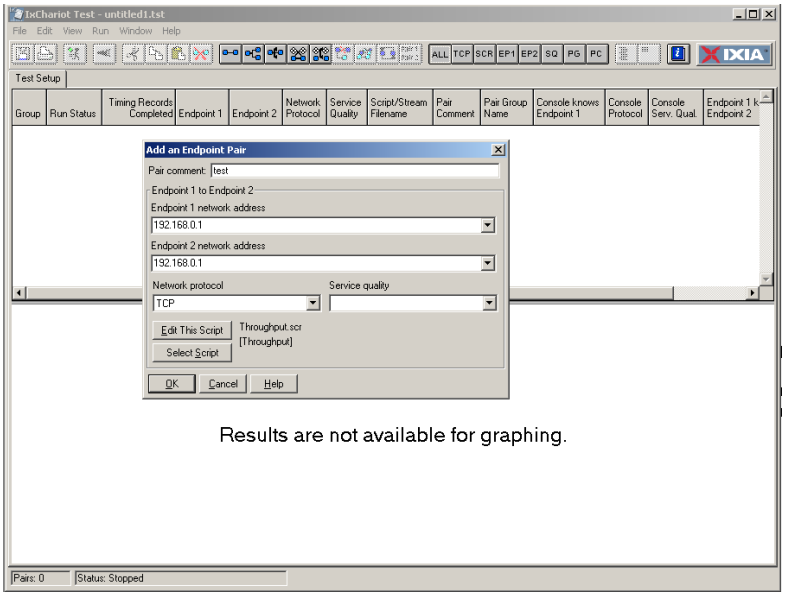


Рисунок 4.80. Консоль управления, создание теста

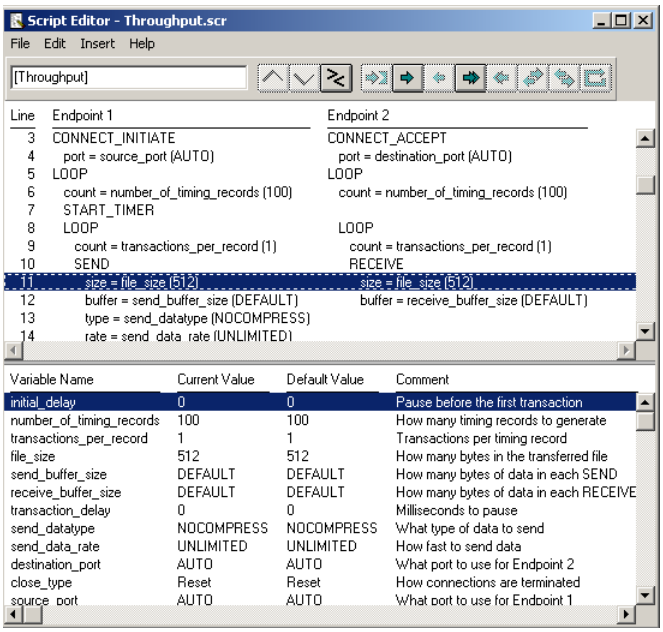


Рисунок 4.81. Изменение размера генерируемого файла

Результаты тестирования

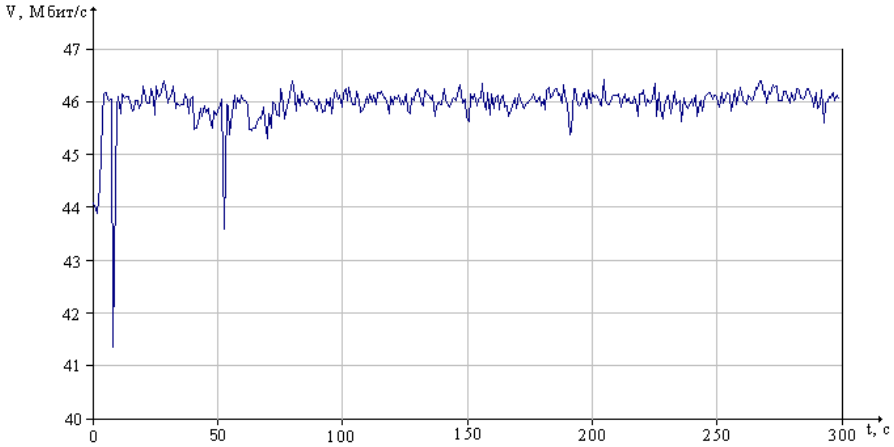


Рисунок 4.82. Скорость передачи данных с размером пакета 1500 байт, в направлении узла Comp2

