А.М. Голиков

Транспортные и мультисервисные системы и сети связи

Сборник компьютерных лабораторных и практических работ

Томск

Голиков А.М. Транспортные и мультисервисные системы и сети связи: Сборник компьютерных лабораторных и практических работ (доработанный). – Томск: Томск. гос. ун-т систем управления и радиоэлектроники, 2015. – 289 с.

Сборник содержит описания компьютерных лабораторно практических работ по курсу «Транспортные и мультисервисные системы и сети связи» специальности 210601-2.65 – Радиоэлектронные системы и комплексы передачи информации. Представлены описания аппаратно-программных комплексов и методики выполнения лабораторно-практических работ. В разработке аппаратно-программных комплексов принимали участие студенты ТУСУР.

ОГЛАВЛЕНИЕ

.

Лабораторная работа 1. Исследование и развертывание виртуальной сети передачи информации на базе технологии VIPNet Custom

1. Цель работ

Исследование защищенной сети передачи данных на базе технологии ViPNet Custom. В результате выполнения дипломного проекта была спроектирована защищенная сеть передачи данных, включающая программное обеспечение ViPNet «Администратор», ViPNet «Координатор», ViPNet «Клиент». В сети применяется шифрования трафика электронно-цифровая подпись, и персональные сетевые экраны.

2. Краткие теоретические сведения

Введение.

Тенденции рынка средств защиты информации сегодня и завтра определяются все большей интеграцией информационных технологий в единое сетевое пространство. Глобальные сети, включая, конечно Интернет, интегрируются с корпоративными сетями. Все большее число корпоративных сетей строится на базе услуг, предоставляемых местными телекоммуникационными провайдерами. Все проще становится получить высокосортной доступ в Интернет, а через него к своим корпоративным ресурсам любым индивидуальным пользователям из любой точки мира. Качество предоставляемых общедоступных услуг возрастает быстрыми темпами. Ясно уже, что современный бизнес не может обойтись без информационных коммуникаций, а процесс интеграции сетевых технологий все более остро предъявляет требования к их безопасности, что позволило бы бизнесу, отраслям экономики, промышленным предприятиям и многим другим с высокой степенью уверенности использовать современные информационные коммуникации для повышения эффективности своей деятельности.

Но, к сожалению, постоянно усложняющиеся операционные и прикладные системы современных компьютеров, повышают возможность проведения различного рода сетевых атак, как из внутренних, так и внешних сетей, что может, наоборот, при активном использовании информационных коммуникаций привести к существенному снижению эффективности деятельности бизнеса и различных секторов экономики.

К серьезным проблемам безопасности может привести и наблюдающаяся сегодня тенденция к безоглядной ориентации на технологии, основанные на открытом распределении ключей, надежность которых очень сильно зависит от достижений современной математики. Эта же проблема относится и к механизмам электронной цифровой подписи, использование которой в критически важных системах без дополнительных мер защиты вызывает серьезные опасения.

Корпоративная сеть подвергается не только внешним атакам. Не менее вероятно присутствие злоумышленника внутри сети предприятия. При атаке со стороны знающего сотрудника последствия могут быть намного серьезнее, так как это лицо хорошо знакомо с инфраструктурой сети. Кроме того, такие злоумышленники часто имеют конкретную цель и причину для атаки, в то время как атаки извне нередко носят случайный характер, и потенциальный ущерб от атаки изнутри, как правило, больше. Особенно важно обеспечить безопасность мобильных пользователей, компьютеры которых могут подключаться в самых непредсказуемых местах, а также в случае утраты, к незащищенной информации на таких компьютерах могут получить доступ злоумышленники. Использование беспроводных соединений с уже имеющимися стандартными настройками безопасности, также нуждается в дополнительных защитных мерах.

Поэтому в условиях интеграции сетевых технологий, все возрастающей роли технологий беспроводных соединений, постоянно повышающейся мобильности пользователей все большее значение приобретают средства сетевой защиты информации, обеспечивающие персональную защиту компьютеров, которые независимо от используемых коммуникаций позволяли бы гарантировать целостность данных, безопасность компьютеров и конфиденциальность информации.

Технологии VPN, интегрированные с сетевыми экранами и допускающие установку соответствующих модулей на компьютеры, находящиеся в любой точке сети, становятся наиболее надежным и чуть ли не единственным способом обеспечения сетевой безопасности в подобных условиях.

К таким средствам, безусловно, относятся программные средства VPN, интегрированные с персональными сетевыми экранами, которые, будучи установленными на компьютеры, позволяют обеспечить высокий уровень безопасности на самых небезопасных коммуникациях и позволяют пользователю спокойно воспользоваться всем спектром сервисов и услуг: защищенной почтой, защищенным файловым обменом, защищенным обменом мгновенных сообщений и др.

Это объясняется тем, что такое программное обеспечение, в отличие от других средств, выполняющих защиту на других более высоких уровнях (SSL и др.), способно контролировать весь трафик данного компьютера, с высокой надежностью предотвратить возможные сетевые атаки, сохранить целостность и конфиденциальность данных. А в наиболее ответственных случаях может осуществлять исключительно криптографическую, (то есть гарантированно аутентифицированную) фильтрацию трафика с блокировкой любого открытого трафика. Это полностью исключает любые возможности по доступу к информации и компьютеру со стороны других компьютеров, не имеющих необходимых ключей шифрования, и гарантирует возможность доступа компьютеров, имеющих соответствующие ключи, только в рамках разрешенных условий.

При использовании таких технологий на существующую информационную инфраструктуру легко накладывается распределенная система персональных и межсетевых экранов, взаимодействующих между собой по технологии VPN и осуществляющих фильтрацию и шифрование трафика, что позволяет обеспечить конфиденциальность и достоверность информации при наличии сетевых атак, как из глобальных, так и из локальных сетей. При этом обеспечивается возможность построения защищенных подсистем произвольных топологий и размерности, возможность создания внутри распределенной сети взаимно – недоступных виртуальных защищенных контуров для обеспечения функционирования в единой телекоммуникационной среде различных по конфиденциальности или назначению информационных задач. В виртуальный контур могут включаться, как отдельные компьютеры, так и группы компьютеров, находящиеся в локальных или глобальных сетях.

Технология виртуальных защищенных сетей ViPNet, одновременно ориентированная на персональную сетевую защиту компьютеров и локальных сетей, в целом, предназначена для решения именно таких задач.

Одновременно с основной задачей технологии ViPNet – обеспечить комфортное безопасное сетевое взаимодействие для любых сетевых служб и приложений на небезопасных коммуникациях, данная система предоставляет целый спектр собственных услуг прикладного уровня. Такие приложения, как Деловая почта, конференции, службы отправки файлов и др. широко используют базисную часть системы – ее ключевую инфраструктуру с различными криптографическими функциями.

Технология ViPNet основана на использовании программных модулей, применяется на любых существующих IP-сетях, коммутируемых и выделенных каналах, сетях MPLS, GPRS, технологиях xDSL, Wireless и др., не требует установки специального оборудования,

совместима с большинством прикладным программным обеспечением. Технология поддерживается в операционных системах Windows, ОС Linux, Sun Solaris.

В работе будет разворачиваться виртуальная сеть на базе технологии VIPNet Custom. Предназначенная, для объединения в единую защищенную виртуальную сеть произвольного числа рабочих станций. Нацеленная на создание защищенной, доверенной среды передачи конфиденциальной информации с использованием публичных и выделенных каналов связи (Интернет, телефонные и телеграфные линии связи и т.п.), путем организации виртуальной частной сети. Будет развернута инфраструктура открытых ключей (PKI) и организован Удостоверяющий Центр с целью интеграции механизмов электронно-цифровой подписи в прикладное программное обеспечение абонента (системы документооборота и делопроизводства, электронную почту).

Общие положения об информационной безопасности для телекоммуникационных систем.

Существует множество классификаций угроз информационной безопасности (по способу воздействия, по результату атаки, по типу атакующего, по происхождению атаки).

Рассмотрим следующие виды угроз информационной безопасности:
незаконное копирование данных и программ;
незаконное уничтожение информации;
нарушение адресности и оперативности информационного обмена;
нарушение технологии обработки данных и информационного обмена;
внедрение программных вирусов;
внедрение программных закладок, позволяющих осуществить несанкционированный доступ или действия по отношению к информации и системам ее защиты, приводящие к компрометации системы защиты.

Результатом подобных действий злоумышленника может стать нарушение целостности и конфиденциальности информации, отказ в доступе к сервисам и информации и нарушение аутентичности передаваемых сведений.

Под целостностью будем понимать способность системы обеспечить точность, достоверность и полноту передаваемой информации. В процессе хранения или передачи данных злоумышленник, получив к ним доступ, может модифицировать их. Тем самым он скомпрометирует их точность и достоверность.

Если говорить о конфиденциальности, то будем рассматривать два вида конфиденциальной информации: государственная тайна и коммерческая тайна. Утечка или утрата этих данных может повлечь за собой материальный ущерб, послужить причиной снижения рейтинга организации, сказаться на лояльности клиентов, вызвать скандал, долгие судебные разбирательства и т.п.

Конфиденциальность защищаемой информации обеспечивают на всех этапах ее циркуляции в системе: при хранении, передаче, использовании.

Установка аутентичности может осуществляться следующим образом**.** Получив какие-либо сведения, получатель может усомниться в их достоверности, то есть поставить под вопрос личность отправителя и факт отправки, время отправки и получения сообщения.

Если говорить о доступности, то существует целый класс атак, целью которых является сделать недоступными какие-либо сервисы или информацию (например, DoS-атаки (Denial of Service)). Результатом DoS-атаки может стать «повисание», перезагрузка компьютера или отказ какого-либо его программного или аппаратного компонента.

Таким образом, целями информационной безопасности являются:
Обеспечение целостности и конфиденциальность информации,
Проверка аутентичности информации, и ее отправителя,
Обеспечение доступности информации.

При создании системы информационной безопасности необходимо учитывать, что защититься от всех атак невозможно, поскольку реализация подобной системы может стоить очень дорого. Поэтому требуется четкое представление о том, какие атаки могут произойти и с какой вероятностью. На основании этих сведений составляется список актуальных угроз, исходя из которого возможно создание комплекса мер противодействия. В него могут быть включены списки методов, средств и способов противодействия угрозам. Все вместе это и составляет политику информационной безопасности. Политика безопасности – это основополагающий документ, регламентирующий работу системы информационной безопасности. Политика безопасности может включать в себя сведения об актуальных угрозах и требования к инструментарию обеспечения защиты информации. Кроме того, в ней могут быть рассмотрены административные процедуры. Примером политики информационной безопасности может быть Доктрина Информационной Безопасности РФ.

Рассмотрим некоторые наиболее популярные методы защиты информации.

Физическая безопасность. Упущения в обеспечении физической безопасности делает бессмысленным защиту более высокого уровня. Так, например, злоумышленник, получив физический доступ к какому-либо компоненту системы информационной безопасности, скорее всего сможет провести удачную атаку.

Шифрование – математическая процедура преобразования открытого текста в закрытый. Может применяться для обеспечения конфиденциальности передаваемой и хранимой информации. Существует множество алгоритмов шифрования (DES, IDEA, ГОСТ и др.).

Электронная цифровая подпись (ЭЦП), цифровые сигнатуры. Применяются для аутентификации получателей и отправителей сообщений. Строятся на основе схем с открытыми ключами.

Резервирование, дублирование. Резервирование оборудования позволяет динамично переходить с вышедшего из строя компонента на дубликат с сохранением функциональной нагрузки. Например, в случае DoS-атаки может стать выход из строя какого-либо программного или аппаратного компонента информационной системы и тогда резервирование позволит «перебросить» часть задач с недоступного или перегруженного элемента на резервные элементы.

Кроме перечисленных методов защиты информации существуют методики, такие как: проверка соответствия стандартам; проверка корректности применения протоколов; ограничение передачи опасных данных; контроль операций на уровне приложений.

Перейдем теперь к вопросу использования отдельных средств защиты информации, позволяющие использовать перечисленные методы защиты.

Аббревиатуру VPN можно расшифровать не только как Virtual Private Network (Виртуальная Частная Сеть), но и как Virtual Protected Network, т.е. Виртуальная Защищенная Сеть.

Термин “private” имеет два основных значения: частный (собственный) и конфиденциальный (закрытый). Если говорить о первом значении, то частная сеть – это сеть, в которой всё оборудование, включая территориальные кабельные системы, коммутирующие устройства, средства управления, являются собственностью предприятия. Такая сеть отвечает требованиям и второго определения, так как в собственной сети легче соблюдать конфиденциальность, поскольку все ресурсы сети используются только сотрудниками предприятия – владельца сети.

VPN – это частная сеть, передачи данных, использующая открытую телекоммуникационную инфраструктуру и сохраняющая при этом конфиденциальность передаваемых данных, посредством применения протоколов туннелирования и средств защиты информации.

Цель VPN-технологий состоит в максимальной степени обособления потоков данных одного предприятия от потоков данных всех других пользователей сети общего пользования.

Обособленность должна быть обеспечена в отношении параметров пропускной способности потоков и в конфиденциальности передаваемых данных.

Таким образом, задачами технологий VPN являются обеспечение в сетях общего пользования гарантированного качества обслуживания для потоков данных, а также защита их от возможного НСД.

Так как основной задачей VPN является защита трафика, поэтому виртуальная сеть должна удовлетворять большому числу требований и, в первую очередь, обладать надежной криптографией, гарантирующей защиту от прослушивания, изменения, отказа от авторства. Кроме того, VPN должна иметь надежную систему управления ключами и криптографический интерфейс, позволяющий осуществлять криптографические операции: защищенная почта, программы шифрования дисков и файлов и др.

В настоящее время интерес к использованию средств, для построения VPN постоянно растёт, что обусловлено целым рядом причин:

Низкой стоимостью эксплуатации за счет использования сетей общего пользования вместо собственных или арендуемых линий связи;

Масштабируемостью решений;

Простотой изменения конфигурации;

“Прозрачностью” для пользователей и приложений.

При использовании VPN-технологий можно обеспечить:

защиту (конфиденциальность, подлинность и целостность) передаваемой по сетям информации;

защиту внутренних сегментов сети от НСД со стороны сетей общего пользования;

контроль доступа в защищаемый периметр сети;

сокрытие внутренней структуры защищаемых сегментов сети;

идентификацию и аутентификацию пользователей сетевых объектов;

централизованное управление политикой корпоративной сетевой безопасности и настройками VPN-сети.

Перейдём к рассмотрению видов виртуальных частных сетей.

По наиболее распространенной классификации существуют следующие виды VPN. Интранет VPN (Intranet VPN) – внутрикорпоративная виртуальная сеть, объединяет в единую защищенную сеть несколько распределенных филиалов одной организации, взаимодействующих по открытым каналам связи.

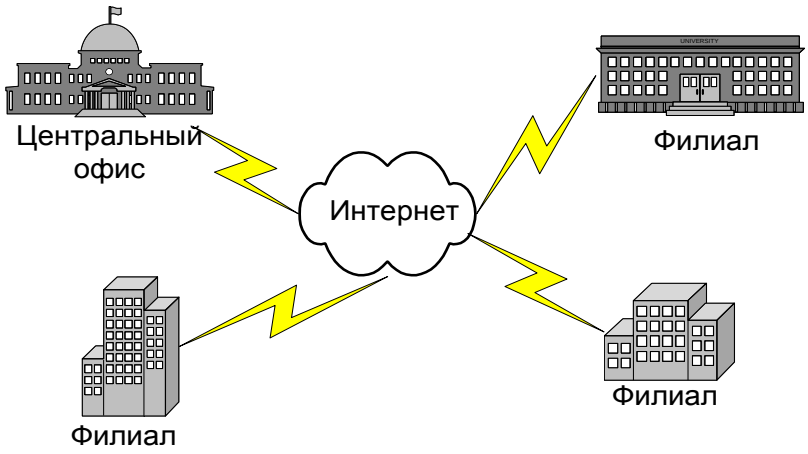


Рис. 1. Интранет VPN

VPN удаленного доступа (Remote Access VPN) – виртуальная сеть с удаленным доступом, реализует защищенное взаимодействие между сегментом корпоративной сети и удаленным пользователем, который подключается к корпоративным ресурсам, используя беспроводные устройства связи и мобильный компьютер (мобильный пользователь), либо модем и компьютер (домашний пользователь).

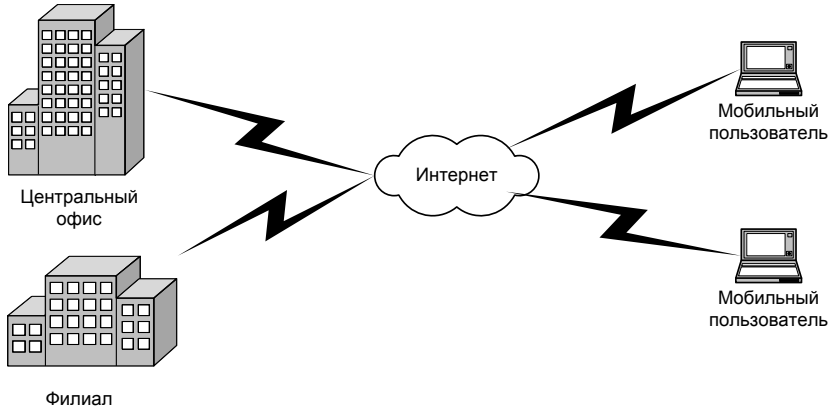


Рис. 2. VPN удаленного доступа

Клиент-сервер VPN (Client-Server VPN) – обеспечивает защиту передаваемых данных между двумя узлами (не сетями) корпоративной сети.

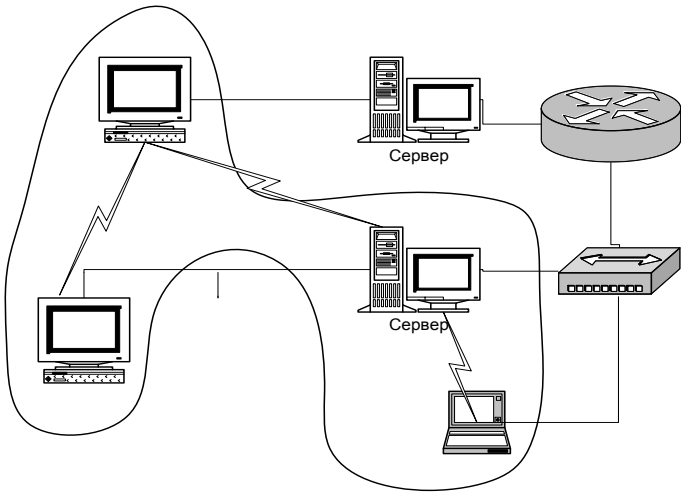


Рис. 3. Взаимодействие клиент-сервер VPN

Экстранет VPN (Extranet VPN) – межкорпоративная виртуальная сеть, реализует защищенное соединение компании с ее деловыми партнерами и клиентами, уровень доверия к которым намного ниже, чем к своим сотрудникам.

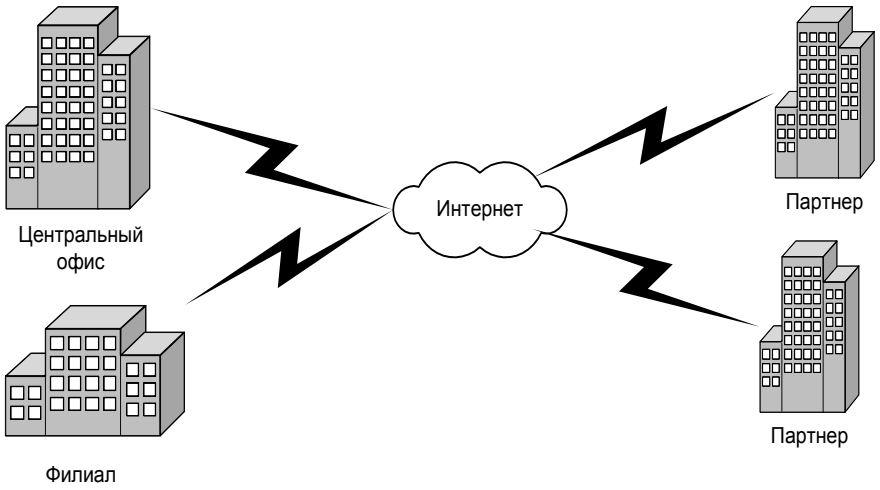


Рис. 4. Экстранет VPN

Все продукты для создания VPN можно условно разделить на следующие категории: программные, аппаратные и интегрированные.

Программное решение для VPN – это, как правило, готовое приложение, которое устанавливается на подключенные к сети компьютеры. С одной стороны, программное решение относительно недорого, но с другой стороны, создание подобной системы предусматривает целый ряд настроек рабочих станций и серверов, что может быть затруднительным даже для опытных специалистов. Особое место в этом случае будет иметь вопрос совместимости программного обеспечения для VPN и операционной системы, а также сетевых настроек каждого отдельного компьютера.

В отличие от них аппаратные VPN-решения включают в себя все, что необходимо для соединения – аппаратное устройство и компьютер, частную (как правило) операционную систему и специальное программное обеспечение. Развертывать аппаратные решения значительно легче, но зато стоимость их достаточно высокая и позволить их себе приобрести может не каждая организация.

Существуют также интегрированные решения, в которых функции построения VPN реализуются наряду с функцией фильтрации сетевого трафика, обеспечения качества обслуживания и др.

Как правило, построение VPN для распределенных компаний даже с небольшим количеством удаленных филиалов является достаточно трудоемкой задачей, сложность которой объясняется следующими причинами:

Неоднородность используемых аппаратно-программных платформ,

разнообразием задач (защищенный обмен между головным офисом и филиалами, офисом и мобильными или удаленными сотрудниками, сегментами внутренней сети),

необходимостью построения централизованной системы управления всей корпоративной VPN,

наличием низкоскоростных каналов связи.

Сложность определяется еще и тем, что у заказчиков определенные критерии отбора средств, для построения VPN, такие как: масштабируемость, интегрируемость, легальность используемых алгоритмов и решений, пропускная способность защищаемой сети, стойкость применяемых криптоалгоритмов, унифицируемость VPN-решений, стоимость.

Перейдем к рассмотрению возможных вариантов построения виртуальных частных сетей.

Варианты построения и средства защиты информации, дополняющие VPN

Построение VPN может быть реализовано сетевыми средствами различных категорий:

серверами удаленного доступа и маршрутизаторами, позволяющими создавать защищенные туннели на канальном уровне сетевой модели (модели OSI);
межсетевыми экранами, включающими в свой состав серверы удаленного доступа и позволяющими создавать VPN как на канальном и сетевом, так и на сеансовом уровнях;
автономным программным обеспечением, позволяющим создавать защищенные виртуальные сети в основном на сетевом и сеансовом уровнях;
отдельными, специализированными аппаратными средствами на основе специализированной ОС реального времени, имеющими два или более сетевых интерфейса и аппаратную криптографическую поддержку и ориентированными на формирование защищенных туннелей на канальном и сетевом уровнях;
комбинированными пограничными устройствами, которые включают в себя функции маршрутизатора, межсетевого экрана, средства управления пропускной способностью и функции VPN.

Гарантируя защиту передаваемой информации, VPN не обеспечивает её защиту во время хранения на конечных компьютерах. Эта задача решается целым рядом специальных средств: систем криптозащиты файлов и дисков; систем защиты от НСД к компьютерам; антивирусных систем; межсетевых экранов (МЭ).

Например, вопрос совместного использования МЭ и VPN возникает в случае защиты компьютерных сетей во всех вариантах, кроме VPN на базе МЭ. МЭ - это “ограда” вокруг сети, которая препятствует проникновению сквозь неё злоумышленников, а VPN - “бронированный автомобиль”, который защищает ценности при вывозе их за пределы такой ограды.

Существуют несколько крайностей – устанавливать МЭ перед VPN-устройством и после него. В первом случае возникает ситуация, когда на МЭ из Интернета попадает нерасшифрованный трафик, что приводит к невозможности контроля передаваемого содержимого. В другом случае само устройство VPN становится уязвимым к внешним атакам. Идеальным решением, к которому пришло большинство зарубежных производителей, а также отечественные разработчики, является совмещение в одном устройстве функций МЭ и VPN. Именно такое использование обоих решений обеспечивает необходимый уровень защищенности информационных ресурсов.

Технология системы защиты информации VIPNet.

Для решения задачи – обеспечение защищенного взаимодействия непосредственно между компьютерами в большой распределенной сети в системе должны присутствовать как минимум 3 обязательных элемента.
ViPNet «Администратор»
ViPNet «Координатор»
ViPNet «Клиент»

ViPNet «Администратор» и его основные модули.

Административная часть, в ПО ViPNet в целях повышения безопасности разделена на две части, отвечающие за разные аспекты её функционирования. При этом ни та, ни другая части администрации по отдельности не могут оказать существенного влияния на функционирование сети, т.е. возможности несанкционированного доступа к информации абонентов тем или иным администратором сведены к минимуму.
ViPNet «Администратор» включает в себя программы:
Центр Управления Сетью
Ключевой и Удостоверяющий Центр

Центр Управления Сетью (ЦУС) является регистрационным центром и предназначен для конфигурации и управления виртуальной сетью.
ЦУС выполняет следующие функции:
Централизованное управление сетью;
Формирование структуры VPN;
Формирование справочной информации;
Управление “логикой” работы VPN;
Централизованное обновление ПО и функционала компонентов VPN;
Мониторинг событий VPN;
Мдаленное управление ресурсами VPN.

Второй модуль ViPNet «Администратора» Удостоверяющий и ключевой центр (УКЦ) предназначен для обеспечения ключевой информацией всех участников VPN и выполнения функций удостоверяющего центра. При этом ключи для первоначальной инсталляции могут быть записаны на дискеты, смарт-карты, touch memory, eToken и прочие аппаратные устройства для передачи участникам VPN. Последующее обновление ключевой информации осуществляется автоматически по защищенным каналам VPN.

УКЦ выполняет следующие функции:
Формирование и автоматическое обновление через ЦУС симметричной ключевой информации и первичной парольной информации для объектов и пользователей сети;
Выполнение функций удостоверяющего центра сертификатов ЭЦП:
издание ключей ЭЦП Главных абонентов ViPNet сети;
формирование запросов на издание сертификатов;
импорт сертификатов Главных абонентов (Уполномоченных лиц) ViPNet сети и уполномоченных лиц Головного УЦ;
ведение справочников сертификатов администраторов УЦ;
формирование и отправка в ЦУС обновлений справочников;
создание ключей электронной цифровой подписи абонентов и издание сертификатов корпоративной сети по запросам ЦУС;
рассмотрение запросов на издание сертификатов ЭЦП от абонентов корпоративной сети;
рассмотрение запросов от Центров регистрации на издание сертификатов ЭЦП внешних абонентов;
хранение информации о запросах и ведение справочников изданных сертификатов;
рассмотрение запросов на отзыв, приостановление и возобновление действия сертификатов;
ведение и отправка в ЦУС для обновлений списков отозванных сертификатов.

УКЦ обеспечивает возможность формирования ключей ЭЦП на основе алгоритмов ГОСТ Р 34.10-94 и ГОСТ Р 34.10-2001.

Особенности взаимодействия ЦУС и УКЦ.

Для обеспечения работоспособности сети, созданной с помощью технологии ViPNet необходимо:
Создать (изменить) её структуру в ЦУС и скопировать в УКЦ данные, необходимые для генерации ключевой информации.

Сгенерировать в УКЦ ключевую информацию.

Предоставить необходимые наборы справочной и ключевой информации абонентам вновь созданных абонентских пунктов или разослать их на уже существующие абонентские пункты.

Для того чтобы один пользователь с одного АП мог обмениваться защищённой информацией с другим пользователем другого АП, каждому пользователю необходимо получить:
Инсталляционный пакет той или иной программы.
Адресную информацию для АП (справочники), предоставляемую ЦУС.

Ключевую и парольную информацию для АП, предоставляемую УКЦ.
Адресная и ключевая информация для упрощения работы с ней предоставляется в виде единого файла-дистрибутива.

В процессе изменения структуры сети ЦУС автоматически доставляет и устанавливает обновленную адресную и ключевую информацию, не требуя от пользователя каких либо дополнительных действий.

Рассмотрим подробнее порядок работы и установки взаимодействия между ЦУС и УКЦ при первоначальном разворачивании сети.
Инсталляция программного обеспечения и развертывание сети ViPNet должны осуществляться в следующей последовательности:
Инсталляция программного обеспечения ЦУСа.

Генерация сетевой структуры с помощью подсистемы адресной администрации ЦУСа.
Генерация прикладной администрации.
Формирование файлов связей для УКЦ.
Инсталляция программного обеспечения УКЦ.
Генерация ключевой информации и дистрибутивов.
Инсталляция программного обеспечения ViPNet Координатора.
Инсталляция программного обеспечения на АП.

Уровень полномочий

Полномочия пользователя ViPNet – это правомерность действий пользователя сетевого узла (АП или СМ) по изменению настроек в различных приложениях ПО ViPNet (совокупность настроек определяет функциональность ПО). Допустимость действий пользователя определяется уровнем полномочий. Уровень полномочий для каждого узла ViPNet задается программой ЦУС. Существует четыре уровня полномочий, три из которых определяются цифрой, а именно: уровень 0 –минимальные полномочия, уровень 1 - средние полномочия и уровень 2 - максимальные полномочия. Четвертый уровень называется уровнем специальных полномочий и имеет несколько значений, каждое из которых определяется специальным символом (цифра или буква).

Полномочия максимального уровня не имеют ограничений по использованию функций ПО пользователем. Полномочия, определяемые другими уровнями, ограничивают действия пользователей по функциям ПО. Все ограничения, накладываемые полномочиями среднего, минимального и специального уровней, снимаются при вводе пароля Администратора сетевых узлов.

Программа ЦУС задает полномочия пользователя, работающего на:
АП и СМ, зарегистрированных в прикладной задаче Защита трафика. Уровень полномочий, заданный для этих сетевых узлов, будет определять функциональность ПО ViPNet «Клиент» или «Координатор» «Монитор» и ViPNet «MFTP».

АП, зарегистрированных в прикладной задаче Деловая почта. Уровень полномочий, заданный для этих сетевых узлов, будет определять функциональность ПО ViPNet «Клиент» «Деловая почта».
АП, зарегистрированные в прикладной задаче Криптосервис. Уровень полномочий, заданный для этих сетевых узлов, будет определять функциональность ПО ViPNet «Криптосервис».

Прикладные задачи и порядок регистрации в них АП и СМ

Прикладная задача (ПЗ*)* – это совокупность программных средств, предназначенных для решения целевых и служебных задач сети.
В настоящее время поддерживаются следующие ПЗ: «Деловая почта», «Диспетчер», «Центр управления сетью», «Ключевой центр», «Защита трафика», «Сервер IP-адресов», «Центр регистрации», «Секретный диск» и др.

Каждой ПЗ присваивается уникальный 4-символьный шестнадцатеричный идентификатор, который включается в транспортные конверты, генерируемые в рамках этих задач. По идентификатору ПЗ прикладная программа понимает, что конверт адресован именно ей.

Регистрация АП в конкретных прикладных задачах является обязательной процедурой в процессе генерации сети. Эта процедура определяет, какие прикладные программы могут быть установлены на том или ином сетевом узле. Если СМ должен выполнять другие функции (Сервер IP-адресов и др.) или на нем должен быть установлен Драйвер сетевой защиты, его также необходимо зарегистрировать в соответствующей задаче.

Если в настройках по умолчанию задана регистрация в каких-либо задачах, то при создании нового АП или СМ такая регистрация будет произведена автоматически .
Возможность регистрации нужного числа узлов в конкретных задачах определяется лицензионным файлом, предоставляемым ОАО «Инфотекс» при поставке ЦУСа.

Таблица.1. Прикладные задачи.

№ п\ п	Название ПЗ	Идентификатор ПЗ	Тип СУ	Примечание
	Деловая почта	0000 и 0015	только АП	Для каждого из зарегистрированных СУ можно задать уровень полномочий: минимальный, средний, максимальный или специальный
	Диспетчер	0005 и 0016)	только АП	
	Центр управления сетью	0004	только АП	Только один АП в локальной сети может быть зарегистрирован в этой прикладной задаче. Для осуществления функций управления сетью и обеспечения взаимодействия ЦУСов разных сетей не забудьте зарегистрировать какой-либо АП в этой задаче.
	Ключевой центр)	0008	только АП	Только один АП в локальной сети может быть зарегистрирован в этой прикладной задаче. Для осуществления функций управления сетью и обеспечения взаимодействия ключевых центров разных сетей не забудьте зарегистрировать какой-либо АП в этой задаче.
	Защита трафика	0017	АП или СМ	При регистрации СУ в задаче защиты IP-трафика есть возможность ввести несколько IP-адресов для каждого из зарегистрированных СУ, а также настроить дополнительные специальные параметры, позволяющие автоматически настроить узлы для их работы в сети. Кроме того, можно задать для каждого из зарегистрированных СУ уровень полномочий при защите IP-трафика: минимальный, средний, максимальный или специальный.

№ п\п	Название ПЗ	Идентификатор ПЗ	Тип СУ	Примечание
	Сервер IP-адресов	0018	только СМ	Для осуществления функций защиты IP-трафика не забудьте зарегистрировать СМ в этой задаче. Серверов IP-адресов в одной сети может быть несколько. Задание IP-адресов и специальных параметров в этой задаче осуществляются так же как в задаче **Ошибка! Источник ссылки не найден.** Настройки полномочий для СМ (координатора) производятся в задаче “Защита трафика”, предварительно зарегистрировав его в этой задаче.
	Сервер Открытого Интернета	001C	только СМ	В этой задаче может быть зарегистрирован только СМ, зарегистрированный в задаче **Ошибка! Источник ссылки не найден.**.
	Секретный диск	001E	АП или СМ	На СУ, зарегистрированных в этой задаче, будет работать программа SafeDisk, интегрированная с ViPNet.
	Центр регистрации	001D	только АП	На АП, зарегистрированных в этой задаче, будет работать программа ViPNet Центр регистрации.
	КриптоСервис	0020	АП или СМ	На СУ, зарегистрированных в этой задаче, будет работать программа ViPNet КриптоСервис. Можно задать для каждого из зарегистрированных СУ уровень полномочий: минимальный, средний, максимальный или специальный. На СУ, зарегистрированных в этой задаче, будет работать программа ViPNet CryptoExtension.
	ViPNet SDK	0029	АП или СМ	На СУ, зарегистрированных в этой задаче, можно будет работать с набором криптофункций на базе криптопровайдера Домен К.
	Кластер Linux	0025	АП или СМ	На СУ, зарегистрированных в этой задаче, будет работать функционал резервирования серверов Linux.
	Solaris	0026	АП или СМ	На СУ, зарегистрированных в этой задаче, будут запускаться программы ViPNet под ОС Solaris.
	Кластер Solaris)	0028	АП или СМ	На СУ, зарегистрированных в этой задаче, будет работать функционал резервирования серверов Solaris. Также эти СУ должны быть зарегистрированы в задаче “Solaris“.
	Терминал Навигатор	002E	только АП	На АП (только для Windows), зарегистрированном в этой задаче, осуществляется защита трафика. Если АП зарегистрирован в этой задаче, то регистрация его в других задачах не требуется. Задание IP-адресов и специальных параметров в этой задаче осуществляются так же как в задаче **Ошибка! Источник ссылки не найден.**

№ п\п	Название ПЗ	Идентификатор ПЗ	Тип СУ	Примечание
	Терминал Спектр	002F	только АП	На АП (только для Linux), зарегистрированном в этой задаче, осуществляется защита трафика. Если АП зарегистрирован в этой задаче, то регистрация его в других задачах не требуется. Задание IP-адресов и специальных параметров в этой задаче осуществляются так же как в задаче **Ошибка! Источник ссылки не найден.**
	Терминал Ареал-Сервис	0030	только АП	На АП (только для Linux), зарегистрированном в этой задаче, осуществляется защита трафика. Если АП зарегистрирован в этой задаче, то регистрация его в других задачах не требуется. Задание IP-адресов и специальных параметров в этой задаче осуществляются так же как в задаче **Ошибка! Источник ссылки не найден.**

Для расширения функциональных характеристик ViPNet сети реализована возможность взаимодействия между собой абонентских пунктов с установленными на них разными прикладными программами (Деловая почта и Диспетчер). При этом следует иметь в виду следующее ограничение:
Прикладная программа «Диспетчер» может принимать почту от прикладной программы «Деловая почта» и наоборот, только, если АП с «Диспетчером» не зарегистрирован также и в задаче «Деловая почта» и наоборот. Если какие-то АП зарегистрированы в обеих задачах, то каждая из задач на этих АП может взаимодействовать только с одноименной задачей. СМ регистрируются только в прикладных задачах Защита трафика, Сервер IP-адресов, Секретный диск и КриптоСервис. АП могут быть зарегистрированы в любой задаче, кроме прикладной задачи Сервер IP-адресов.

Особенности ключевой структуры сети ViPNet

Система защиты информации ViPNet использует комбинацию криптографических алгоритмов с симметричными и асимметричными ключами.

Симметричный ключ – это случайная комбинация заданной длины двоичных символов (в СКЗИ «Домен-К» – 256 бит), которая полностью определяет алгоритм шифрования. Иначе говоря, кто знает симметричный ключ, может зашифровать на этом ключе и расшифровать все зашифрованное на этом же ключе. По–другому, симметричный ключ – любой ключ из пары идентичных ключей, такой, что если он используется для шифрования, то другой ключ может быть использован для расшифрования и наоборот.

Асимметричный ключ – это пара ключей: асимметричный секретный ключ (АСК) и асимметричный открытый ключ (АОК).

Симметричные алгоритмы используются для шифрования и проверки целостности информации. Асимметричные алгоритмы используются для обмена ключами и создания электронной цифровой подписи.

Особенность комбинирования криптографических алгоритмов с симметричными и асимметричными ключами заключается в том, что шифрование информации происходит на комбинации симметричного ключа, созданного администратором УКЦ, и ключа, созданного на основе асимметричных ключей, создаваемых пользователями.

Такая схема позволяет ограничить доступ к информации со стороны администратора безопасности, которому известны все симметричные ключи в сети, но неизвестны асимметричные ключи пользователей.

В технологии ViPNet используются следующие симметричные алгоритмы: ГОСТ 28147-89 (256 бит), DES (56 бит), 3DES (168 бит), RC6 (256 бит), AES (256 бит).

В асимметричном алгоритме ГОСТ Р 34.10-2001 для распределения ключей используются открытый и закрытый ключи длиной 256 бит и 512 бит.

Когда говорят, что какой-то объект (это может быть сеть, сетевой объект, коллектив, абонент) имеет асимметричный ключ, то это означает, что данный объект сам создал АСК (как случайную комбинацию путем использования ДСЧ) и хранит этот АСК в секрете наравне с остальными ключами. Кроме того, этот объект создает соответствующий АОК и помещает его в справочник. В системе ViPNet реализована строгая рассылка справочников открытых ключей. Во-первых, эти справочники рассылаются под защитой симметричных ключей, во-вторых, они рассылаются только тем, с кем разрешены связи. Это обеспечивает значительно более высокий уровень защиты справочников от подмены, по сравнению с системами, допускающими свободный доступ к справочникам открытых ключей.

Имеются два типа асимметричных ключей (АК) - асимметричные ключи подписи (АКП) и асимметричные ключи шифрования (АКШ).

Использование асимметричных ключей шифрования предполагает определенный протокол, в результате которого на основе открытого распределения ключей вырабатывается симметричный ключ обмена. В системе ViPNet этот протокол выполняется на прикладном уровне. Полученный в результате протокола симметричный ключ, свернутый с соответствующим ключом обмена коллективов, передается Драйверу ViPNet для использования на сетевом уровне при создании VPN и приложениям для использования на прикладном уровне, например Деловой почте. В системе ViPNet используется алгоритм Диффи-Хелмана, и в целом этот протокол выглядит следующим образом.

Пусть (АСКШ1, АОКШ1) - асимметричная пара первого объекта и (АСКШ2, АОКШ2) - асимметричная пара второго объекта. Первый объект формирует значение L12 = АОКШ2 ** АСКШ1 (mod P), второй объект формирует значение L21 = АОКШ1 ** АСКШ2 (mod P). В силу природы открытых ключей имеем L12 = L21. Величины Lij имеют размерность модуля, т.е. 1024 бита. Симметричный ключ из данных величин получается следующим образом: вектор Lij делится на четыре подвектора размера 256 бит каждый и затем эти подвекторы складываются поразрядно по модулю 2. Получившееся значение (32 байта) используется для создания производного симметричного ключа шифрования (путем криптографической свертки с симметричным ключом, созданным вУКЦ).

Таким образом, в системе ViPNet ключ обмена - это свертка двух ключей, один из которых есть элемент симметричной матрицы ключей, второй получается из открытого распределения ключей посредством описанного выше протокола.

В системе ViPNet имеются свои особенности в использовании открытых ключей ЭЦП. А именно, нет необходимости использовать систему рассылки или организации доступа к справочникам для АОКП (сертификатам ЭЦП). Каждый АОКП прикрепляется к подписанной информации, хранится и рассылается вместе с ней, что значительно упрощает контроль сроков действия подписи. В отношении генерации ключей ЭЦП предусмотрены две возможности: централизованное изготовление этих ключей в УКЦ и изготовление этих ключей самими пользователями.

Для реализации процедуры сертификации открытых ключей введено понятие «Администратор УКЦ». Главных абонентов в сети может быть один или несколько и им доверяется сертифицировать (подписывать) АОКП абонентов своей сети.

АОКШ сертифицируются опосредованно: эти ключи подписываются абонентами (пользователями) их сформировавшими, подпись которых сертифицирована УЛ. Выпуск сертификатов ЭЦП осуществляет УКЦ ViPNet.

На Рисунке показана процедура формирования симметричных ключей шифрования в УКЦ.

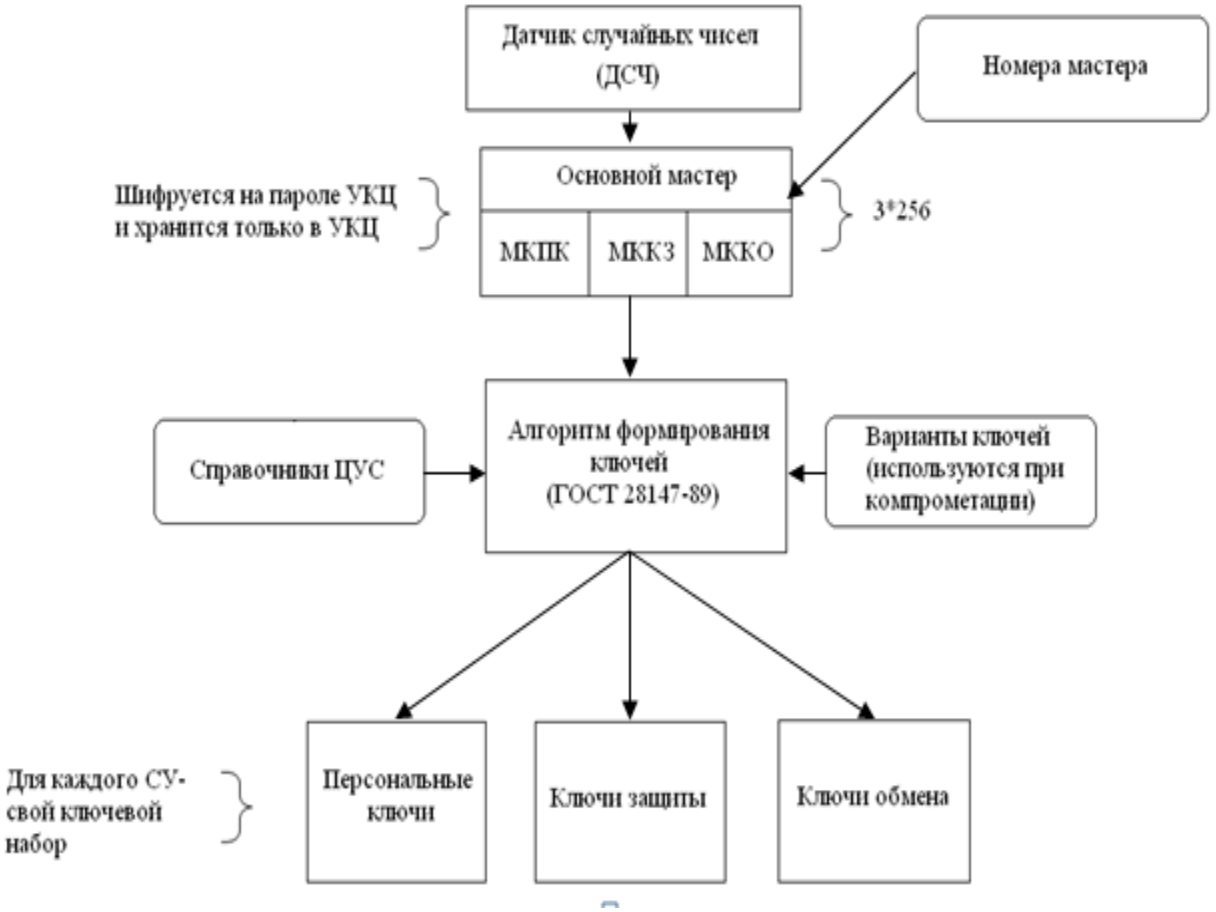


Рис. 5. Формирование симметричных ключей шифрования и идентификации

Роль сертификационного центра выполняет Удостоверяющий Ключевой Центр (УКЦ). Открытые асимметричные ключи подписи Уполномоченных лиц сети помещаются на ключевые дискеты (КД) пользователей, на которые помещается индивидуальная ключевая информация пользователя. На HBceyrt3 представлена процедура сертификации ЭЦП пользователя.