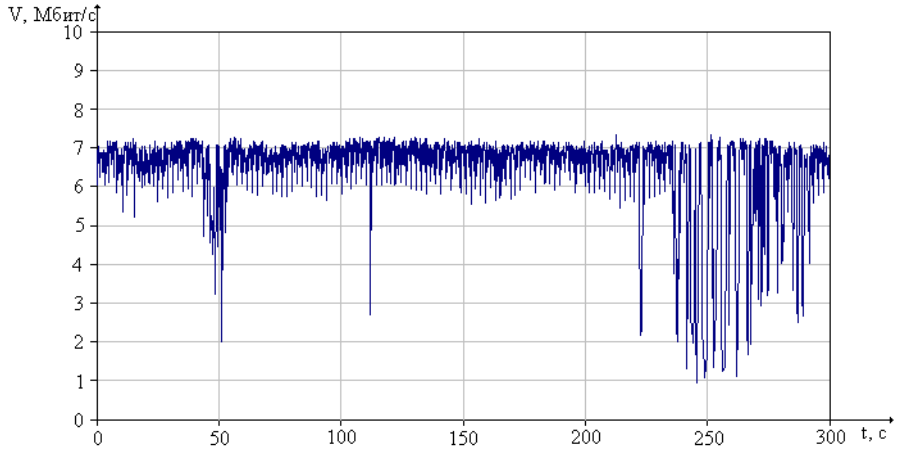


Рисунок 4.83. Скорость передачи данных с размером пакета 512 байт, в направлении узла Comp2

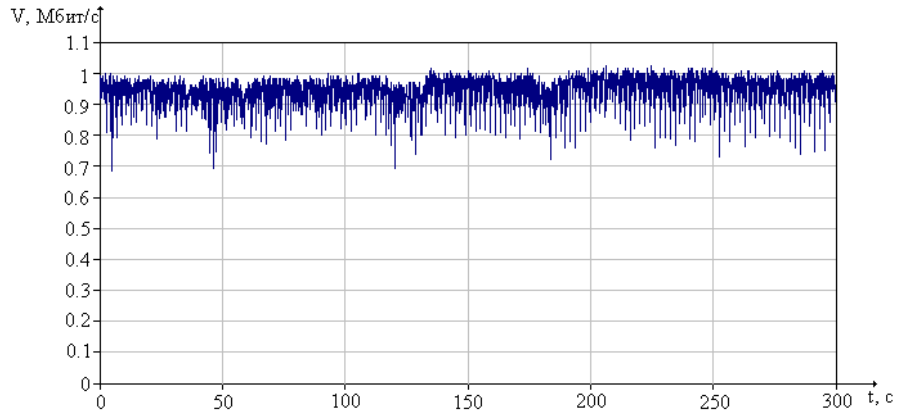


Рисунок 4.84. Скорость передачи данных с размером пакета 64 байт, в направлении узла Comp2

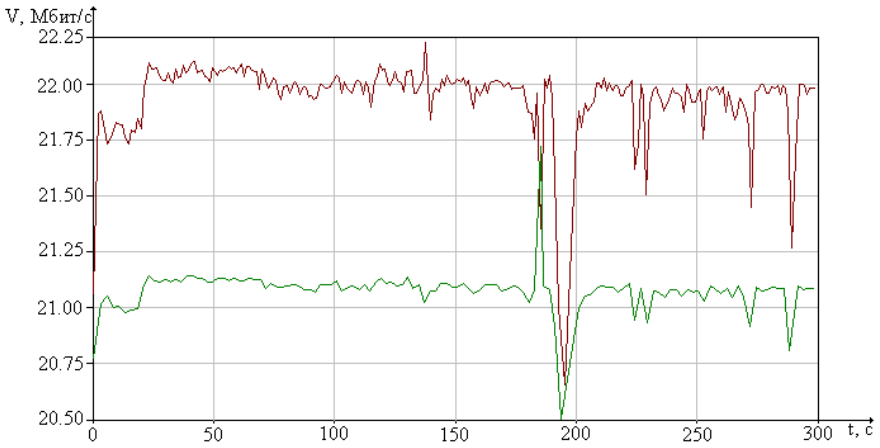


Рисунок 4.85. Скорость передачи данных с размером пакета 1500 байт, в обоих направлениях

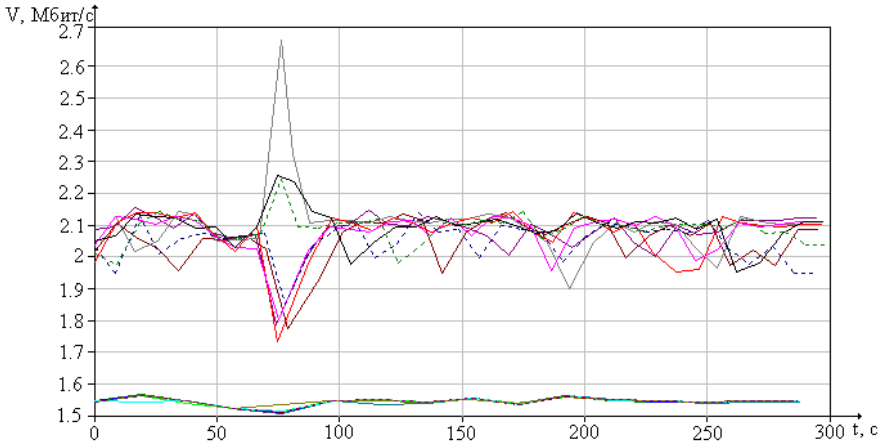


Рисунок 4.86. Скорость передачи данных с размером пакета 1500 байт, 16 потоков

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 4.21

Таблица 4.21 - Результаты измерения времени отклика

№ теста	Время отклика, мсек
1a	16
1b	14
1c	12
2	17
3	27

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 4.79. 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 5 минут.