Открытые асимметричные ключи шифрования сертифицируются опосредованно: эти ключи подписываются пользователями их сформировавшими, подпись которых сертифицирована УЛ».

При первоначальном развертывании ViPNet-сети асимметричные ключи ЭЦП формируются в Удостоверяющем Ключевом Центре (УКЦ).

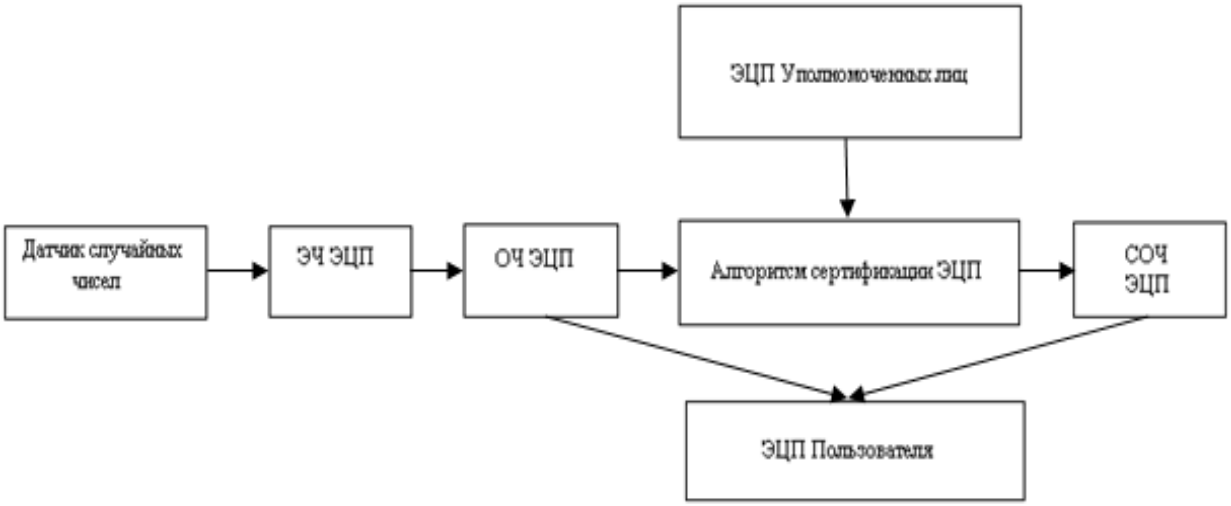


Рис. 6. Формирование ЭЦП для пользователей (ГОСТ Р. 34.10-2001)

Вся ключевая информация в сети ViPNet подразделяется на следующие основные группы:
Персональная ключевая информация пользователя (администратора УКЦ)
Парольный ключ пользователя (администратора УКЦ)
Ключи защиты пользователя (администратора УКЦ)
Ключи подписи пользователя (администратора УКЦ)
Ключи защиты
Ключи защиты УКЦ
Ключи защиты коллективов
Мастер–ключи УКЦ
Основные
Межсетевые
Ключи обмена
Симметричные
Асимметричные
Сеансовые ключи шифрования
Производные
Случайные
Ключевую информацию для отдельного пользователя сети ViPNet можно условно разбить на две группы:
Ключевая информация для каждого узла и его коллективов (ключевой набор или КН), хранящаяся на жестком диске в каталоге D-STATION или другом носителе. Здесь содержатся массивы симметричных и асимметричных ключей для обеспечения связи данного узла и его коллективов с другими узлами и коллективами, с которыми такая связь разрешена в ЦУСе.

Индивидуальная ключевая информация для каждого пользователя (ключевая дискета или КД), хранящаяся на жестком диске в каталоге KEY_DISK или другом носителе. Здесь хранится небольшой объем ключевой информации пользователя, предназначенной для получения доступа (расшифрования) к разрешенной ему информации в каталоге STATION, а также некоторые другие персональные ключи, доступные только данному пользователю, в том числе закрытый ключ подписи (ЗЧ ЭЦП).

Индивидуальная ключевая информация зашифрована на пароле, а ключи связи в каталоге STATION зашифрованы на ключах защиты, о которых речь пойдет ниже.

Криптоядро «Домен-К»

СКЗИ «Домен-К» представляет собой пакет библиотек и программ, реализующих ключевой центр, прикладной криптографический интерфейс, криптографический драйвер. СКЗИ «Домен-К» при соблюдении правил пользования обеспечивают:

Высокую стойкость шифрования информации.

Гарантированное подтверждение авторства и подлинности электронных документов.

Обнаружение случайных или намеренных искажений защищаемой информации с вероятностью, не меньшей $1 - 10^{-9}$.

Защиту используемых ключей.

Контроль целостности программного обеспечения.

Надежное автоматизированное управление ключевой системой.

Допускается использование программных средств СКЗИ «Домен-К» в операционных системах Windows 2000, Windows XP, Linux Red Hat 7.2, FreeBSD 4.4, функционирующих на платфорие Intel, и Solaris 8, функционирующей на платформе Sparc.

В СКЗИ «Домен–К» используются алгоритмы:

Шифрование гаммированием с обратной связью в соответствии с ГОСТ 28147–89 «Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования». Шифрование выполняется на ключах, которые надлежит хранить в тайне.

Вычисление имитозащитной вставки в соответствии с ГОСТ 28147–89. Предназначено для защиты передаваемой (или хранимой) информации от случайных или преднамеренных искажений. Выполняется на ключах, которые надлежит хранить в тайне.

Вычисление и проверка электронной цифровой подписи в соответствии с ГОСТ Р 34.10–2001 «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи». Вычисление ЭЦП производится с использованием секретных ключей.

Хэширование информации в соответствии с ГОСТ Р 34.11–94 «Информационная технология. Криптографическая защита информации. Функция хэширования». Представляет собой однонаправленное преобразование свертки, независящее от ключа.

Используется в алгоритмах ЭЦП, а также для подтверждения достоверности данных (в частности, паролей).

Размер секретных ключей шифрования, секретных ключей ЭЦП и секретных ключей Диффи-Хелмана (секретных ключей для открытого распределения ключей) составляет 256 битов (32 байта). Размер открытых ключей ЭЦП и открытых ключей для протокола Диффи-Хелмана составляет 1024 бита (128 байтов) при использовании 512 бит (64 байта) для ГОСТ Р 34.10–2001.

Рис. 7. Виды ключей

Ключи защиты

В СКЗИ «Домен-К» используются четыре уровня ключей защиты.

Ключи защиты первого уровня – ключи защиты мастер-ключей.

Ключи защиты второго уровня – ключи защиты классических секретных ключей обмена коллективов. Данные ключи называются ключами защиты ключей обмена. Ключ защиты ключей обмена данного коллектива является общим для всех абонентов данного коллектива.

Ключи защиты третьего уровня или персональные ключи – ключи защиты ключей защиты первого и второго уровней. Используются

также для защиты секретных асимметричных ключей шифрования, секретных ключей электронной подписи и jump-ключей и некоторых других ключей.

Ключи защиты четвертого уровня или парольные ключи – ключи, получаемые из паролей с помощью функции хэширования. Предназначаются для защиты персональных ключей.

Мастер-ключи

Мастер–ключи (МК) подразделяются на 2 группы:

Основные (внутрисетевые) «мастер–ключи» – предназначены для формирования ключей защиты и ключей обмена СУ в рамках одной сети. Первое формирование ключей производится автоматически после установки ПО УКЦ. Последующее формирование

инициируется администратором по истечении срока действия ключа. В данной группе находятся 3 типа ключей:

Мастер персональный ключей – Mp_N Предназначен для генерации персональных ключей защиты абонентов;

Мастер ключей защиты коллективов - Md_N Предназначен для генерации ключей защиты коллективов;

Мастер ключей обмена - Mc_N Предназначен для генерации ключей обмена коллективов.

2. Межсетевые мастер–ключи – предназначены для формирования симметричных ключей обмена между СУ, зарегистрированными в разных сетях. Данные ключи формируются при необходимости установления связи между СУ, зарегистрированными в разных сетях. В УКЦ могут присутствовать межсетевые мастер – ключи 3 типов:

Индивидуальный симметричный мастер–ключ – создается для установления связи с одной конкретной сетью - Mi_{MN}. Характеризуется номером сети, создавшей ключ N, номером сети для связи с которой предназначен М и своим серийным номером. Для передачи ключа администратор УКЦ осуществляет его экспорт. При экспорте ключ шифруется на парольном ключе экспорта. Пароль, в зависимости от настроек УКЦ, либо задается администратором, либо формируется как случайный, при экспорте ключа. Передача экспортированного ключа должна осуществляться по доверенному каналу связи. Импортирован данный ключ может быть только в ту сеть, для связи с которой он предназначен. При импорте ключа производится проверка имитовставки на парольном ключе экспорта. Если проверка успешна, то ключ перешифровывается на ключе защиты ключевого центра импортирующей сети.

Асимметричный мастер–ключ – пара ключей $Ma_N = (MSa_N, MPa_N)$ для выработки общего мастер–ключа между сетями по протоколу Диффи – Хелмана с параметрами ГОСТ Р 34.10–94 или ГОСТ Р 34.11–94. Алгоритм и параметры выбираются администратором при формировании ключа. Характеризуется номером сети, создавшей ключ N и своим серийным номером. Секретная составляющая ключа MSa_N защищается на ключе защиты ключевого центра и хранится в УКЦ. Экспорт этой части не производится. Открытая часть ключа подписывается действующим ключом подписи администратора УКЦ, создавшего мастер–ключ и передается по произвольным каналам связи в УКЦ других сетей. При импорте открытых частей асимметричных мастер–ключей из других сетей MPa_M производится проверка подписи под ключом. Импорт производится только в случае успешной проверки подписи и сертификата администратора УКЦ, подписавшего ключ. В отличии от симметричных мастер–ключей срок действия ключа дополнительно ограничивается сроком действия сертификата администратора УКЦ, подписавшего данный ключ.

Универсальный симметричный мастер–ключ - Mu_M предназначен для установления связи между 2 и более сетями. Характеризуется номером сети, создавшей ключ и своим серийным номером. Методы формирования экспорта и импорта идентичны индивидуальным мастер–ключам, но импортирован ключ может быть в несколько сетей одновременно. Формировать и использовать данный ключ рекомендуется только в случае отсутствия других типов мастер–ключей для обеспечения бесперебойной генерации ключевой информации СУ или для организации временной защищенной связи в условиях отсутствия возможности обмена другими типами мастер-ключей.

Все МК располагаются в подкаталоге MASTERS.

В составе каждого мастер-ключа хранится информация о его создании, импорте/экспорте и вводе в действие. Импорт, экспорт, ввод в действие и удаление старых версий ключа осуществляется администратором УКЦ.

Ключи ЭЦП

Ключ ЭЦП пользователя представляет собой асимметричную пару ключей, сформированную по алгоритму ГОСТ Р 34.10-94 или ГОСТ Р 34.10-2001: $S_I = (SS_I, SP_I)$.

Ключи ЭЦП могут формироваться как в УКЦ, так и на СУ при создании запроса на сертификат подписи.

При создании ключа в УКЦ секретный ключ подписи защищается на персональном ключе пользователя. На СУ при получении ключа подписи из УКЦ секретный ключ перешифровывается на случайном ключе защиты пользователя. При создании ключа подписи на СУ секретный ключ шифруется на случайном ключе защиты пользователя. При переносе на отделяемые носители (eToken, SmardCard и т.д.) ключ подписи перешифровывается на парольном ключе пользователя

Номера и варианты ключей шифрования.

В ключевой системе используются понятия «номер ключа» и «вариант ключа», используемые для смены ключей (при окончании срока действия или компрометации ключей).

Номер ключа – это номер, определяемый номером мастер-ключа, из которого он создан в УКЦ, и номером собственного асимметричного ключа, если такой используется. Номер используется для плановой смены ключа. Если на одном узле имеются ключи, рожденные из мастер-ключа N5, а на другом узле – рожденные из мастер-ключа N6, то сообщение, переданное с одного узла на другой, не может быть расшифровано, так как рожденные из разных мастеров ключи парной связи будут разными. Точно также два узла могут связаться, если на каждом из этих узлов есть действующая открытая часть ключа второго пользователя.

В связи с этим в системе ViPNet реализована система синхронизации смены ключей, позволяющая автоматически произвести замену ключей не ранее заданного времени и при наличии дополнительных подтверждений о возможности такой замены. При этом в течение некоторого времени поддерживается возможность расшифрования информации на ранее действующих ключах.

Номер ключа, определяемый мастер-ключом, может изменяться от 0 до 255.

Номер ключа, определяемый номером собственного асимметричного ключа, может изменяться от 0 до 65535. Срок действия такого ключа определяется пользователем и составляет не менее суток. ***Вариант ключа*** - это порядковый номер (он и называется вариантом) генерации ключей для этого узла. Он используется для смены симметричных ключей при компрометации ключей на одном узле. Вариант как бы удлиняет идентификатор данного узла. Ключи обмена создаются из мастер-ключа на основе идентификаторов коллективов и вариантов для обоих узлов. При компрометации ключей на одном узле в ключевом центре увеличивается на единицу вариант для данного узла, и создаются ключи обмена только для данного узла с другими узлами. Измененные ключи затем рассылаются из УКЦ через ЦУС по тем узлам, которых это касается. Вариант может изменяться, как и номер, от 0 до 255. При изменении варианта ключа используется та же система синхронизации обновления ключей, как и при смене номера ключа.

Назначение ключей для связи АП с ЦУСом и сервером.

В составе ключевой информации пользователя всегда имеются симметричные ключи обмена общих коллективов тех АП, на которых зарегистрирован данный пользователь, с общими коллективами ЦУСа и соответствующих универсальных серверов. Используются данные ключи в следующих целях:

для защиты управляющего трафика между АП и ЦУСом. В состав этого трафика могут входить, в частности, запросы на управление очередями конвертов, журналы, обновление адресных справочников и т.д. Естественно, что этот трафик надо защищать. По этому же каналу можно передавать и обновления ключевой информации. (Обновления защищены так,

что их можно передавать по любым каналам связи, в том числе открытым. Защита обновлений ключевой информации на ключе связи с ЦУСом является дополнительной, а не обязательной мерой защиты) для аутентификации, применяемой в транспортном модуле при установлении связи между АП и его сервером.

Парольная защита

Пароль – последовательность алфавитно-цифровых символов длиной от 9 до 32. Пароль может быть двух типов: собственный или случайный. Собственный пароль задается самим пользователем или администратором УКЦ.

Случайный пароль формируется средствами СКЗИ «Домен-К» из парольной фразы. При формировании случайного пароля также задается число начальных букв в каждом слове фразы, используемых для составления пароля. Слова для парольной фразы выбираются случайным образом (с использованием генератора случайных чисел) из специальных словарей. Например, парольной фразе из 4 слов летний прадедушка покушал бродягу в случае, когда из каждого слова берутся первых три буквы, соответствует пароль ktnghfgjr,hj .

Парольный ключ – последовательность байт длиной 32 байта, получаемая путем хэширования пароля.

Ключи, хранящиеся на ключевых носителях, зашифрованы на персональном ключе или на сумме по модулю 2 парольного и персонального ключей абонента. Шифрованию на сумме парольного и персонального ключей подвергаются секретные асимметричные ключи шифрования и подписи, чтобы сделать их недоступными для УКЦ. Персональный ключ абонента зашифрован на текущем парольном ключе.

Для проверки пароля на ключевую дискету помещается хэш-значение парольного ключа. Таким образом, контрольное хэш-значение для проверки пароля вычисляется посредством двух последовательных хэшированиий пароля. Первое хэш-значение и играет роль парольного ключа.

Файл-дистрибутив (DST-файл)

Файл-дистрибутив (или дистрибутив для начальной инсталляции) – файл, создаваемый для каждого пользователя сетевого узла и содержащий следующую информацию (в склеенном виде): набор ключей для пользователя и сетевого узла (из УКЦ), регистрационный файл (infotecs.re), а также адресные справочники (из ЦУС). Эта информация необходима для обеспечения первичного запуска прикладной программы сети ViPNet.

Различают два вида дистрибутивов: полный и минимальный. Полный дистрибутив содержит полный набор файлов справочников, ключевую дискету пользователя и ключевой набор для сетевого узла.

Минимальный дистрибутив содержит выборку файлов справочников и ключевую дискету пользователя. Использование минимального дистрибутива достаточно для того, чтобы войти в прикладную программу и дистанционно принять от ЦУСа всю остальную ключевую и адресную информацию (полный набор адресных справочников и ключевой набор для сетевого узла). Учитывая малый объем информации на ключевой дискете, эту информацию можно также размещать на Touch memory или смарткарте для первичной выдачи пользователю. Формирование полного дистрибутива целесообразно, если связь с ЦУСом по каким-либо причинам невозможна. Но в то же время необходимо учитывать, что при большом размере сети файл полного дистрибутива может не поместиться на дискете.

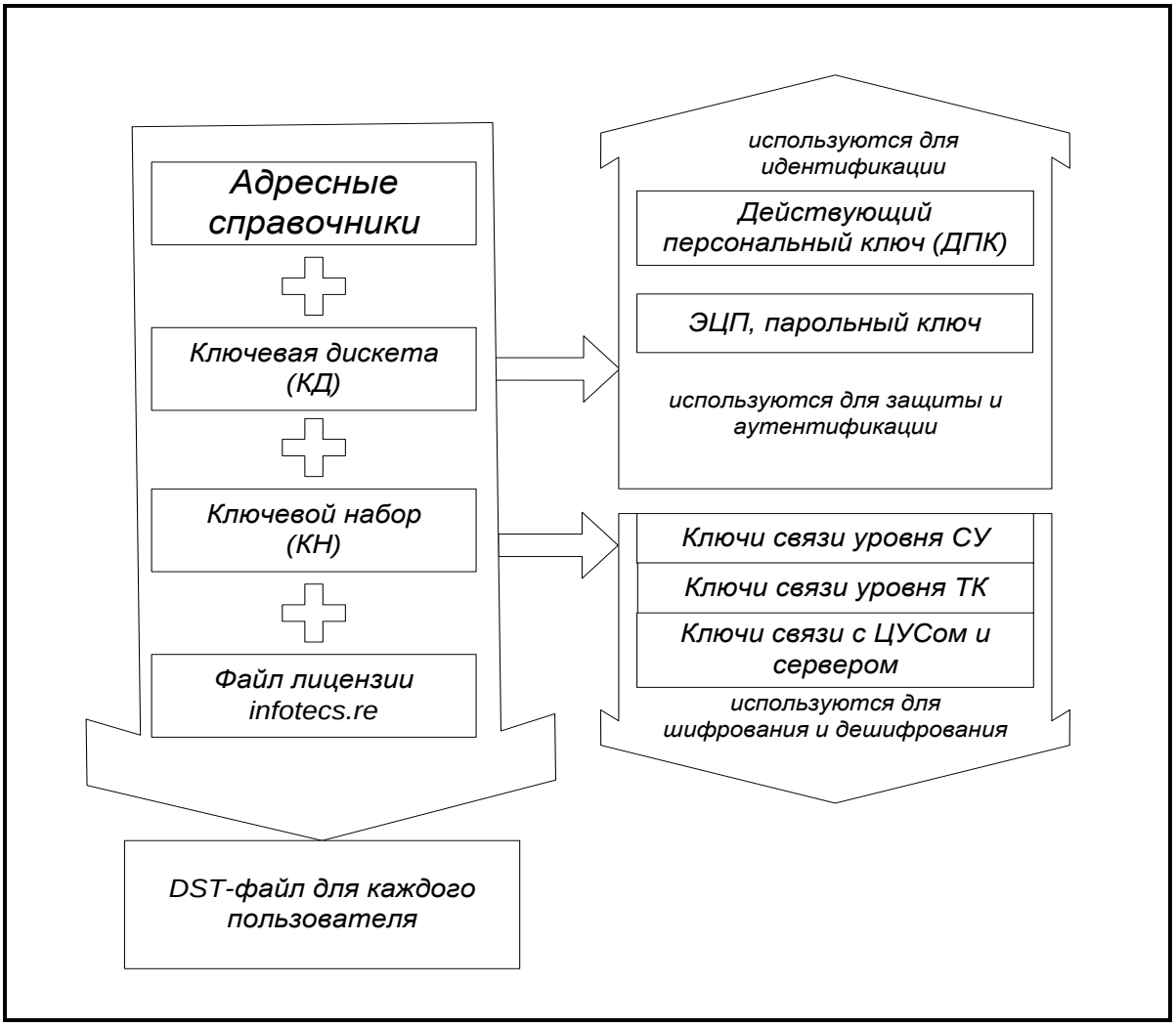


Рис. 8. Формирование дистрибутива справочно-ключевой информации для пользователя сети ViPNet

Ключевые дискеты пользователей (КД). Для каждого пользователя в УКЦ создается своя ключевая дискета. Основное содержание ключевой дискеты пользователя – информация, его идентифицирующая и позволяющая работать с прикладными задачами сети ViPNet. Кроме того, на дискете находятся ключи ЭЦП данного абонента, если ЦУС разрешил абоненту подписывать документы, а также хэш-функция, служащая для проверки пароля.

Для удобства отправки ключевая дискета создается в склеенном виде (Склеенный вид – файлы в неизменном виде склеиваются в один файл с добавлением информации для расклейки).

Перед использованием ключевой дискеты ее надо обязательно расклеить. Расклеить ключевую дискету означает преобразовать файл из склеенного вида к набору из нескольких файлов. Расклеить КД можно несколькими способами. Для пользователей, получивших DST-файл от Администратора сети, расклейка проходит автоматически.

Ключевые наборы для сетевых узлов (КН). Для каждого сетевого узла создается один ключевой набор, и все пользователи этого сетевого узла пользуются им при шифровании и дешифровании. Основное содержание ключевого набора – ключи для шифрования между коллективами и между сетевыми узлами. Ключевой набор также создается в склеенном виде.

Асимметричные ключи шифрования

Асимметричные ключи шифрования (АКШ) могут формироваться на АП, на которых не зарегистрированы ЦУС и УКЦ и при условии, что пользователь данного АП имеет право подписи. На СМ АКШ не формируются. Использование АКШ может быть включено пользователем через настройки ПО. Включение использования АКШ не означает отказа от использования симметричной ключевой системы ViPNet. АКШ являются дополнительными и используются совместно с симметричными ключами шифрования.

Процедура формирования АКШ выполняется при включенной опции "Использовать АКШ" и выполнении хотя бы одного из условий:

Отсутствует действующий ключ АКШ хотя бы для одного из коллективов, в котором зарегистрирован пользователь.

Срок действия ключа АКШ для одного из коллективов истекает менее чем через 12 часов.

С момента последнего формирования ключей (определяется как дата начала срока действия ключа АКШ общего коллектива АП) прошло более T суток, где T – период формирования АКШ, задаваемый в настройках ПО.

Использование криптографии различными приложениями системы ViPNet

Основными потребителями криптографических модулей, а, следовательно, созданной ключевой инфраструктуры в системе ViPNet являются подсистема VPN, работающая на сетевом уровне, а также Деловая почта, ЦУС, транспортный модуль MFTP, работающие на прикладном уровне.

На рабочих местах управление и настройку криптографической подсистемы обеспечивает специальный модуль криптосервиса, который входит, как непосредственно в приложения системы ViPNet, так и поставляется в виде отдельного приложения. Основное назначение криптосервиса в виде самостоятельного приложения – это обслуживание внешних прикладных программ, которые используют криптографические модули ViPNet – СКЗИ “Домен-К” для своих целей. Для использования криптографии “Домен-К” другими системами предоставлены разнообразные возможности в виде программных криптографических интерфейсов, COM объектов, плагинов.

Подсистема Деловой почты использует все типы ключей, формируемые в системе, что позволяет при необходимости обеспечить многочисленные уровни разграничения доступа к письмам и документам в соответствии с типом регистрации пользователей в ЦУСе. Если на узле зарегистрировано несколько пользователей и несколько коллективов пользователей, то в зависимости от конфиденциальности документов пользователь может обеспечить доступ к ним:

только себя и, соответственно, направить письмо и документы, доступные только конкретному пользователю. Для этого в ЦУСе должны быть созданы коллективы, где такие пользователи зарегистрированы единолично;

только пользователей, зарегистрированных в своем коллективе, и направить письмо и документы, доступные только пользователям конкретного коллектива;

всех пользователей, зарегистрированных на данном узле, и направить письмо и документы, доступные всем пользователям узла – получателя.

Такое разграничение достигается путем шифрования документов на ключах соответствующего уровня.

При отправке письма и документов – вложений для каждого письма - конверта формируется случайный ключ, синхропосылка (SP), на которых осуществляется шифрование и которые вставляются в почтовый конверт и передаются получателю вместе с письмом. Случайный ключ (32 байта) шифруется на ключе обмена с соответствующим коллективом. Одновременно формируется имитозащитная сигнатура (IM), которая позволяет проконтролировать целостность документа и защитить пользователей от навязывания ложной информации.

При сохранении письма с документами в почтовых папках, если письмо зашифровано, то оно также сохраняется в них в зашифрованном виде. Однако всегда производится перешифрование случайного ключа на ключе обмена с самим собой. При сменах ключей все такие ключи сохраняются в специальном файле в зашифрованном на текущем ключе виде. Это позволяет обеспечить возможность расшифрования старых документов и после многочисленных смен текущих ключей.

В деловой почте используются все стандартные механизмы электронной цифровой подписи, которые позволяют обеспечить юридическую значимость документа и его доставки получателю. Каждое письмо и каждый вложенный документ может быть подписан несколькими подписями независимо друг от друга.

На рисунке 9 приведен порядок шифрования в Деловой почте.

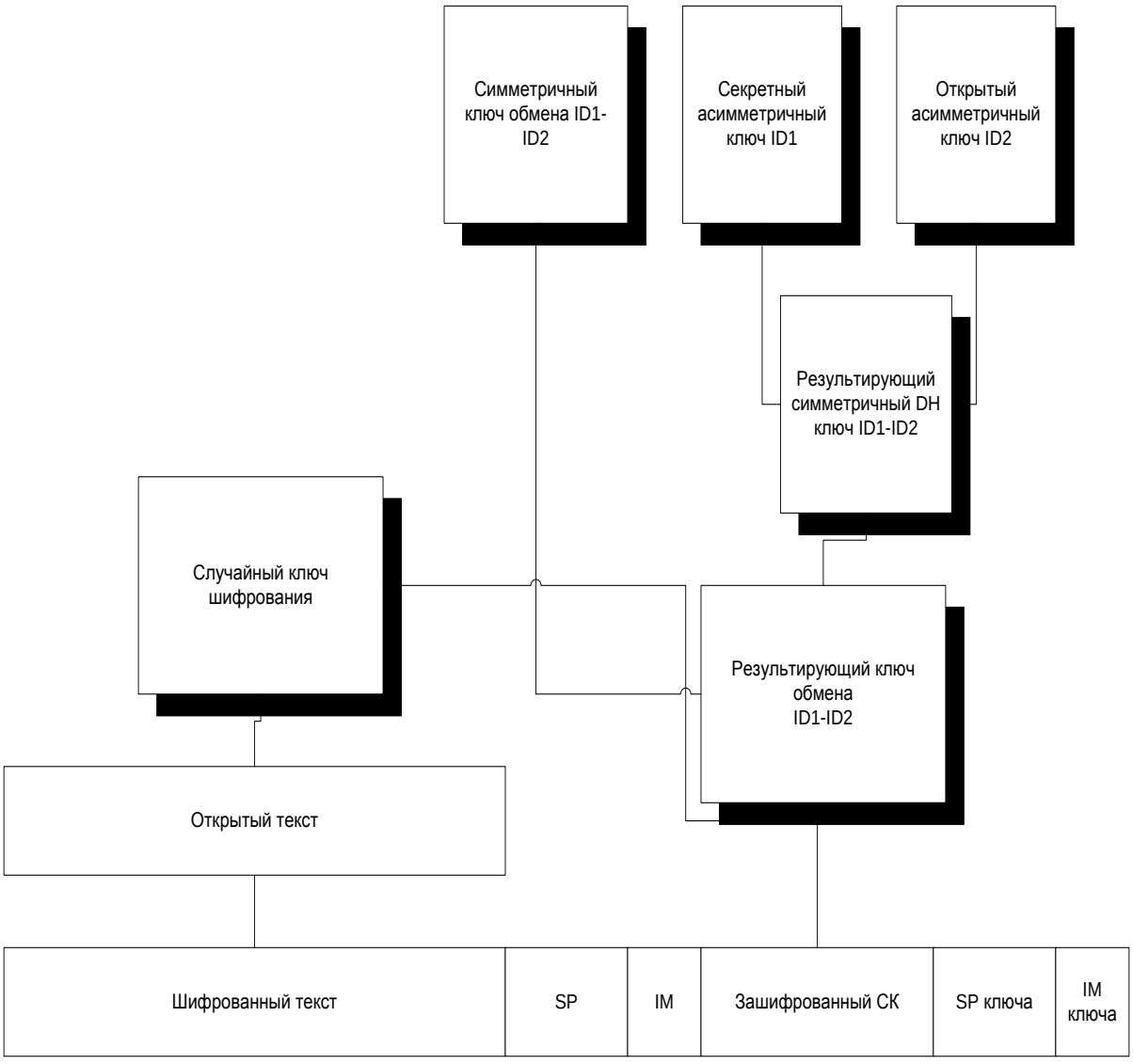


Рис. 9. Шифрование на прикладном уровне

Центр управления сетью и транспортный модуль MFTP. ЦУС обеспечивает управление узлами сети путем отправки на узлы через транспортный модуль обновлений адресных справочников, ключевой информации, сформированной УКЦ, программного обеспечения, выпущенных в УКЦ сертификатов ЭЦП и др.

Вся указанная информация при отправке из ЦУСа упаковывается в почтовые конверты и шифруется на ключах обмена общих коллективов ЦУСа и узла адресата.

На узле данная информация расшифровывается транспортным модулем и передается приложению. Поступившая информация для отправки обратно в ЦУС зашифровывается транспортным модулем.

Шифрование в этих случаях производится аналогично шифрованию почтовых сообщений, то есть с использованием случайного ключа (Рисунок 9).

Следует отметить, что ключевая информация, поступающая из УКЦ в ЦУС для передачи на узлы, уже зашифрована на ключах защиты, имеющихся только в УКЦ и на узлах, в связи с чем, эта информация на ЦУСе не доступна.

VPN и фильтрация трафика. Подсистема VPN, в отличие от Деловой почты, работающей на прикладном уровне, функционирует на сетевом уровне и использует криптографическую подсистему для шифрования и расшифрования IP-трафика, которым компьютер обменивается с другими компьютерами с установленными модулями ViPNet. Для шифрования трафика эта подсистема использует ключи уровня узла («общего коллектива»), то есть доступных для всех пользователей, зарегистрированных на данном узле. Шифрование и фильтрацию сетевого трафика осуществляет специализированный Драйвер ViPNet.

Управление работой драйвера обеспечивает прикладная программа ViPNet – Монитор. Данная программа обеспечивает загрузку драйверу необходимых правил фильтрации открытого и зашифрованного трафика и соответствующей ключевой информации. При этом данная программа использует предоставленные ключевой системой ViPNet возможности для активной аутентификации пользователей, зарегистрированных на данном компьютере, и обеспечивает:

опционально блокировку управления компьютером через клавиатуру и мышку, блокировку сетевого трафика без ввода пароля и наличия ключевой дискеты (носителя) пользователя;

загрузку заданных пользователем или администратором персональных правил для данного пользователя по фильтрации открытого и зашифрованного трафика. Это обеспечивает разграничение возможностей разных пользователей по доступу к различным сетевым ресурсам.

Для ViPNet-драйвера конечным объектом при шифровании трафика является IP-пакет. То есть для драйвера не требуется Online процедур для выработки ключей и синхронизации, что обеспечивает мгновенность соединений, точнее отсутствие в необходимости специальных сеансов для организации соединений, что могло бы приводить к задержкам и повлиять на надежность работы различных сетевых служб. При шифровании каждого IP-пакета драйвер вырабатывает случайную синхропосылку (8 байт), выполняет свертку (Хэширование) этой синхропосылки с ключом обмена с соответствующим узлом и полученную последовательность (32 байта) использует в качестве ключа для шифрования IP-пакета. То есть сам ключ обмена никогда непосредственно не используется для шифрования пакета.

Для каждого IP-пакета вырабатывается также имитозащитная сигнатура (4 байта), которая вместе с синхропосылкой и зашифрованным IP-пакетом помещается в новый IP-пакет, отправляемый в сеть. О структуре и преобразованиях IP-пакета будет подробно рассказано ниже.

На рисунке 10 приведен порядок шифрования на сетевом уровне.

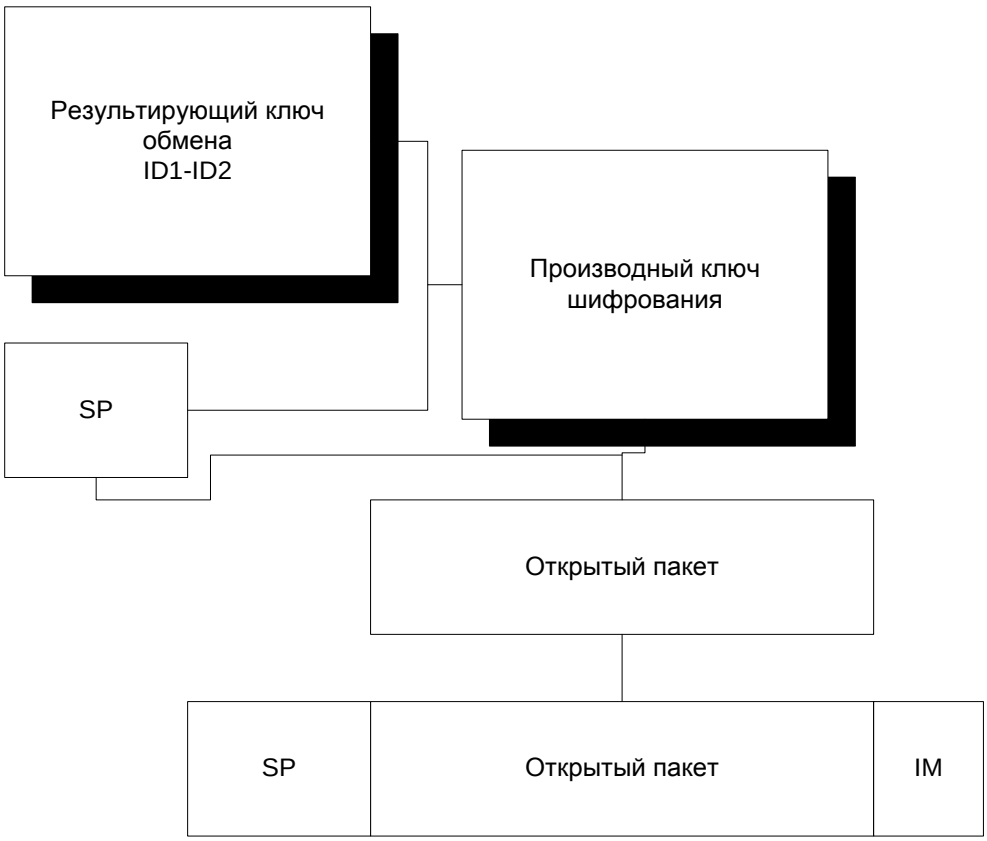


Рис. 10. Шифрование на сетевом уровне

Технология Удостоверяющих центров ViPNet

Обратимся к процедурам выпуска, обработки сертификатов, а также способам построения справочников для неиерархических PKI. В таких инфраструктурах существующие решения основаны на применении специализированных ЦС, выполняющих функцию «моста», и обеспечивающих взаимодействие инфраструктур отрытых ключей с дифференцированной топологией. Технологические возможности стандарта X.509 составляют основу механизма согласованного управления PKI с различной топологией в рамках приложений, отвечающих за выпуск и обработку сертификатов.

Неиерархическая PKI может быть представлена в виде графа, в котором строгое иерархическое отношение узлов нарушено или отличается высокой неоднородностью. Такие PKI могут возникнуть в результате развертывания инфраструктуры с топологией узловой сети или объединения иерархических и неиерархических инфраструктур в ходе перекрестной сертификации.

Ниже приводится описание инфраструктур с различной топологией и способы их комбинирования.

Объединенная иерархическая инфраструктура

В иерархической инфраструктуре, представленной на рис.11 подписчики и другие субъекты PKI доверяют единственному корневому ЦС.

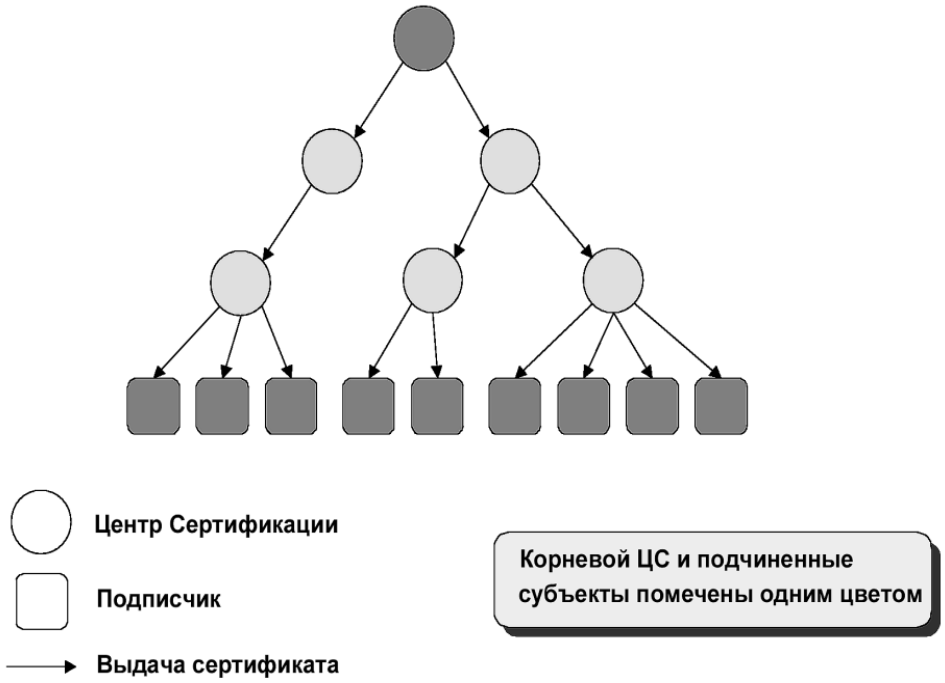


Рис. 11. Иерархическая PKI

Корневой ЦС сертифицирует открытые ключи подчиненных ЦС. Последние в свою очередь сертифицируют открытые ключи подписчиков или же, в случае масштабных PKI, открытые ключи других ЦС. В такой архитектуре процесс сертификации разворачивается строго в направлении подчиненных узлов иерархии, и никогда – в направлении узлов, находящихся на вышестоящих уровнях иерархии. Как правило, только один вышестоящий ЦС выполняет сертификацию каждого подчиненного Центра сертификации. Сертификационный путь в иерархической PKI представляет собой простой и логичный процесс, который заключается в последовательной проверке подлинности открытых ключей из сертификатов (*подтверждение сертификатов*), вплоть сертификатов, выпущенных корневым ЦС. Тогда открытый ключ, с целью проверки которого выполняется построение сертификационного пути, считается подлинным, если подтверждены все сертификаты пути. На практике широко распространен подход, когда несколько иерархических PKI, каждая со своим единственным корневым ЦС, объединяются в общую структуру (Рис. 1.2.7). В такой поликорневой инфраструктуре подтверждение сертификатов субъектов выполняется также как и в монокорневой иерархической PKI. Различие заключается в том, что сертификат принимается только тогда, когда подтверждается всеми корневыми ЦС поликорневой инфраструктуры. Такое решение применяется, например, в популярных web-браузерах, которые распространяются вместе с обширным списком доверенных ЦС. Несмотря на то, что такой подход несколько упрощает процедуру проверки сертификатов, существует и ряд недостатков. Например, пользователь, как правило, не располагает сведениями о сертификационной политике или практике того или иного корневого ЦС, и обычно точно не знает, какой именно корневой ЦС использовался для проверки конкретного сертификата.

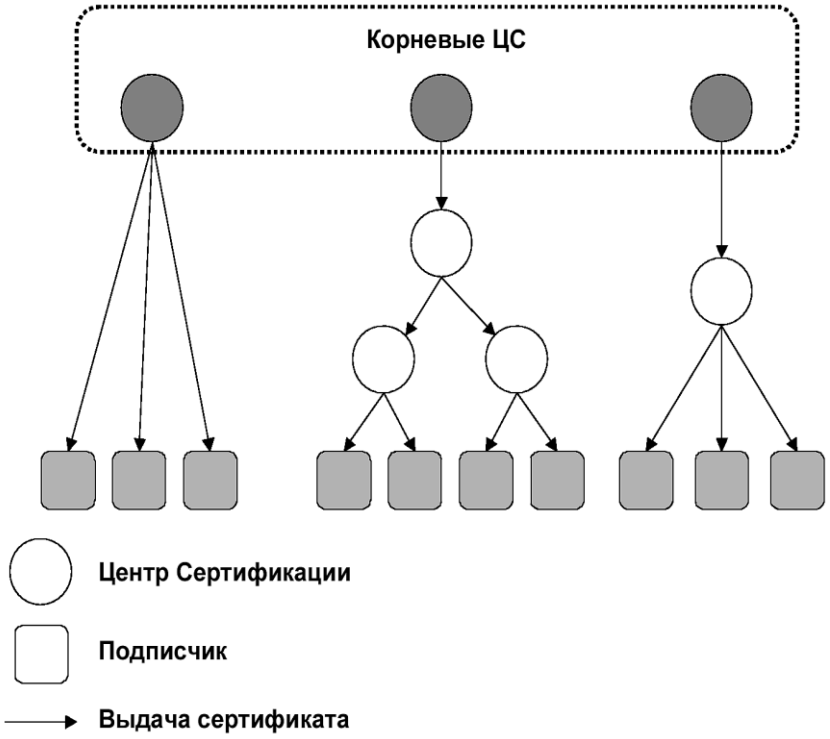


Рис. 12. Поликорневая иерархическая PKI

В PKI с архитектурой узловой сети (Рис. 9-а) каждый подписчик доверяет только тому ЦС, который отвечает за выпуск сертификата данного подписчика. Особенность такой архитектуры – отсутствие промежуточных узлов (ЦС) между корневым ЦС и подписчиком. ЦС в такой архитектуре охватываются перекрестной сертификацией. Каждый ЦС одновременно выпускает сертификаты и обеспечивается сертификатом со стороны других равноправных ЦС, входящих в инфраструктуру. На рисунке представлена PKI с архитектурой узловой сети, где каждый ЦС участвует в процессе перекрестной сертификации. Существует принципиальная возможность проектирования и развертывания узловой PKI со смешанной однонаправленной и перекрестной сертификацией.

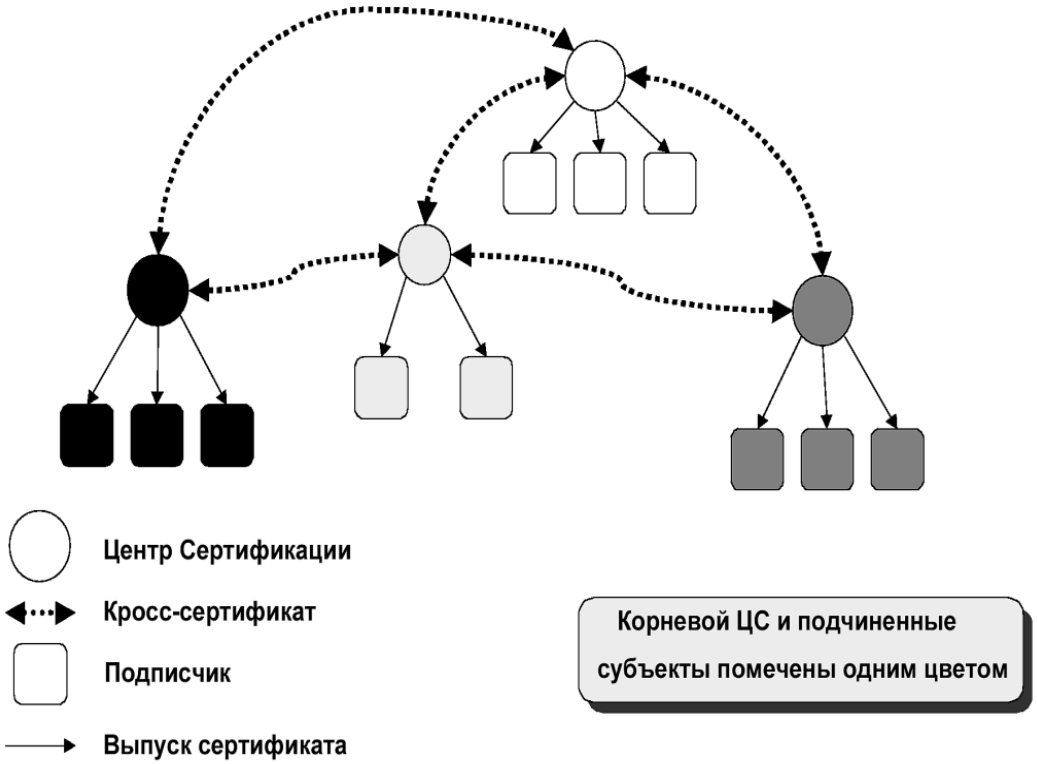


Рис. 13. PKI с топологией узловой сети

Конструкция сертификационного пути в PKI с такой топологией несколько сложнее по сравнению с иерархической инфраструктурой. Основная причина – наличие множественных связей между доверенным центром и проверяемым сертификатом, потенциальная возможность возникновения замкнутых контуров и тупиков в графах, отражающих топологию неиерархических PKI. Дополнительно, несмотря на то обстоятельство, что топологии узловой и иерархической инфраструктур могут различаться незначительно, сертификаты в ходе двусторонней перекрестной сертификации в узловой PKI сохраняются не как индивидуальные сертификаты, а как сертификационные пары. Такие пары, в отличие от сертификатов иерархической инфраструктуры, регистрируются в специальном поле записи в справочнике.

Двунаправленная перекрестная сертификация.

Различные инфраструктуры открытых ключей могут быть связаны при помощи перекрестной сертификации, что позволяет субъектам подтверждать сертификаты, выпущенные другими PKI. В случае иерархических PKI, типичный процесс перекрестной сертификации сводится к тому, что каждый корневой ЦС выпускает сертификаты для других корневых Центров сертификации данной PKI. В результате образуется несколько усложненная, но все еще иерархическая инфраструктура. Для осуществления перекрестной сертификации в инфраструктурах с топологией узловой сети, ЦС внутри каждой PKI выбираются более или менее произвольно. Основной критерий выбора – эффективное построение результирующей PKI. На рис. 14 представлена гибридная инфраструктура, полученная в результате объединения иерархической и узловой PKI.

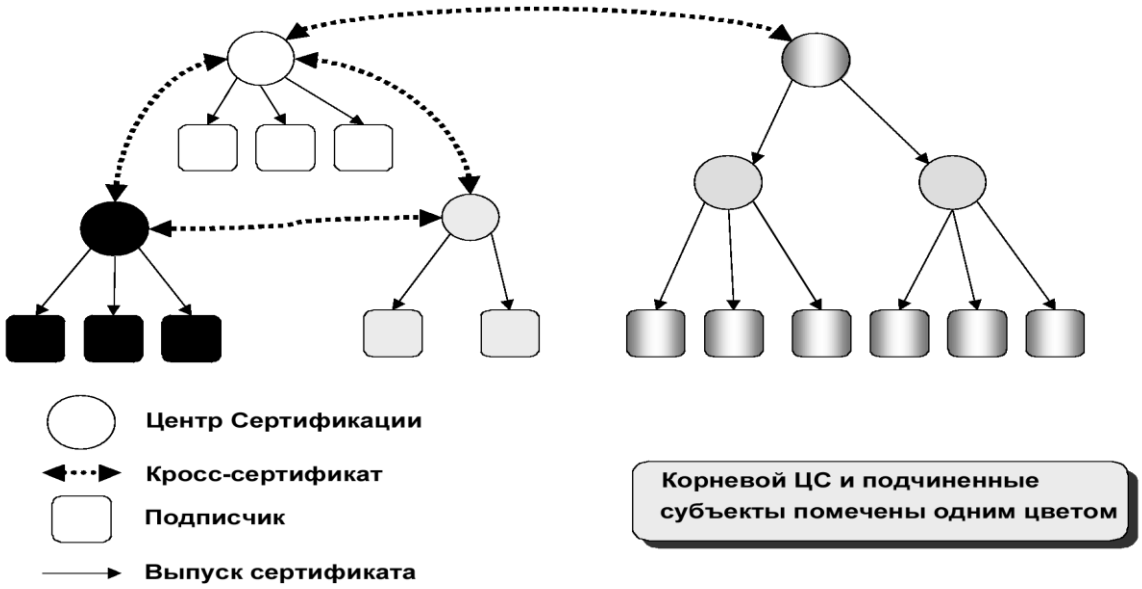


Рис. 14. Гибридная PKI

Число связей между различными, подлежащими перекрестной сертификации инфраструктурами, возрастает экспоненциально с ростом числа таких PKI. В ходе перекрестной сертификации пара субъектов устанавливает прямое отношение доверия за счет снижения общей безопасности, так как PKI с высоким уровнем безопасности и строго ограниченными сертификационными политикой и практикой подлежат перекрестной сертификации со стороны PKI с существенно менее ограниченными политикой и практикой и соответственно более низким уровнем безопасности.

Типовые варианты подключения программно-аппаратного комплекса УЦКУ ViPNet

Взаимодействие пользователей ПК ViPNet с ресурсами Ключевого и Удостоверяющего центра ПК УЦ ViPNet производится только через ПО «Центр управления сетью». Обмен информацией между ПО «Центр управления сетью» и ПО «Ключевой и Удостоверяющий центр» производится через общие папки файловой системы компьютера. Для обеспечения информационной безопасности ресурсов данных компонент системы необходимо строго соблюдать правила настроек, отвечающие различным схемам подключения и взаимодействия.

Установка ПО ViPNet «Администратор» на один компьютер

В данной схеме пакеты программ ViPNet»Администратор» «Центр управления сетью» и ViPNet «Администратор» «Удостоверяющий и ключевой центр» взаимодействуют через общие папки файловой системы компьютера. При такой конфигурации необходимо обеспечить выполнение следующих требований:

Абонентам, не входящим в группу администраторов, связи с ЦУС не устанавливаются.

Все абонентские пункты, имеющие связь с ЦУС, должны находиться в 1 режиме безопасности.

Запрещается регистрация открытых адресов глобальной сети для компьютеров, находящихся в одном сегменте с данным компьютером.

Установка ПО ViPNet «Администратор» на разные компьютеры

В данной конфигурации взаимодействие между ЦУС и УКЦ может осуществляться тремя различными способами:
Изолированный режим работы Удостоверяющего и ключевого центра. В этом случае компьютер с установленным ПО ViPNet «Администратор» «Удостоверяющий и ключевой центр» не имеет физического подключения к локальной сети. Обмен информации между Центром управления сетью и Удостоверяющим и ключевым центром осуществляется с использованием физических носителей информации (дискеты, компакт-диски, флэш-память, и т.д.). В данном случае допускается установление связей абонентов сети с абонентским пунктом Центра управления сетью

Обмен файлами через общие сетевые папки. В этом случае компьютер с установленным ПО ViPNet «Администратор» «Удостоверяющий и ключевой центр» оснащается пакетом программ ViPNet «Клиент». Режим безопасности 1. На компьютере, оснащенном ПО ViPNet «Администратор» «Удостоверяющий и ключевой центр» ПО ViPNet «Клиент» «Монитор» настраивается на блокирование всех пакетов, кроме зашифрованного трафика от ЦУС. Связь для данного АП устанавливается только с АП Центра управления сетью.

Обмен файлами через режим автопроцессинга. В этом случае компьютер с установленным ПО ViPet «Администратор» «Удостоверяющий и ключевой центр» оснащается пакетом программ ViPNet «Клиент». Режим безопасности 1. Связь для данного АП устанавливается только с АП Центра управления сетью. На компьютере, оснащенном ПО ViPNet «Администратор» «Удостоверяющий и ключевой центр», монитор настраивается на блокирование всех пакетов, кроме зашифрованного трафика от ЦУС. При первом запуске оба компьютера отключаются от сети, доставка исходных справочников для первичного развертывания ключевой системы осуществляется на отделяемых носителях. После формирования ключевых дистрибутивов для ПО ViPNet «Клиент» «Деловая почта» осуществляется настройка правил приема – передачи файлов из каталогов для ЦУСа. Для транспортного модуля MFTP настройка канала связи выбирается «MFTP» с указанием реального IP адреса получателя.

Разграничение полномочий администраторов УЦКУ

Для обеспечения безопасной эксплуатации комплекса рекомендуется формировать 3 группы администраторов со следующими полномочиями.

Группа администраторов безопасности.

Администратор безопасности выполняет следующие функции:
Несет ответственность за соблюдением правил безопасной эксплуатации комплекса в целом.

Осуществляет контроль за соблюдением правил эксплуатации и соблюдением мер защиты от НСД.

Осуществляет проверку целостности ПО.

Контролирует по журналам «ViPNet «Клиент» «Монитор» попытки несанкционированного доступа к ПО, попытки сетевых атак и проявления сетевой активности приложений.

Для обеспечения своих функций Администратор безопасности должен:
Быть зарегистрирован как пользователь сети ViPNet на подконтрольных ему абонентских пунктах с максимальными полномочиями и обладать соответствующими ключами доступа на данные абонентские пункты.
Обладать паролями входа в ОС с правами администратора и паролем администратора АП сети ViPNet.

Группа адресной администрации

Данная группа включает в себя администраторов ЦУС и ЦР.
Администратор ЦУСа выполняет следующие функции:

1. Осуществляет регистрацию абонентских пунктов и пользователей сети ViPNet.
2. Назначает связи между объектами сети.
3. Формирует и рассылает справочники для абонентских пунктов и Удостоверяющего и Ключевого центра, а также обновления ключевой и справочной информации.
4. Обеспечивает взаимодействие с ЦУСами других сетей ViPNet
Для обеспечения своих функций Администратор ЦУСа должен:
Быть зарегистрирован как абонент сети ViPNet на абонентском пункте Центр управления сетью с минимальными полномочиями.
Обладать паролями входа в ОС с правами, достаточными для выполнения своих обязанностей.
Иметь полный доступ к программе ViPNet [Администратор] [Центр управления сетью] и ее рабочим каталогам.

Администратор ЦР выполняет следующие функции:
Осуществляет регистрацию внешних пользователей.
Создает запросы на издание обновление и отзыв сертификатов внешних пользователей.
Осуществляет, при необходимости, проверку сертификатов внешних пользователей.
Для обеспечения своих функций Администратор ЦР должен:
Быть зарегистрирован как абонент сети ViPNet на абонентском пункте Центр регистрации с минимальными полномочиями.
Иметь действительный ключ подписи и сертификат для подписи запросов к Удостоверяющему Центру.
Обладать паролями входа в ОС с правами, достаточными для выполнения своих обязанностей.
Иметь полный доступ к программе ViPNet «Администратор» «Центр регистрации» и ее рабочим каталогам.

Группа администраторов УКЦ

Данная группа включает в себя администраторов УКЦ. В соответствии с функциональностью программы УКЦ администраторы данной группы могут разделяться на подгруппы Уполномоченное лицо Удостоверяющего центра, Администратор Ключевого Центра.
Администратор УКЦ, как администратор КЦ, выполняет следующие функции:
1. Осуществляет первичную генерацию ключевой информации УКЦ и абонентских пунктов сети.
2. Осуществляет формирование симметричных ключей шифрования для абонентских пунктов сети.
3. Осуществляет формирование и своевременную смену «мастер-ключей» своей сети и для межсетевого взаимодействия.
4. Обеспечивает своевременную передачу в ЦУС сформированной ключевой и справочной информации.

Администратор УКЦ, как Уполномоченное лицо УЦ, выполняет следующие функции:
1. Формирует ключ подписи УЛ и издает корневой сертификат УЛ.
2. Формирует ключи подписи УЛ и запросы на сертификаты УЛ к вышестоящему УЦ.
3. Осуществляет первичную генерацию ключевой ключей подписи и издание сертификатов для пользователей сети.
4. Издает сертификаты ключей подписи по запросам ЦР и запросам на обновление сертификатов.
5. Отзывает, приостанавливает и возобновляет сертификаты пользователей по их запросам или по запросам ЦР.
6. Осуществляет экспорт и отправку в ЦУС справочников сертификатов УЛ, пользователей, списков отозванных сертификатов.

В общие обязанности Администраторов УКЦ включаются:

1. Своевременное создание архивов баз данных и восстановление при сбоях.
2. Настройка и ведение журналов УКЦ.
3. Ведение документации УКЦ в соответствии с «Регламентом УЦКУ» и должностными инструкциями.

Для обеспечения своих функций Администратор УКЦ должен:
1. Быть зарегистрирован как пользователь сети ViPNet на абонентском пункте Удостоверяющий и Ключевой Центр с минимальными полномочиями.
2. Обладать паролями входа в ОС с правами, достаточными для выполнения своих обязанностей.
3. Иметь полный доступ к программе ViPNet «Администратор» «Удостоверяющий и ключевой центр» и ее рабочим каталогам.

Обеспечение безопасности функционирования инфраструктуры ЭЦП в корпоративных сетях.

К основным техническим мерам, которые гарантируют высокий уровень безопасности использования инфраструктуры ЭЦП, можно отнести следующие:
Весь информационный обмен, связанный с обеспечением работы инфраструктуры ЭЦП (получение сертификатов, их отзыв, приостановление, возобновление, получение и обновление справочников отозванных сертификатов, справочников сертификатов Главных абонентов сети и др.), производится в зашифрованном виде, что исключает любые стратегии модификации, подмены, навязывания ложной информации, несанкционированного доступа к передаваемой информации.

Весь служебный информационный обмен по ЭЦП обеспечивается специализированным защищенным транспортным модулем MFTP, входящим в состав сертифицированного продукта и использующим протокол сетевого уровня TCP по портам 5000, 5001, 5002, что позволяет путем настроек для пропуска этого протокола на межсетевых экранах исключить возможные сетевые атаки через стандартные протоколы.
Программное обеспечение ViPNet на клиентских станциях обеспечивает криптографический контроль целостности справочников сертификатов Главных абонентов УКЦ, что гарантирует их защиту от подмены. Все другие справочники защищены от подмены криптографическими контрольными суммами и подписью УКЦ.

УКЦ ViPNet производит кросс сертификацию сертификатов других удостоверяющих центров, что позволяет центральной администрации контролировать надежность других удостоверяющих центров. Подпись лица, которому сертификат выдан другим удостоверяющим центром, признается действительной, только в случае наличия на компьютере заверенного своим УКЦ сертификата этого другого удостоверяющего центра, выдавшего сертификат данному лицу.

Межсетевой экран ViPNet «Координатор», защищающий УКЦ, совмещен с сервером транспортного модуля MFTP. Сетевые узлы имеют возможность взаимодействовать только с координатором и не имеют возможности прямого взаимодействия с УКЦ и Центром управления, что позволяет на межсетевом экране пресечь любые сетевые атаки даже со стороны зарегистрированных пользователей.

Если на клиентские компьютеры возможны сетевые атаки, то для защиты криптографических модулей и ключей ЭЦП на них целесообразна установка модуля ViPNet «Клиент» или его составляющей ViPNet «Персональный сетевой экран», сертифицированной ФАПСИ для использования в органах государственной власти. Модуль ViPNet «Клиент» дополнительно к персональному сетевому экрану создает зашифрованный туннель до ViPNet «Координатора», блокируя при этом любой открытый трафик, что полностью исключает любые сетевые атаки на компьютер пользователя.

Масштабируемость решения

ЦУС и УКЦ ViPNet могут обеспечить автоматическое защищенное взаимодействие более чем с 65000 сетевыми узлами. При этом в одном УКЦ может быть зарегистрировано более чем 65000 абонентов сети для выдачи им сертификатов.

В рамках существующих положений «Закона об ЭЦП» предполагается работа УКЦ ViPNet в следующей схеме:

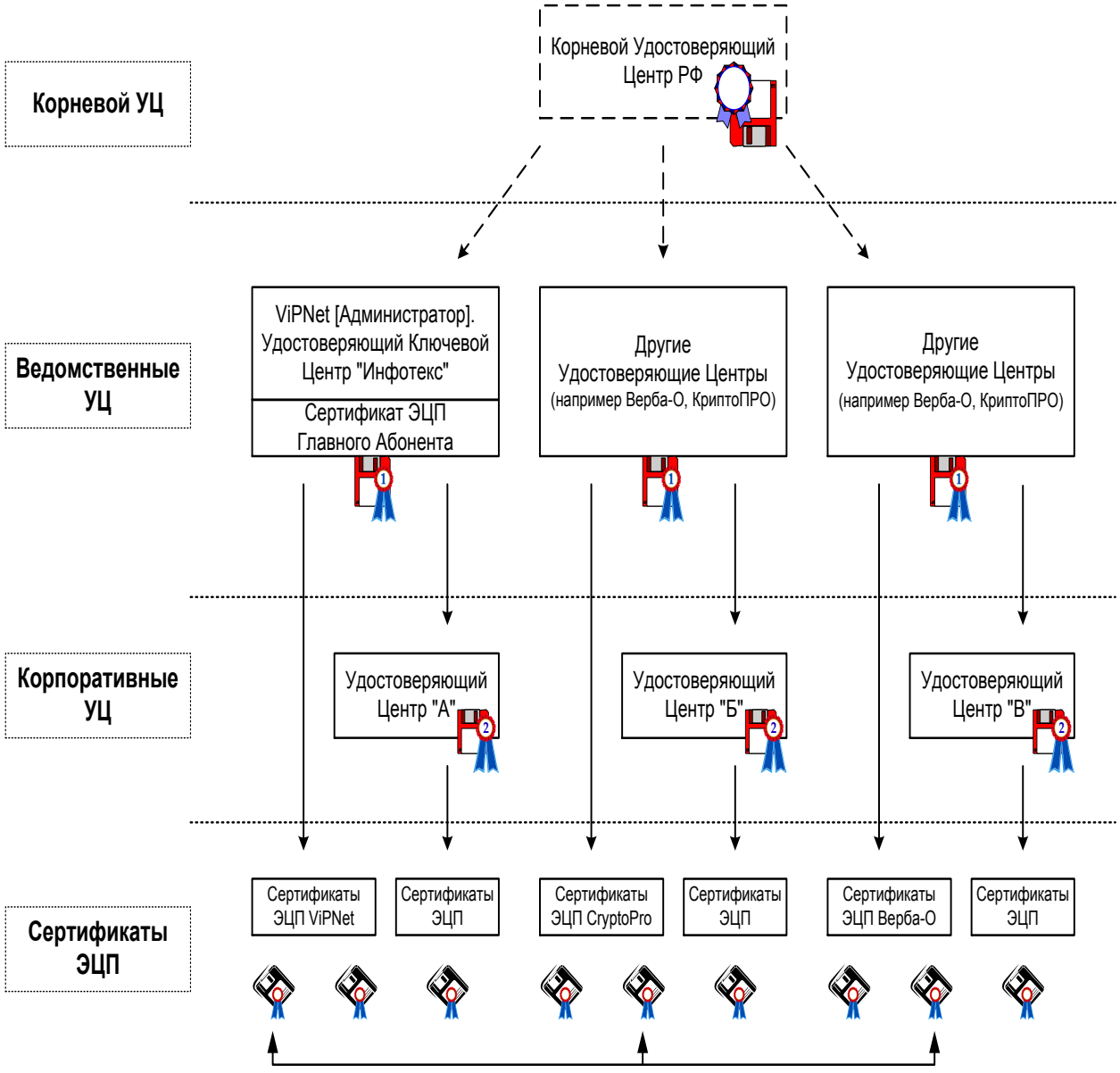


Рис. 15. Работа УКЦ ViPNet

При этом, работа ведомственных УЦ сертифицируется Корневым Удостоверяющим центром.

При необходимости легко могут быть созданы подведомственные Центры управления и УКЦ (Корпоративные УЦ) с делегированием им прав по выдаче сертификатов и автоматическим взаимодействием между собой.

Технология разграничения доступа к информации

Информация может предназначаться для пользователя, коллектива или узла. Пользователь имеет доступ к информации (за исключением персональной ключевой информации), предназначенной для любого другого пользователя, зарегистрированного в тех же коллективах, что и данный пользователь; пользователь не имеет доступа к информации пользователей коллективов, в которых данный пользователь не зарегистрирован.

Пользователь имеет доступ к информации, предназначенной для любого коллектива, где зарегистрирован данный пользователь; пользователь не имеет доступа к информации коллективов, где пользователь не зарегистрирован.

Пользователь имеет доступ к информации, предназначенной для любого узла, в коллективе которого зарегистрирован данный пользователь; пользователь не имеет доступ к информации узлов, в коллективах которых данный пользователь не зарегистрирован.

Пользователь, желающий обеспечить защиту от доступа к своей информации со стороны других пользователей, должен быть зарегистрирован в некотором коллективе один.

Пользователь, коллектив или узел может получить (отправить) информацию только от (для) объектов, с которыми есть связь; связь между объектами одного уровня определяется наличием связи между соответствующими коллективами, заданной в Центре управления сетью.

Возможность доступа различных объектов к соответствующей информации определяется двумя Центрами, не имеющими возможность модифицировать полномочия в сети друг без друга, - Центром управления сетью (ЦУС) и Ключевым центром (КЦ) с использованием двух независимых средств:

Индивидуальных для каждого узла Адресных справочников доступа, модификация и формирование которых возможна только в ЦУСе.

Наличием доступа каждого объекта только к той ключевой информации, сформированной Ключевым центром и недоступной для ЦУСа, состав которой определен соответствующими Адресными справочниками доступа.

Информационная независимость объектов сети от Центров достигается формированием каждым объектом сети дополнительных ключей шифрования на принципах открытого распределения, не доступных Центрам. Достоверность открытой части ключа шифрования каждого объекта сети подтверждается электронной подписью пользователя, сформировавшего данный ключ.

Для каждого пользователя сети Ключевым центром или непосредственно самим пользователем в своей программе формируется Ключ электронной подписи, используемый для достоверной привязки информации, за которую отвечает данный пользователь, к этому пользователю.

Достоверность открытой части Ключа электронной подписи пользователей каждой сети, подтверждается сертификатами (подписями) УЛ соответствующей сети. При наличии межсетевого взаимодействия открытые части ключей электронных подписей УЛ других сетей подтверждаются сертификатами УЛ данной сети.

Открытые части ключей электронных подписей УЛ данной сети хранятся на ключевой дискете каждого пользователя.

ViPNet [Координатор] и его основные функции

Координатор в терминологии ViPNet - это программное обеспечение для СУ, в функции которого входят:

Функция Сервер-маршрутизатор, обеспечивающая:

Маршрутизацию почтовых конвертов и управляющих сообщений при взаимодействии ЦУСа, УКЦ и объектов сети между собой.

Функция Сервер IP-адресов, обеспечивающая:
Регистрацию и предоставление информации о текущих IP-адресах и способах подключения объектов корпоративной сети.
Функция Сервер ViPNet-Firewall, обеспечивающая:
Работу защищенных компьютеров локальной сети (сегмента сети) в VPN от имени одного адреса.
Работу защищенных компьютеров локальной сети через другие Firewall (или устройства с NAT).
Туннелирование пакетов в защищенное соединение от заданных адресов незащищенных компьютеров.
Фильтрацию открытых пакетов, в том числе и туннелируемых, в соответствии с заданной политикой безопасности (функции межсетевого экрана).
Функция ViPNet-сервер открытого Интернета, обеспечивающая:
Организацию безопасного подключения части компьютеров локальной сети к Интернет без их физического отключения от локальной сети организации.

Функциональность ViPNet [Координатор] определяется Центром Управления Сетью и формируемыми им справочниками и маршрутными таблицами.

Функция Сервер-маршрутизатор

В соответствии с логикой построения виртуальных защищенных сетей (VPN) ViPNet абонентские пункты (АП) регистрируются на координаторах. Это означает, что почтовая и управляющая информация данного АП будет проходить через его сервер.

Между серверами-маршрутизаторами в ЦУСе задаются логические каналы связи:
Либо полная связность, тогда управляющая и почтовая информация будет передаваться от сервера к серверу по кратчайшему маршруту;
Либо конкретная цепочка связей, тогда управляющая и почтовая информация будет передаваться от сервера к серверу по заданным маршрутам.

Задание в ЦУСе связей между АП, определяет, с какими другими АП будет обмениваться информацией данный АП.

При организации взаимодействия между двумя различными виртуальными сетями, в каждой из сетей выбирается по одному серверу, через которые и осуществляется обмен между сетями.

При поступлении почтового или управляющего конверта, сервер в соответствии с заданными в ЦУСе маршрутными таблицами определяет дальнейшее движение этого конверта. Если конверт многоадресный, то расщепляет его на соответствующие части. В зависимости от заданной логики, сервер, при наличии конверта либо сам начинает устанавливать соединение с другим сервером или АП (по умолчанию такая логика установлена при отправке конверта на другой сервер) или ожидает, когда с ним установит соединение другая сторона (по умолчанию эта логика работает при наличии конвертов для АП). Может быть задан и период опроса других объектов в независимости от наличия для них конвертов.
При разрывах соединений передача информации всегда продолжается с точки разрыва, что особенно важно на коммутируемых каналах.

В координаторе функцию сервера-маршрутизатора реализует модуль ViPNet «MFTP».

Функция Сервер IP-адресов

Координатор будет выполнять функции сервера IP-адресов, если в ЦУСе он зарегистрирован в задаче Сервер IP-адресов.

При загрузке любого компьютера с ViPNet «Клиент» программа сообщает свой IP-адрес своему серверу IP-адресов и получает от него список IP-адресов всех включенных в данный момент объектов ViPNet, с которыми связан данный АП. В соответствии с этим списком в окне Защищенная сеть, где находятся пользователи защищенной сети, объекты ViPNet, находящиеся в данный момент в сети отобразятся, как включенные, а также отобразятся их текущие IP-адреса. Периодически (в среднем раз в 5 минут), а также при изменении своего IP-адреса АП сообщает на свой сервер информацию о себе. При отключении компьютера от сети также посылается информация об этом на сервер.
По аналогичной логике серверы обмениваются между собой информацией о своем включении и отключении.

После того, как АП узнают о состоянии друг друга и текущих IP-адресах весь информационный обмен между ними производится напрямую (если между ними нет никаких Firewall).

На компьютере с ПО ViPNet «Координатор» также могут устанавливаться любые другие сетевые приложения. Например, это может быть одновременно Сервер домена или WEB-сервер или сервер баз данных и др.

Сервер IP-адресов работает по следующей логике:
При появлении новой информации о каком-то своем АП рассылает ее всем другим серверам своей сети, а также подключенным к нему в данный момент другим АП.
При появлении новой информации с других серверов об их АП высылает эту информацию своим включенным АП.
При отсутствии информации от своих АП более 6 минут считает этот АП отключившимся и рассылает эту информацию.

Если данный сервер взаимодействует с другой сетью, то высылает на шлюзовой сервер той сети информацию об изменении состояния всех объектов своей сети, связанных с объектами другой сети ViPNet. При получении такой информации из другой сети, рассылает эту информацию на все Серверы своей сети, а также на подключенные в данный момент свои АП, связанные с объектами другой сети.

По умолчанию на АП выбирается работа с сервером IP-адресов, на котором данный АП зарегистрирован в ЦУСе.
В ЦУСе могут быть заданы связи АП и с другими координаторами с функцией сервер IP-адресов. Это означает, что данный АП, при необходимости может выбрать в качестве Сервера IP-адресов любой другой координатор, с которым ему разрешили связь.

Функция Сервер ViPNet-Firewall

Координатор будет выполнять функции сервера ViPNet-Firewall, если в ЦУСе он зарегистрирован в задаче Сервер IP-адресов.

ViPNet-координатор может устанавливаться на рабочей станции с одним сетевым адаптером или маршрутизаторе с несколькими сетевыми адаптерами, разделяющими сети друг от друга.

ViPNet-координатор, установленный на границе сетей, выполняет функции NAT для VPN-соединений между узлами ViPNet в сторону каждой из сетей. То есть все IP-пакеты, упакованные в UDP-формат и проходящие через ViPNet-координатор, передаются в сеть от имени адреса соответствующего интерфейса координатора.

Трафик узлов, работающих через координатор, предназначенный для других узлов: находящихся со стороны других сетевых интерфейсов координатора, или не работающих через этот координатор, и недоступных по широковещательным пакетам, автоматически маршрутизируется на адрес своего координатора (производится подмена IP и MAC-адреса), который, выполнив подмену адресов, направляет эти пакеты дальше от имени своего адреса. Аналогичным образом трафик следует и в обратную сторону.

Одновременно ViPNet «Координатор» осуществляет фильтрацию открытых пакетов на каждом сетевом интерфейсе (функции межсетевого экрана) в соответствии с заданными настройками по адресам, протоколам и портам, но преобразования адресов для таких пакетов не производится.

В ряде случаев на границе локальной сети может быть уже установлен другой Firewall, выполняющий функции NAT, и в соответствии с политикой безопасности организации, или просто, если нет возможности получить дополнительные внешние адреса, любой трафик во внешние сети должен проходить именно через этот сетевой экран. В таком случае на координаторе для одного из интерфейсов настраивается работа через этот Firewall. Другие узлы ViPNet автоматически (если в ЦУСе не указано иное) будут работать через этот координатор. В этом случае пакеты от всех узлов будут попадать на внешний Firewall через координатор и от имени его адреса.

ViPNet-координатор может также работать через другой ViPNet-координатор.

Все объекты ViPNet, работающие через ViPNet «Координатор» или другойсетевой экран, могут быть видны с защищенных компьютеров под виртуальными адресами, вырабатываемыми непосредственно на этих компьютерах. Программы ViPNet при взаимодействии с компьютерами, по умолчанию используют виртуальные адреса, если состояние этих компьютеров определилось, как «работающие через сетевой экран», и имеющие частные IP-адреса.

Функция туннелирования открытого трафика локальной сети

ViPNet «Координатор» может выполнять шифрование, преобразование в UDP-формат (туннелирование) заданного открытого трафика локальной сети, который должен быть передан другим узлам ViPNet или открытым компьютерам, находящимся за другими координаторами, если в ЦУСе для этого координатора задано максимальное число IP-адресов для туннелирования.

Туннелироваться может трафик любых устройств, находящихся со стороны любого сетевого интерфейса. При этом передача закрытого трафика производится от имени адреса интерфейса координатора, с которого уходит этот трафик, то есть выполняется NAT.

Если узел ViPNet взаимодействует с туннелируемым некоторым координатором компьютером, и этот компьютер находится в одной подсети, заданной для узла ViPNet, то в этом случае узел ViPNet взаимодействует с этим компьютером напрямую без шифрования трафика.

Локальные сети, соединенные через туннели могут быть и не согласованы по IP-адресам (IP-адреса могут пересекаться). В этом случае работа может производиться по виртуальным адресам, выделяемым ViPNet «Координаторами».

Расшифрованные пакеты для туннелируемых компьютеров всегда отправляются в сеть от имени реального или виртуального адреса компьютера, пославшего этот пакет.

Списки IP-адресов, подлежащих защите, задаются в виде диапазонов и отдельных значений непосредственно на объектах виртуальной сети (АП и Координаторах) или в ЦУСе.

Пакеты, не подлежащие защите, подвергаются фильтрации в соответствии с заданными настройками. Для туннелируемых пакетов также могут быть настроены необходимые фильтры.

Использование ViPNet «Координатора» для туннелирования целесообразно, если на какие-либо компьютеры не удается или нет необходимости устанавливать ViPNet «Клиент» для индивидуальной защиты.

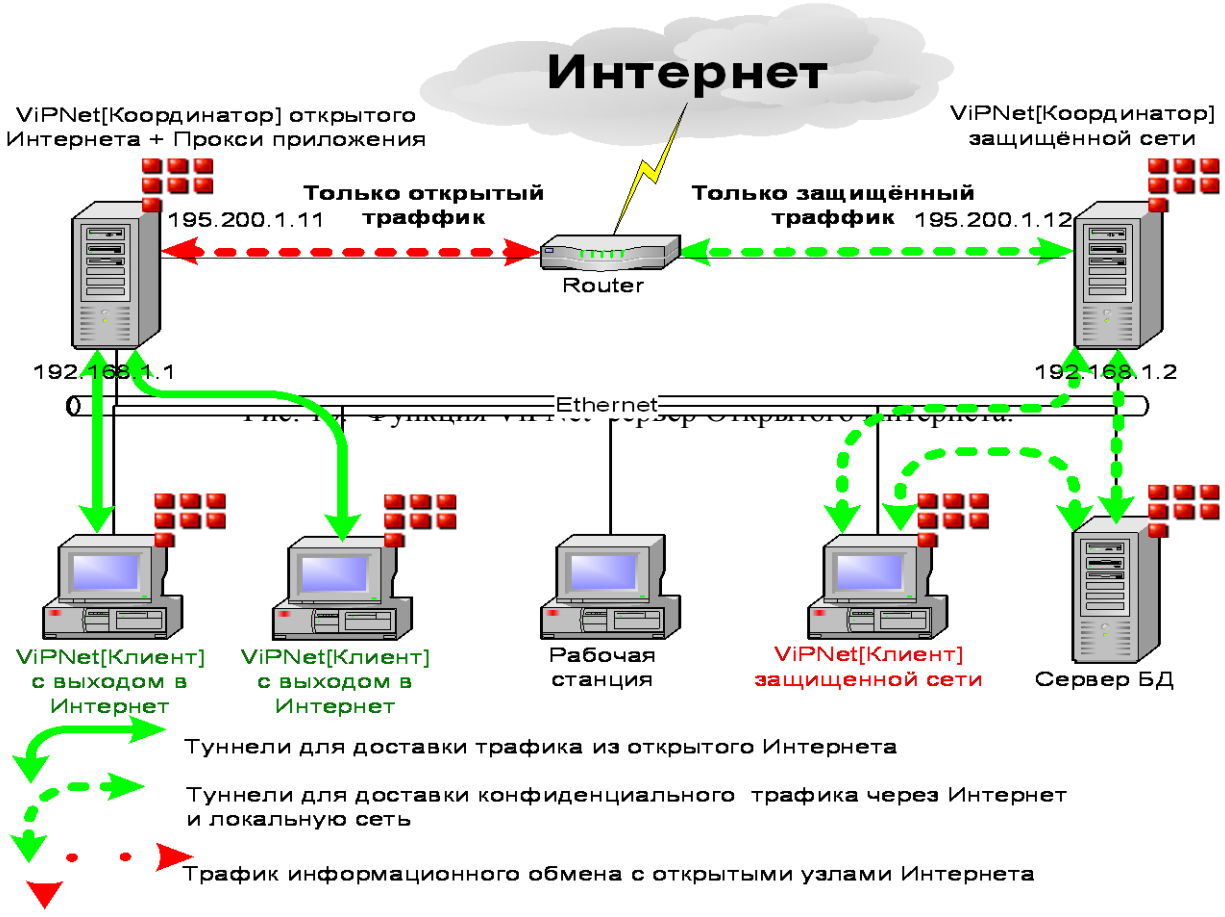
Функция ViPNet–сервер Открытого Интернета

Если в организации, из соображений политики безопасности, компьютерам локальной сети запрещен выход в Интернет (назовем их группой компьютеров А), но отдельным компьютерам необходим такой доступ (группа компьютеров Б), то технология с

использованием ViPNet–сервера Открытого Интернета (технология выхода в «Открытый Интернет») поможет решить эту проблему удобным и надежным способом. Технология позволит организовать работу каждого компьютера группы Б в одном из двух вариантов:
либо в Интернете, с блокировкой любого трафика в локальную сеть;
либо в локальной сети, с блокировкой любого трафика в/из Интернет.
Для выбора варианта работы (в Интернете или в локальной сети), необходимо просто переключить опцию в программе ViPNet «Клиент» [Монитор].

При этом физически отключать компьютеры группы Б от локальной сети не нужно, т.к. при любом варианте работы компьютера группы Б (в Интернете или в локальной сети) компьютеры группы А будут полностью защищены от атак из Интернет через компьютеры группы Б.

Для реализации технологии выхода в «Открытый Интернет» необходимо произвести следующие действия:
установить ПО ViPNet «Координатор» с функцией ViPNet–Сервер Открытого Интернета (такая функция координатора задается в ЦУСе) на компьютер, размещенный на границе локальной сети с Интернет. Назовем этот компьютер (с ПО ViPNet) Координатором Открытого Интернета;
на этом же компьютере (Координатор Открытого Интернета) также должен быть установлен Firewall типа WinProxy, WinGate, MSProxy и т.д. для организации доступа к ресурсам открытого Интернета от имени своего IP-адреса для компьютеров группы Б;
установить на компьютеры локальной сети ПО ViPNet «Клиент». Каждый компьютер группы Б должен быть связан с Координатором Открытого Интернета (такая связь задается в ЦУСе). Для компьютера группы А такая связь не обеспечивается.



Координатор Открытого Интернета выполняет следующие функции:
Организовывает доступ к ресурсам открытого Интернета от имени своего IP-адреса для компьютеров группы Б, за счет установленного на этом же компьютере Firewall;
Запрещает доступ к ресурсам открытого Интернета для компьютеров группы А;
Организовывает защищенный туннель между собой и компьютером группы Б на время его работы с ресурсами открытого Интернета без возможности доступа к этому туннелю со стороны всех остальных пользователей локальной сети;
является «Межсетевым Экраном», который запрещает доступ в локальную сеть из открытого Интернета.

При этом на компьютерах группы Б в процессе работы с Координатором Открытого Интернета блокируется любой трафик (открытый и закрытый), кроме трафика с открытым Интернетом. И, наоборот, при работе с ресурсами локальной сети – блокируется любая работа с Координатором Открытого Интернета.

Такая технология гарантирует, что никакие стратегии атак как снаружи, так и изнутри сети не могут привести к нарушению безопасности компьютеров сети, подключение которых к Интернет запрещено (компьютеры группы А). На такие компьютеры, при любых атаках трафик из Интернет может попасть только в зашифрованном виде, что не будет воспринято компьютером, и в связи с этим не опасно. Попытки проведения атак на сеть через компьютеры группы Б невозможны, так как блокируется посторонний трафик от них, кроме трафика с Координатором Открытого Интернета.

Одновременно исключаются любые возможности несанкционированного подключения из локальной сети к Интернет.

Если требуется не только обеспечить возможность подключения к открытому Интернету заданных компьютеров локальной сети, но и одновременно обеспечить возможность подключения локальной сети к Интернету для защищенного обмена с другими локальными сетями (с ПО ViPNet) и защищенными мобильными компьютерами, то в этом случае на границе сети необходим еще один ViPNet «Координатор» с двумя и более сетевыми интерфейсами. В этом случае в ЦУСе задаются необходимые логические связи для разделения информационных потоков.

Функция трансляции IP-адресов (NAT)

ViPNet Coordinator поддерживает технологию трансляции сетевых адресов (NAT – Network Address Translation).

Трансляция сетевых адресов (NAT) – это технология, позволяющая преобразовывать IP-адреса, использующиеся в одной сети в адреса, использующиеся в другой.

NAT обычно применяется для решения двух основных задач:
При необходимости подключения локальной сети к Интернет, когда количество узлов локальной сети превышает выданное поставщиком услуг Интернет количество публичных IP-адресов. Таким образом, NAT позволяет локальным сетям, использующим частные адреса, получать доступ к ресурсам Интернет.

Для сокрытия внутренней структуры локальной сети. В результате применения технологии NAT, локальные сети, имеющие частные адреса, могут работать с Интернетом, при помощи трансляции своих частных адресов в адреса, допустимые в Интернете (публичные), и при этом выглядеть снаружи так, как будто они используют адресное пространство, отличное от пространства, используемого на самом деле. Таким образом, не имея информации о закрытом адресном пространстве локальной сети, становится практически невозможным напрямую атаковать тот или иной узел локальной сети.

Функции NAT конфигурируются на компьютере, разграничивающем локальную (внутреннюю) сеть и глобальную (внешнюю) сеть (например, Интернет). Компьютер должен иметь, как минимум два сетевых интерфейса, один из которых обеспечивает доступ в

Интернет и имеет публичный IP-адрес, назовем этот интерфейс внешним. Остальным сетевым интерфейсам (внутренним) могут быть присвоены любые адреса (как частные, так и публичные). При прохождении сетевых пакетов через компьютер с функциями NAT, с внутреннего интерфейса на внешний, а затем обратно, происходит трансляция сетевых адресов (NAT).

В ПО ViPNet Coordinator трансляция адресов выполняется для любых IP-протоколов. Однако для всех протоколов кроме TCP, UDP и ICMP выполняется частичная трансляция.

ПО ViPNet Coordinator может производить трансляцию двух типов – статическую трансляцию и динамическую трансляцию (или точнее разновидность динамической трансляции, известной под названием "Masquerading"):

Статическая трансляция адресов устанавливает соответствие адресов по типу «один к одному», т.е. один глобальный (публичный) адрес маршрутизатора соответствует одному частному адресу внутренней сети. Статическая трансляция применяется в тех случаях, когда некий внутренний узел должен быть доступен извне по постоянному адресу (например, сервер www).