Настройка оборудования:

Оставляем все настройки сделанные для проведения первого теста. На точках необходимо включить шифрование. Для этого необходимо перейти на вкладку Security Profile Settings. Для использования WEP в пункте Network Authentication необходимо выбрать Shared Key, в поле Data Encryption выбрать 152 bits WEP и задать ключ. Для использования TKIP в пункте Network Authentication выбираем WPA-PSK. Для использования AES в пункте Network Authentication выбираем WPA2-PSK. В последних двух случаях также необходимо задать ключ.

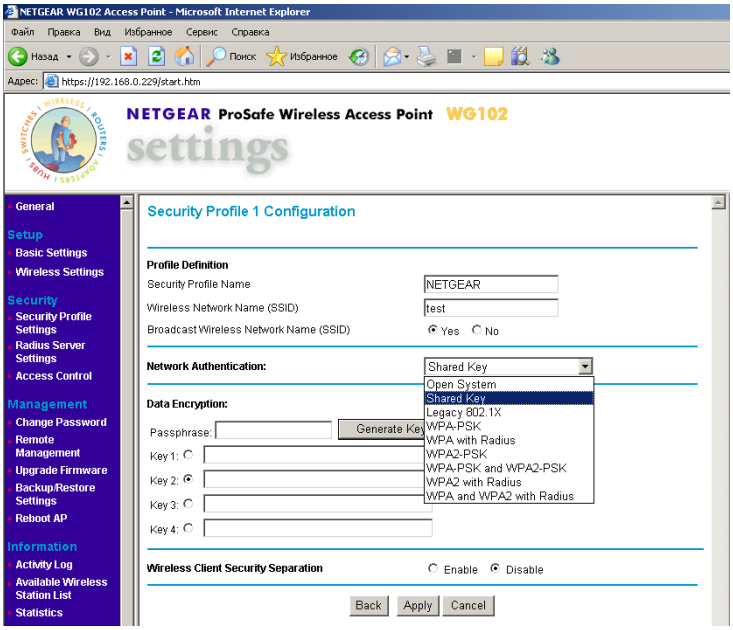


Рисунок 4.87. Настройка шифрования

Результаты тестирования:

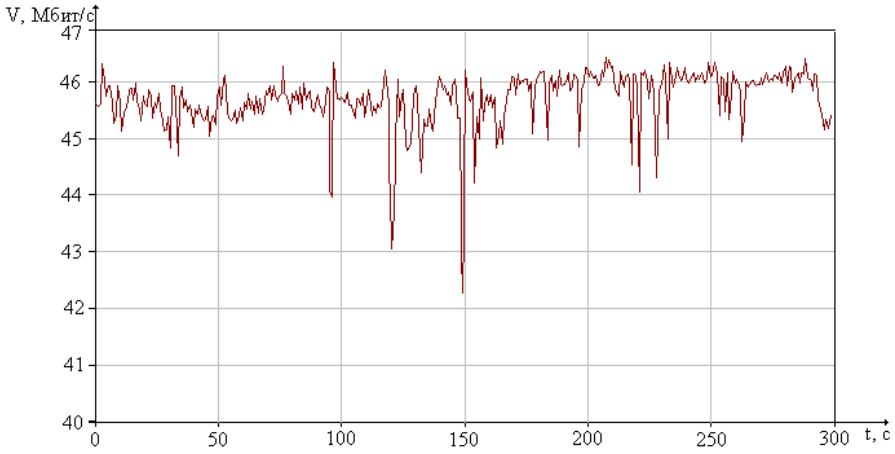


Рисунок 4.88. Скорость передачи данных в направлении узла comp2, при использовании алгоритма шифрования WEP

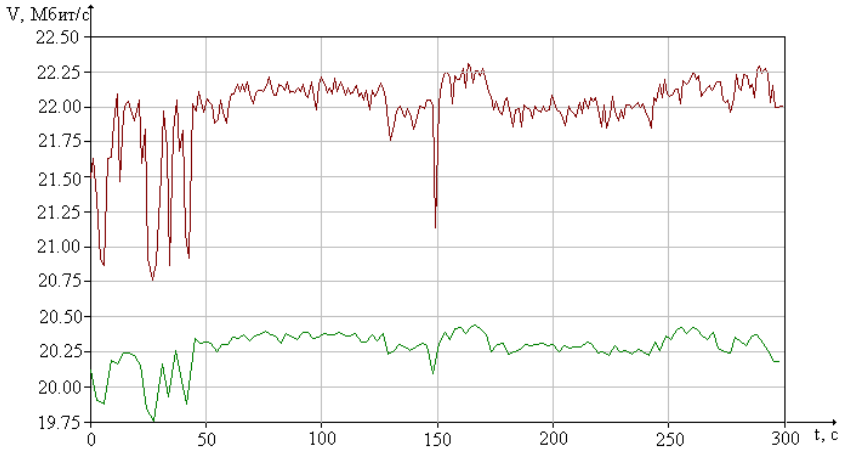


Рисунок 4.89. Скорость передачи данных в обоих направлениях, при использовании алгоритма шифрования WEP

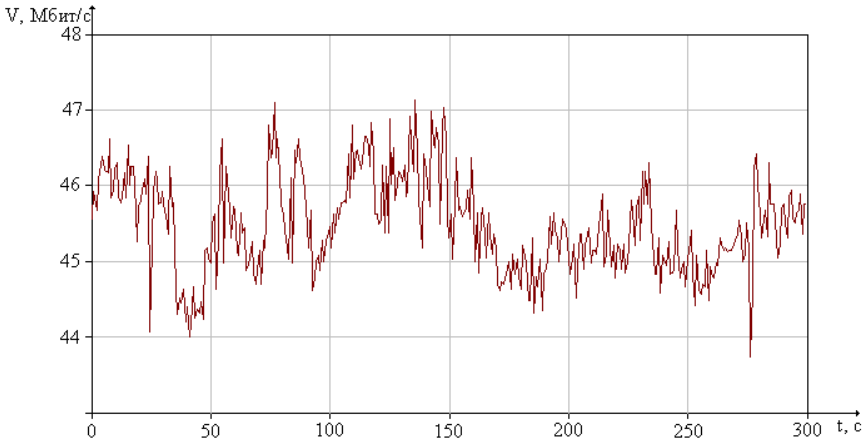


Рисунок 4.90. Скорость передачи данных в направлении узла comp2, при использовании алгоритма шифрования TKIP

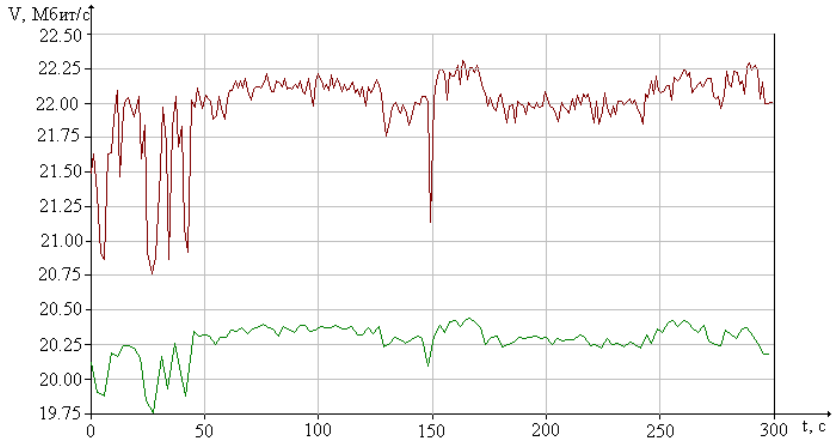


Рисунок 4.91. Скорость передачи данных в обоих направлениях, при использовании алгоритма шифрования TKIP

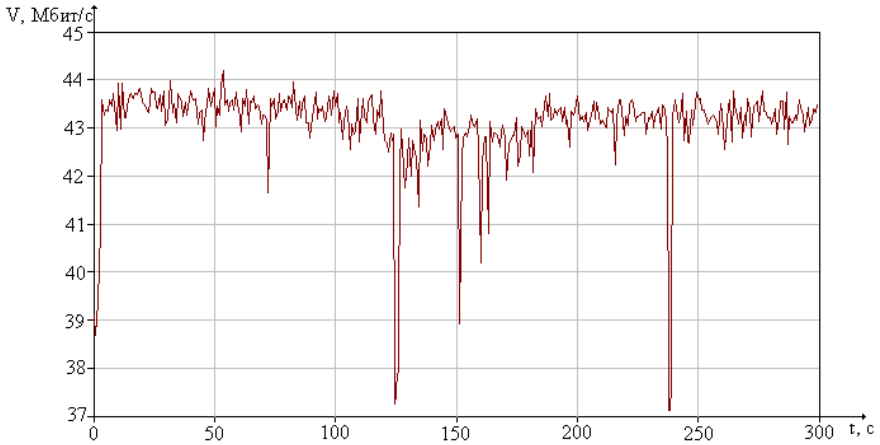


Рисунок 4.92. Скорость передачи данных в направлении узла comp2, при использовании алгоритма шифрования AES