Динамическая трансляция адресов устанавливает соответствие между несколькими частными адресами внутренней сети и одним публичным адресом маршрутизатора путем присвоения уникальных дополнительных параметров (например, портов). Данная разновидность NAT, как правило, используется для предоставления доступа компьютеров из локальной сети с частными адресами к сети Интернет через маршрутизатор, имеющий всего один публичный адрес, т.к. позволяет в такой ситуации задействовать этот публичный IP-адрес одновременно для нескольких сетевых компонентов локальной сети.

Статическая и динамическая трансляция адресов производится только при настройках соответствующих правил трансляции на ViPNet-координаторе.

Для обеспечения возможности работы FTP-клиентов в активном режиме, ViPNet Coordinator производит также трансляцию сетевых адресов на прикладном уровне для протокола FTP в автоматическом режиме, без каких-либо настроек правил трансляции.

ViPNet «Клиент»

ViPNet «Клиент» - модуль, реализующий на рабочем месте следующие функции:

1. Персональный сетевой экран - позволяет защитить компьютер от попыток несанкционированного доступа, как из глобальной, так и из локальной сети.

Персональный сетевой экран позволяет системному администратору или пользователю (при наличии присвоенных ему полномочий):

Управлять доступом к данным компьютера из локальной или глобальной сети;

Определять адреса злоумышленников, пытающихся получить доступ к информации на Вашем компьютере;

Обеспечивать режим установления соединений с другими открытыми узлами локальной или глобальной сети только по инициативе пользователя, при этом компьютер пользователя остается «невидимым» для открытых узлов локальной и глобальной сетей (технология Stealth), что исключает возможность запуска по инициативе извне всевозможных программ «шпионов»;

Формировать «черные» и «белые» списки узлов открытой сети, соединение с которыми соответственно «запрещено» или «разрешено»;

Осуществлять фильтрацию трафика по типам сервисов и протоколов для данного адреса открытой сети или диапазона адресов, что позволяет, в случае необходимости, ограничить использование «опасных» сервисов на «сомнительных» узлах открытой сети; осуществлять фильтрацию трафика по типам сервисов и протоколов для связанных с данным узлом других защищенных узлов.

Контролировать активность сетевых приложений на данном компьютере, где установлен ViPNet [Клиент], что позволяет вовремя обнаружить и заблокировать активность несанкционированно установленных и запущенных программ «шпионов», которые могут передавать злоумышленникам сведения об информации, обрабатываемой на данном компьютере (пароли доступа, данные о кредитных картах, идентификаторы для доступа в корпоративные базы данных и др.)

Установление защищенных соединений между компьютерами, оснащенными ViPNet [Клиент], для любых стандартных сетевых приложений.

Для любых сетевых приложений обеспечиваются следующие основные функции:

Шифрование IP-пакетов с добавлением в них информации для обеспечения целостности, контроля времени, идентификации (авторизации) и скрытия первоначальной структуры пакета;

Блокировка шифрованных пакетов при нарушении их целостности, превышении допустимой разницы между временем отправки и текущим временем (защита от переповторов) или при невозможности аутентифицировать пакет;

Предоставление COM интерфейса для вызова криптографических функций и их использования Web приложениями.

Возможность установления защищенных соединений между компьютерами, оснащенными ViPNet [Клиент] позволяет:

Организовать схему защищенного использования всевозможных Web-приложений, в том числе Web-trading, Web-ordering, Web-хостинга, Web-вещания и т.д., с доступом к Web-платформе, на которой установлен ViPNet [Клиент], только определенному списку участников VPN. Данная схема обеспечивает пользователям и корпорации гибкое и безопасное использование всевозможных Web-приложений как наиболее простого и доступного средства коллективной работы корпорации и ее партнеров;

Защитить и дополнительно авторизовать все соединения между локальными, мобильными и удаленными пользователями, оснащенными ViPNet [Клиентом], и корпоративными серверами приложений, баз данных, SQL-серверами, также оснащенными ViPNet [Клиентом]. Это открывает широкие возможности по безопасному внедрению всевозможных ERP-систем, финансово-учетных систем, работающих в реальном времени, систем типа «Клиент-Банк», «Интернет-Банкинг», CRM (Customer Relationship Management) систем и прочих систем, где с одной стороны накапливается конфиденциальная информация, требующая соблюдения правил информационной безопасности и управления доступом, а с другой стороны необходима коллективная работа с приложениями на сети разных категорий пользователей;

Использовать недорогие и общедоступные сетевые ресурсы открытой сети для передачи конфиденциальной информации.

Услуги защищенных служб реального времени для организации обмена сообщениями, проведения конференций, защищенных аудио- и видео-переговоров позволяют:

Обмениваться сообщениями или организовывать циркулярный обмен сообщениями, в процессе которого организатор такого обмена видит все сообщения, в то же время участники обмена сообщений друг друга не видят. При этом ведутся и могут быть сохранены протоколы всех сообщений;

Проводить защищенные конференции;

Оперативно видеть подтверждения доставки и прочтения сообщений;

Проводить защищенные аудио- (Voice over IP) и видео-переговоры (конференции)

При этом, технология ViPNet поддерживает любые стандартные программные и аппаратные средства для проведения аудио- и видео-конференций, основанные на IP-технологиях.

Сервис защищенных почтовых услуг – защищенный почтовый клиент с возможностями аутентификации отправителя и получателя, а также обеспечивающий контроль за прохождением и использованием документов.

Деловая почта - модуль, входящий в состав ViPNet [Клиент], позволяет:
Передавать электронные сообщения по открытым каналам связи с защитой на всем маршруте следования от отправителя до получателя, при этом в качестве открытого канала могут быть использованы стандартные сервера SMTP/POP3;
Одновременно с самим сообщением защитить прикрепленные к нему файлы;
Организовать по установленным правилам защищенный автопроцессинг стандартных документов, «рождаемых» другими приложениями и системами управления бизнесом (бухгалтерскими, банковскими, управленческими и пр.);
Осуществлять поиск документа в почтовой базе документов по множеству параметров (отправитель, получатель, тема, дата, период, контекст и т.п.);
Подтверждать личность отправителя, используя ЭЦП, встроенную в общую систему безопасности;
Передать сообщение только тем получателям, для которых оно предназначалось, а также при необходимости автоматически отправить копии сообщений на заданные в ЦУС узлы;
Подтвердить получение и использование сообщений, а также дату, время получения и личности получателей;
Вести учетную нумерацию сообщений
Кроме вышеперечисленных функций ViPNet «Клиент» предоставляет COM интерфейс для вызова криптофункций и их совместного использования с Web приложениями.

Логика обработки IP-трафика

Основным программным модулем для построения виртуальной сети является ViPNet-драйвер. Драйвер работает на уровне IP-пакетов, до того, как они передаются стандартному стеку TCP/IP, поэтому он контролирует весь IP-трафик, поступающий в сеть и из сети, и обеспечивает защиту для любых приложений не меняя их привычного использования пользователями. Это позволяет внедрять ViPNet как систему информационной безопасности без «насилия» над принятыми в корпорации бизнес-процессами и приложениями, поддерживающими эти бизнес-процессы, начиная от простейших Web-приложений и кончая сложнейшими ERP-системами.

Основными функциями ViPNet драйвера является принятие решения по каждому отправляемому или получаемому IP-пакету.
Для каждого отправляемого IP-пакета (Рисунок 217) осуществляется одно из трех действий: пропустить в незащищенном виде, не пропускать вообще, зашифровать и отправить в зашифрованном виде.

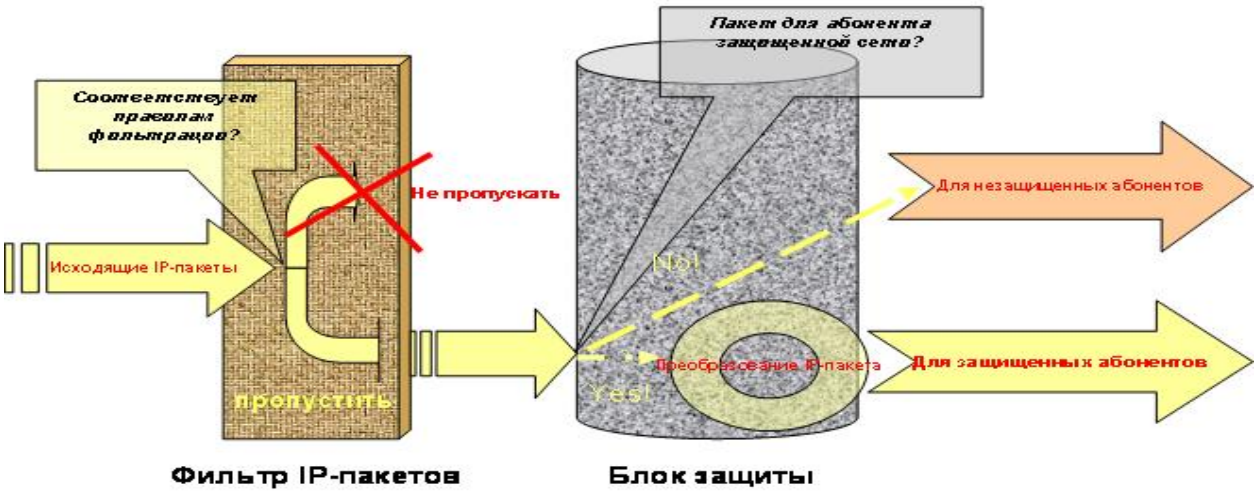


Рис. 17. Обработка исходящих IP-пакетов

Для каждого получаемого IP-пакета осуществляется одно из трех действий: пропустить в незащищенном виде (если пакет незашифрован), не пропускать вообще, расшифровать (если пакет зашифрован) и передать приложению в открытом виде.

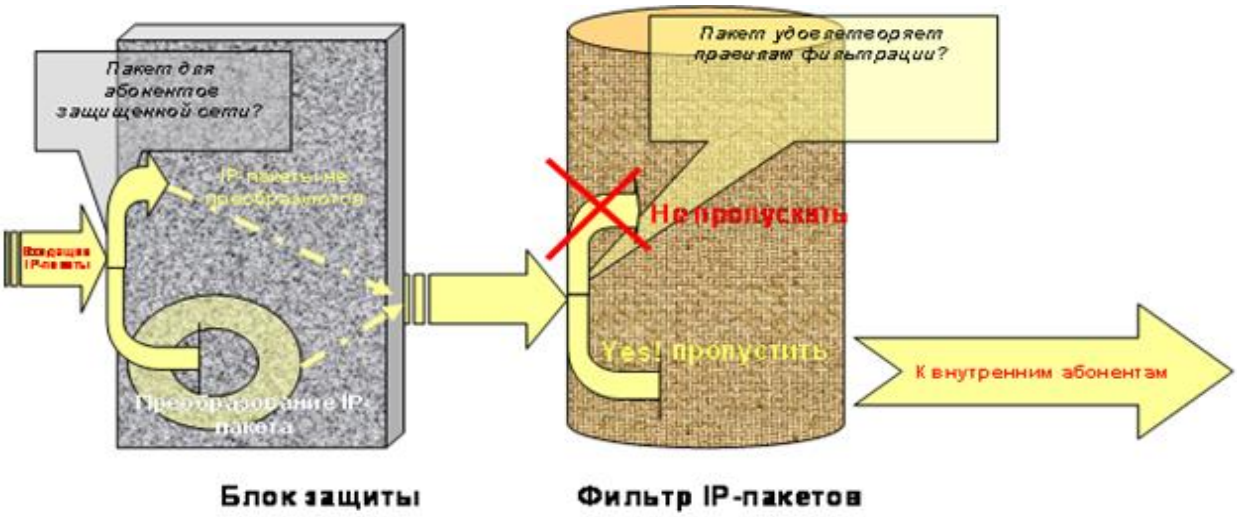


Рис.18. Обработка входящих IP-пакетов

Производительность работы Драйвера защиты трафика (для компьютеров класса P4) составляет ~ 50 Мбит/сек.

Режимы работы ViPNet-драйвера

ViPNet-драйвер может работать в одном из следующих режимов:

«Блокировать открытый IP-трафик».

С компьютерами VPN-сети разрешена шифрованная связь.

С открытыми ресурсами связь блокируется.

«Разрешить зарегистрированный открытый IP- трафик».

С компьютерами VPN-сети разрешена шифрованная связь.

Компьютер защищенной сети, может устанавливать открытые соединения с компьютерами или устройствами, в VPN-сеть не входящими, зарегистрировав их IP-адреса.

«Бумеранг (Разрешить инициативные открытые соединения)».

С компьютерами VPN-сети разрешена шифрованная связь.

В то же время этот режим используется для безопасной работы с открытыми ресурсами сети Интернет. Его суть заключается в том, что открытые соединения допускаются только в тех случаях, когда защищенный компьютер инициирует эти соединения.

Есть «Жесткий Бумеранг» и «Мягкий Бумеранг».

«Жесткий Бумеранг» - это режим Бумеранга, в котором анализ поступающей во время соединения информации производится по большому числу параметров (адрес, протокол, порт).

«Мягкий бумеранг» - анализ поступающей во время соединения информации производится по меньшему числу параметров (адрес, протокол).

В жестком режиме не удастся работать с теми прикладными протоколами, которые пытаются передавать ответную информацию не по тому порту, который был открыт для исходящего трафика. Если есть необходимость работы по таким протоколам, то следует перейти в мягкий режим. Исключение составляют протокол FTP, для которого выполняется специальная обработка в режиме жесткого бумеранга.

В случае работы с протоколом FTP в активном режиме (режиме, в котором FTP-сервер открывает соединение с клиентом) при прохождении команды PORT создается специальный частный фильтр, пропускающий TCP-соединение от FTP-сервера на локальную машину по соответствующим портам. Этот фильтр не отображается для пользователей.
«Не блокировать открытый IP-трафик».
С компьютерами VPN-сети разрешена шифрованная связь.
Со всеми открытыми ресурсам устанавливаются открытые соединения.
«Отключить драйвер» - работа в открытом режиме со всеми существующими ресурсами.

Фильтрация: критерии и правила

Критерии фильтрации - параметры, атрибуты, характеристики, на основе которых осуществляется разрешение или запрещение дальнейшей передачи пакета (данных) в соответствии с заданными правилами разграничения доступа (правилами фильтрации). В качестве таких параметров могут использоваться служебные поля пакетов (данных), содержащие сетевые адреса, идентификаторы, адреса интерфейсов, портов и другие значимые данные, а также внешние характеристики, например, временные, частотные характеристики, объем данных и т.п.
Правила фильтрации - перечень условий, по которым с использованием заданных критериев фильтрации осуществляется разрешение или запрещение дальнейшей передачи пакетов (данных) и перечень действий, производимых МЭ по регистрации и/или осуществлению дополнительных защитных функций.

Правила фильтрации IP-трафика являются результатом действия выбранного режима безопасности и заданных пользователем списка фильтров для конкретных IP-адресов, протоколов и портов. Список сетевых фильтров задается пользователем в виде древовидной структуры отдельно для Защищенной сети и Открытой сети. Это дерево фильтров позволяет задавать фильтры, как на отдельный IP-адрес, так и на диапазон IP-адресов (первый уровень). Далее могут быть определены фильтры на типы протоколов, направление установления соединения (прохождения IP-пакетов) и номера портов (второй уровень). Настройку правил фильтрации открытого IP-трафика (в окне Открытая сеть) всегда следует начинать с выбора режима безопасности, а затем при необходимости уточнять его заданием сетевых фильтров.

Виды фильтров.

Ряд фильтров в ПО ViPNet «Клиент»-«Монитор» определен по умолчанию. Эти фильтры нельзя удалять, но при определенных полномочиях их можно менять: инвертировать, а также добавлять, удалять и модифицировать фильтры протоколов. Различают следующие виды фильтров:
Широковещательный фильтр
Главный фильтр
Индивидуальный фильтр (фильтр для конкретного пользователя)
Фильтр протоколов – определяет правило фильтрации пакетов в зависимости от протокола, параметров протокола, адресата пакета и направления прохождения IP-пакета, может быть настроен для широковещательного, главного и индивидуального фильтров. Фильтр протоколов всегда подчинен какому-либо фильтру из указанных выше.
Microsoft SQL фильтр - может быть использован при установке ViPNet [Клиент] на Microsoft SQL сервер с целью ограничения доступа пользователей (с установленным ПО ViPNet) на SQL сервер, либо для предотвращения прихода нежелательных данных. Фильтр работает на уровне протокола TDS (протокол передачи данных для MS SQL). Microsoft SQL фильтр всегда подчинен какому-либо индивидуальному фильтру.

Туннелирование (инкапсуляция) и маршрутизация шифрованных пакетов, структура инкапсулированного IP-пакета

Для выполнения процедур преобразования IP-пакетов драйвер должен владеть информацией о ряде параметров взаимодействующих с данным узлом других узлов (идентификаторы, номера ключей, IP-адреса, порты и др.) Регистрация драйвером параметров о чужих узлах осуществляется:

при загрузке данных Монитором, которые он получил по технологии оповещения от соответствующего сервера IP-адресов, или из ЦУСа, или сохраненные от драйвера в предыдущем сеансе загрузки монитора,

путем регистрации драйвером информации из поступивших входящих пакетов, адресованных данному узлу.

Монитор может загрузить драйверу информацию об узлах, с которыми данный узел и не имеет связи. О таких узлах грузится вся информация за исключением ключей. На координаторах – это информация об абонентских пунктах, а также координаторах, за которыми стоят другие узлы. На абонентских пунктах это информация только о координаторах, за которыми стоят другие узлы. Данная информация может быть получена Монитором только от сервера IP-адресов и необходима для обеспечения маршрутизации пакета.

Драйвер узла по всем зашифрованным входящим UDP/2046 пакетам, предназначенным данному узлу, а также по бродкастам UDP/2048 и 2050 (это служебные пакеты, формируемые монитором, внутрь тела инкапсулированного ViPNet-пакета которых драйвер вставляет всю необходимую информацию), а в некоторых случаях по внешним параметрам любых пакетов (Source IP-адрес и Source порт ViPNet-пакета) на каждом из интерфейсов осуществляет регистрацию списков адресов узла другого узла и параметров доступа к нему через внешние устройства (NATSETTING). При наличии отличий драйвер формирует события 42 или 46 и передает новые зарегистрированные параметры монитору.

При регистрации параметров определяет также тип протокола, который он должен использовать для инкапсуляции и тип адреса видимости узла (реальный или виртуальный).

Вся полученная информация драйвером хранится в соответствующей таблице для каждого идентификатора узла. А также передается для хранения и монитору.

Кроме того, драйвер формирует специальную ХЭШ таблицу: IP-адрес (реальный или виртуальный) – Идентификатор узла, по которой он при получении пакета для отправки в сеть быстро по IP-адресу назначения пакета определяет идентификатор нужного узла, а по нему ключи и всю необходимую информацию для его отправки этому узлу. В аналогичной таблице для каждого идентификатора координатора хранятся туннелируемые этими координаторами IP-адреса, по которым также определяется идентификатор координатора, на ключах связи с которым производится шифрование туннелируемых им пакетов.

Выбор протоколов инкапсуляции, выбор типа адреса видимости узла (реальный или виртуальный)

Драйвер сетевой защиты ViPNet для всех типов исходящих или туннелируемых пакетов, IP-адреса которых сопоставлены для определенного идентификатора, производит упаковку (инкапсуляцию) этих пакетов в другой пакет протокола UDP или IP/241. Протокол UDP драйвер автоматически использует, если считает, что на пути следования IP-пакета присутствуют устройства, осуществляющие преобразование адресов (NAT). В ином случае используется более экономичный с точки зрения добавляемой избыточной информации протокол IP/241, в котором отсутствует UDP-заголовок.

Критериями, по которым драйвер решает, что между данным и некоторым удаленным узлом есть устройство NAT и, соответственно следует использовать UDP-протокол, являются:

наличие у удаленного узла зарегистрированного адреса доступа через некоторое внешнее NAT-устройство (в, том числе, координатор), через который к нему возможен доступ,
сам этот узел установлен за такое устройство.

Исключениями из этих правил являются:
свой собственный внешний адрес доступа и адрес доступа к другому узлу совпадают, то есть оба узла расположены в одной маршрутизируемой сети за одним устройством NAT,
другой узел доступен по широковещательным пакетам, то есть находится в этой же локальной сети.
В этих случаях, а также всех остальных случаях драйвер применяет протокол IP/241.

Как уже указывалось Выше, исходящий пакет от приложения может поступить с реальным или виртуальным адресом назначения. А также при получении входящего пакета драйвер должен подменить IP-адрес источника пакета на адрес, соответствующий адресу видимости.

Реальный адрес автоматически используется, если используется протокол IP-241, а также в случае, если другой узел не имеет никаких внешних адресов доступа. Во всех остальных случаях по умолчанию используется виртуальный адрес, но пользователь может вручную в программе Монитор, управляющей работой драйвера, определить, что следует использовать реальные адреса. И если Монитор не обнаружит конфликтов с имеющимися адресами, то это позволено ему будет сделать.

Протоколирование событий.

Все IP-пакеты, поступившие от внутренних пользователей защищаемой сети, вначале подвергаются фильтрации. Фильтрация IP-пакетов осуществляется в соответствии с установленными настройками. В качестве параметров фильтрации можно задавать IP-адреса, протоколы, порты. Можно запретить прохождение IP-пакетов заданного вида, разрешив все остальные, а можно сделать наоборот, разрешить прохождение пакетов заданного вида, а все остальные не пропускать.

Если пакет не удовлетворяет правилам фильтрации, он отвергается. IP-пакеты, удовлетворяющие правилам фильтрации, обрабатываются блоком криптографической защиты. Он обеспечивает шифрование, имитозащиту и инкапсуляцию в новый IP-пакет, в котором в качестве IP-адреса приемника выступает IP-адрес ViPNet «Координатора»-получателя пакета, а в качестве IP-адреса источника выступает IP-адрес ViPNet «Координатора»-отправителя.

Входящие IP-пакеты от открытых пользователей блоком защиты не обрабатываются и поступают непосредственно в фильтр IP-пакетов. Для пакетов, полученных от абонентов VPN, блок защиты осуществляет их преобразование, после чего пакеты так же поступают в фильтр IP-пакетов. IP-пакеты, удовлетворяющие правилам фильтрации, передаются внутренним абонентам.

Результаты обработки входящих и исходящих IP-пакетов фиксируются в журнале.

Транспортный модуль MFTP

Транспортный модуль предназначен для обеспечения надежной и безопасной передачи транспортных конвертов между узлами сети ViPNet посредством протоколов TCP (этот канал передачи называется MFTP) и SMTP/POP3.

Транспортные конверты для передачи формируются прикладными задачами этой сети, например, Деловой почтой и Центром управления сетью (ЦУС) в подкаталоге OUT рабочего каталога транспортного модуля. Транспортный модуль передает конверты в соответствии с адресами получателей, прописанными в заголовках этих конвертов. Полностью принятые конверты транспортный модуль помещает в подкаталог IN.

При связи по каналу MFTP устанавливается соединение TCP с узлом-получателем конвертов, проводится взаимная аутентификация узлов и осуществляется прием/передача конвертов друг для друга.

При связи по каналу SMTP/POP3 транспортный модуль переадресует конверты для отправки модулю MailTrans, который передает их через сервер SMTP, а также забирает с сервера POP3 конверты, предназначенные для этого узла.

Функциональность транспортного модуля обеспечивается 32-разрядной библиотекой mftpdgx.dll, работающей в среде Win32 (Windows NT/2000/XP). Для выполнения ряда функций (в частности, поиска ключей и IP-адресов, шифрования и передачи по протоколам SMTP/POP3) эта библиотека взаимодействует с другими модулями пакета прикладных программ ViPNet**.** Транспортный модуль вызывается из прикладных задач (mftpdgx.dll), либо может работать отдельно (mftpgx.exe). В любом случае при запуске транспортного модуля в зависимости от тонкой настройки MFTP появится либо внизу экрана в его правом нижнем углу значок «Синий грузовичок» (по умолчанию), либо откроется окно MFTP.

В составе ПО ViPNet «Клиент» транспортный модуль MFTP работает в режиме клиента и передает конверты другим АП напрямую или через свой координатор.

В процессе работы транспортного модуля при появлении в каталоге приема IN почтовых конвертов, имя которых начинается с символа «@», фон значка транспортного модуля краснеет. Кроме того, в этом случае на экран может быть выведено сообщение о приеме новых файлов и воспроизведен звуковой сигнал.

В составе ПО ViPNet «Координатор» транспортный модуль работает в режиме сервера (этот режим распознается по наличию в рабочем каталоге транспортного модуля файла node*.map). В этом случае передача конвертов осуществляется в соответствии с таблицами маршрутизации. В случае, если конверт многоадресный, то он расщепляется на части, соответствующие адресам. При поступлении конверта, в зависимости от настроек, транспортный модуль либо начинает устанавливать соединение своего сервера с другим сервером или своим АП (по умолчанию эта настройка действует при отправке конверта на другой сервер) либо ожидает, когда с ним установит соединение другая сторона (по умолчанию эта настройка работает при наличии конвертов для АП). В программе может быть задан период опроса других объектов независимо от наличия для них конвертов.

При разрывах соединений передача информации всегда продолжается с точки разрыва, что особенно важно как на коммутируемых каналах, так и каналах плохого качества соединений с Интернет-провайдером.

Деловая почта

Программа ViPNet «Деловая почта» предназначена для организации защищенной передачи электронных документов по открытым каналам связи по всему маршруту следования документа от отправителя к получателю в сети ViPNet.

В почтовый защищенный сервис входят следующие услуги, предоставляемые программой:
Отправка и получение писем с прикрепленными к ним вложениями;
Получение подтверждений (квитанций) о доставке и использовании документов;
Шифрование писем и вложений к ним;
Электронная подпись писем и вложений к ним;
Предоставление информации о документе: дате и времени создания и получения документа, размере документа, информации о получателях и отправителях;
Ведение регистрационной нумерации документов.
Кроме того, программа предоставляет гибкие возможности по работе с документами: сортировка документов, архивация документов, поиск нужного документа, автоматическая обработка файлов и входящих писем в соответствии с различными правилами, задаваемыми пользователем (автопроцессинг) и др.

Деловая почта может быть установлена в составе программы ViPNet «Клиент», а также отдельно, как самостоятельная программа.
Адресация в ДП имеет также трехуровневую структуру.

Первый уровень - сетевой и соответствует различным абонентским пунктам. Зашифрованная информация при выборе адресата на этом уровне может быть прочитана всеми абонентами АП – получателя (рис. 19). На абонентском пункте может быть несколько коллективов.

Второй уровень соответствует коллективам абонентского пункта, выбранного на первом уровне, и имеющим различные ключи для шифрования информации. Зашифрованная информация при выборе адресата на этом уровне может быть прочитана всеми абонентами выбранного коллектива АП - получателя. В коллективе может быть несколько абонентов.

Третий уровень соответствует конкретным лицам коллектива, выбранного на втором уровне. Этот уровень называется Абонент. Зашифрованная информация при выборе адресата на этом уровне также может быть прочитана всеми абонентами выбранного коллектива. Этот адрес служит для информации и нигде не используется с точки зрения разграничения доступа.

У пользователя Деловой Почты нет возможности создавать или удалять абонентские пункты, коллективы, пользователей.

В адресном справочнике абонентские пункты обозначены пиктограммой в виде компьютера. Если раскрыть эту пиктограмму, то она раскрывается и показывает все коллективы данного пункта. Если аналогичным образом раскрыть коллектив, то становятся видны все пользователи данного коллектива.

При выборе получателя можно воспользоваться любым уровнем адресации.

Абонентские пункты в адресном справочнике можно группировать. После инсталляции имеется всего одна группа, называемая Адресная книга ИнфоТеКС. В программе имеется возможность создавать новые группы и помещать в них (как копировать, так и перемещать) имеющиеся абонентские пункты.

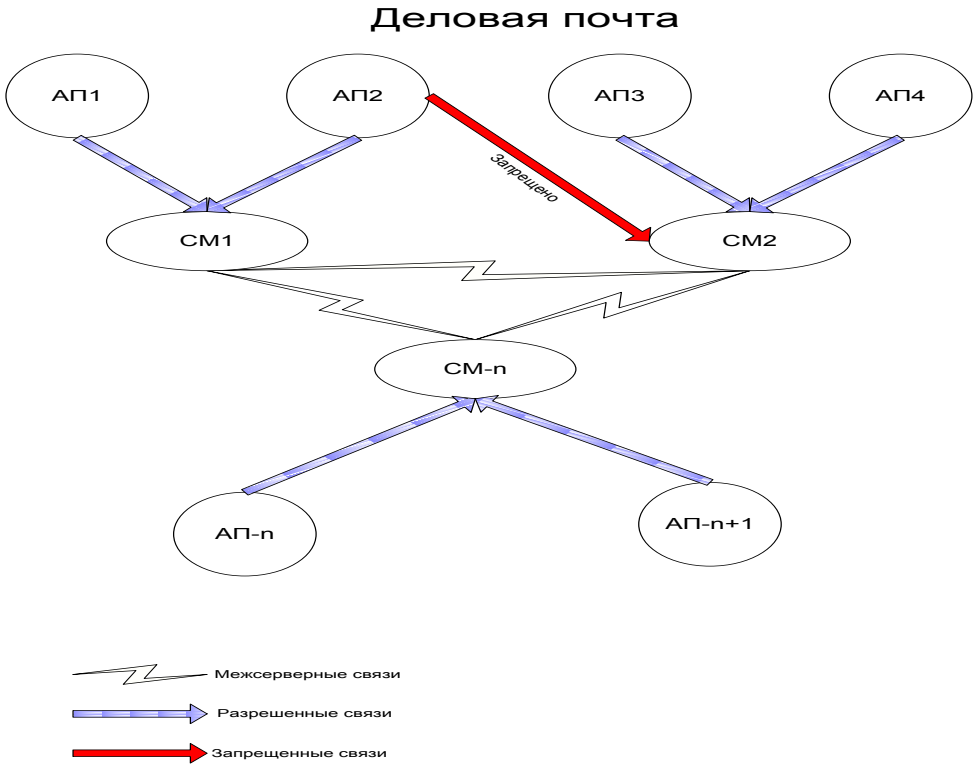


Рис. 19. Связи сетевого уровня, используемые Деловой почтой

Автопроцессинг предназначен для автоматизации работы с входящей корреспонденцией (автопроцессинг писем), а также для автоматической пересылки файлов (файловый автопроцессинг). Письма и файлы, обрабатываемые автоматически, называются объектами автопроцессинга.

Пользователь конфигурирует автопроцессинг, задавая правила (фильтры) автопроцессинга.

Правило (фильтр) автопроцессинга представляет собой совокупность условий и набор действий, автоматически выполняемых над объектами автопроцессинга при выполнении условий.

Правила выделяют из всей корреспонденции (или всего множества файлов) объекты, подлежащие автоматической обработке. Различные условия могут комбинироваться с помощью логических операций И/ИЛИ. Допускается вложенность логических выражений. Отсутствие условий означает выбор всех объектов.

В соответствии с типом обрабатываемых объектов фильтры автопроцессинга разбиваются на две группы: фильтры автопроцессинга входящей корреспонденции; фильтры файлового автопроцессинга.

Каждый из фильтров принадлежит одной и только одной группе. Для каждой группы пользователь задает список фильтров. Любой фильтр может быть в активном (включенном) или неактивном (выключенном) состоянии. Фильтры в каждой группе просматриваются в порядке их расположения в списке.

Правило для обработки файлов означает, что файлы с заданной маской, предварительно положенные пользователем в заданную папку, будут автоматически отправлены Деловой почтой в заданные адреса.

При создании очередного правила программа не допустит повторения имени существующего правила. Кроме того, программа проверяет, нет ли совпадения маски и каталога одновременно для разных правил. Об этом программа выдаст соответствующие сообщения.

Правило для обработки входящих писем означает, что файлы вложений и текст письма, поступившие от заданного отправителя, будут автоматически положены в заданную папку. Файлы вложений в этой папке будут иметь имена, под которыми они были отправлены.

Все события автопроцессинга фиксируются в отдельном журнале (рис. 20).

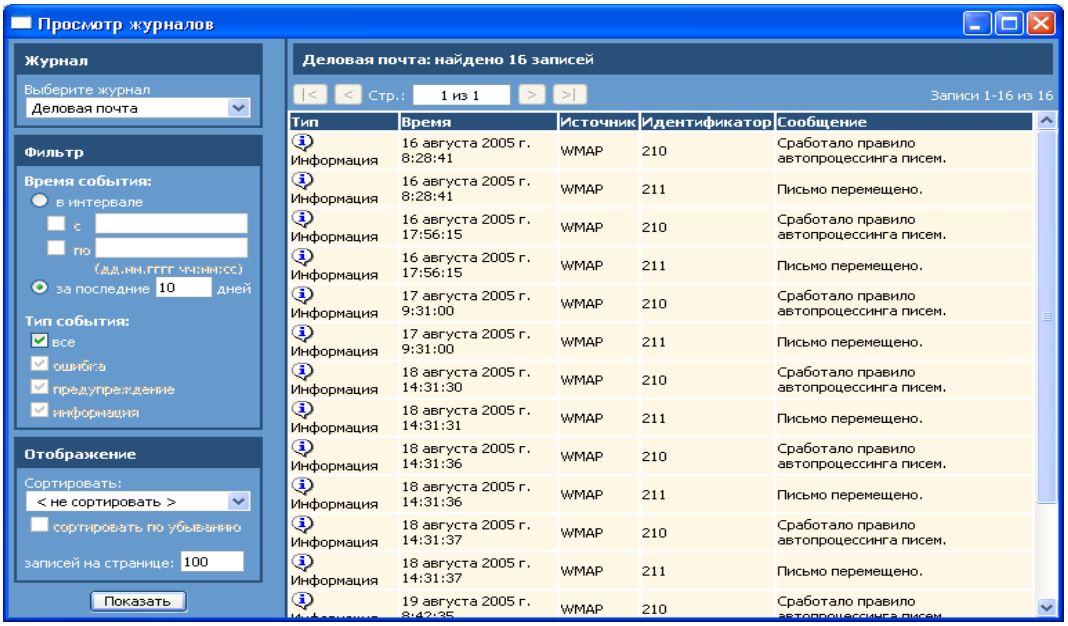


Рис. 20. Просмотр журнала автопроцессинга

Выбор и обоснование структурной схемы сети

Защищенная сеть будет разворачиваться в городе, причем «Администратор», «Координатор» и часть «Клиентов» находятся в
в центральном офисе, а остальная клиентская часть, разбросана по городу (Удаленные пользователи сети). Связь с удаленными пользователями происходит с использованием открытого канала связи (Интернет).

Сеть будет развернута для двух задач:
Защита исходящего и входящего трафика.
Обмен почтовыми сообщениями.

Минимально необходимое программное обеспечение ViPNet Custom для реализации этих задач:
ViPNet «Администратор».
ViPNet «Координатор».
ViPNet «Клиент».

Оборудование которое необходимо для построение этой сети:
Свитч.
Клиентские рабочие станции.
Рабочая станция ViPNet «Администратор».
Рабочая станция ViPNet «Координатор».
Исходя из выше изложенного можно построить структурную схему защищенной сети.

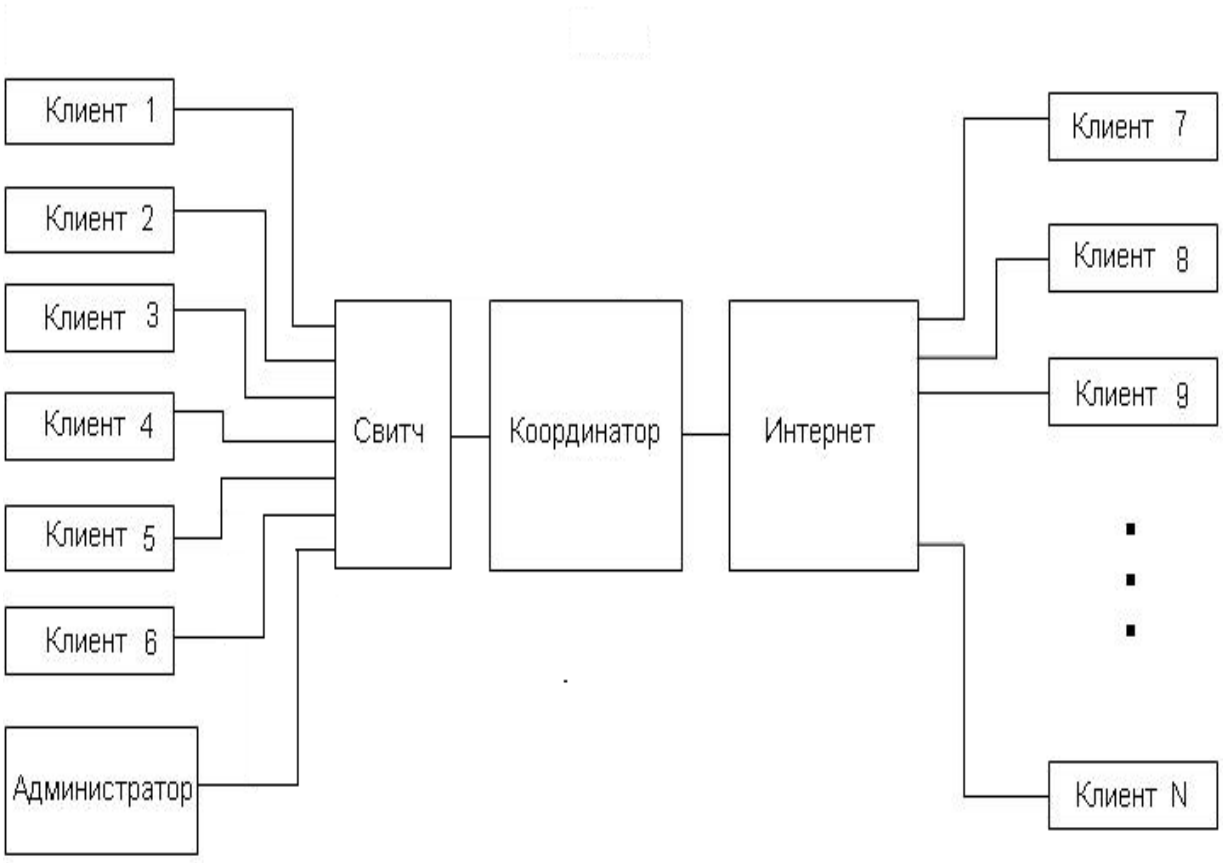


Рис. 21. Структурная схема защищенной сети ViPNet Custom.

Клиентские рабочие станции (Клиент с ПО ViPNet «Клиент») и рабочая станция с ПО ViPNet «Администратор» подключены к свитчу, устройство предназначенное для соединения нескольких узлов компьютерной сети в пределах одного сегмента. Администратор предназначен для конфигурирования и управления виртуальной защищенной сетью ViPNet , выполняет функции центра выработки ключей шифрования и персональных ключей пользователей, а также Удостоверяющего Центра для организации PKI .

Клиентские рабочие станции выполняют функции VPN -клиента, персонального сетевого экрана, надежно защищает рабочую станцию от возможных сетевых атак, как из глобальной, так и из локальной сети. При этом:

Осуществляется фильтрация защищенного и открытого трафиков по множеству параметров («белый» и «черный» списки IP-адресов, порты, протоколы, типы сервисов и приложений);

Реализуется режим «stealth» (режим инициативных соединений), позволяющий сделать невидимым компьютер защищенной сети из открытой сети;

Имеет встроенную систему обнаружения вторжений (IDS);

Обеспечивает мониторинг сетевой активности приложений, позволяющий обнаружить и блокировать несанкционированную активность программ-«троянцев».

Обеспечивает защиту (конфиденциальность, подлинность и целостность) любого вида трафика (приложений, систем управления и служебного трафика ОС), передаваемого между любыми объектами защищенной сети, будь-то рабочие станции, информационные серверы, серверы приложений, сетевые устройства и узлы.

Позволяет пользоваться услугами сервиса обмена защищенными сообщениями и организации чат-конференций между объектами защищенной сети ViPNet , на которых установлены ViPNet Client или ViPNet Coordinator (Windows).

Клиента службы обмена файлами – позволяет обмениваться между объектами защищенной сети ViPNet любыми файлами без установки дополнительного ПО или использования функций ОС по общему доступу к файлам через сеть. Обмен файлами производится через защищенную транспортную сеть ViPNet с гарантированной доставкой и «докачкой» файлов при обрыве связи.

Используется в качестве клиента защищенной почтовой системы.

Координатор выполняет функции:

Сервера IP-адресов — обеспечивает регистрацию и доступ в реальном времени к информации о состоянии объектов защищенной сети и текущем значении их сетевых настроек (IP- адресов и т.п.);

Прокси-сервера защищенных соединений — обеспечивает подключение локальной ViPNet сети к другим аналогичным сетям через публичные сети (Интернет);

Туннельного сервера (криптошлюза) — обеспечивает туннелирование (шифрование) трафика от незащищенных компьютеров и серверов локальной сети для его передачи к другим объектам защищенной сети (в том числе мобильным и удаленным) в зашифрованном виде по открытым каналам публичных сетей. Для мобильных и удаленных объектов защищенной сети туннельный сервер выступает в роли сервера доступа к ресурсам локальной сети;

Межсетевого экрана — обеспечивает в соответствии с заданной политикой безопасности фильтрацию трафика по множеству параметров (порты, протоколы, диапазоны адресов и др.) между сегментами защищенной и открытой сетей.

Сервера защищенной почты — обеспечивает маршрутизацию почтовых сообщений для сервиса ViPNet Business Mail и служебных рассылок в рамках защищенной сети.

Алгоритм шифрования на прикладном и транспортном уровнях.

При отправке письма и документов – вложений для каждого письма - конверта формируется случайный ключ, синхропосылка (SP), на которых осуществляется шифрование), путем выполнении свертки (Хэширование) этой синхропосылки с ключом

обмена с соответствующим узлом и которые вставляются в почтовый конверт и передаются получателю вместе с письмом. Случайный ключ (32 байта) шифруется на результирующем ключе обмена и синхропосылке ключа. Результирующий ключ обмена шифруется на симметричных и асимметричных ключах обмена. Одновременно формируется имитозащитная сигнатура (IM), которая позволяет проконтролировать целостность документа и защитить пользователей от навязывания ложной информации.

При сохранении письма с документами в почтовых папках, если письмо зашифровано, то оно также сохраняется в них в зашифрованном виде. Однако всегда производится перешифрование случайного ключа на ключе обмена с самим собой. При сменах ключей все такие ключи сохраняются в специальном файле в зашифрованном на текущем ключе виде. Это позволяет обеспечить возможность расшифрования старых документов и после многочисленных смен текущих ключей.