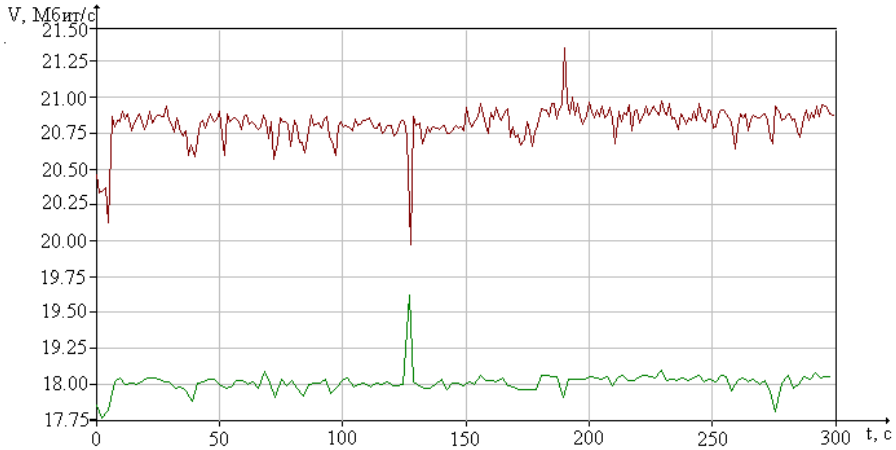


Рисунок 4.93. Скорость передачи данных в обоих направлениях, при использовании алгоритма шифрования AES

Результаты измерения среднего времени отклика приведены в таблице 4.22

Таблица 4.22 - Результаты измерения времени отклика

№ теста	Время отклика, мсек
WEP один поток	15
WEP два потока	12
TKIP один поток	14
TKIP два потока	12
AES один поток	17
AES два потока	23

Фрагментация фреймов

В пункте 4.3 описывается механизм фрагментации 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 Comp1 и Comp2, при этом в настройках точки изменяется значение поля данных (Fragmentation Length) в диапазоне 256 – 2346 бит. Измерение скорости производится в течении 5-ти 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 Settings, в поле Fragmentation Length ввести соответствующее значение рисунок 4.94.

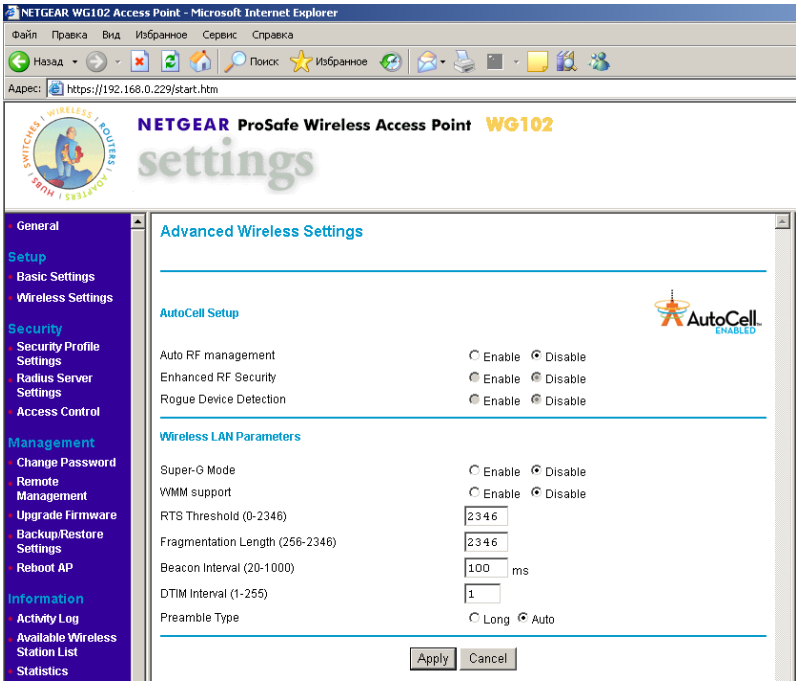


Рисунок 4.94. Настройка длины поля данных передаваемого фрейма

Результаты тестирования

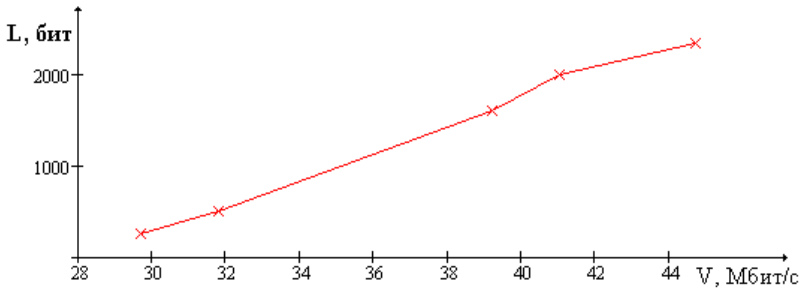


Рисунок 4.94. Зависимость скорости передачи от длины поля данных

Оценка взаимного влияния точек работающих на одном канале

Данный тест направлен на получение количественных характеристик позволяющих оценить взаимное влияние точек работающих на одном канале, и находящихся в зоне покрытия друг друга. В ходе эксперимента будут измеряться скорость передачи данных, среднее время отклика и количество потерянных пакетов при изменении расстояния L, между тестируемыми точками доступа.

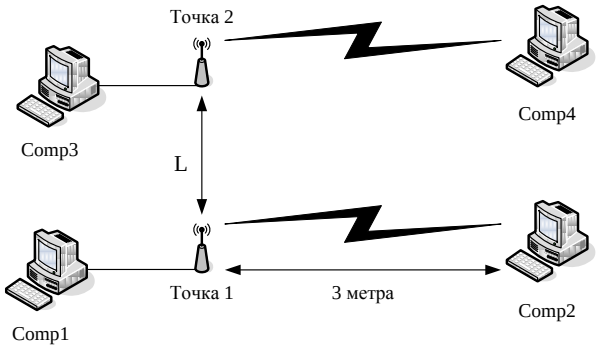


Рисунок 4.95. Тестовый стенд для оценки взаимного влияния точек работающих на одном канале

Методика тестирования:

Тестовый стенд изображен на рисунке 4.95. Точки доступа переводятся на один частотный канал, в моем случае первый. 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. Первые измерения проводятся при выключенной точки доступа №2. Исходя из теоретических соображений именно в этих условиях должны быть получены самые лучшие результаты. Результаты измерений заносятся в таблицу 4.23.

Настройка оборудования:

На обоих точках выключается шифрование трафика. Точки переводятся на работу в первый частотный канал. Точкам назначаются разные SIDD, точка один имеет SIDD «work»,

точка 2 «qqq». 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 4.23 - Результаты измерения

Расстояние между точками L, м	Скорость передачи Мбит/с	Среднее время отклика, мс	Количество потер 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. В точки NETGEAR WG102 встроена утилита AutoCell которая способна автоматически выбирать не занятые каналы подстраивать мощность передатчика, она отключена, но при конфликтах самостоятельно активируется.

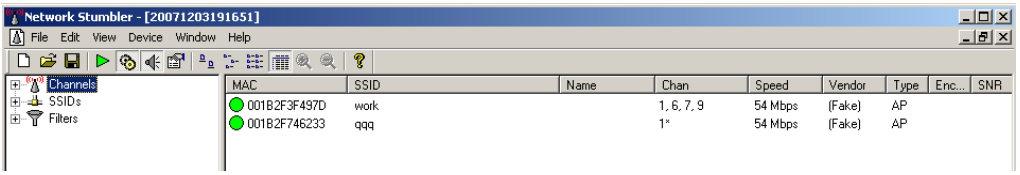


Рисунок 4.96. Сканирование эфира при проведении эксперимента

Итоги тестирования:

Тестируемое оборудование показало достаточно хорошие результаты. Среднее значение скорости передачи без шифрования в одном направлении составило 46 Мбит/с. Применение шифрования даже самого стойкого не намного снижает производительность точек доступа, применение WEP и TKIP практически не оказывают влияние на производительность (скорость передачи равна 45,5 Мбит/с), при использовании AES скорость передачи снижается

до 43.3 Мбит/с. Измеренные значение среднего времени отклика говорят о том, что устройства не испытывают перегрузок при передачи большого объема трафика, с применением шифрования. Построенная зависимость скорости передачи от длины поля данных в передаваемых пакетах может быть использована для выбора оптимального размера поля данных в среде с потерями, в нашем случае процент потерь пакетов не велик по этому будет установлен максимальный размер. На протяжении всех этапов тестирования точки доступа сохраняли стабильные показатели.

Приложение А

Программа комплексных испытаний

Объект испытаний: объектом комплексных испытаний является беспроводная сеть передачи данных стандарта 802.11g.

Во время проведения комплексных испытаний исследованию подлежат следующие вопросы:

1. Физические параметры и характеристики работы сети.

1.1 Получение физических характеристик и параметров связи мобильных клиентских устройств с беспроводной точкой доступа.

1.2 Определение зоны покрытия радиоизлучением беспроводной сети.

2. Передача информации в беспроводной сети.

2.1 Измерение скоростных характеристик беспроводной сети.

2.2 Оценка стабильности работы сети.

3. Защита информации.

3.2 Проверка работы режимов безопасности на уровне беспроводной сети.

Аппаратный и программный состав тестируемой системы:

1. Устройство беспроводного доступа в ЛВС предприятия: беспроводная точка доступа NETGEAR WG102.

Базовая рабочая конфигурация токи доступа представлена в следующей таблице:

Таблица А.1 – Базовая рабочая конфигурация точки доступа.

Параметр		Конфигурация												
1. Скорость передачи информации		1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, 54Мбит/с (по требованию)												
2. Мощность передатчика:		16 дБ												
3. Лимит мощности для клиента		16 дБ												
4. Используемые каналы передачи	№ канала	1	2	3	4	5	6	7	8	9	10	11	12	13
	Частота, МГц	2412	2417	2422	2427	2432	2437	2442	2447	2452	2457	2462	2467	2472
5. Преамбула (preamble)		Короткая 72 бита: 56 бит синхронизации + 16 бит SFD												
6. Период маяка (beacon period)		100 мкс												
7. Период индикатора сообщения доставки трафика (DTIM)		200 мкс												
8. Максимальное число попыток отправки пакета		64												
9. Максимальная разрешенная		2346 бит												

фрагментация пакетов	
10. Максимальное число попыток отправки RTS	64
11. Максимальный размер пакета с RTS	2346 бит
12. Сетевой идентификатор SSID	“work”
13. Длина AES-ключа	128 бит
14. Тип протокола аутентификации	WPA2 – with RADIUS