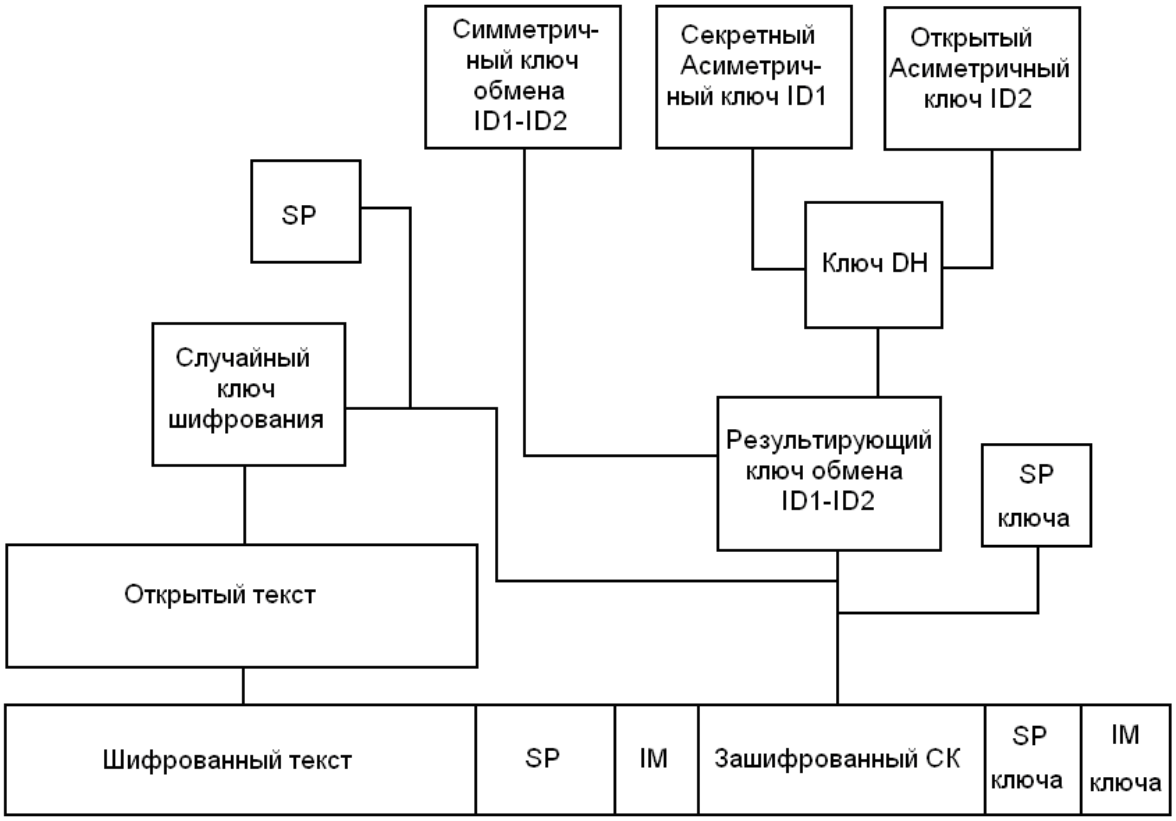


Рис. 22. Алгоритм шифрования на прикладном уровне

При шифровании каждого IP-пакета драйвер вырабатывает случайную синхропосылку (8 байт), выполняет свертку (Хэширование) этой синхропосылки с ключом обмена, получаемым аналогично, что и при шифровании на прикладном уровне, соответствующего узла и полученную последовательность (32 байта) использует в качестве ключа для шифрования IP-пакета.

Для каждого IP-пакета вырабатывается также имитозащитная сигнатура (4 байта), которая вместе с синхропосылкой и зашифрованным IP-пакетом помещается в новый IP-пакет, отправляемый в сеть

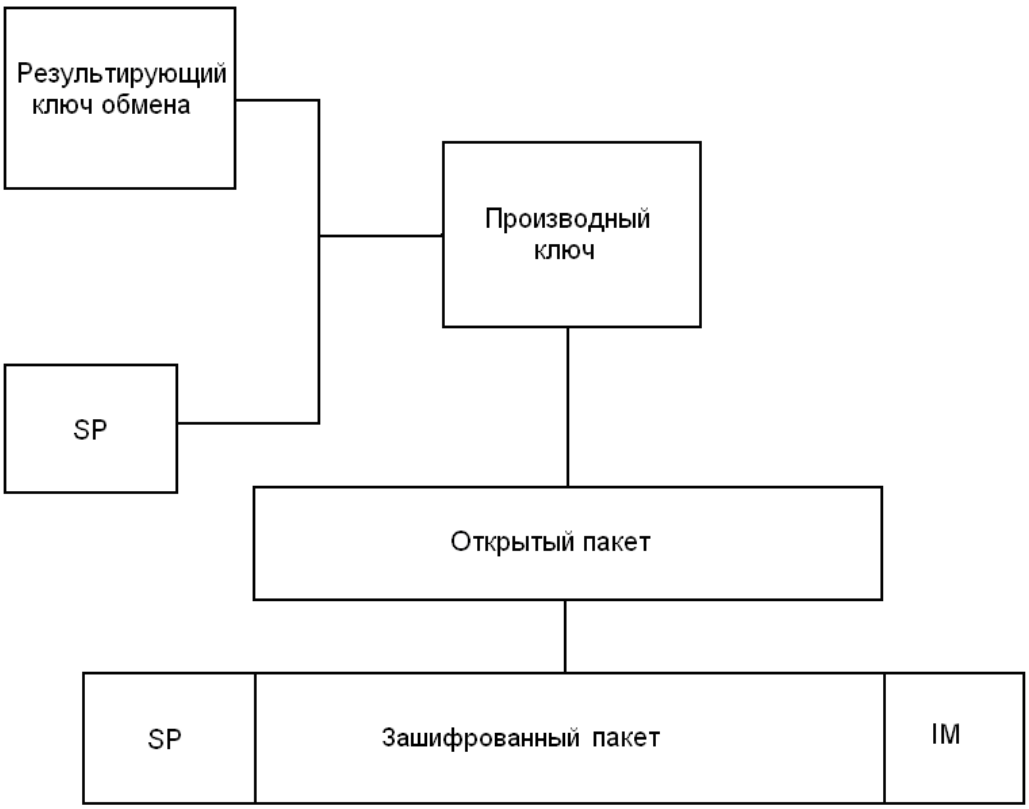


Рис. 23. Шифрование IP-пакета на сетевом уровне.

4. Развертывание и настройка сети ViPNet Custom.

Установка ViPNet «Администратора».

Для установки защищенного рабочего места Администратора сети VPN необходимы следующие составляющие:

ПО ViPNet [Администратор] версии 3.0;

ПО ViPNet [Клиент] версии 3.0;

набор лицензионных файлов ОАО «ИнфоТеКС»:

infotecs.re – лицензионный справочник;

infotecs.reg – файл лицензий на ПО и ПЗ;

Для установки на локальном компьютере ПО ViPNet Administrator необходимо запустить программу Setup.exe, после появления окна (Рис 24.) – нажать кнопку Далее.

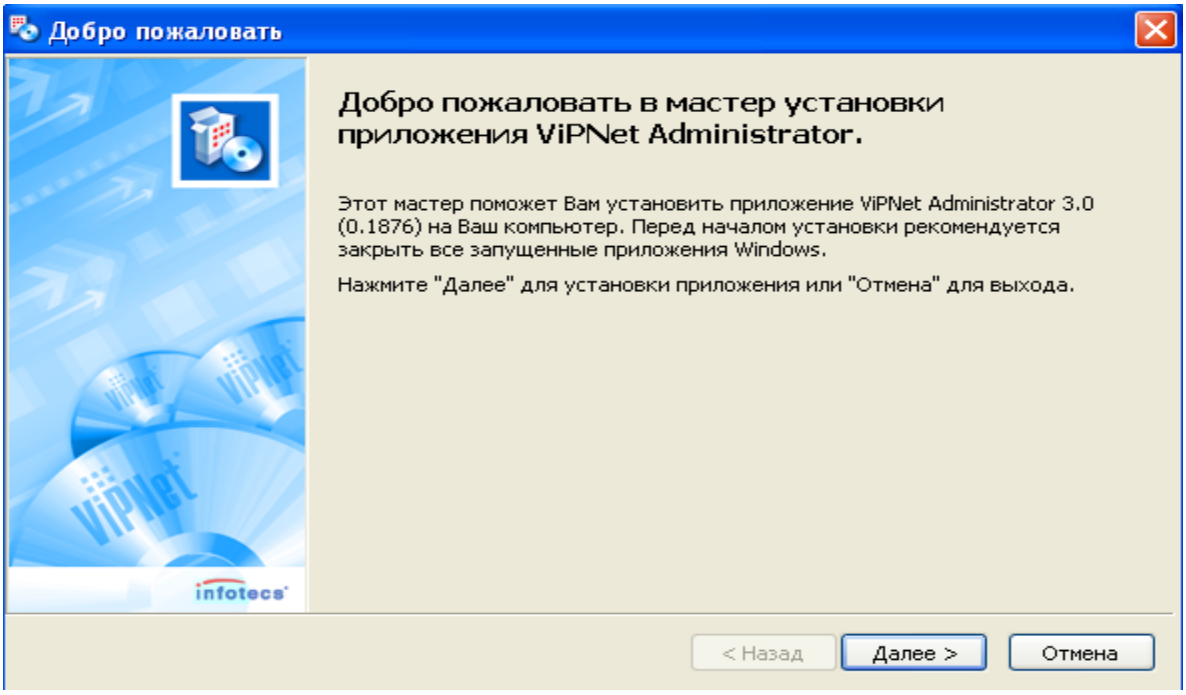


Рис. 24. Мастер установки программы ViPNet «Администратор»

В следующих окнах необходимо ввести имя пользователя и название организации, после чего предлагается указать каталог установки рабочих файлов программы (по умолчанию программу предлагается установить в каталог C:\Program Files\Infotecs\ViPNet Administrator\). В появившемся окне следует выбрать тип установки программы (из каких компонентов будет состоять рабочее ПО) (Рис.25). Поскольку рабочее место Администратора 3 0 будет являться одновременно и центром управления виртуальной сетью и центром обработки ключевой структуры виртуальной сети, необходимо установить оба компонента (Центр управления сетью и Удостоверяющий ключевой центр) на данную машину. Следует выбрать строку «Выборочная установка» и установить «галочки» напротив обеих строк (по умолчанию «галочки» установлены). После выбора необходимых компонентов следует нажать кнопку «Далее». Удостоверившись, что все настройки сделаны правильно, необходимо нажать кнопку «Готово».

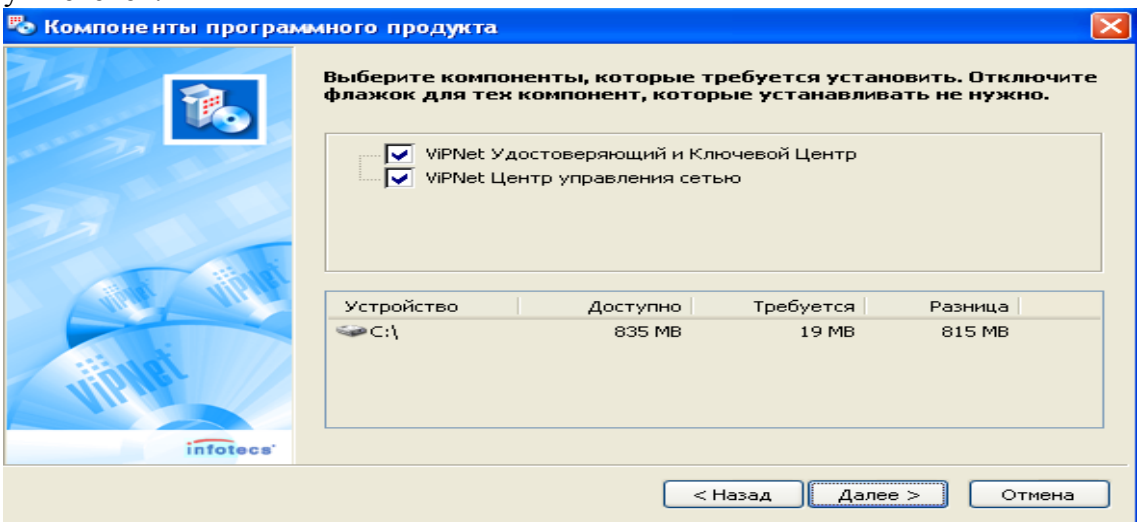


Рис.25. Выбор вида установки программы ViPNet «Администратор»

В следующих окнах вводим имя пользователя и название организации, после чего предлагается указать каталог установки рабочих файлов программы (по умолчанию программу предлагается установить в каталог C:\Program Files\Infotecs\ViPNet Administrator\SS).

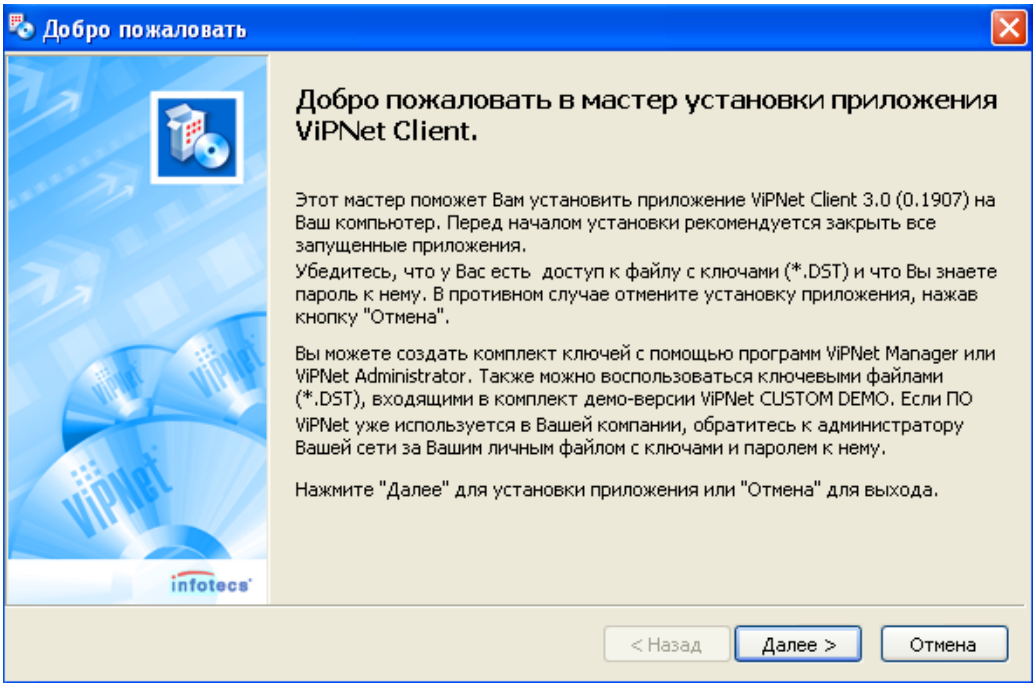


Рис. 26. установки программы ViPNet Клиет

В появившемся окне следует выбрать тип установки программы (из каких компонентов будет состоять рабочее ПО) (Рис.26). Рабочее место Администратора 3.0 должно полнофункциональным, поэтому необходимо установить оба компонента (Монитор и Деловая почта) на данную машину. Следует выбрать строку Выборочная установка и установить «галочки» напротив обеих строк (по умолчанию «галочки» установлены).

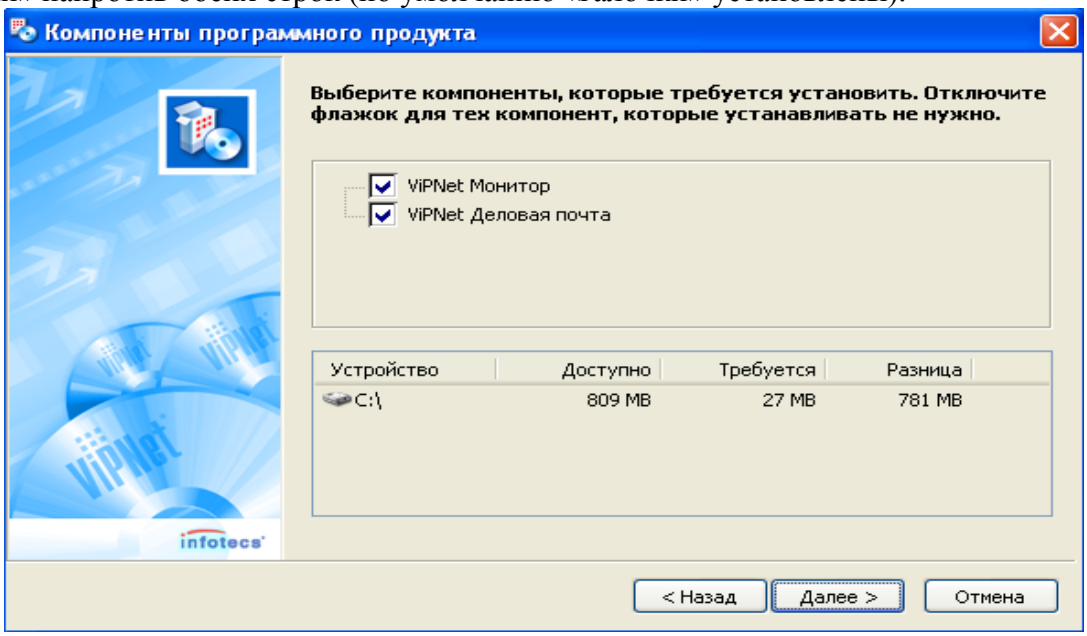


Рис. 27. Выбор вида установки программы ViPNet Client

После выбора необходимых компонентов нажимаем кнопку «Далее». Удостоверившись, что все настройки сделаны правильно, необходимо нажать кнопку «Готово» и подождать, пока программа установки завершит копирование необходимых файлов на жесткий диск компьютера. В результате установки ПО ViPNet «Клиент»будет предложено перегрузить ОС компьютера. Пока это делать нет необходимости (нажать кнопку «Нет»), так как не произведена первоначальная настройка рабочего места администратора защищенной сети.

Для завершения инсталляции рабочего места Администратора защищенной сети необходимо скопировать файлы в указанные папки:
infotecs.reg, infotecs.re и RK.com в каталог ..\NCC\ (каталог установки ЦУСа); infotecs.re – в каталог ..\KC\ (каталог установки УКЦ).

Файлы infotecs.re и infotecs.reg являются наиболее важными файлами с точки зрения защиты авторских прав ОАО «ИнфоТеКС» и прав еѐ клиентов, поэтому следует хранить их отдельно от основного инсталляционного комплекта и не допускать их свободного распространения. Вся ответственность за незаконное распространение файлов лицензий целиком возложено на Клиента ОАО «ИнфоТеКС».

Работа в Адресной администрации ЦУСа.

Создание защищенной сети, установка режимов и параметров работы сети производится в Центре управления сетью (ЦУСе).
Работа с виртуальной сетью ViPNet начинается в Центре управления сетью (ЦУСе). Для загрузки ЦУСа необходимо запустить файл _start.bat, находящийся в рабочем каталоге ЦУСа ..\NCC\

После запуска программа ЦУС, предлагает создать несколько служебных каталогов и запрашивает место, в котором будет храниться информация транспортного каталога и каталогов обмена информацией с УКЦ (Рис.28.). Оставляем каталоги, предложенные программой по умолчанию.

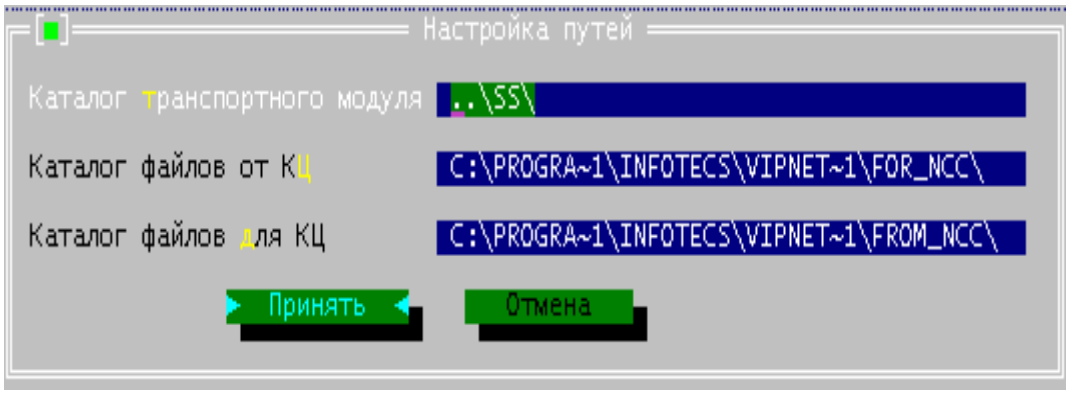


Рис. 28. Настройка по умолчанию для каталогов хранения ключевой информации

При выборе настроек по умолчанию необходимо изменить позиции «Автоматически связывать новый ТК со всеми другими ТК» (поставить крестик напротив этой строки) и указать «Максимальный» уровень полномочий (Рис.28).

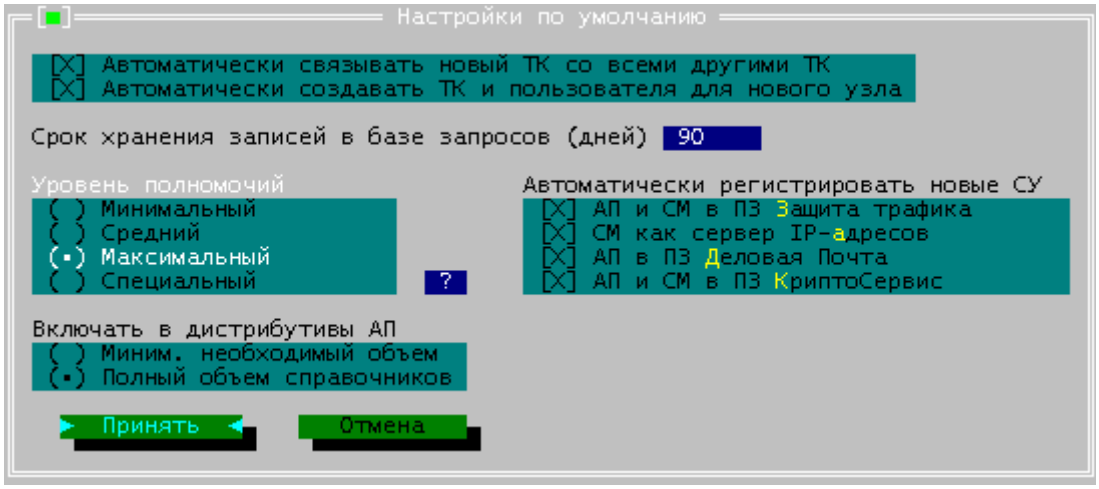


Рис. 29. Настройки по умолчанию параметров работы ЦУСа

После нажатия кнопки «принять» программа ЦУС приветствует администратора сети и предлагает начать с адресной администрации и появляется главное окно Центра управления сетью (Рис.29). Для начала работы по созданию виртуальной сети необходимо выбрать меню «Службы» → «Адресная администрация» → «Структура сети ViPNet»…

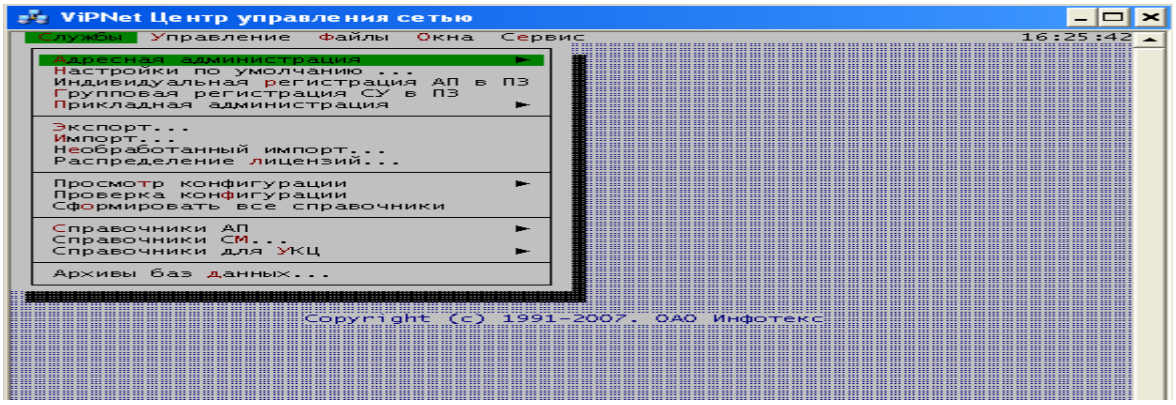


Рис.30. Главное окно Центра управления сетью

Лицензию на виртуальную сеть ViPNet можно посмотреть в меню «Сервис» → «Лицензия»

Для введения в виртуальную сеть серверов-маршрутизаторов (СМ) необходимо выделить строку «Серверы-маршрутизаторы», нажать Enter и ввести имя нового сервера – «СМ Координатор 3 0». Затем в этом же окне необходимо нажать Alt+I для добавления нового СМ –Координатор-ОИ 3 0.

Абонентские пункты должны быть зарегистрированы за «Серверами-маршрутизаторами». За координатором, зарегистрированном в задаче «Открытый Интернет», не должно быть зарегистрировано ни одного АП.

Для добавления в виртуальную сеть Абонентских пунктов (АП) необходимо выделить строку с «СМ Координатор 3.0», за которым будет зарегистрирован новый АП, нажать «Enter» и нажать комбинацию клавиш Alt+I. В предложенной строке следует ввести наименование нового АП «АП Администратор 3.0»

Для создания межсерверных каналов связи, прописываем взаимодействие на защищенном уровне между двумя координаторами сети. Для этого необходимо зайти в меню Серверы-маршрутизаторы и выбрать один из СМ. Для указания начала межсерверного канала следует

нажать комбинацию клавиш Alt+M, после чего слева в данной строке появится «звездочка» со стрелкой. Для указания конца канала выделяем другой координатор и нажать ту же комбинацию клавиш - Alt+M. Теперь программе следует указать, что межсерверный канал будет между СМ Координатор 3.0 и СМ Координатор–ОИ 3.0 – для этого нажимаем комбинацию клавиш Alt+C. В столбце МСК обоих координаторов будет показано количество межсерверных каналов (в данном случае - один). В столбце АП обоих координаторов указано количество сетевых узлов (СУ), которые зарегистрированы за данным СМ (количество АП плюс сам СМ).

Окно регистрации Серверов-маршрутизаторов должно выглядеть так, как показано на Рис.31, а окно регистрации АП за СМ Координатор 3 0 – на Рис.32.

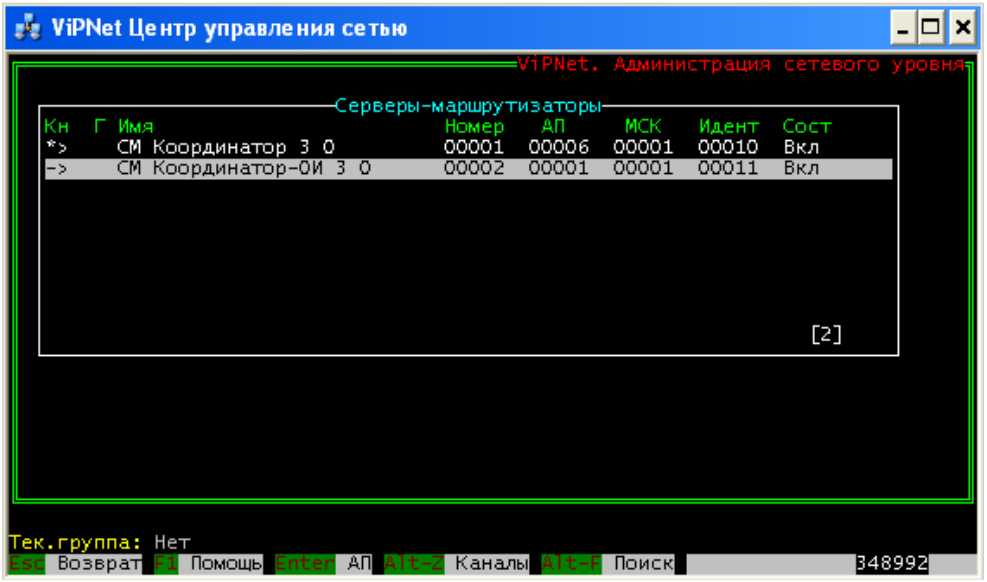


Рис.31. Создание Координаторов сети и указание межсерверного канала

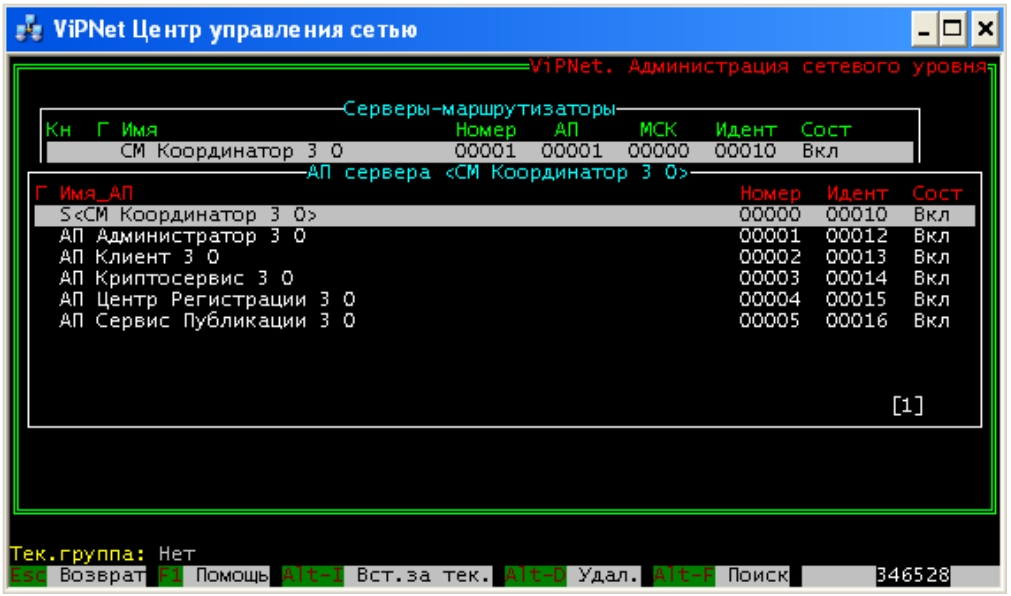


Рис. 32. Регистрация АП за СМ Координатор 3.0

Поскольку работа в Адресной администрации ЦУСа по созданию виртуальной сети завершена, следует выйти в основное окно (Рис.32) и сформировать таблицы маршрутизации (часть справочников ЦУСа). Справа зеленым цветом программа показывает, что в виртуальной сети были произведены изменения и необходимо создание новых таблиц маршрутизации. Для создания новых таблиц необходимо выделить строку Выдать таблицы маршрутизации и нажать Enter, после чего программа подтвердит создание новых таблиц. Теперь работа в Адресной администрации полностью завершена и необходимо выйти в главное меню ЦУСа (либо нажав кнопку Esc либо выделить строку Выход и нажать Enter).

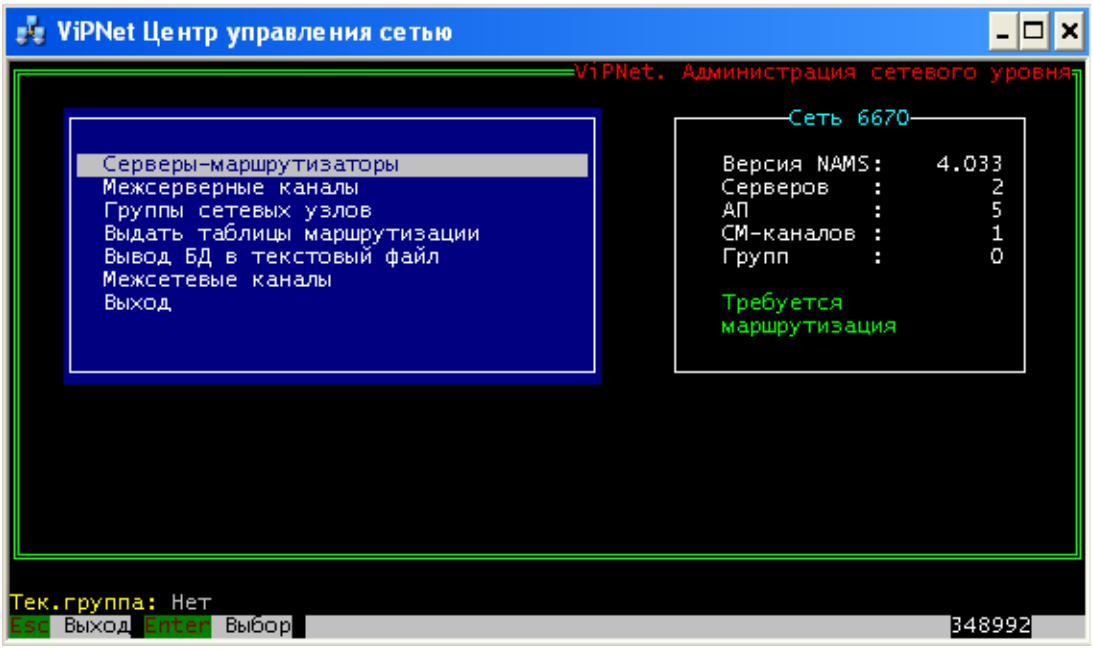


Рис. 33. Основное окно Адресной администрации ЦУСа

Индивидуальная регистрация Абонентских пунктов в Прикладных задачах.

АП Администратор 3.0, АП Центр регистрации 3.0, АП Криптосервис 3.0 необходимо зарегистрировать в прикладных задачах (ПЗ) ЦУС и УКЦ; Центр регистрации; Криптосервис соответственно. Для этого необходимо зайти в меню Службы → Индивидуальная регистрация АП в ПЗ и выделить строку с записью одного из АП, нуждающегося в регистрации. Например, для регистрации АП Администратор 3 0 в задачах ЦУС и УКЦ выделяем строку с записью и нажимаем кнопку «Регистрация». В появившемся окне выделяем «крестиком» строки ЦУС и УКЦ, снять «крестик» с записи Криптосервис (поскольку АП уже зарегистрирован в задаче Защита трафика) и нажимаем кнопку «Принять».

Для АП Центр Регистрации 3 0 необходимо поставить «крестик» в записи Центр регистрации и снять его в записи Криптосервис. Для АП Криптосервис 3 0 необходимо снять «крестики» в записи Деловая почта и оставить в записи Криптосервис. Для АП Клиент 3.0 необходимо снять «крестик» в записи Криптосервис, а для АП Сервис Публикации 3.0 необходимо снять «крестики» в записях Деловая почта и Криптосервис.

В результате указанных действий окно регистрации АП в ПЗ приобретет следующий вид

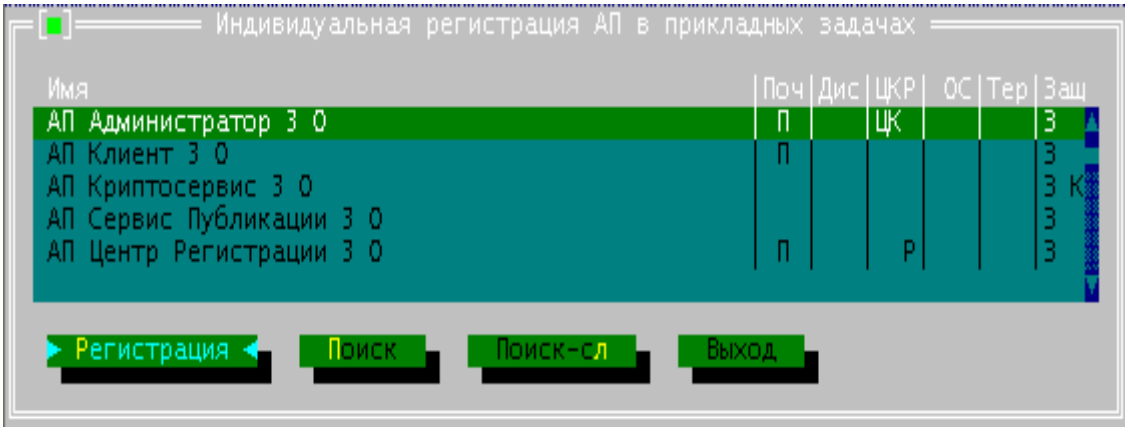


Рис. 34. Регистрация АП в прикладных задачах

Групповая регистрация Сетевых узлов в Прикладных задачах.

Серверы-маршрутизаторы виртуальной сети необходимо зарегистрировать в задаче «Сервер IP-адресов» и ее подзадачах. Для этого заходим в меню «Службы» → «Групповая регистрация СУ» в ПЗ, выделяем строку с записью «Сервер IP-адресов» и нажимаем кнопку «Регистрация». В прикладной задаче «Сервер IP-адресов» для каждого из Координаторов необходимо задать следующие параметры работы (изменение параметров производится посредством кнопок в правом столбце):

1. Для СМ Координатор-ОИ 3 0 включаем функцию «Сервер Открытого Интернета» (Рис.34).
2. Для СМ Координатор 3.0 включаем функцию «Туннелирование» и задаем необходимое количество туннельных соединений (Рис.35).

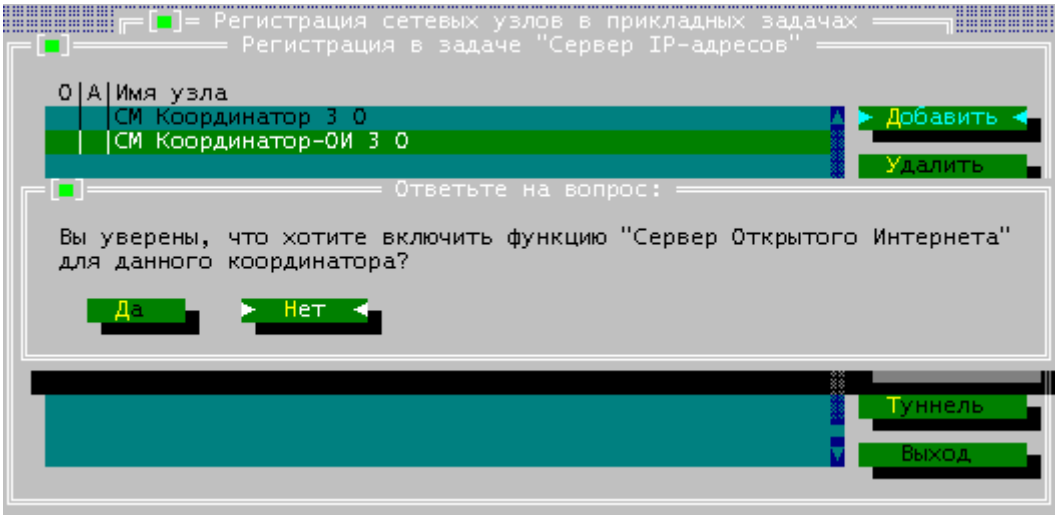


Рис. 35. Включение функции Открытый Интернет

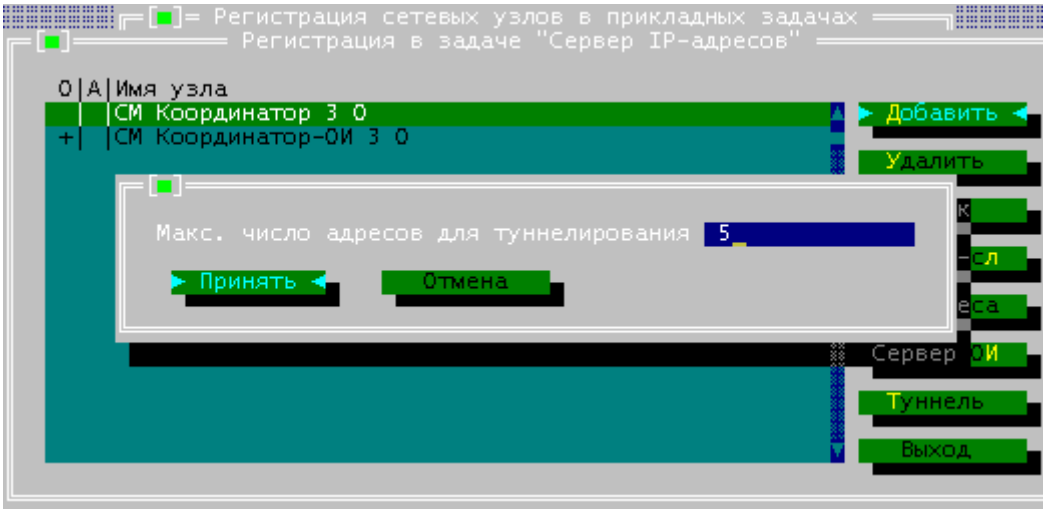


Рис. 36. Включение функции туннелирования

Работа в Прикладной администрации ЦУСа.

В Прикладной администрации при регистрации типов коллективов (ТК) необходимо проверить их связи. При регистрации пользователей необходимо снять право владения ЭЦП у Координаторов сети. Для формирования связей между ТК различных СУ сети ViPNet необходимо зайти в меню «Прикладная администрация» → «Регистрация типов коллективов»… и проверить с помощью кнопки справа Связи, какие связи имеют каждый из ТК сети ViPNet.

Далее, для различия СУ и ТК этих СУ необходимо переименовать записи в меню типов коллективов (с помощью кнопки справа Изм. имя). Например, АП Администратор 3.0 в ТК Администратор 3.0. То же самое сделать для всех записей ТК всех СУ. С помощью кнопки «Область» можно просмотреть, на каком сетевом узле зарегистрирован данный ТК (область действия данного ТК).

После работы с ТК необходимо проверить параметры работы пользователей (абонентов). Для этого необходимо зайти в меню «Прикладная администрация» → «Регистрация пользователей»… В этом окне следует отключить право иметь ЭЦП обоим СМ и переименовать названия пользователей (с помощью кнопки справа Изм. имя), удалив приставки «АП» и «СМ».

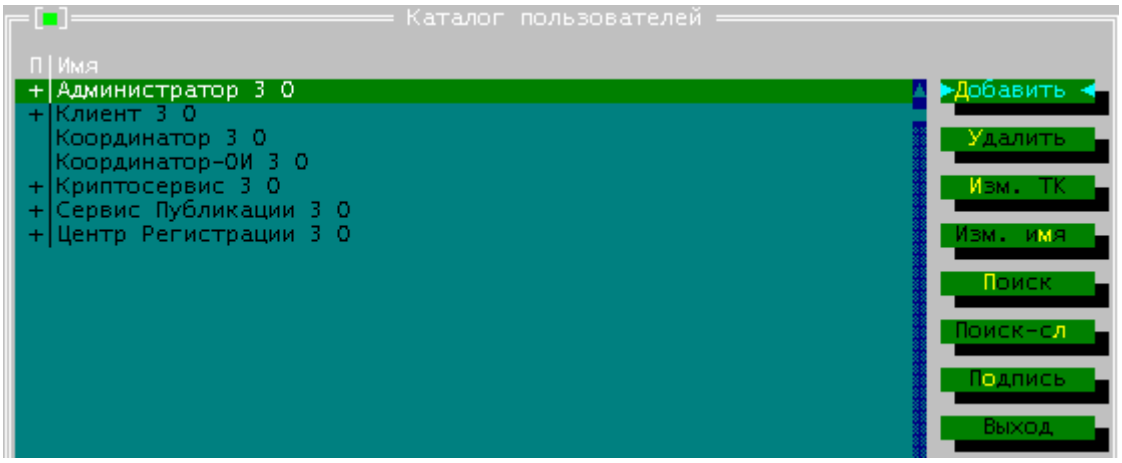


Рис. 37. Окно Регистрация пользователей

Формирование справочной информации и архивов баз данных.

По завершении формирования защищенной сети необходимо создать справочники, в которых отображается информация, необходимая для работы прикладных программ ViPNet (Монитор, Деловая Почта и др.). До формирования справочников необходимо произвести логическую проверку виртуальной сети ViPNet, для чего необходимо выбрать меню «Службы» → «Проверка конфигурации». В случае отсутствия логических ошибок в сети ViPNet (например, пользователь не зарегистрирован ни в одном типе коллектива) программа выдаст окно с записью «Аномальные ситуации не обнаружены». Если же логические ошибки имеют место быть (аномальные ситуации), необходимо произвести оценку этих моментов и принять решение о том, нужно ли продолжать дальше работу с виртуальной сетью.

Если аномальные ситуации не проявились необходимо выбрать меню «Службы» → «Сформировать все справочники». В результате такой операции программа ЦУС сконфигурирует структуру защищенной сети, зафиксирует изменения, которые были введены в сеть и сформирует набор справочников (Рис.38). Изменения, произведенные в ЦУСе, будут переданы в УКЦ для формирования ключевой структуры сети ViPNet. В последующем окне можно будет увидеть, какие справочники и файлы были сформированы.

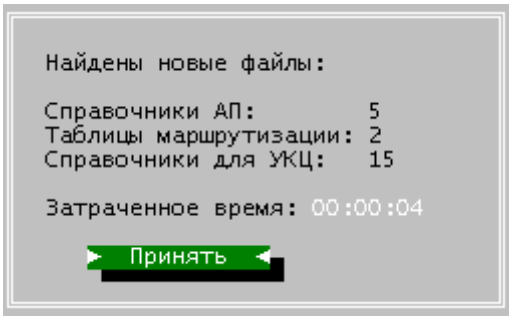


Рис. 38. Формирование справочников

После формирования справочников необходимо создать базы данных, которые будут служить для восстановления информации на определенный момент времени (меню «Службы» → «Архивы баз данных»… → «Создать»). Структуру созданной виртуальной сети можно просмотреть в меню «Службы» → «Просмотр конфигурации» → «Структура сети». В широком формате показана сеть в виде таблицы объектов, в узком – в виде иерархической структуры объектов сети.

Первичная инициализация Удостоверяющего и ключевого центра.

Работа по созданию ключевой инфраструктуры виртуальной сети ViPNet производится в Удостоверяющем и ключевом центре (УКЦ). Для загрузки УКЦ необходимо запустить файл keycenter.exe, находящийся в рабочем каталоге УКЦ ..\КС.

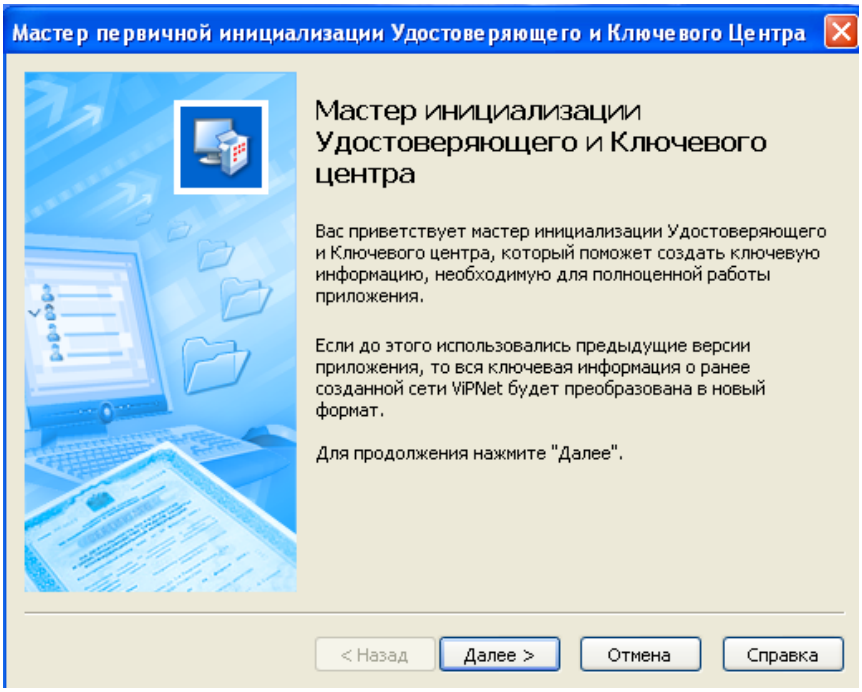


Рис. 39. Начало инициализации УКЦ

Для работы мастера требуется наличие файлов из программы ЦУС. Используя эти файлы, мастер создаст начальную ключевую информацию для работы программы УКЦ. В результате работы Мастера будут созданы:
персональный ключ защиты Администратора;
пароль Администратора;
ключ защиты КЦ;
ключ подписи и сертификат Администратора;
Мастер-ключи:
Мастер-ключ персональных ключей (МКПК),
Мастер-ключ ключей защиты (МККЗ),
Мастер-ключ ключей обмена (МККО).

Мастер инициализации поэтапно предложит ввести параметры работы УКЦ и завершит первоначальную установку УКЦ развертыванием ключевой инфраструктуры защищенной сети. После этого необходимо будет лишь создать саму ключевую информацию, предназначенную пользователям, и передать эту информацию объектам защищенной сети.
Далее мастер предложит выбрать способ взаимодействия с базой данных, в которой будет храниться информация, необходимая для УКЦ. Поскольку УКЦ версии 3.0 использует формат данных в виде базы данных, на компьютере, на котором установлен УКЦ, необходимо иметь одну из систем управления базами данных (СУБД).

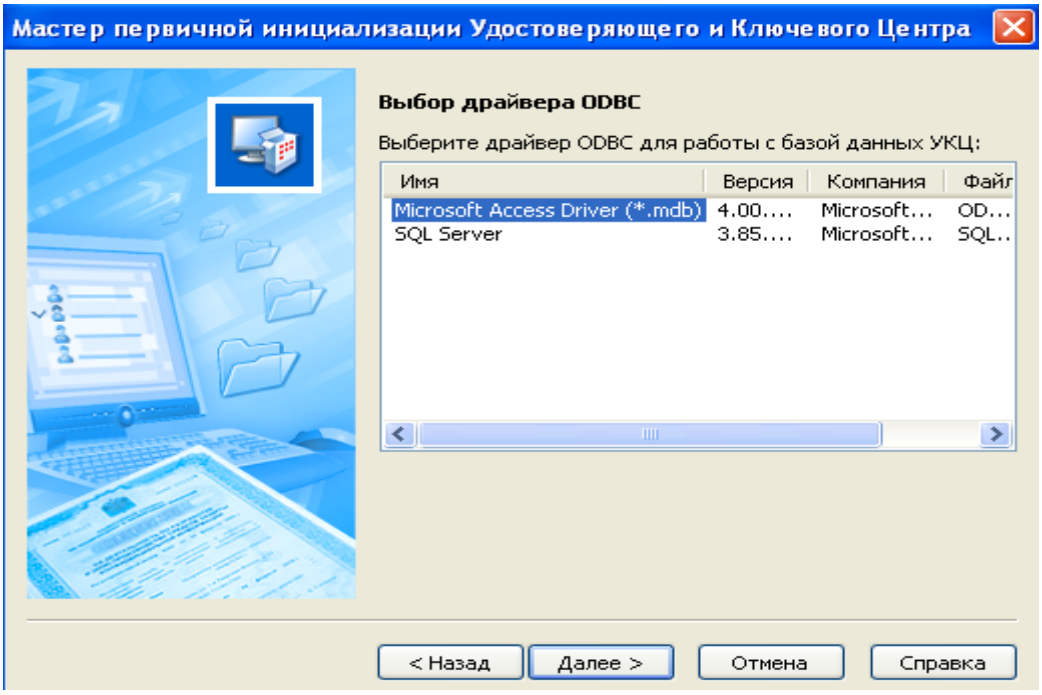


Рис. 40. Выбор базы данных для УКЦ

На выбор предлагается два вида СУБД – Microsoft Office Access и Microsoft SQL Server. При выборе одной из СУБД файлы, в которой УКЦ будет сохранять информацию, будут переведены в формат файлов СУБД. После этого необходимо указать те каталоги, которые необходимы для работы УКЦ и взаимодействия его с ЦУСом.

На следующем этапе следует указать то лицо (администратор сети ViPNet), которое будет обладать полномочиями заверять своей электронной цифровой подписью сертификаты ЭЦП остальных пользователей системы . А также на этом этапе необходимо ввести данные для сертификата ЭЦП этого лица – информацию о местоположении, адрес электронной почты, алгоритм формирования ключей ЭЦП (Рис.41), срок действия сертификата и другое.

Лицо, которое имеет право работать в УКЦ, называется уполномоченным. В дальнейшем можно будет поменять уполномоченное лицо либо добавить еще одно.

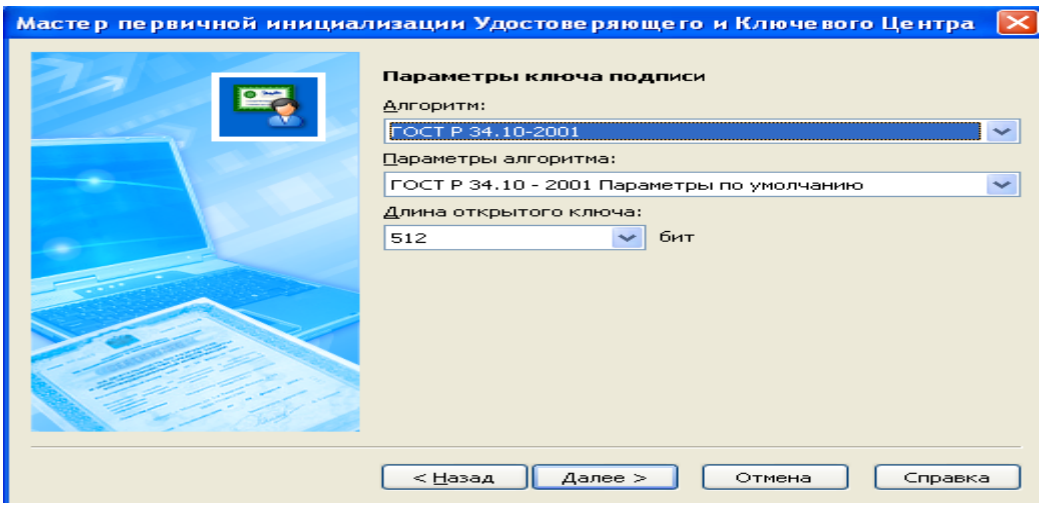


Рис. 41. Указание параметров ключа подписи.

После создания ключей ЭЦП и сертификата ЭЦП следует указать, в каком месте будет храниться контейнер ключа подписи и пароль для входа в УКЦ . При задании собственного типа пароля – все пароли в УКЦ должны быть длиной не менее 6 символов.

Следующим этапом станет создание набора Мастер-ключей (МК) (Рис.42). В ПО ViPNet версии 3.0 используются несколько мастер-ключей для отдельного вида ключевой информации. Все типы МК защищаются шифрованием на ключе защиты УКЦ. МК персональных ключей используется для создания персональных ключей пользователей (в т.ч. резервного набора персональных ключей). МК ключей защиты используется формирования ключей шифрования защиты ключей обмена коллективов. МК ключей обмена используется для формирования ключей шифрования обмена (связи) коллективов.

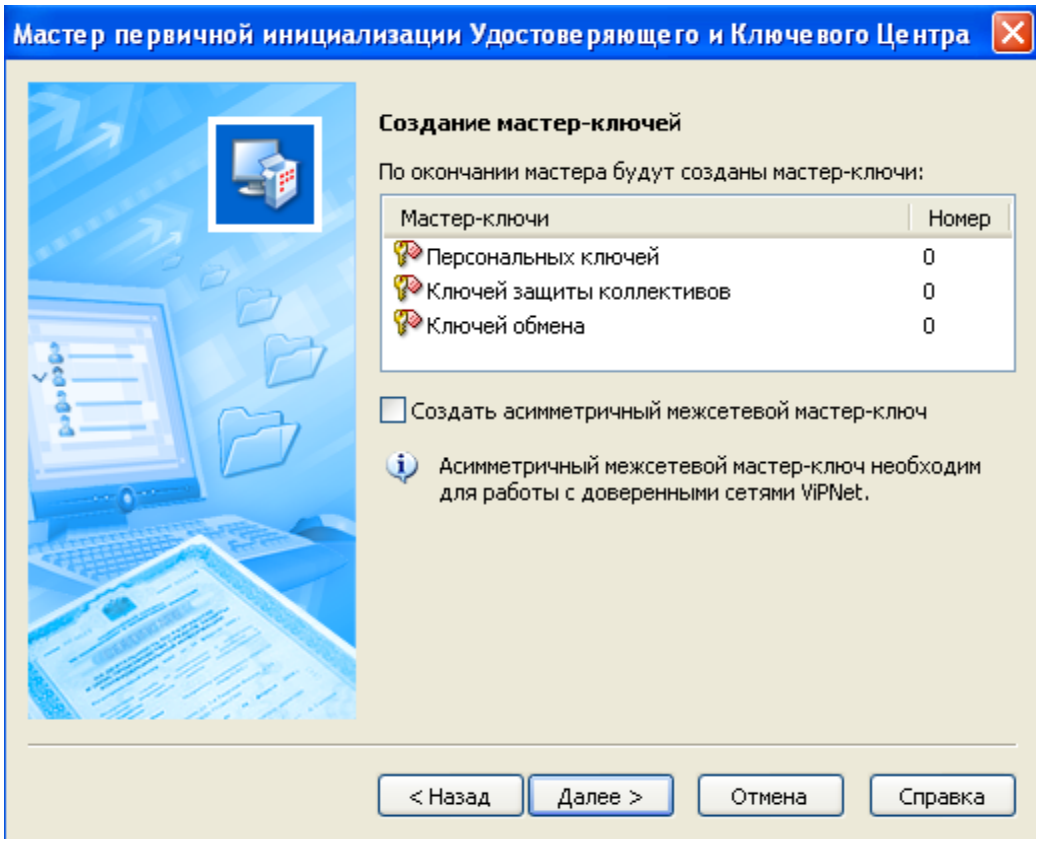


Рис. 42. Формирование Мастер-ключей системы

После проведения всех этапов по инициализации УКЦ программа установки начнет формирование ключевой инфраструктуры сети ViPNet (Рис.43), а затем на экран будет выведено окно программной оболочки УКЦ (Рис.44.)

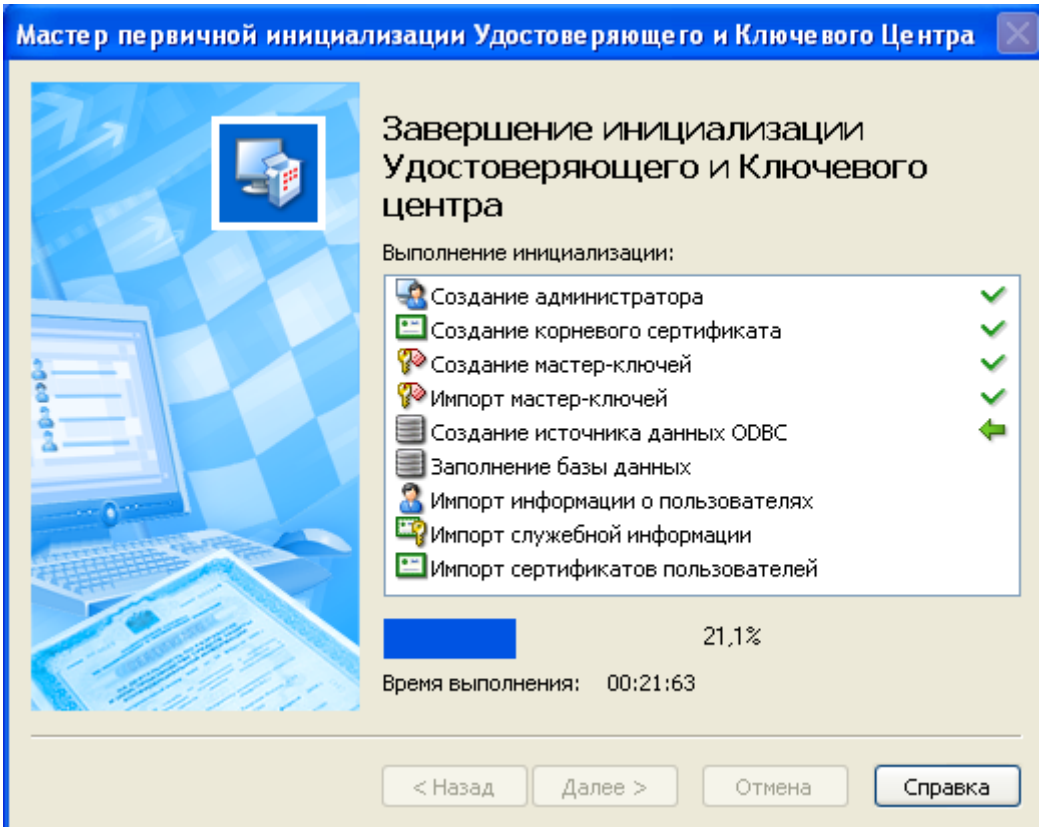


Рис. 43. Завершение инициализации УКЦ и формирование ключевой информации

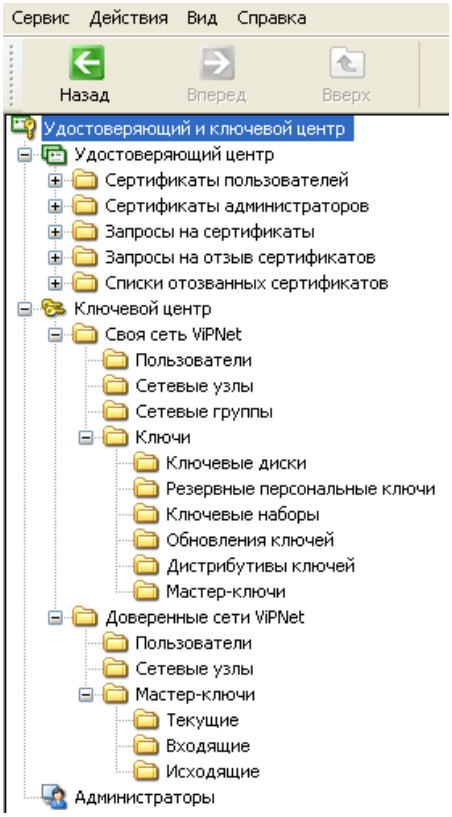


Рис. 44. Окно каталогов УКЦ

Работа в Удостоверяющем и ключевом центре.

Перед началом работы в УКЦ рекомендуется произвести первоначальные настройки программы. Это можно сделать в меню «Сервис» → «Настройка»… или нажав кнопку «Настройка» в панели инструментов программы. В окне «Пароли» настраиваем парольные параметры работы УКЦ.

После прохождения этапа первичной инициализации и произведения настроек программы необходимо сформировать дистрибутивы для пользователей созданной защищенной сети. Для этого выбираем пункт меню «Сервис» → «Автоматически создать» → «Дистрибутивы ключей»

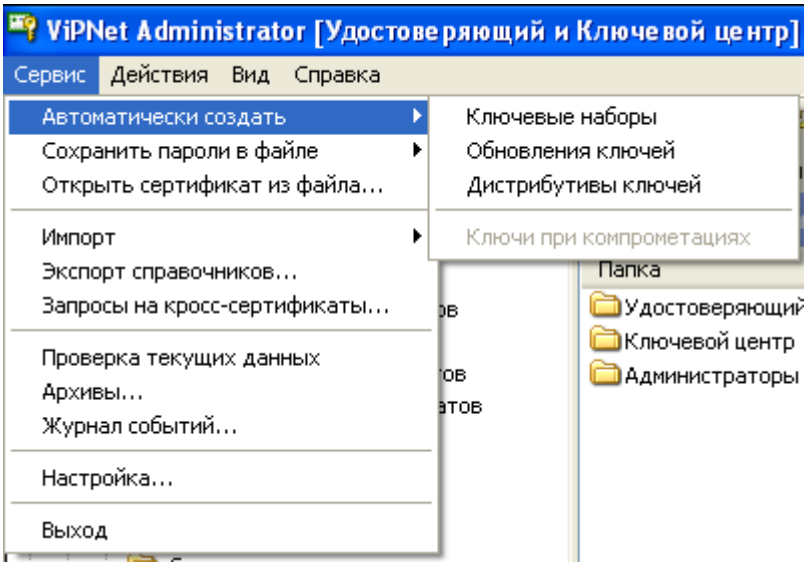


Рис. 45. Меню формирования ключевой информации

При создании дистрибутива пользователя автоматически формируется его сертификат ЭЦП. В случае если срок действия сертификата уполномоченного лица истекает до конца действия рядового пользователя VPN сети, будет выведено предупреждение о том, что срок действия сертификата пользователя будет ограничен сроком действия сертификата уполномоченного лица (Рис.45).

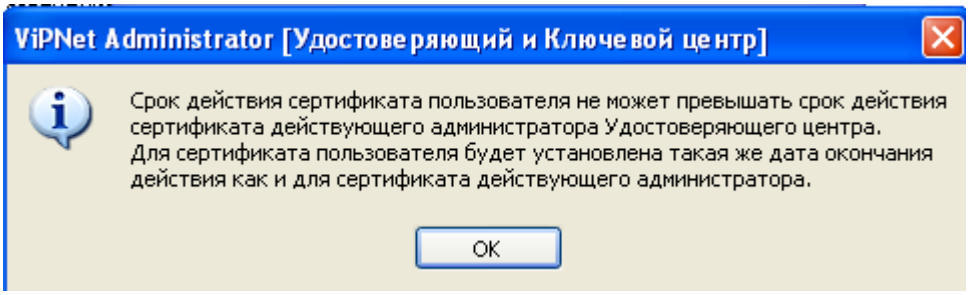


Рис. 46. Предупреждение о сроке действия сертификата

При формировании ключевой информации, входящей в файл-дистрибутив, мастером также будет предложено ввести пароль Администратора сетевого узла (Рис.46), который позволяет получить расширенные права по управлению системой защиты на конкретном узле

защищенной сети. Пароль может быть собственным, случайным и цифровым и имеет срок действия и может быть изменен в дальнейшем на самом узле пользователя VPN.

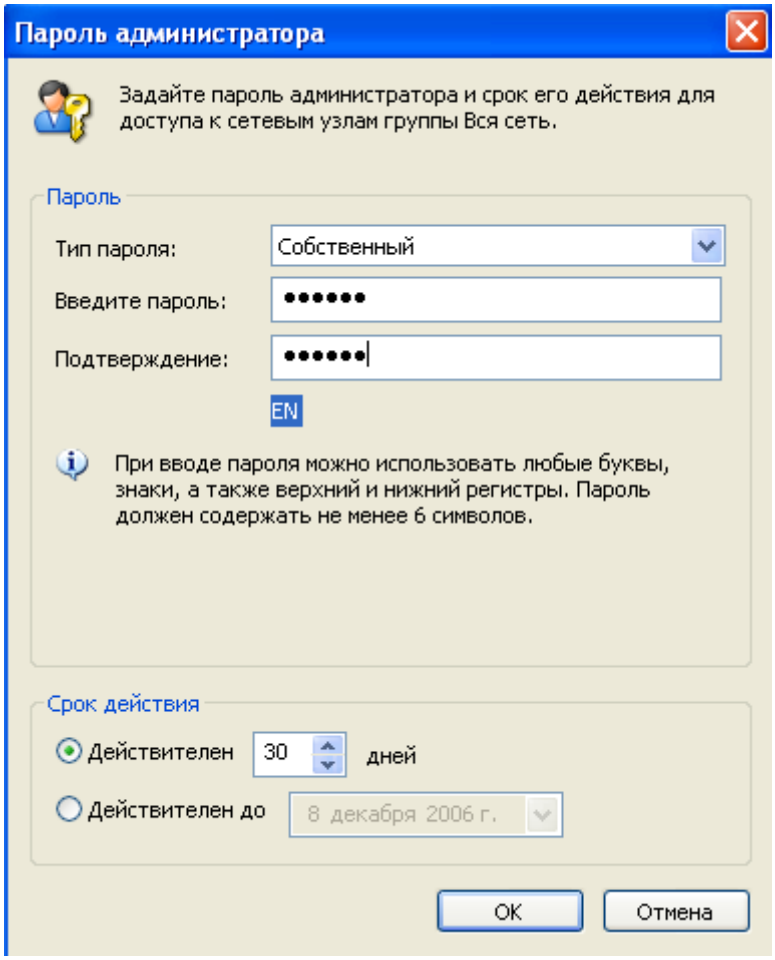


Рис. 47. Выбор типа пароля для администратора СУ всей группы

Формирование паролей Администраторов СУ осуществляется отдельно от формирования паролей на дистрибутив. Пароль Администратора СУ может быть задан как на отдельный компьютер, так и на всю группу, в которую входят несколько компьютеров.

После создания дистрибутивов необходимо их раздать пользователям защищенной сети. Это производится в окне Ключевой центр / Ключи / Дистрибутивы ключей. Действия можно производить как с отдельным дистрибутивом, так и с набором файлов-дистрибутивов (Рис.48). В данном случае необходимо выделить все записи, щелкнуть правой кнопкой «мыши» на одной из записей (или сразу на все записи) и выбрать пункт меню Перенести в папку…

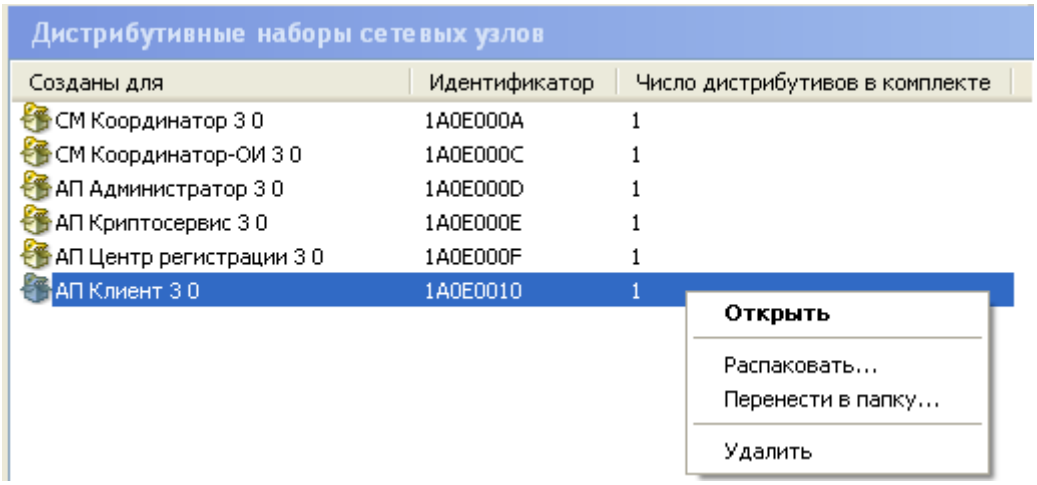


Рис. 48. Контекстное меню в каталоге Дистрибутивы

В появившемся окне мастера (Рис.48) необходимо выбрать каталог на диске , в котором будут храниться файлы-дистрибутивы до их передачи пользователям. Для проведения операции переноса для всех файлов-дистрибутивов напротив строки «Применить ко всем» слева внизу окна следует поставить «галочку».

Аналогичную операцию необходимо провести с наборами персональных ключей пользователей защищенной сети.

В УКЦ в окне Администраторы возможно указать еще лица (Уполномоченные лица), которые будут иметь право входить в УКЦ и формировать ключевую информацию для пользователей системы ViPNet.

По умолчанию действующим становится тот Администратор (УЛ), пароль которого введен для входа в УКЦ.

В меню «Сервис» → «Журнал событий» с помощью фильтров поиска можно просмотреть действия и события, произошедшие в УКЦ.

Развертывание защищенного узла Администратора сети ViPNet.

Для развертывания защищенного узла Администратора 3.0 необходимо зайти в каталог, где были сохранены файлы dst – дистрибутивы и скопировать dst–файл Администратора 3 0 в каталог установки ViPNet Client (по умолчанию – это каталог ..\SS\). Развертывание защищенного узла может быть произведено двумя способами:

запуском файла dst – в этом случае программа запросит каталог, в котором будет храниться ключевая информация;

запуском программы ViPNet Client Монитор, при этом необходимо будет указать, где хранится файл-дистрибутив и куда нужно будет сохранить ключевую информацию;

После перезагрузки драйвер ViPNet запросит пароль на вход в виртуальную сеть и на начало работы с защищенным узлом. Необходимо ввести тот пароль, который был дан Администратору 3.0 в УКЦ и начать первичную инициализацию по развертыванию защищенного узла. Без первичной инициализации (ее производят только один раз в самом начале развертывания защищенного узла) драйвер не будет загружаться.

Для проведения первичной инициализации в окне запроса пароля драйвером необходимо справа от кнопки «Настройка» выбрать выпадающее меню (треугольник вниз) и выбрать строку Первичная Инициализация (Рис.49).

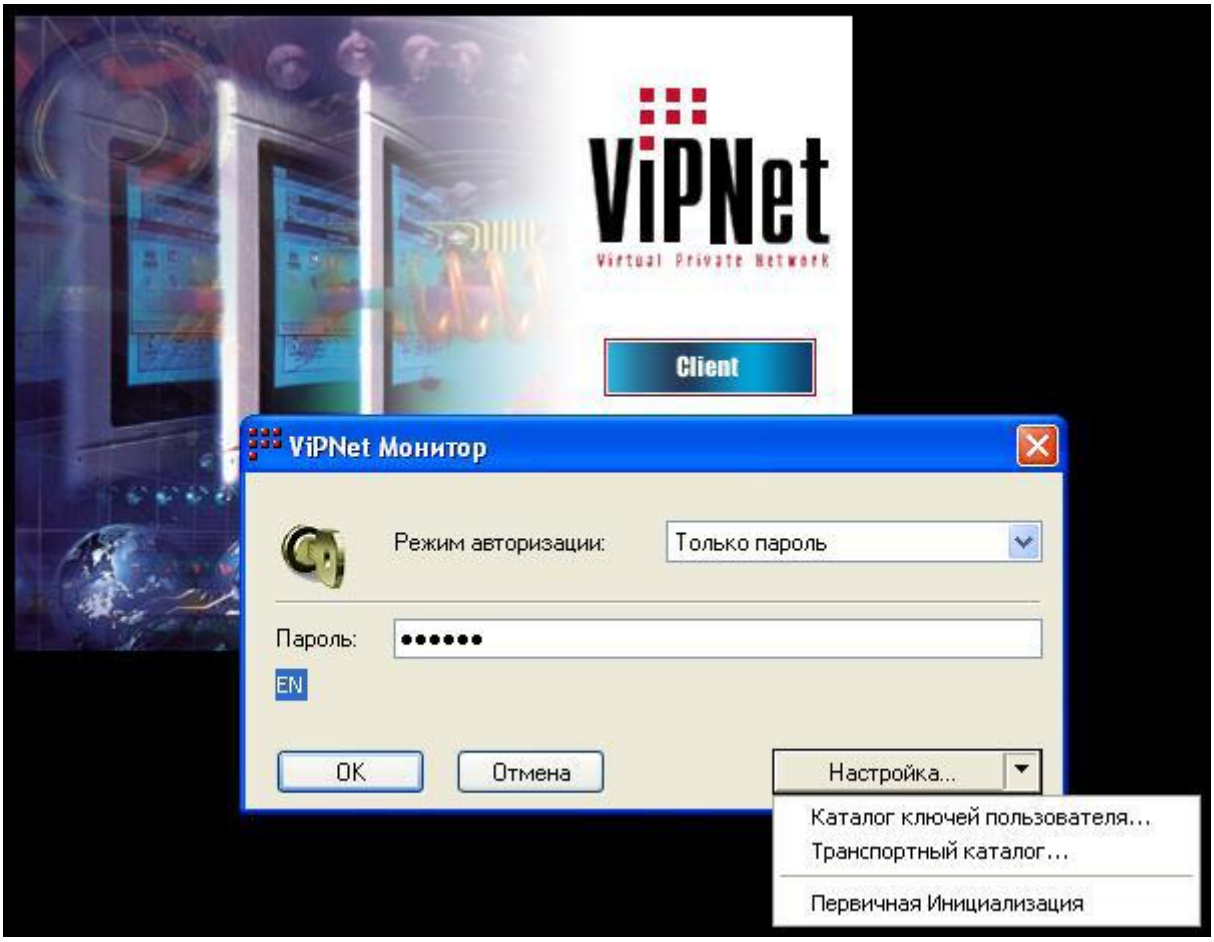


Рис. 49. Начало первичной инициализации ViPNet «Клиент» Монитор

Появится «Мастер» первичной инициализации (Рис.50), который поможет развернуть СУ виртуальной сети ViPNet.

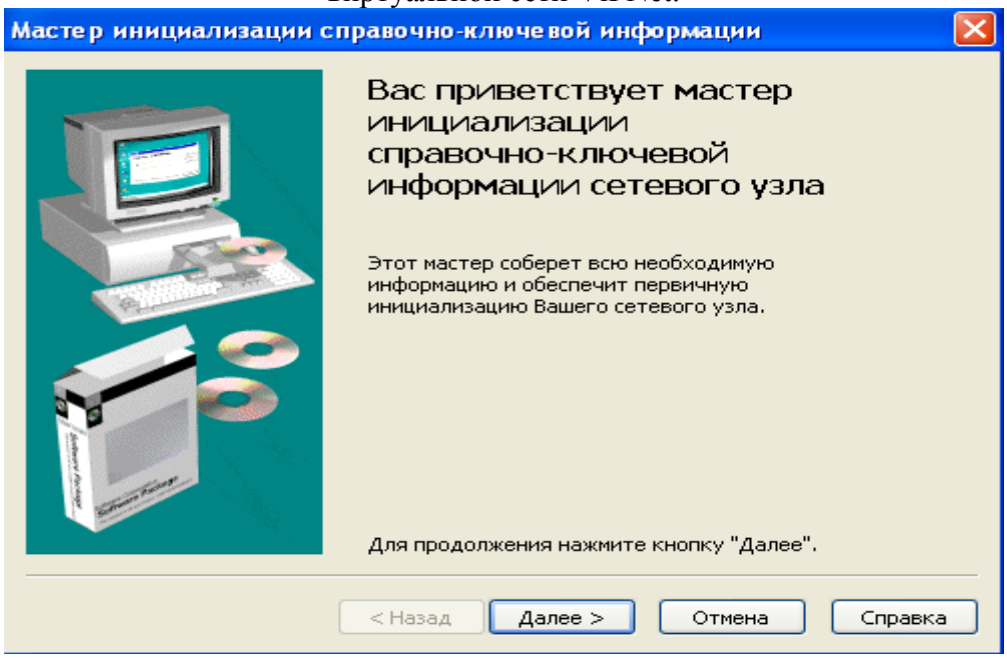


Рис. 50. Мастер первичной инициализации ViPNet «Клиент»

Мастер запросит месторасположение файла dst для пользователя, запросит информацию о том, какие аппаратные носители информации будет использовать абонент для хранения ключевой информации и пароль к дистрибутиву, а также потребует указать место для хранения справочников и ключевой информации.
Перед загрузкой «Монитора» программа спросит пользователя о том, в какой конфигурации тот желает работать – в обычной или в конфигурации Открытого Интернета. Следует выбрать обычную конфигурацию (Рис.51).

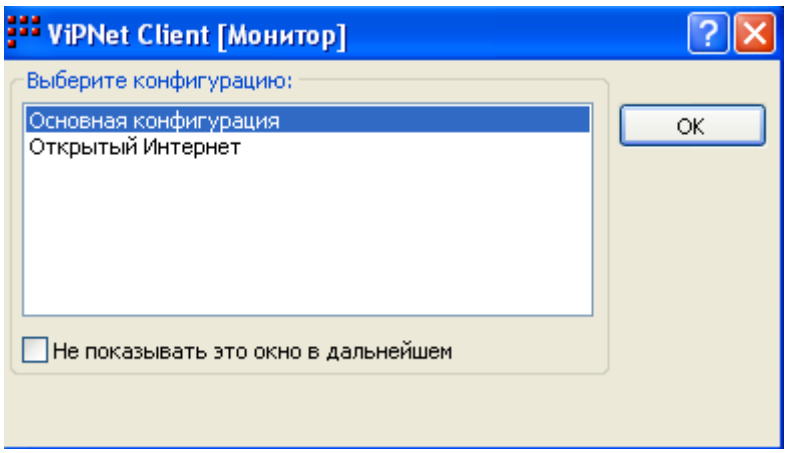


Рис. 51. Окно выбора конфигурации «Монитора»

После входа в операционную систему и загрузки «Монитора» некоторые из приложений, установленных на компьютере, попытаются получить доступ к сетевой карте. Программа «Контроль приложений», входящая в состав ПО ViPNet «Клиент» заблокирует выход этих приложений в сеть (как открытую, так и закрытую) и запросит пользователя о том, какие действия надо предпринять в отношении этих приложений (Рис. 52). В настоящем случае необходимо разрешить работу в сети службы ОС Windows Generic Host Process. Решение в отношении других программ, запросивших доступ в сеть, остается за пользователем.

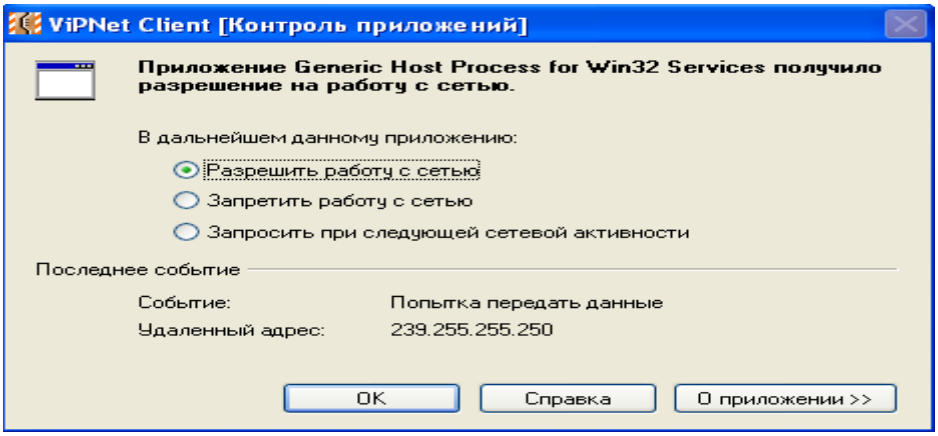


Рис. 52. Окно программы «Контроль приложений»

В итоге на СУ Администратора 3.0 окно «Защищенная сеть» в «Мониторе» должно выглядеть, как показано на Рис.53.

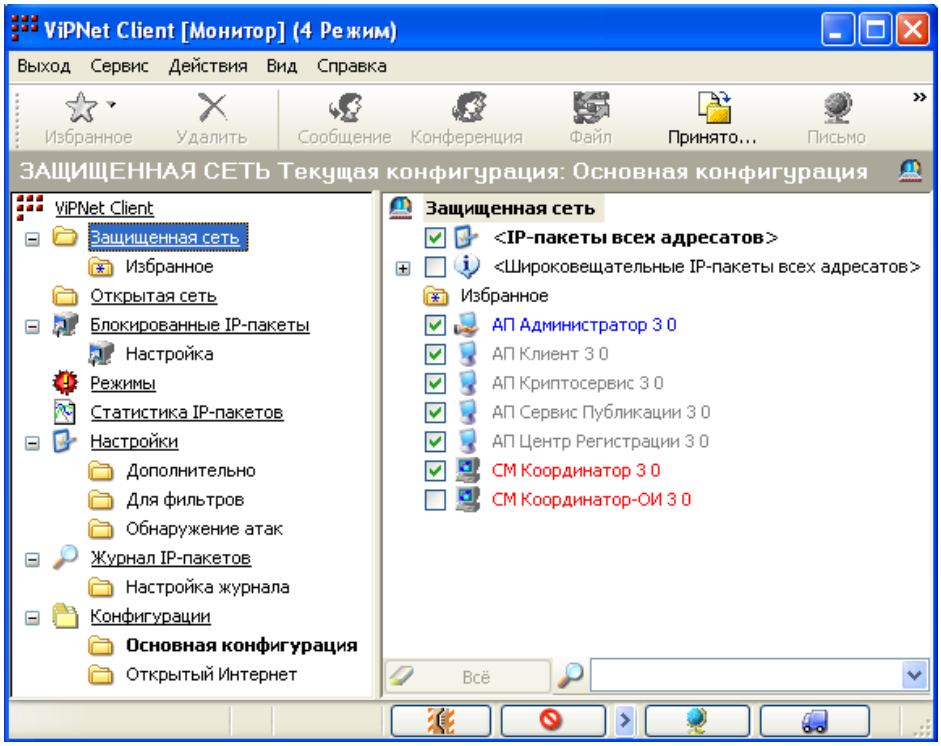


Рис. 53. Окно «Защищенная сеть» Администратора 3.0

В окне «Защищенная сеть» «Монитора» показаны:
Синим цветом – настоящий СУ.
Красным цветом – координаторы сети.
Серым и сиреневым цветом – СУ сети ViPNet, связь с которыми есть на уровне типов коллективов. Если настоящий узел не обменялся служебной информацией с конкретным СУ, то тот СУ будет показан серым цветом. Если же настоящий узел обменялся служебной информацией с конкретным СУ, то тот СУ будет показан сиреневым цветом.
После развертывания защищенного узла ОС Windows должны появиться значки программ MFTP (грузовичок), Монитор (семь красных квадратиков) и Контроль приложений (зеленый шарик на полосатом фоне) (Рис.54).

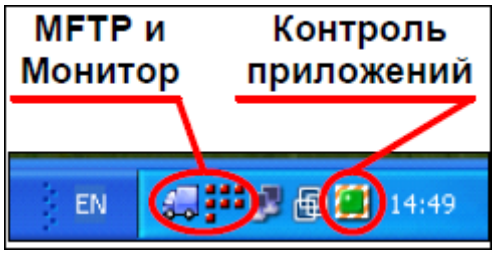


Рис. 54. Трей ОС Windows со значками ПО ViPNet

Значок MFTP (грузовичок) становится красным, если пришла информация от абонентов защищенной сети. По значку «Монитора» при отправке или приеме пакетов бегает белый квадратик. Значок «Контроля приложений» становится серым, если программа отключена (не производится контроль доступа в сеть).

Установка ПО ViPNet «Координатор».

Для установки ViPNet Координатор необходимо иметь инсталляционный комплект - файл setup.exe, ключевой дистрибутив – файл abn_AAAA.dst (где AAAA – последние четыре цифры идентификатора пользователя, зарегистрированного на данном Координаторе), в котором в склеенном виде помещена необходимая адресная и ключевая информация для обеспечения первичного запуска и последующей работы прикладной программы ViPNet Координатор (предоставляется администратором Удостоверяющего и Ключевого Центра), а также парольная информация (пароль) для рабочей станции (предоставляется администратором Удостоверяющего и Ключевого Центра). Для начала процесса установки ViPNet «Координатор» необходимо запустить файл setup.exe, находящийся в инсталляционном комплекте. В этом случае в составе ViPNet «Координатор» будет установлена также программа ViPNet «Контроль приложений». Если необходимости устанавливать программу ViPNet «Контроль приложений» нет, то следует запустить файл setup.exe из командной строки с параметром norf, а именно: setup.exe /norf.

После запуска программы установки на экране появится окно «Добро пожаловать» (Рис.55). Далее все окна во время установки программного обеспечения будут появляться так же, как и при установке ViPNet «Клиента».