2. Мобильное клиентское устройство: на базе персонального компьютера HP nx6310 T1350 (1.83)/512/60/DVDRW SM/BT/WiFi. Рабочие конфигурации мобильного клиентского устройства приведены в следующей таблице:

Таблица А.2 - Рабочие конфигурации мобильного клиентского устройства

Параметр	Конфигурация
1. Скорость передачи информации	1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, 54Мбит/с (автоматическая поддержка)
2. Сетевой идентификатор SSID	“work”
3. Длина AES-ключа	128 бит
4. Тип протокола аутентификации	WPA2

3 Персональный компьютер DualCore Intel Pentium E2140/RAM1Гб/HDD 80Гб/Acorp WPCI-G ver2.0

Таблица А.3 - Рабочие конфигурации мобильного клиентского устройства

Параметр	Конфигурация
1. Скорость передачи информации	1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, 54Мбит/с (автоматическая поддержка)
2. Сетевой идентификатор SSID	“work”
3. Длина AES-ключа	128 бит
4. Тип протокола аутентификации	WPA2

4. Программные средства для исследования:

4.1 Netstumbler 4.0 – сетевой сканер, с помощью которой можно собрать данные о беспроводной сети, позволяет определить радиус действия сети - в реальном времени на диаграмме можно увидеть величину полезного сигнала. Эта же функция программы поможет точно направить антенну для связи на дальние расстояния. Для каждой найденной точки доступа можно узнать MAC-адрес, соотношение сигнал/шум, название сервиса и степень его защищенности.

4.2 NetIQ Chariot – программный пакет позволяющий определить реальную скорость передачи между узами сети. Имеет богатые функциональные возможности (выбирается тип генерируемого трафика, размер пакетов, протокол передачи, направления и число потоков).

4.3 Команда ping – основная команда TCP/IP используется для тестирования соединения, проверки возможности доступа и разрешения имен.

Алгоритм комплексных испытаний системы:

1. Производится запуск беспроводной сети, на базы беспроводных точек доступа NETGEAR WG102.

2. Запуск радиосистемы 802.11g мобильного клиентского устройства на базе

персонального компьютера HP nx6310.

3. Запуск программы NetStumbler 4.0 и перемещение мобильного клиентского устройства по территории предприятия, проверяется работоспособность установленных точек. Сверяются зоны покрытия и частотные каналы каждой из точек. Уровень сигнала в зонах обслуживаемых точками не должен быть менее -84 дБм.

4. Оценивается стабильность работы сети, на границах зон покрытия, на основе наблюдения процентного соотношения верно и ошибочно принятых пакетов с данными. Для этого выполняется отправка и прием данных количеством пакетов $n_{пакетов} = 1000$. В завершение делается оценка количественного соотношения успешно и не успешно отправленных и принятых пакетов.

5. Оценка скоростных характеристик сети. В зоне покрытия одной из точек размещается ПК с беспроводным адаптером и ноутбук, на обоих ЭВМ запускается программный пакет NetIQ Chariot, и осуществляется передача трафика между узлами в течении 10 минут, измеряется среднее значение скорости, затем ноутбук перемещается в зону покрытия следующей точки доступа и эксперимент повторяется, и.т.д.

Оценка скоростных характеристик беспроводного канала. К точкам доступа подключаются ПК и ноутбук, обоим ЭВМ выдаются адреса из одной подсети, запускается программный пакет NetIQ Chariot, и осуществляется передача трафика между узлами в течении 10 минут, измеряется среднее значение скорости.

6. Проверка защищенности беспроводной сети. В проектируемой сети для шифрования передаваемого трафика используется алгоритм AES, на сегодняшний день данный алгоритм является не уязвимым. Оценка защищенности сводится к проверке конфигураций точек, с помощью программы NetStumbler 4.0, определяется метод зашиты.

7. Измерение времени требующегося для авторизации пользователя. Измеряется время которое требуется для авторизации и получения сетевого адреса, измерения проводятся для каждой из 9 точек, высчитывается среднее значение.

Приложение Б

Протокол комплексных испытаний системы

1. Объект испытаний: беспроводная сеть передачи данных.

2. Цель испытаний: выявление следующих параметров и характеристик спроектированной системы, сравнение их с расчетными и теоретическими значениями.

3. Физические параметры и характеристики работы сети.

3.1.1. Получение физических характеристик и параметров связи мобильных клиентских устройств с беспроводными точками доступа.

3.1.2. Определение зон покрытия радиоизлучением беспроводной сети.

4. Передача информации в беспроводной сети.

4.1.Измерение скоростных характеристик беспроводной сети.

4.2.Оценка стабильности работы сети.

5.Защита информации.

Проверка работы режимов безопасности на уровне беспроводной сети.

6. Используемы приборы и оборудование

1. Устройство беспроводного доступа в ЛВС предприятия: беспроводная точка доступа NETGEAR WG102.

2. Мобильное клиентское устройство: на базе персонального компьютера HP nx6310

3. Рабочая станция DualCore Intel Pentium E2140/RAM1Гб/HDD 80Гб/Acorp WPCI-G, под управлением операционной системы Windows XP SP2.