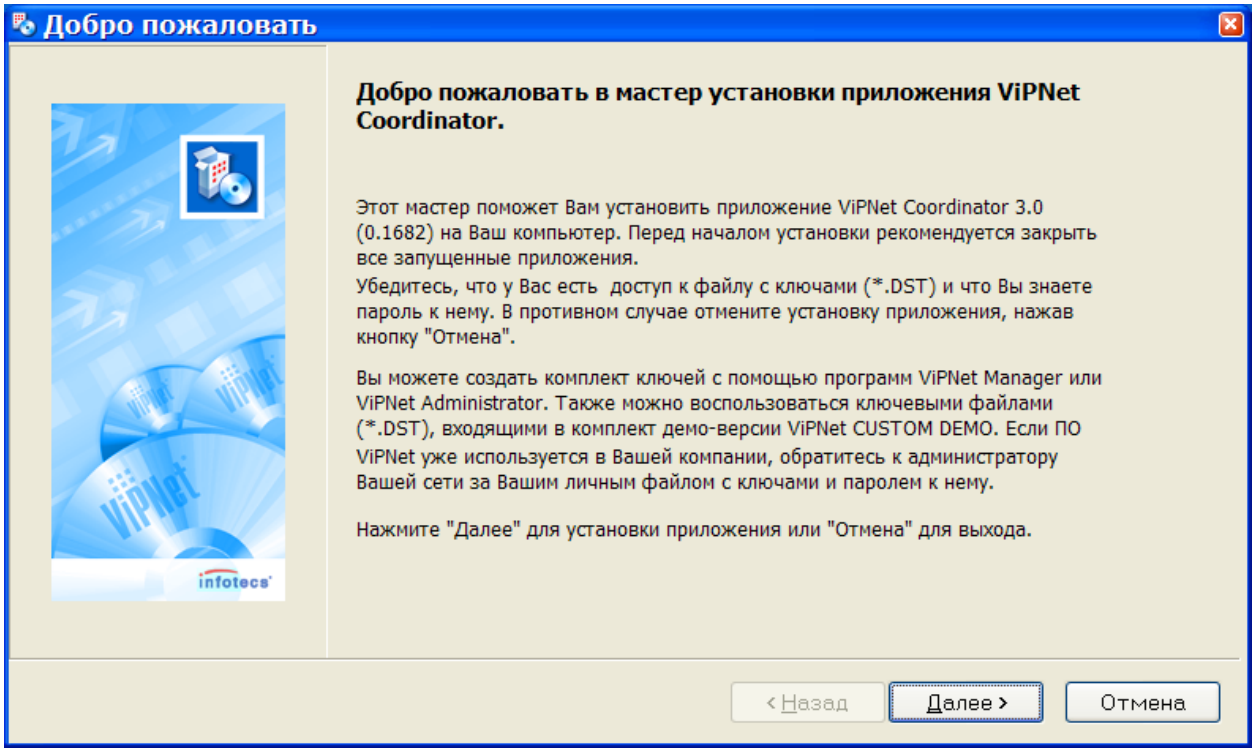


Рис. 55.. Установка ViPNet «Координатор»

Если в сетевых настройках компьютера не была включена функция IP-forwarding, то программа установки включит ее, о чем будет выдано соответствующее сообщение. После окончания установки появится окно с сообщением об успешном завершении установки программы и окно с ярлыками для запуска ПО ViPNet «Координатор». Далее программа установки предложит перезагрузить компьютер. Если администратор защищенной сети уже выдал dst-файл для данного компьютера, необходимо этот файл скопировать в каталог установки ПО ViPNet «Координатор», запомнить пароль доступа к dst-файлу и перегрузить ОС компьютера. При перезагрузке ОС драйвер ViPNet начнет защищать компьютер с

помощью систем шифрования и сетевого экрана. Если администратор защищенной сети не выдавал dst-файл для данного компьютера, перегружать ОС нет необходимости.

Первичная инициализация справочно-ключевой информации пользователя ViPNet Координатор.

Авторизация пользователей

В процессе загрузки (или перезагрузки) компьютера откроется окно для идентификации пользователя с приглашением ввести пароль (Рис.56). Во время загрузки компьютера драйвер ПО ViPNet «Координатор» блокирует весь трафик, кроме некоторых протоколов, отвечающих за работу сетевых служб, например DHCP. При отказе от введения пароля драйвер ViPNet будет загружен в пятом режиме безопасности (т.е. в нерабочем состоянии).

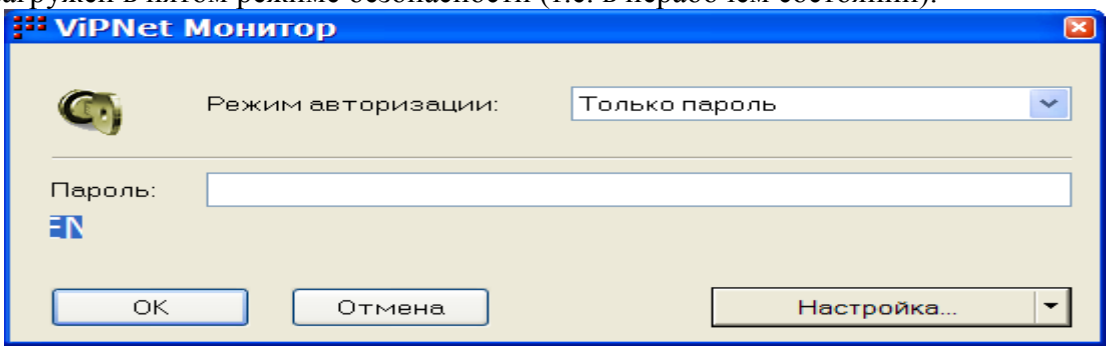


Рис. 56. Окно авторизации пользователя

Если программа ViPNet запускается в первый раз, то пользователю необходимо выполнить процедуру первичной инициализации справочно-ключевой информации.

В программе имеется возможность провести идентификация пользователя ViPNet тремя способами (Рис.57) – посредством ввода пароля пользователя с клавиатуры, посредством ввода пароля пользователя с какого-либо внешнего устройства хранения данных, путем авторизации при помощи пароля и устройства одновременно.

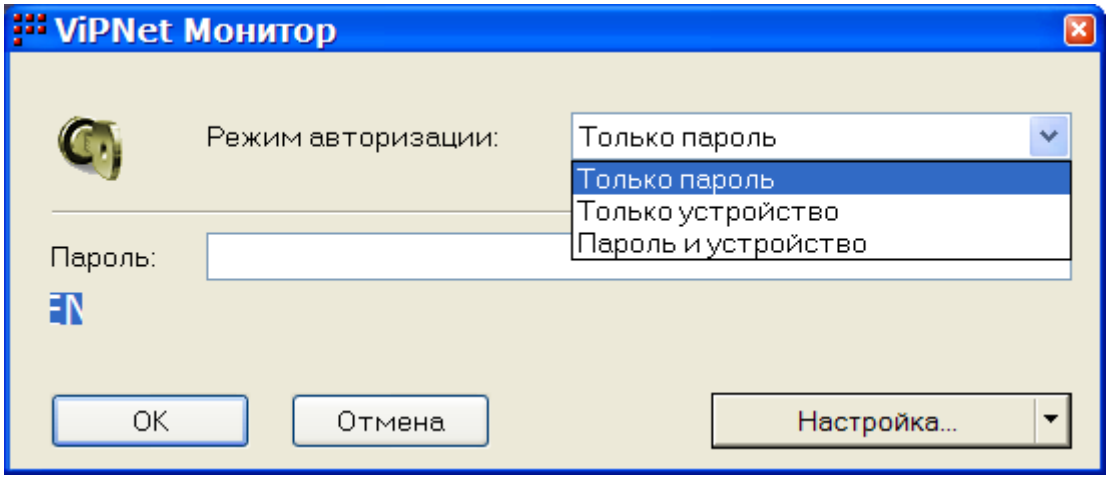


Рис. 57. Режимы авторизации

После ввода пароля и полной загрузки ViPNet «Координатор» «Монитор» на каждом сетевом интерфейсе устанавливается режим, назначенный пользователем, либо, если

программа запускается впервые, запустится мастер настройки сетевых интерфейсов (процедура настройки описана ниже).

После успешной настройки сетевых интерфейсов откроется окно ViPNet «Координатор» «Монитор» (Рис.58) и появится значок в области уведомлений на панели задач. В дальнейшем, в процессе работы, при передаче информации по сетевому адаптеру, по красным квадратам значка будет «бегать» белый квадратик. Для обеспечения обмена почтовой и управляющей информацией между объектами сети будет загружен модуль ViPNet MFTP (в области уведомлений на панели задач появится значок «грузовичок»).

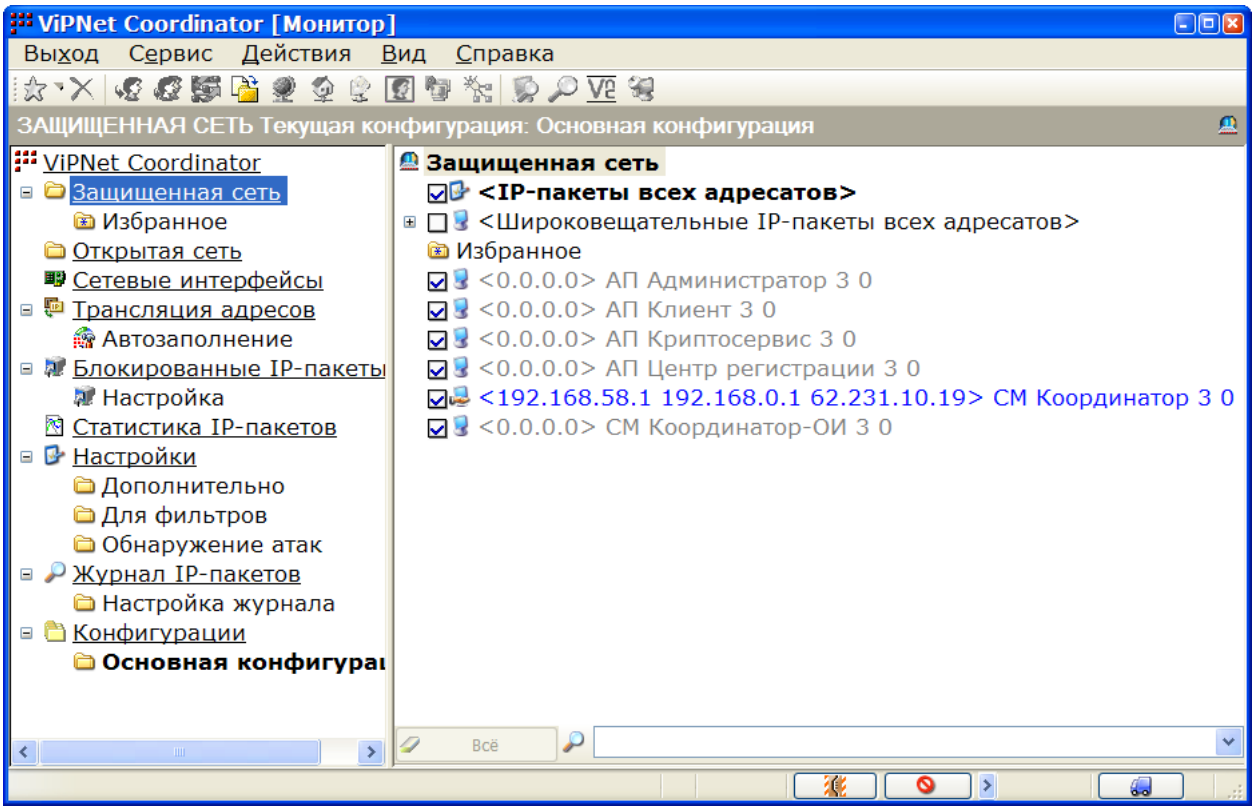


Рис. 58. Окно ViPNet «Координатор» «Монитор»

Первичная инициализация (при первом запуске программы ViPNet).

При первом запуске программы ViPNet в окне ввода пароля (Рис.57) следует нажать стрелку слева от кнопки «Настройка» и, в появившемся меню, выбрать опцию «Первичная инициализация». Появится окно мастера инициализации справочно-ключевой информации пользователя (Рис.59).

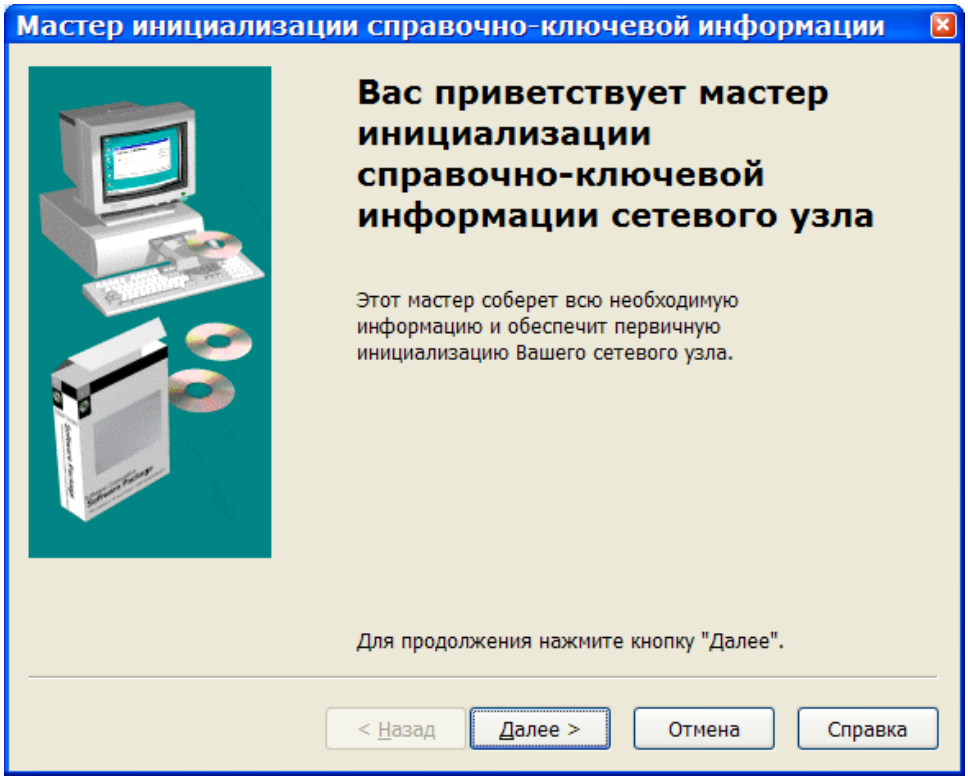


Рис. 59. Окно мастера инициализации

После нажатия кнопки «Далее» откроется окно (Рис. 60), в котором, воспользовавшись кнопкой «Обзор»…, следует указать путь к файлу дистрибутива. После указания нужно нажать кнопку «Далее».

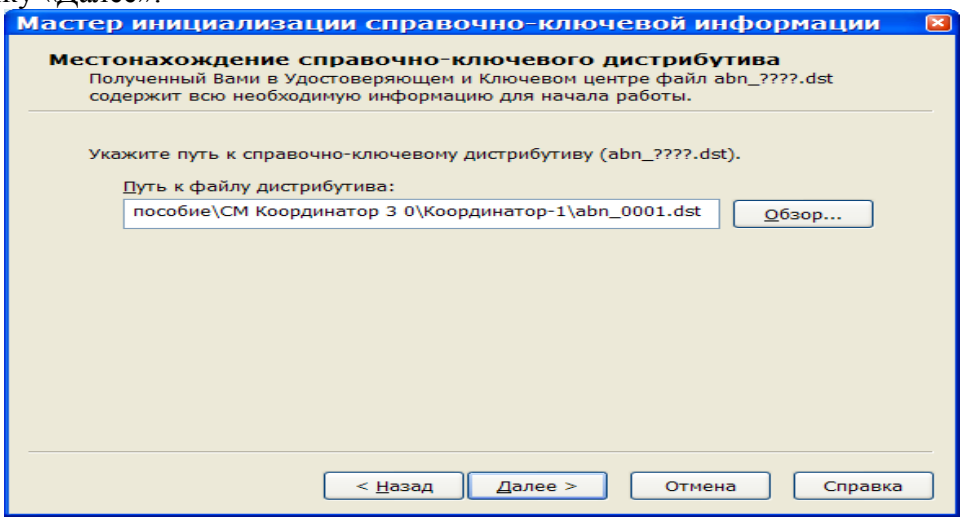


Рис. 60. Путь к справочно-ключевому дистрибутиву

Откроется окно Местонахождение справочно-ключевого дистрибутива, в котором нужно указать, где находится dst-файл.

В случае, если часть ключевой информации в УКЦ была перенесена на некоторое ключевое устройство и выдана пользователю вместе с дистрибутивом, на данной странице следует отметить галочкой опцию Использовать дополнительный носитель. Затем выбрать

нужное устройство считывания в поле «Доступные считыватели» и «Доступные устройства» и нажать кнопку «Далее».

Откроется окно ввода пароля к выбранному дистрибутиву. Следует ввести пароль и нажать кнопку «Далее».

Если дистрибутив содержит набор резервных персональных ключей пользователя (AAAA.pk), то откроется страница для указания пути для распаковки резервного набора персональных ключей. Если нет, то откроется страница готовности к выполнению инициализации, в которой отображается собранная информация. Для отмены инициализации нужно нажать кнопку «Отмена». Для возврата к предыдущему окну нажать кнопку «Назад».

Когда откроется окно завершения работы «Мастера инициализации» (Рис.61). В этом окне отмечена галочкой опция «Запустить приложение». Это означает, что при нажатии кнопки Готово будет запущена программа ViPNet (Рис.62).

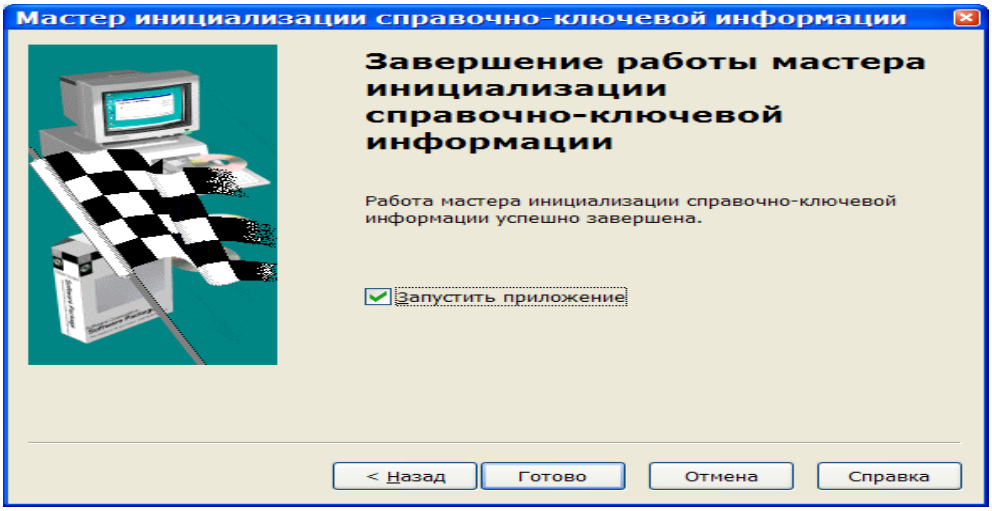


Рис. 61. Завершение работы Мастера инициализации

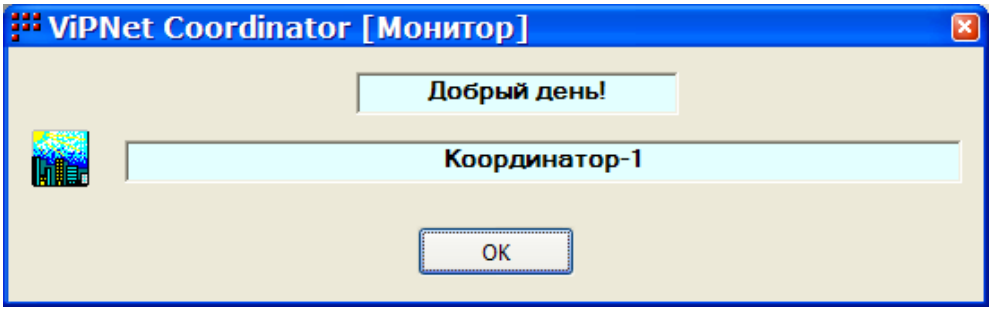


Рис. 62. Запуск программы ViPNet «Координатор.Монитор»

Настройка параметров защиты и свойств сетевых интерфейсов

Для обеспечения работоспособности ViPNet «Координатор .Монитор» требуется произвести настройки сетевых интерфейсов компьютера – выбрать типы сетевых интерфейсов, задать режимы безопасности и настройки антиспуфинга. Спуфинг-это вид хакерской атаки, заключающийся в использовании чужого IP-адреса с целью обмана системы безопасности.

При первом запуске ViPNet «Координатор.Монитор», появится окно «Произвести автонастройку сетевых интерфейсов?».

Для выбора типа сетевого интерфейса следует разместить интерфейс в нужном списке Внешние интерфейсы или Внутренние интерфейсы при помощи соответствующих кнопок. По умолчанию (при первом появлении окна Тип интерфейсов) все интерфейсы размещены в списке Внешние интерфейсы. Внешний тип сетевого интерфейса выбираем для подключения к внешним сетям (в т.ч. глобальной сети Интернет), внутренний тип – для подключения к локальной защищаемой сети.

В нашей сети устанавливаем дda сетевых интерфейса, один внутренний для локальной сети «Local subnet» и внешний «internet».

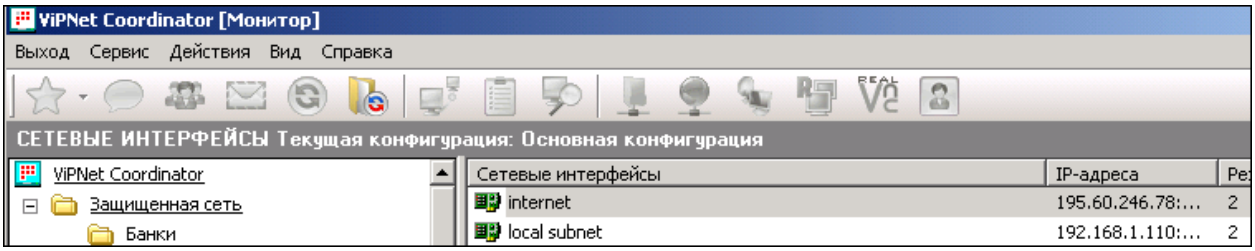


Рис. 63. Настройка типов сетевых интерфейсов

После настройки типов сетевых нужно открыть окно Режимы безопасности интерфейсов. В этом окне для каждого сетевого интерфейса следует настроить режим безопасности, в данном случае устанавливается второй уровень для обоих типов сетевых интерфейсов (Рис. 64). При включенном антиспуфинге происходит блокирование пакетов с неправильным адресом отправителя.

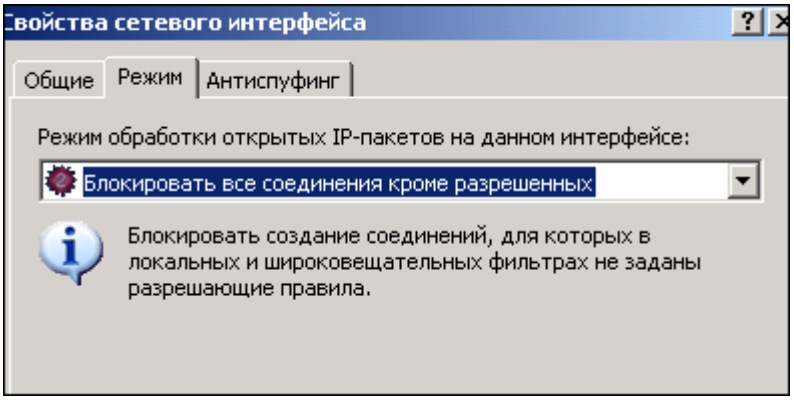


Рис. 64. Режим безопасности сетевого интерфейса

В правилах антиспуфинга для каждого сетевого интерфейса заданы диапазоны IP-адресов, пакеты от которых допустимы на интерфейсе. При этом пакеты, в которых IP-адрес отправителя не попадает в допустимый диапазон адресов, указанный на сетевом интерфейсе, будут блокироваться. (Рис. 65)

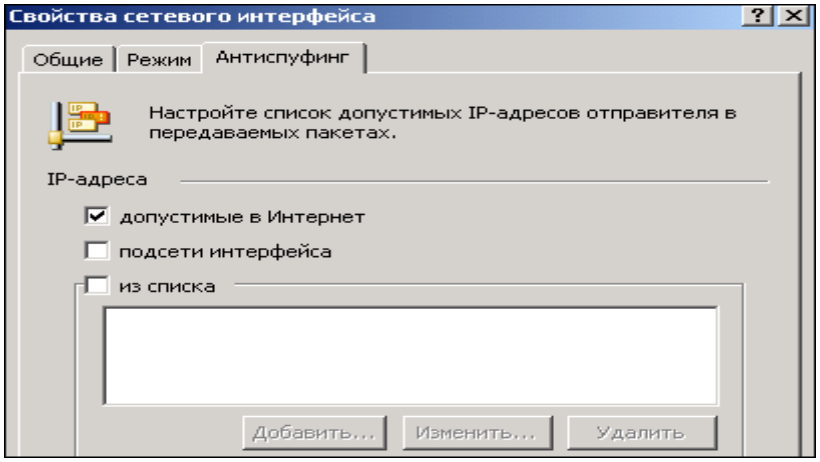


Рис. 65. Настройки антиспуфинга

При необходимости допустимые адреса можно изменять. Пакеты, прошедшие через механизм антиспуфинга, попадают на обработку правилами фильтрации пакетов. В дальнейшем следуем указанием мастера установки до ее завершения.

На этом настройка сетевых интерфейсов считается завершенной, все данные о настройке будут помещены в окне Сетевые интерфейсы программы ViPNet «Координатор. Монитор», где в дальнейшем можно изменять настройки сетевых интерфейсов. Для завершения работы мастера необходимо нажать кнопку «Готово» и откроется главное окно ViPNet «Координатор. Монитор».

Сетевые фильтры.

Правила фильтрации IP-трафика являются результатом действия правил антиспуфинга, характеристик выбранного режима безопасности для каждого сетевого интерфейса и списка сетевых фильтров для конкретных IP-адресов, протоколов и портов, заданных пользователем. Список сетевых фильтров задается пользователем в виде древовидной структуры отдельно для Защищенной сети и Открытой сети. Принципы фильтрации различаются для защищенной и открытой сети.

Для Защищенной сети

Дерево фильтров позволяет задавать фильтры на отдельный IP-адрес (первый уровень фильтрации) и определять фильтры на типы протоколов, направление установления соединения (прохождения IP-пакетов) и номера портов (второй уровень фильтрации). Существуют автоматически создаваемые сетевые фильтры, которые можно модифицировать, но нельзя удалять: главный и широковещательный фильтры для Защищенной сети.

Для Открытой сети

Сетевые фильтры настраиваются по паре адресов пакета (IP-адресу отправителя и получателя или диапазону IP-адресов отправителей и получателей). Окно Открытая сеть поделено на четыре группы фильтрации для разных типов пакетов:

Широковещательные IP-пакеты;

Локальные входящие IP-пакеты;

Локальные исходящие IP-пакеты;

Транзитные IP-пакеты.

В группе фильтрации Широковещательные IP-пакеты существует автоматически созданный сетевой фильтр Все широковещательные IP-пакеты, который пользователь при

необходимости может модифицировать, отключить или удалить. В остальных группах фильтрации по умолчанию фильтры не заданы, т.е. фильтрация осуществляется в рамках установленного режима безопасности. Дерево фильтров позволяет пользователю задавать собственные сетевые фильтры в каждой группе фильтрации.. Каждый сетевой фильтр изначально состоит из Правила доступа и подчиненного ему фильтра протоколов с именем «Все протоколы». В Правиле доступа настраиваются адреса (отправителя и получателя пакета) по которым будет осуществляться отбор пакетов для фильтрации. Подчиненный фильтр «Все протоколы» определяет условия фильтрации пакетов и действие фильтра (Пропускать или Блокировать пакеты). Для каждого Правила доступа можно добавлять дополнительные фильтры протоколов. Фильтрация пакетов может быть настроена в зависимости от времени.

Список сетевых фильтров для Защищенной сети

Окно Защищенной сеть поделено на три группы фильтрации.

Главный фильтр с именем IP-пакеты всех адресатов – определяет общее правило фильтрации для всех сетевых узлов из окна Защищенная сеть. Широковещательный фильтр с именем Широковещательные IP-пакеты всех адресатов – определяет правило фильтрации для всех шифрованных широковещательных пакетов. Работа фильтров для широковещательных пакетов не зависит от настроек других фильтров. Индивидуальные фильтры - фильтры для конкретных сетевых узлов Защищенной сети.

Фильтр протоколов – может быть настроен для широковещательного, главного и индивидуального фильтров. Фильтр протоколов всегда подчинен какому-либо фильтру из указанных выше. Microsoft SQL фильтр – может быть использован при установке ViPNet Координатор на Microsoft SQL сервер для предотвращения прихода нежелательных данных. Фильтр работает на уровне протокола TDS (протокол передачи данных для MS SQL). Microsoft SQL фильтр всегда подчинен какому-либо индивидуальному фильтру для пользователя Защищенной сети.

Фильры в защищенной сети настраиваются для каждого клиента индивидуально.

Стандартно, для клиента прописываются фильтры (Рис. 66.).

«TCP: 5000-5003» предназначен для задач деловой почты(только входящий трафик).

«http-80» для входящих пакетов из интернета.

«UDP 2046-iplirdatagram»- для проверки связи с координатором.

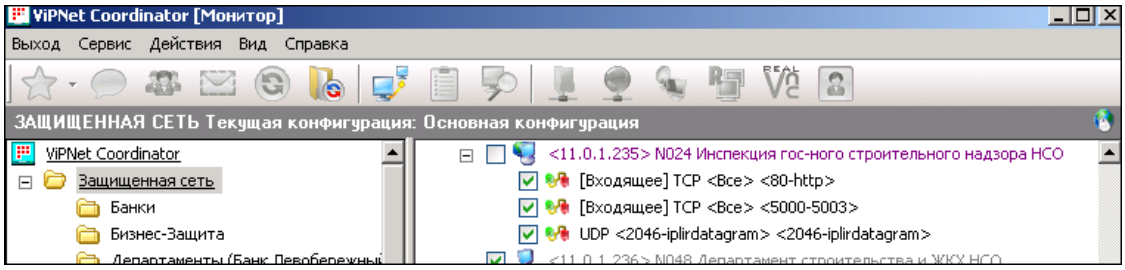


Рис. 66. Настройка ильтров Защищенной сети

Список сетевых фильтров для Открытой сети.

Окно Открытая сеть поделено на четыре группы фильтрации (по типам обрабатываемых пакетов): Широковещательные IP-пакеты – группа фильтрации предназначена для настройки правил фильтрации широковещательных пакетов. Правила фильтрации широковещательных пакетов задаются только для входящего трафика (т.е. адресованных на один из адресов компьютера с ViPNet Координатор [Монитор]). Для исходящего трафика действуют правила установленного режима. По умолчанию этот фильтр блокирует все входящие

широковещательные пакеты, за исключением пакетов для отдельных протоколов, а именно разрешены: Широковещательные пакеты nbname (порт 137) и nbdatagram (порт 138) предназначены для организации работы службы имен NETBIOS – определения имен компьютеров, входящих в Microsoft Network. Широковещательные пакеты bootp (порты 67 и 68) предназначены для организации работы службы DHCP – получения компьютером IP-адреса при его загрузке.

Для внутреннего интерфейса, в фильтре «Доступ из локальной сети»: Служба «TCP: 5000-5003» предназначена для задач деловой почты(только входящий трафик). Служба http для входящих пакетов из интернета. «ICMP 8-Echo»- для проверки связи с координатором.

Для внешнего интерфейса в фильтре «Все внешние IP-адреса» разрешен пропуск входящего трафика деловой почты(служба Mftp), и исходящий и входящий трафик глобальной сети(Служба Http).

На этом этапе настройка ПО ViPNet «Координатор» закончена, теперь необходимо устанавливать ПО клиентов(ViPNet «Клиент»).

Установка ПО ViPNet «Клиент» и первичная инициализация справочно-ключевой информации пользователя

Для установки ViPNet «Клиент» на рабочую станцию необходимо иметь:

Установочный комплект в виде файла setup.exe.

Ключевой дистрибутив – файл с расширением .DST, в котором в склеенном виде помещена необходимая адресная и ключевая информация для обеспечения первичного запуска и последующей работы прикладной программы ViPNet.

Парольная информация (пароль) для рабочей станции (предоставляется администратором Удостоверяющего и Ключевого Центра).

Для начала процесса установки ViPNet Клиент:

Двойным кликом левой клавишей «мышки» запускаем файл setup.exe, находящийся в установочном комплекте, при этом в составе ViPNet «Клиента» будет установлена также программа ViPNet «Контроль приложений».

После запуска программы установки на экране появится окно «Добро пожаловать» (Рис.67).

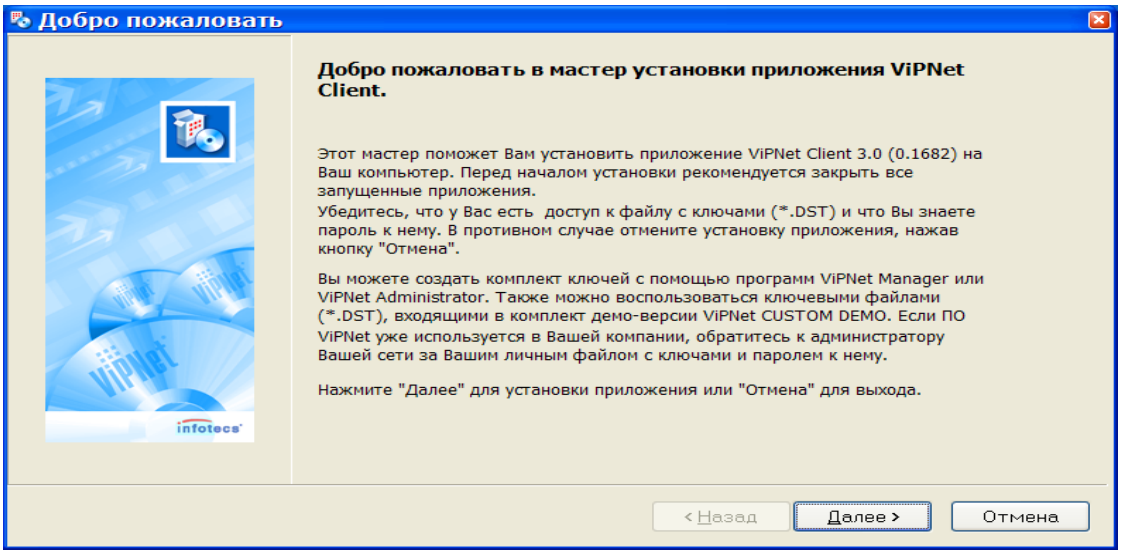


Рис. 67. Установка ViPNet Клиент

При запросе вида установки (Рис.68) следует выбрать «Деловая почта» и «Монитор». При выборе вида Выборочная можно будет выбрать любую из указанных ПЗ. После установки программа предложит перезагрузить ОС компьютер. Файл «dst» для необходимо поместить в каталог установки ViPNet «Клиента» (C:\Program Files\Infotecs\ViPNet «Клиент») и перегрузить ОС компьютера. После перезагрузки ViPNet «Клиент» автоматически предложит использовать файл «dst» для развертывания защищенного узла сети и, после введения пароля для входя в защищенную сеть, компьютер будет защищен сетевым экраном и системой шифрования.

В процессе перезагрузки ОС компьютера откроется окно для идентификации пользователя с приглашением ввести пароль (Рис.68). Существует три способа авторизации пользователя ViPNet: посредством ввода пароля пользователя с клавиатуры, посредством ввода пароля пользователя с какого-либо внешнего устройства хранения данных, путем авторизации при помощи пароля и устройства одновременно.

Необходимо выполнить процедуру первичной инициализации справочно-ключевой информации, которая находится в файле дистрибутиве. Эту же процедуру необходимо выполнить при обновления ключевой и справочной информации при помощи ключевого дистрибутива (dst-файла).

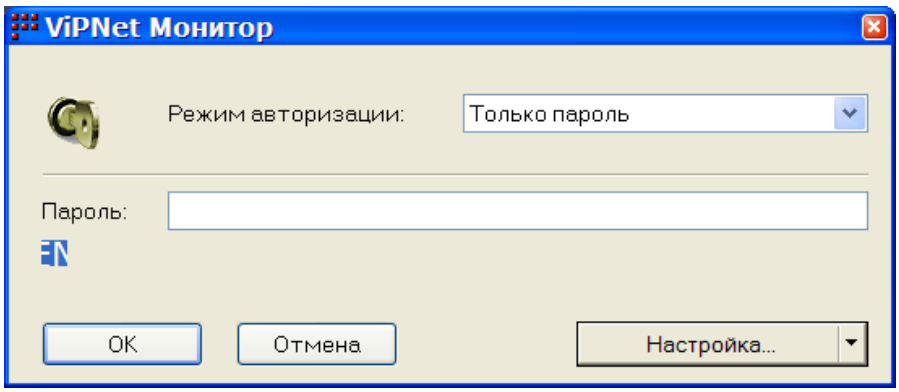


Рис.68. Окно авторизации пользователя

При первом запуске программы ViPNet в окне ввода пароля (Рис.69) следует нажать кнопку Настройка и выбрать опцию Первичная инициализация. Появится окно Мастера инициализации справочно-ключевой информации пользователя. Необходимо нажать кнопку «Далее», откроется окно, в котором следует указать путь к файлу дистрибутива, воспользовавшись кнопкой Обзор…. После выполнения поиска и указания пути следует нажать кнопку «Далее». Откроется окно Местонахождение справочно-ключевого дистрибутива. В открывшемся окне ввода пароля следует ввести пароль для доступа к информации, хранящейся в dst-файле.

Откроется окно выбора места хранения адресных справочников и ключевой информации, в котором следует указать путь к каталогу, в котором будут храниться адресные справочники, а также путь к каталогу, в котором будут храниться ключи пользователя. После завершения выбора нажать кнопку «Далее». Откроется страница готовности к выполнению инициализации (Рис.70), в которой отображается собранная информация.

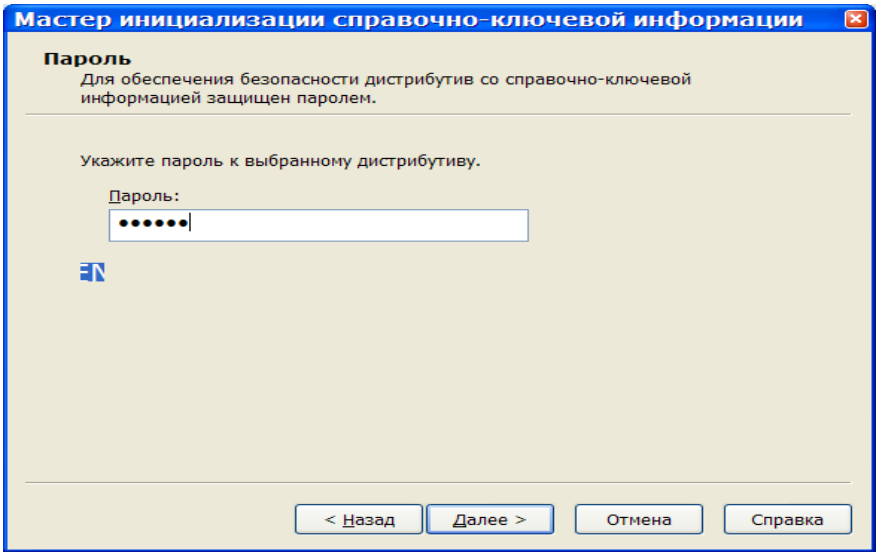


Рис.70. Окно ввода пароля

В окне указываются выбранные на предыдущих этапах установки ПО параметры. Если информация верна, необходимо нажать кнопку «Далее». Откроется окно завершения работы мастера инициализации. В окне завершения работы мастера по умолчанию отмечена галочкой опция «Запустить приложение», которая показывает, что, при нажатии кнопки «Готово», будет запущена программа ViPNet «Клиент. Монитор».

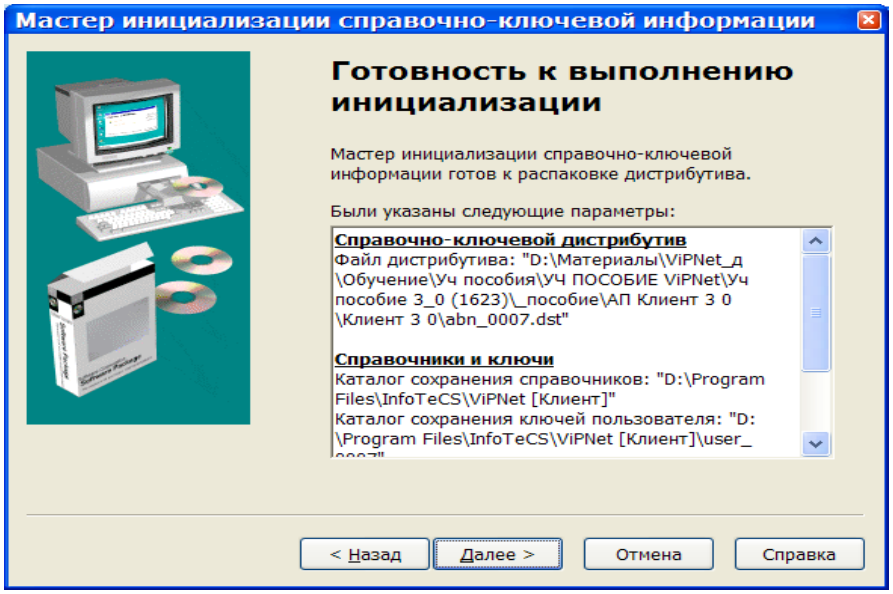


Рис.71. Готовность к выполнению инициализации

После успешной установки ключей программа ViPNet «Клиент. Монитор» стартует автоматически и откроется окно ViPNet «Клиент. Монитор» (Рис.71), в котором появится значок (Рис 72), в области уведомлений на панели задач.

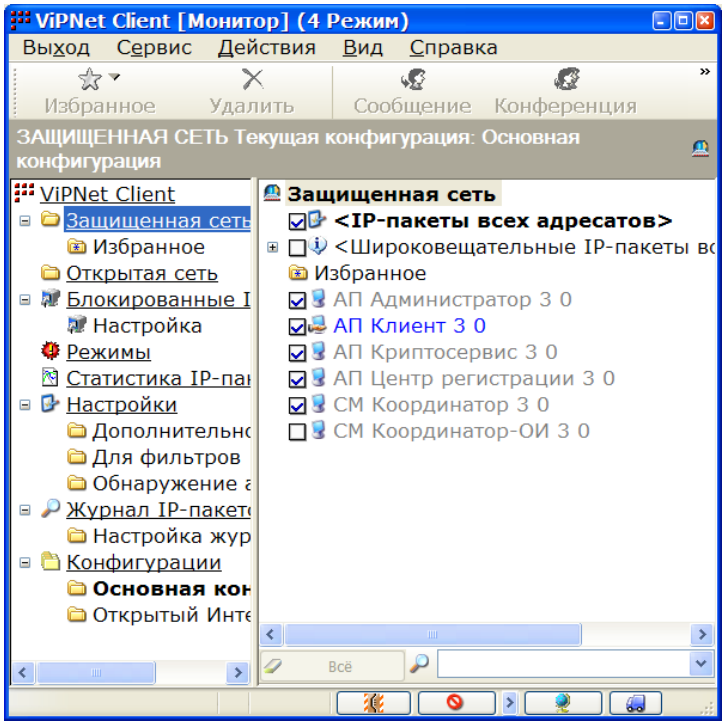


Рис.72. Окно ViPNet «Клиент. Монитор»

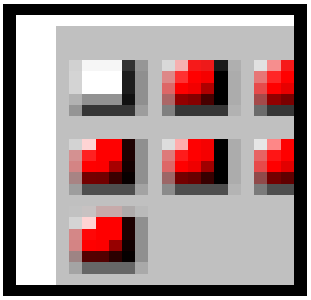


Рис. 73. Значок на панели задач ViPNet «Клиент. Монитор»

Настройка программы ViPNet «Клиент».

Перед тем, как производить настройки ViPNet, на компьютере должна быть произведена сетевая настройка Windows, которая необходима для работы данного компьютера в сети без использования ПО ViPNet Клиент. Т.к. ViPNet «Клиент. Монитор» был сконфигурирован администратором сети ViPNet в программе ЦУС, то для обеспечения корректной работы АП в сети никаких ручных настроек ViPNet «Клиент. Монитор» производить не нужно.

Настройка IP-адреса компьютеров защищенной сети.

В качестве сервера IP- адресов нужно выбрать Координатор ViPNet сети. Для этого в окне Настройки в поле Сервер IP-адресов необходимо выбрать Координатор, который будет являться сервером IP-адресов, и нажать кнопку Применить.

Компьютеры защищенной сети периодически высылают в широковещательном режиме информацию о себе другим узлам сети. В этой информации указаны IP-адреса самого компьютера, его идентификатор, выданный в ЦУСе, IP-адреса доступа к компьютеру через устройство сопряжения и др.