4. Программные средства для исследования:

4.1. Netstumbler 4.0 – сетевой сканер, с помощью которой можно собрать данные о беспроводной сети, позволяет определить радиус действия сети - в реальном времени на диаграмме можно увидеть величину полезного сигнала. Для каждой найденной точки доступа

можно узнать MAC-адрес, соотношение сигнал/шум, название сервиса и степень его защищенности.

4.2. NetIQ Chariot – программный пакет позволяющий определить реальную скорость передачи между узами сети. Имеет богатые функциональные возможности (выбирается тип генерируемого трафика, размер пакетов, протокол передачи, направления и число потоков).

4.3. Команда ping – основная команда TCP/IP используется для тестирования соединения, проверки возможности доступа и разрешения имен.

7. Результаты испытаний

7.1 Оценка стабильности работы беспроводной сети

Произведена оценка стабильности работы сети в выбранных скоростных режимах, на границах зон покрытия, на основе наблюдения процентного соотношения верно и ошибочно принятых пакетов с данными.

Таблица Б.1 – Стабильность работы беспроводной сети.

Число отправленных пакетов	№ точки в соответствии с планом приложение	Скорость передачи информации, Мбит/с	Верно переданные пакеты, %	Ошибочно переданные пакеты, %
$n_{пакетов} = 1000$	1	24	98.4	1.6
	2	24	98.7	1.3
	3	24	99.9	0,1
	4	24	99.6	0,4
	5	24	97.5	2,5
	6	24	99.7	0.3
	7	24	99.8	0.2
	8	24	98.1	1.9
	9	24	97.5	2.5

7.2 Оценка скоростных характеристик сети

В зоне покрытия точки №4 размещается ПК с беспроводным адаптером и ноутбук, на обоих ЭВМ запускался программный пакет NetIQ Chariot. Осуществлялась передача трафика (один поток) между узлами в течении 10 минут, измерялось среднее значение скорости, затем ноутбук перемещался в зону покрытия следующей точки доступа и эксперимент повторялся. Результаты измерений представлены в таблице Б.2

Таблица Б.2 - скоростных характеристик сети

№ точки в зоне которой находится ноутбук	Скорость передачи информации, Мбит/с	Уровень сигнала в месте приема, дБм
1	39	- 80
2	34	- 79
3	40	- 76
4	19	- 75
5	32	-77
6	38	-76
7	37	-75
8	35	-78
9	33	-80

Скорость передачи по беспроводному каналу составила 45 Мбит/с.

7.3 Проверка защищенности беспроводной сети

С помощью программы NetStumbler 4.0 удостоверился в том, что все точки для зашиты передаваемого трафика используют алгоритм шифрования AES.

7.4 Произведена проверка времени авторизации мобильного клиентского устройства в беспроводной сети. Время потребовавшееся на авторизацию и получение сетевого адреса составило 9 секунд.

8. Выводы

В результате проведения испытаний системы, выполненных в соответствии с программой комплексных испытаний, сделаны следующие заключения:

8.1 Беспроводная сеть характеризуется довольно высокой скоростью передачи информации не менее 24 Мбит/с (в расчете на одного пользователя).

8.2 Сеть работает достаточно стабильно, процент потерянных пакетов крайне мал (число потерянных пакетов не превышает 2.5%, от общего числа переданных).

8.3 Для защиты передаваемого трафика используется алгоритм шифрования AES-128 (алгоритм не подвержен всем известным видам атак).

8.4 Дальность радиосвязи для выбранного значения скорости не превышает 27 метров. Основными причинами снижения дальности являются:

а) прием и передача данных беспроводной сети в условиях повышенной интерференции радиосигналов, возникающей из-за переотражения полезного сигнала от сложных конструкций внутри здания;

б) затухание радиосигнала из-за поглощения его железобетонными конструкциями, межкомнатными перегородками, стеллажами.

5. Рекомендуемая литература

1.Педжман Рошан, Джонатан Лиэри Основы построения беспроводных локальных сетей стандарта 802.11. пер. с англ. – М.: Издательский дом “Вильямс”, 2004.-304с.
2. Прокис Дж. К.: Цифровая связь. Пер. с англ. / М. Радио и связь, 2000. – 800 с.
3. Олифер В.Г., Олифер Н.А.: Компьютерные сети. Принципы, технологии, протоколы: СПб. Питер, 2000. – 672 с.
4. http://www.ixbt.com/comm/prac-wpa-eap_2.shtml - ст. Защита беспроводных сетей, WPA2: теория и практика (часть первая).
5. http://www.thg.ru/network/20030828/print.html -ст. Технологии беспроводных сетей семейства 802.11, 2005 г.
6. http://www.tayle.com/documents/18_11_03.php - ст. Упрощенная методика расчета СВЧ радиолиний 2.4GHz / 2003.11.18
7. http://www.tayle.com/documents/14_10_03.php - ст. Информационная безопасность беспроводных сетей.
8. http://www.netgaer.com/products - описание оборудования NETGEAR