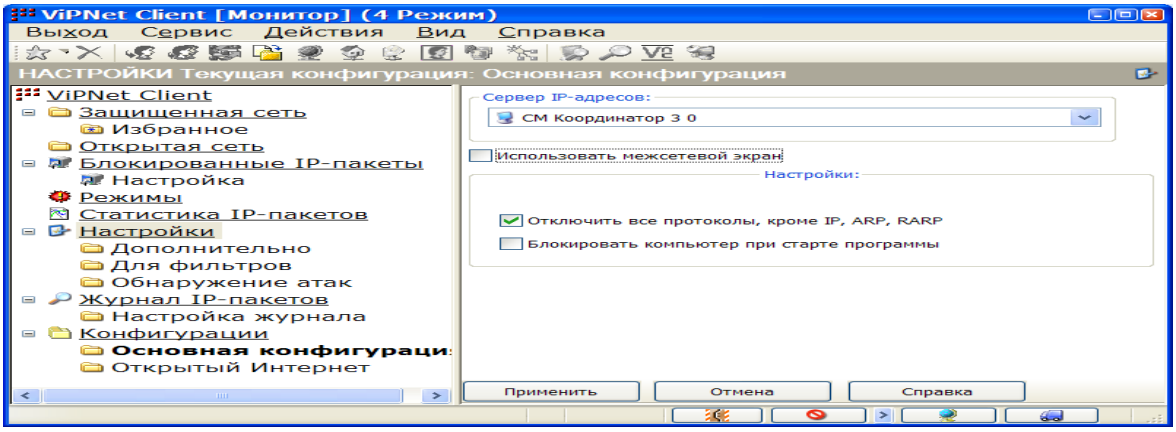


Рис. 74. Окно Настройки

Смена режимов безопасности программы Монитор.

Режим безопасности определяет типовое правило фильтрации IP-пакетов, которое в дальнейшем можно модифицировать настройками сетевых фильтров для пакетов определенного типа (для конкретных адресов, протоколов и портов) в окне Защищенная или Открытая сеть. Изменение режима безопасности работы компьютера в сети можно произвести в окне Режимы (Рис.74). Можно произвести ряд настроек в разделе При старте программы.

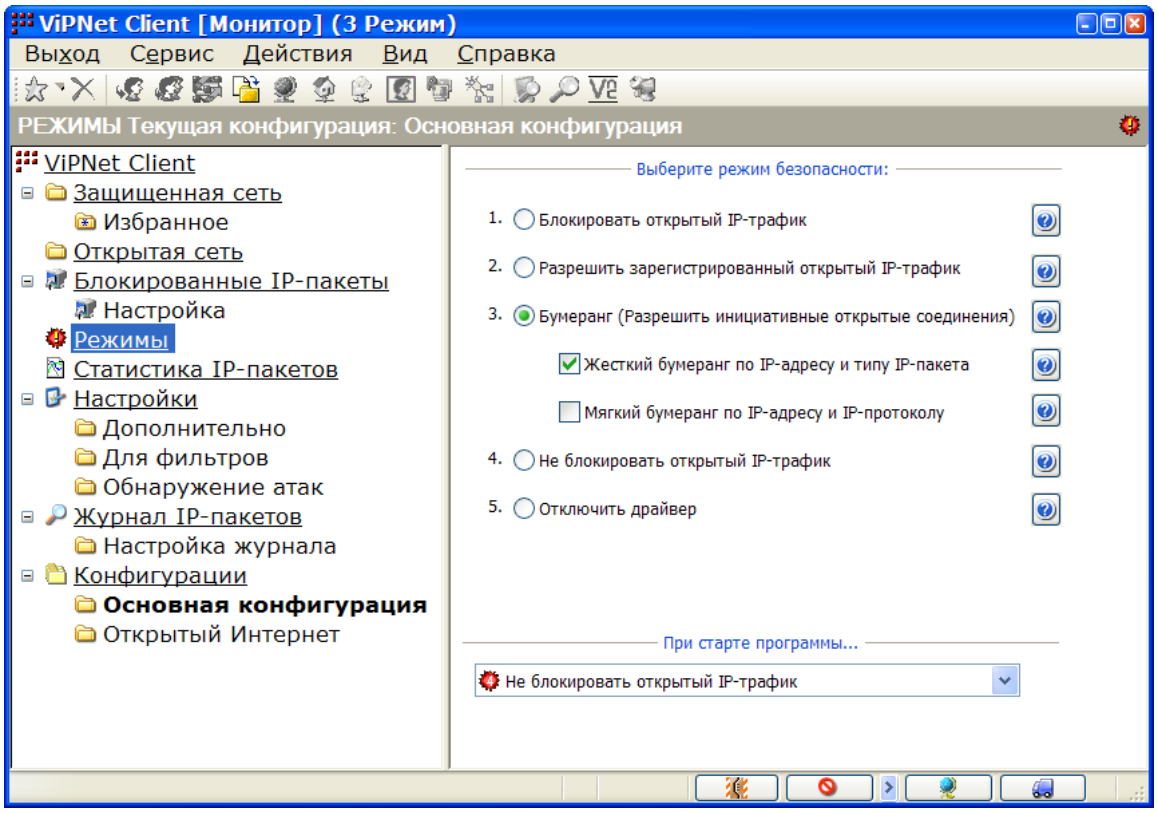


Рис. 75. Режимы безопасности ПО ViPNet

Устанавливаем третий режим (Разрешить инициативные открытые соединения) разрешает взаимодействие только с теми компьютерами, информацию от которых запросил сам пользователь, работающий за сетевым экраном ViPNet. Причем трафик будет фильтроваться по нескольким параметрам в зависимости от того, какой вид Бумеранга используется: При

использовании Жесткого Бумеранга фильтрация IP-пакетов будет производиться по IP-адресам назначения и отправки, протоколу передачи и порту работы соединения. При использовании Мягкого Бумеранга фильтрация IP-пакетов будет производиться по IP-адресам назначения и отправки и протоколу передачи.

Настройка параметров безопасности в программах Монитор и Деловая Почта.

Для редактирования параметров безопасности из настроек программы ViPNet «Клиент. Монитор» в панели инструментов необходимо выбрать меню Сервис, Настройка параметров безопасности (Рис.76).

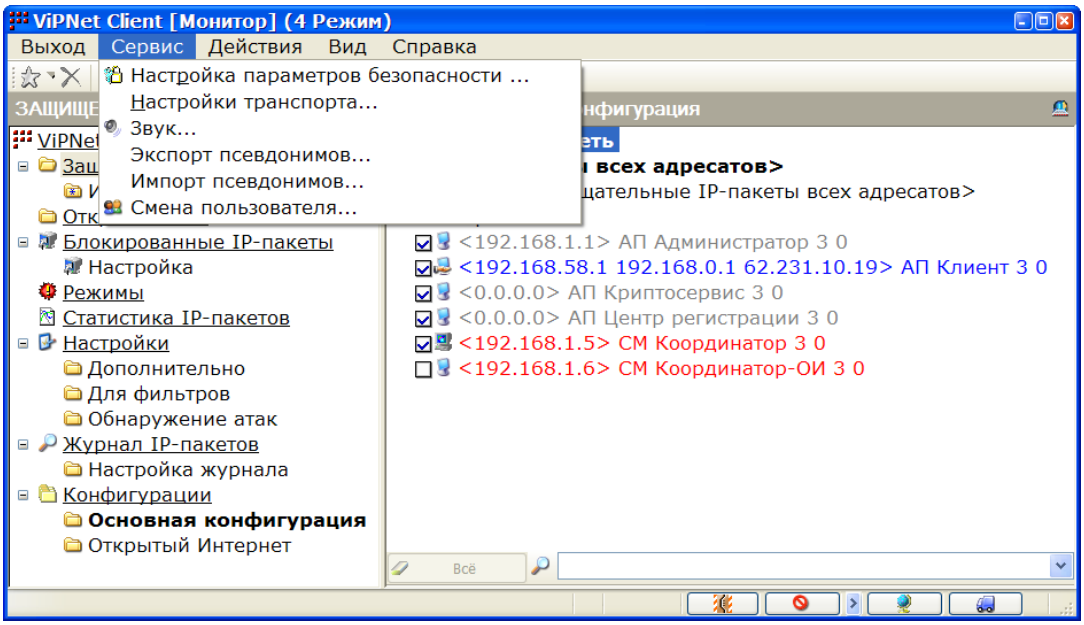


Рис. 76. Меню Сервис

В появившемся окне Настройка параметров безопасности (Рис.77) указаны следующие вкладки: Пользователь – содержит информацию о пользователе, вошедшем в программу «Монитор» или «Деловая Почта», а также предоставляет возможность сменить пользователя. Подпись – предназначена для работы с сертификатами ЭЦП. Шифрование – предназначена для задания параметров шифрования и настройки работы на асимметричных ключах шифрования. Пароль – предназначена для задания параметров пароля и последующей смены пароля.

Ключи – предназначены для задания параметров авторизации (способов входа в основную программу ViPNet) и для работы с контейнерами ключей подписи. Администратор – предназначена для входа в основные программы ViPNet с правами администратора и последующего выхода, а режиме администратора становятся доступны дополнительные настройки. Криптопровайдер – предназначена для настройки работы с контейнерами и сертификатами, необходимыми для работы с криптопровайдером ViPNet CSP.

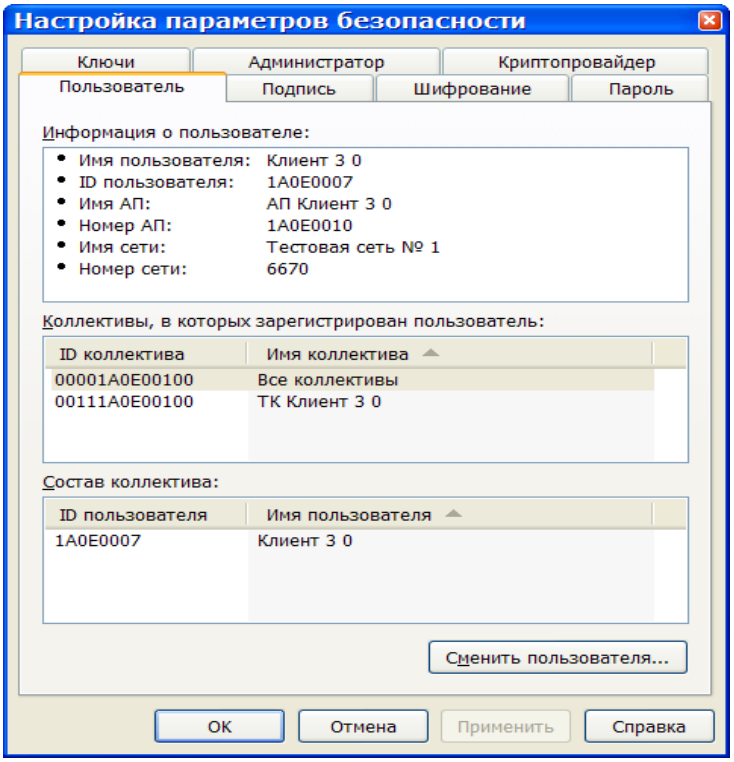


Рис. 77.Окно Настройка параметров безопасности

Настройка фильтров открытой сети.

Как только ПО ViPNet «Клиент» установлено, фильтров в «Открытой сети» у него нет. При необходимости можно прописывать для каждого клиента IP-адреса локальной сети в которую он входит. Для каждого клиента в зависимости от его постребностей можно добавлять различные фильтры откроой сети.

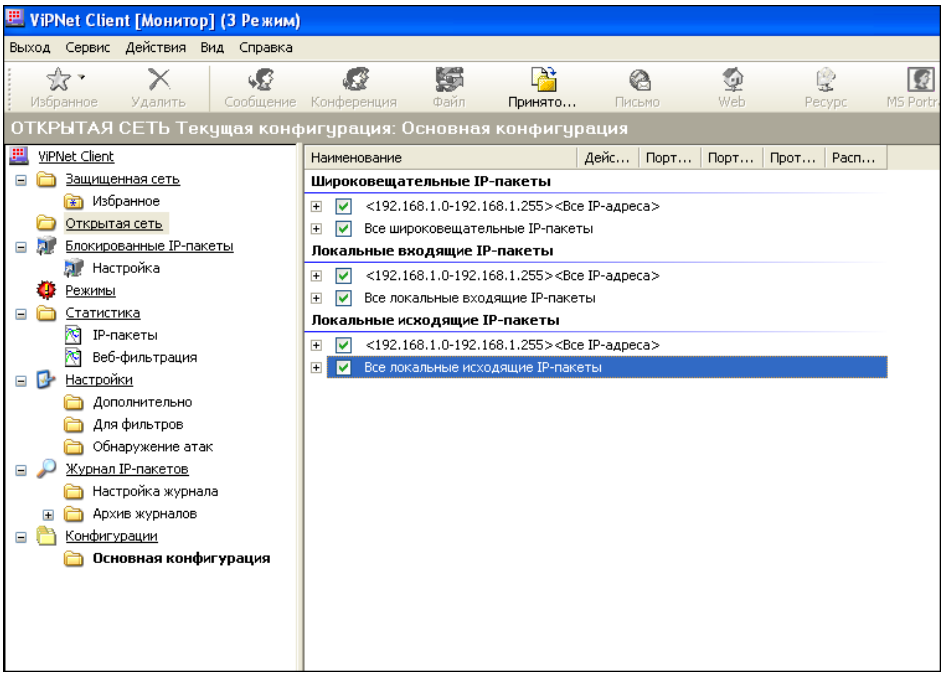


Рис. 78. Фильтры открытой сети

4. Испытание системы ViPNet Custom.

Целью испытания является выявления возможности несанкционированного доступа к информации передаваемой между узлами защищенной сети ViPNet Custom. Эксперимент будет проводится в локальной сети компании «Бизнес защита». Два абонентских пункта с ПО ViPNet «Клиент» и подключенных к защищенной сети ViPNet Custom будут обмениваться мгновенными сообщениями, а с третьего абонентского пункта(Злоумышленника) не имеющего ПО ViPNet «Клиент» будет проводится попытка перехвата информации. Злоумышленнику будет известны IP-адреса компьютеров между которыми происходит обмен информацией и время начала обмена.

Злоумышленник будет подключен в общий свитч вместе с компьютерами ViPNet сети. Схема испытания на Рис.79.

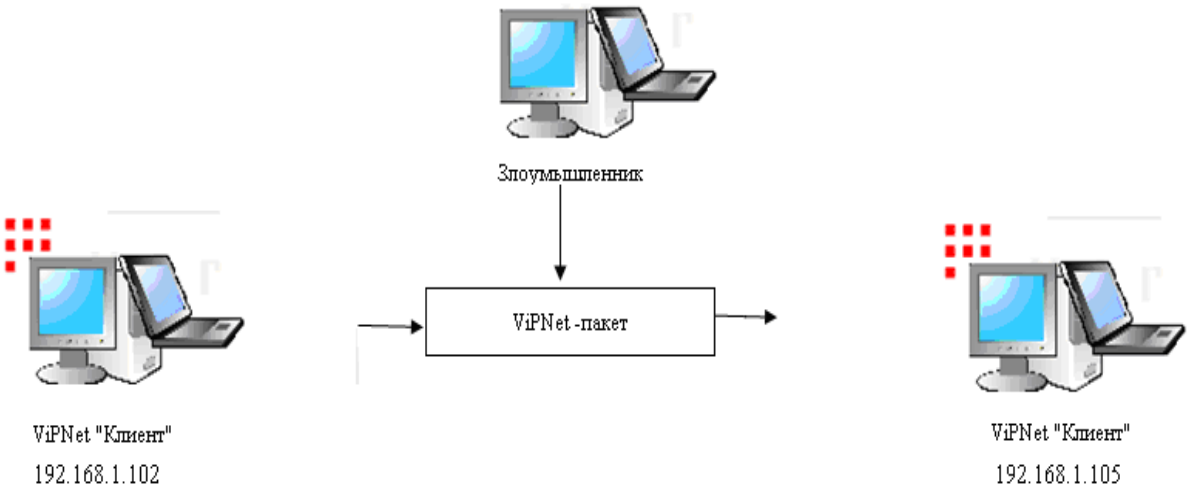


Рис. 79. Схема эксперимента

ПО Злоумышленника.

Программа-сниффер Wireshark программа для анализа пакетов Ethernet и некоторых других сетей. Функциональность, которую предоставляет. Программа позволяет пользователю просматривать весь проходящий по сети трафик в режиме реального времени, переводя сетевую карту в широковещательный режим. Wireshark различает структуру самых различных сетевых протоколов, и поэтому позволяет разобрать сетевой пакет, отображая значение каждого поля протокола любого уровня. Wireshark умеет работать с множеством форматов исходных данных, соответственно, можно открывать файлы данных, захваченных другими программами, что расширяет возможности захвата.

Программа расшифровки данных. Advanced EFS Data Recovery (AEFSDR) - программа для расшифровки файлов, зашифрованных под операционными системами Windows 2000 и Windows XP, Windows 2003 Server и Windows Vista. Программа позволяет расшифровывать файлы даже в том случае, если система не грузится или повреждены некоторые записи о ключах шифрования. Даже если база пользователей системы защищена SYSKEY, AEFSDR .

Действия злоумышленника

С помощью программы снифер Wireshark во время обмена сообщениями между узлами сети с ПО ViPNet «Клиент», перехватить передаваемые пакеты и экспортировать их в файл.

С помощью программы расшифровки данных расшифровать информацию содержащуюся в экспортированном из Wireshark файле.

Ход испытания

С АП с ПО ViPNet «Клиент» с IP-адресом «192.168.1.102» посылается сообщение через службу мгновенного обмена сообщениями ViPNet другому АП с ПО ViPNet «Клиент» с IP-адресом «192.168.1.104».

Во время обмена сообщениями одного компьютера с другим, злоумышленник начинает «прослушивать» локальную сеть со своего компьютера с помощью снифера Wireshark (Рис 80). Программа обнаруживает сеанс связи между машинами, записывает информацию, проходящую от одного абонента к другому, распознает пакеты и записывает их в файл.

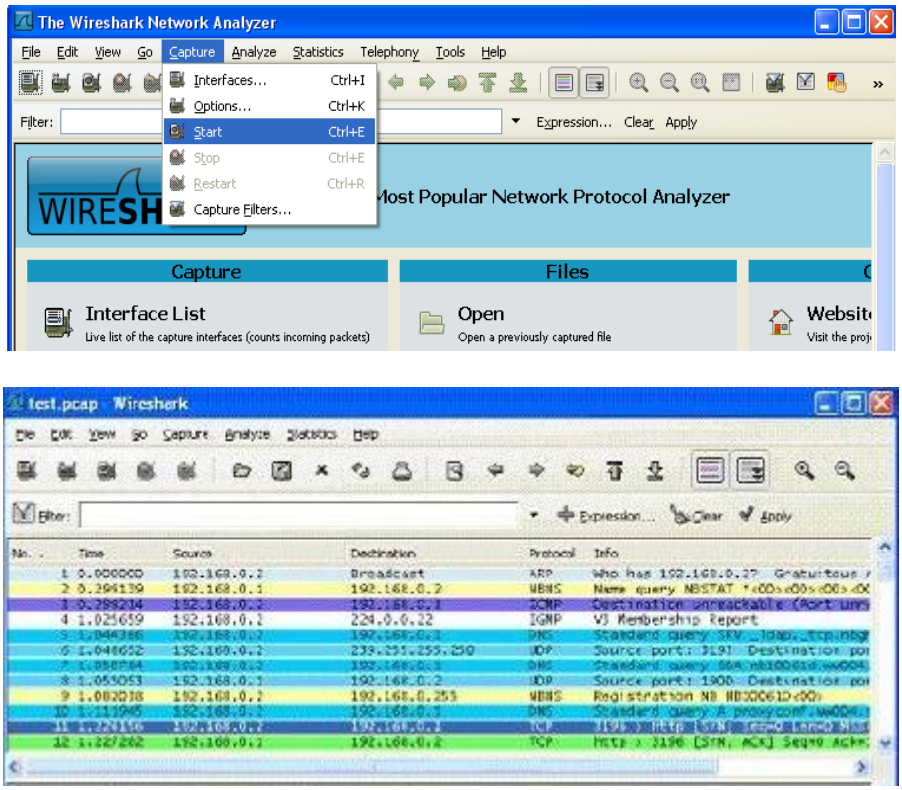


Рис. 80. Старт программы Wireshark

Файл, в который были записаны перехваченные пакеты нужно расшифровать при помощи программы (Брутфорс) Advanced EFS Data Recovery (Рис.81, Рис.82).

Рис. 81. Меню программы Advanced EFS Data Recovery

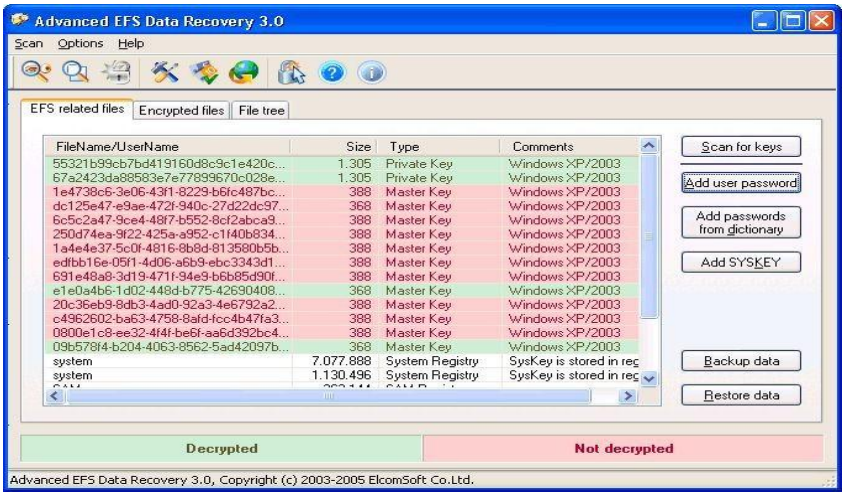


Рис. 82. Старт программы Advanced EFS Data Recovery

После старта брутфорсер начинает расшифровывать содержимое ViPNet-пакетов и зависает. После жесткой перезагрузки операционной системы, злоумышленник повторяет попытку расшифровки, после чего процесс длится на протяжении пяти дней без результатов.

Результаты эксперимента и их анализ

В ходе эксперимента было установлено:

Злоумышленнику удалось перехватить ViPNet-пакеты, с помощью специализированной программы Wireshark и записать содержимое в файл.

Содержимое ViPNet-пакета невозможно расшифровать с помощью программы предназначенной для взлома, в течении пяти дней.

Злоумышленнику были предоставлены достаточно благоприятные условия для несанкционированного доступа к защищенной информации ViPNet сети, но даже в этих условиях имея в своем распоряжении программы сниффер и брутфорс, злоумышленнику не удается получить доступ к защищаемой информации.

Заключение

В результате проделанной работы была спроектирована защищенная сеть передачи данных использующая открытые каналы связи. Для построения сети было использовано программное обеспечение: ViPNet «Администратор 3.0», ViPNet «Координатор 3.0», ViPNet «Клиент».

На рабочей станции администратора, используя ПО ViPNet «Администратор 3.0 , в адресной администрации, Центра управления сетью.

Были зарегистрированы серверы-маршрутизаторы, криптосервис, абонентские пункты, центр регистрации, сервис публикации. Были созданы межсерверные каналы связи между координаторами. «СМ-Координатор 3.0» и «СМ-Координатор-ОИ3.0» и заданы параметры их работы.

Для «СМ Координатор-ОИ 3 0» включена функция «Сервер Открытого Интернета», для «СМ Координатор 3.0» функция «Туннелирование». Созданы справочники, в которых отображается информация, необходимая для работы прикладных программ ViPNet (Монитор, Деловая Почта и др.), а так же базы данных, которые будут служить для восстановления информации о структуре сети.

В Удостоверяющем ключевом центре создана ключевая инфраструктура защищенной сети, сформированы дистрибутивы для пользователей созданной защищенной сети. При создании дистрибутива пользователя автоматически формируется его сертификат ЭЦП.

Был развернут защищенный узел Администратора 3.0.

На Координаторе сети

В программе «Координатор .Монитор» созданы два сетевых интерфейса внешний «internet» для глобальной сети и внутренний «Local subnet» для локальной сети. На обоих интерфейсах установлен второй режим безопасности.

Произведены настройки сетевых интерфейсов компьютера, заданы режимы безопасности и настройки антиспуфинга.

В правилах антиспуфинга для каждого сетевого интерфейса заданы диапазоны IP-адресов, пакеты от которых допустимы на интерфейсе. При этом пакеты, в которых IP-адрес отправителя не попадает в допустимый диапазон адресов, указанный на сетевом интерфейсе, будут блокироваться.

Былы настроены параметры и режимы соединения узлов сети, установлены сетевые фильтры в защищенной и открытой сети.

На клиентских рабочих станциях с ПО ViPNet «Клиент», установлены программы: ViPNet «Клиент.Деловая почта», ViPNet «Клиент.Монитор»,

В качестве сервера IP- адресов выбран Координатор ViPNet сети.

Установлен третий режим безопасности (Разрешить инициативные открытые соединения) разрешает взаимодействие только с теми компьютерами, информацию от которых запросил сам пользователь, работающий за сетевым экраном ViPNet.

Осуществлена настройка фильтров открытой сети.

После завершения создания защищенной сети было произведено испытание.

Целью испытания являлось выявления возможности несанкционированного доступа к информации, передаваемой между узлами защищенной сети ViPNet Custom.

Эксперимент проводился в локальной сети компании «Бизнес защита». Результаты эксперимента приведены в Приложении Б.

Защищенная сеть передачи данных на базе технологии ViPNet Custom найдет широкое применение в организациях, которые заботятся о безопасности своих информационных ресурсах и материальной благополучности, так как восстановить, утраченную информацию, бывает гораздо дороже, чем защитить.

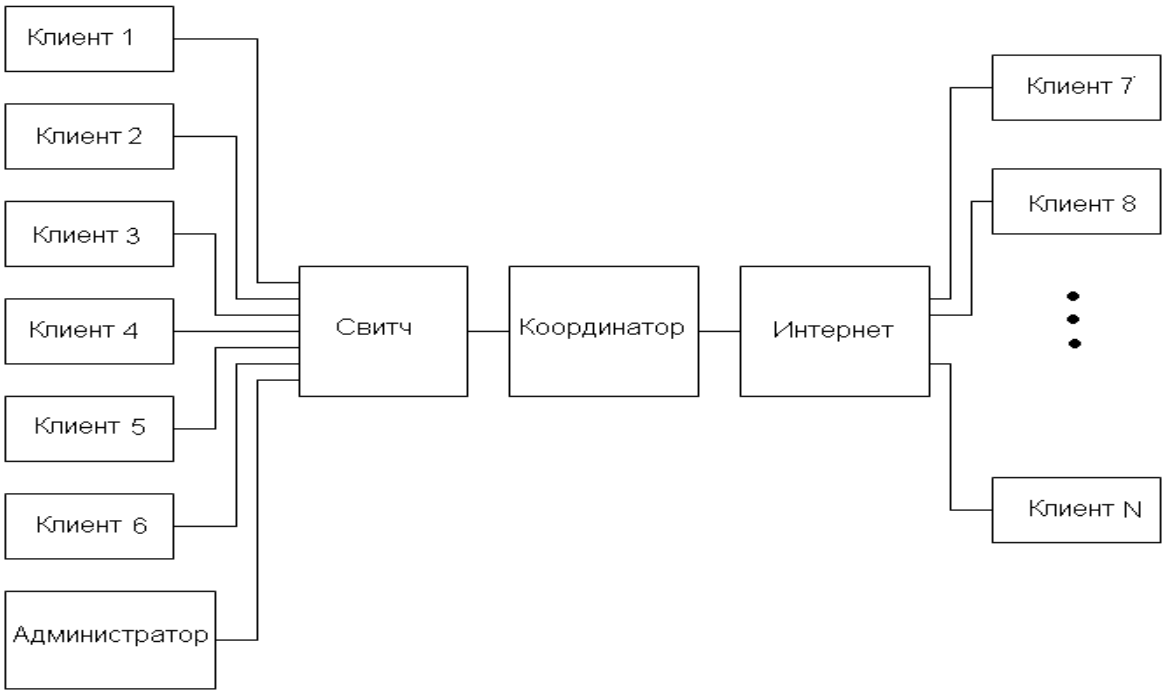


Рис. 83. Защищенная сеть на базе технологии ViPNet Custom

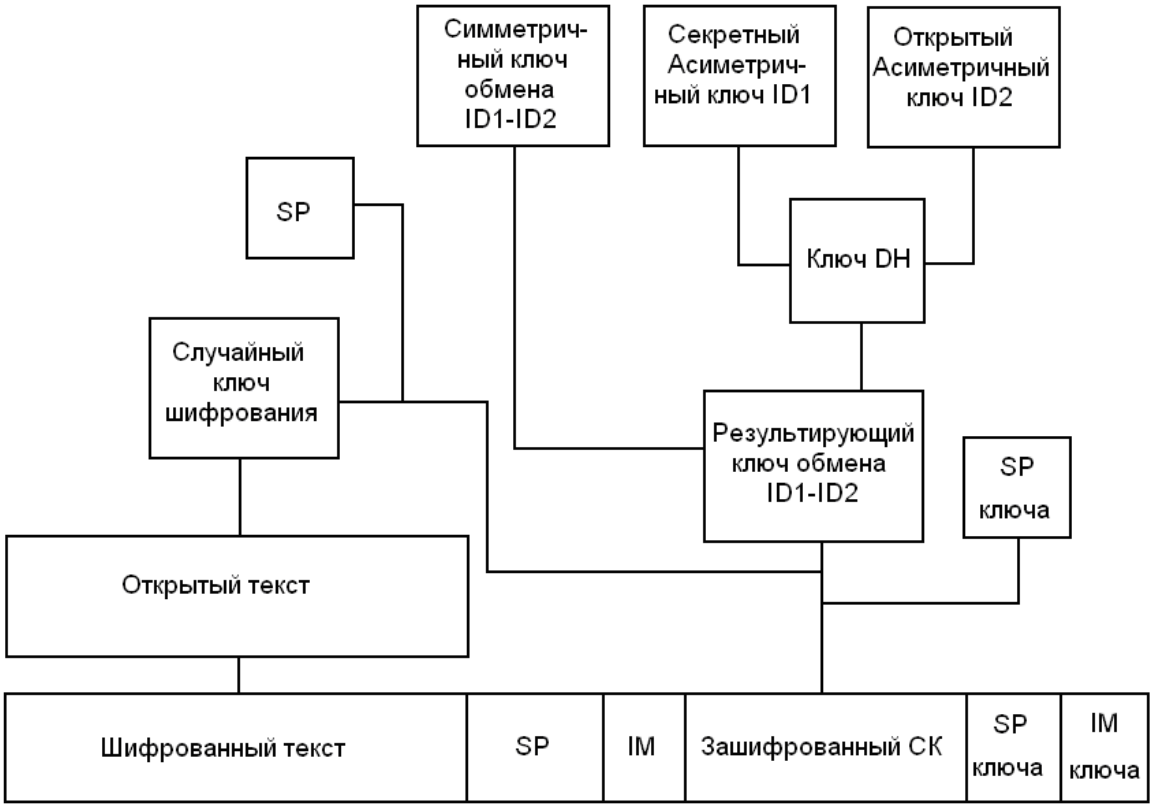


Рис. 84. Шифрование на прикладном уровне

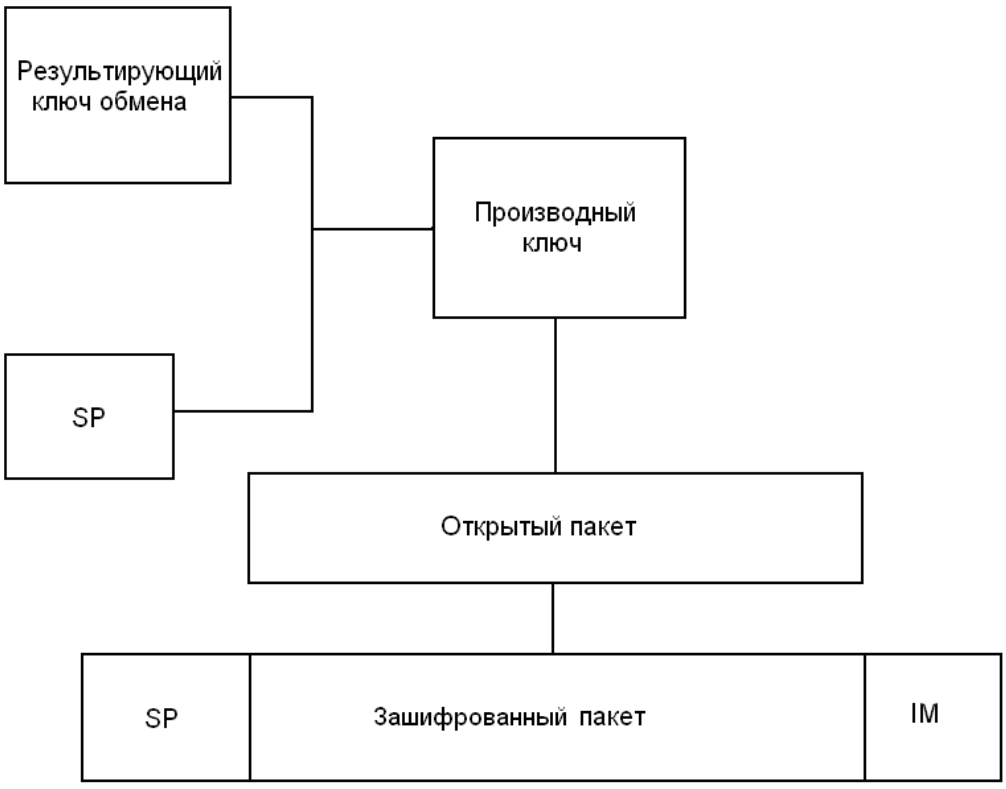


Рис.85. Шифрование на сетевом уровне

Порядок испытаний защищенной сети ViPNet Custom

Объект испытаний: защищенная сеть передачи данных ViPNet Custom.

Цель испытаний: выявления возможности несанкционированного доступа к информации, передаваемой между узлами защищенной сети ViPNet Custom.

Время ценности информации один день.

Программные средства для исследования.

1. Две рабочие станции с ПО ViPNet «Клиент».
2. Рабочая станция (Злоумышленник) с программй-сниффер Wireshark и брутфорс Advanced EFS Data Recovery.

Результаты испытаний.

1. С рабочей станции подключенной в сеть с ViPNet Custom произведен перехват информации передающейся между двумя клиентами ViPNet сети при помощи программы Wireshark.
2. Перехваченные пакеты распознаны и записаны в файл программой Wireshark.
3. Произведена попытка расшифровать записанный файл с перехваченными информационными пакетами при помощи программы Advanced EFS Data Recovery.
4. Программа Advanced EFS Data Recovery не смогла расшифровать файл в течении пяти суток.
5. Перехваченная информация потеряла свою ценность нерасшифрованной.

Выводы

В результате проведения испытаний системы.

Злоумышленнику удалось перехватить ViPNet-пакеты, с помощью специализированной программы Wireshark и записать содержимое в файл.

Содержимое ViPNet-пакета невозможно расшифровать с помощью программы предназначенной для взлома, в течении пяти суток.

Злоумышленнику были предоставлены достаточно благоприятные условия для несанкционированного доступа к защищенной информации ViPNet сети, но даже в этих условиях имея в своем распоряжении программы сниффер и брутфорс, злоумышленнику не удается получить доступ к защищаемой информации.

Защищенная сеть передачи данных ViPNet Custom является криптостойкой.

5. Рекомендованная литература.

1. Чефранова А. О. Игнатов В. В. Уривский А. В. И др. Виртуальные защищенные сети VIPNet. Курс лекций: Учебное пособие.-3 изд., переработанное. - М.: Изд-во «Прометей», 2008. – 172 с.
2. Чефранова А. О. Горбачук А. П. Стародубов А. Г. Технология построения виртуальных защищенных сетей VIPNet версии 3.0: Практикум: Учебно-методическое пособие. – М.: Изд-во «11-формат», 2008. -260 с.
3. Олифер В. Г., Олифер Н. А. Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов. — СПб.: Изд-во «Питер», 2001.-672с.
4. Иванов М. А. Криптографические методы защиты информации в компьютерных системах и сетях. — М.: Изд-во «КУДИЦ-ОБРАЗ», 2001. - 368 с.
5. Запечников С. В. , Милославская Н. Г. , Толстой А. И. . Основы построения виртуальных частных сетей. Курс лекций: Для высших учебных заведений. – М.: Изд-во «Горячая Линия – Телеком», 2003. – 248 с.

Лабораторная работа 2. Исследование характеристик системы IP-видеонаблюдения на основе стандарта IEEE 802.11 и технологии VPN

1. **Цель работы**
   - Исследование информационной безопасности беспроводных сетей.
   - Изучение основных стандартов и принципов построения, работы и защиты беспроводных сетей.
   - Исследование модели Системы IP-видеонаблюдения на основе технологии Wi-Fi VPN.

2. **Краткие теоретические сведения**

Введение

Целью данной работы является ознакомление с информацией по информационной безопасности беспроводных сетей и создание макета системы IP-видеонаблюдения посредством технологии Wi-Fi.

Беспроводные технологии — подкласс информационных технологий, служат для передачи информации на расстояние между двумя и более точками, не требуя связи их проводами. Для передачи информации может использоваться инфракрасное излучение, радиоволны, оптическое или лазерное излучение.

Сейчас существует множество беспроводных технологий, наиболее часто известных пользователям по их маркетинговым названиям, таким как Wi-Fi, WiMAX, Bluetooth. Каждая технология обладает определёнными характеристиками, которые определяют её область применения.

В настоящее время широкое распространение стали получать системы наружного видеонаблюдения, устанавливаемые на зданиях и других объектах на улицах наших городов.
В зависимости от предназначения системы видеонаблюдения (СВН) могут иметь различные масштабы. Это может быть система, обслуживающая одно здание, комплекс зданий, охраняемых частной охранной организацией. В этом случае система разворачивается сразу в полном объеме и в будущем подвергается не слишком сильной трансформации. Либо это может быть СВН, охватывающая группу жилых зданий, квартал, улицу, а иногда и целый населенный пункт для передачи информации на пульт дежурных отдела внутренних дел, управления вневедомственной охраны или других структур, обеспечивающих безопасность населения. В этом случае структура СВН должна быть изначально разработана таким образом, чтобы в будущем допускать простое масштабирование путем подключения дополнительных устройств видеонаблюдения без внесений кардинальных изменений в структуру системы.

В последнее время все большую популярность приобретают системы видеонаблюдения на базе сетевых или иначе IP-видеокамер, так как они имеют ряд несомненных преимуществ по сравнению с аналоговыми системами. Отметим некоторые из них: возможность построения распределенных систем с использованием публичных сетей (например, Интернет) для передачи видео, возможность предоставления доступа к просмотру видео или к архиву большому числу пользователей, удаленный доступ к системе и другие.

Существует мнение, что самой слабой точкой систем IP-видеонаблюдения является использование стандартного сетевого оборудования, что позволяет говорить об их общей ненадежности и незащищенности перед злоумышленниками.

При правильном выборе сетевого оборудования и его настройке процесс обеспечения безопасности сети для IP-видеонаблюдения принципиально ничем не отличается от корпоративной компьютерной сети, и, более того, эти сети могут сосуществовать в пределах одной корпоративной компьютерной сети. Системы IP-видеонаблюдения не только не

уступают аналоговым системам по показателям безопасности, но и, при условии грамотного применения механизмов защиты, значительно более защищены от воздействий как неопытных хакеров, так и достаточно квалифицированных злоумышленников.

1 Теоретическая часть

1.1 IEEE 802.11

IEEE 802.11 - набор стандартов связи, для коммуникации в беспроводной локальной сетевой зоне частотных диапазонов 2,4; 3,6 и 5 ГГц.

Пользователям более известен по названию Wi-Fi, фактически являющийся брендом, предложенным и продвигаемым организацией Wi-Fi Alliance. Получил широкое распространение благодаря развитию в мобильных электронно-вычислительных устройствах: КПК и ноутбуков.

Изначально стандарт IEEE 802.11 предполагал возможность передачи данных по радиоканалу на скорости не более 1 Мбит/с и опционально на скорости 2 Мбит/с. Один из первых высокоскоростных стандартов беспроводных сетей - IEEE 802.11a - определяет скорость передачи уже до 54 Мбит/с. Рабочий диапазон стандарта 5ГГц.

Вопреки своему названию, принятый в 1999 году стандарт IEEE 802.11b не является продолжением стандарта 802.11a, поскольку в них используются различные технологии: DSSS (точнее, его улучшенная версия HR-DSSS) в 802.11b против OFDM в 802.11a. Стандарт предусматривает использование нелицензируемого диапазона частот 2,4 ГГц.Скорость передачи до 11Мбит/с

Продукты стандарта IEEE 802.11b, поставляемые разными изготовителями, тестируются на совместимость и сертифицируются организацией Wireless Ethernet Compatibility Alliance (WECA), которая в настоящее время больше известна под названием Wi-Fi Alliance. Совместимые беспроводные продукты, прошедшие испытания по программе «Альянса Wi-Fi», могут быть маркированы знаком Wi-Fi.

В настоящее время IEEE 802.11b - самый распространённый стандарт, на базе которого построено большинство беспроводных локальных сетей.

Проект стандарта IEEE 802.11g был утверждён в октябре 2002 г. Этот стандарт предусматривает использование диапазона частот 2,4 ГГц, обеспечивая скорость передачи 54 Мбит/с и превосходя, таким образом, ныне действующий стандарт IEEE 802.11b, который обеспечивает скорость передачи 11 Мбит/с. Кроме того, он гарантирует обратную совместимость со стандартом 802.11b. Обратная совместимость стандарта IEEE 802.11g может быть реализована в режиме модуляции DSSS, и тогда скорость передачи будет ограничена одиннадцатью мегабитами в секунду либо в режиме модуляции OFDM, при котором скорость составляет 54 Мбит/с. Таким образом, данный стандарт является наиболее приемлемым при построении беспроводных сетей.

1.2 Подходы к классификации беспроводных технологий

Существуют различные подходы к классификации беспроводных технологий.

1. По дальности действия можно выделить:

- Беспроводные персональные сети (WPAN - Wireless Personal Area Networks). Примеры технологий - Bluetooth.
- Беспроводные локальные сети (WLAN - Wireless Local Area Networks). Примеры технологий -Wi-Fi.
- Беспроводные сети масштаба города (WMAN - Wireless Metropolitan Area Networks). Примеры технологий - WiMAX.

I. По топологии:

- "Точка-точка".

- "Точка-многоточка".

II. По области применения можно выделить:

- Корпоративные (ведомственные) беспроводные сети - создаваемые компаниями для собственных нужд.
- Операторские беспроводные сети - создаваемые операторами связи для возмездного оказания услуг.

Кратким, но ёмким способом классификации может служить одновременное отображение двух наиболее существенных характеристик беспроводных технологий на двух осях: максимальная скорость передачи информации и максимальное расстояние.

1.2.1 Отличия проводных и беспроводных технологий передачи данных

Таблица 1.2.1 Отличия проводных и беспроводных технологий передачи данных

Характеристика	Проводные	Беспроводные
Среда передачи	Кабель (медный, оптический)	Кабель не требуется, передача при помощи электромагнитных волн
Пропускная способность	Высокая	Ограниченная
Расстояния между точками	Большие	Как правило, ограничены
Мобильность абонентов	Не обеспечивается	Может быть обеспечена
Характеристика	Проводные	Беспроводные

1.2.2 Список стандартов серии 802.11

Замечание: 802.11F и 802.11T являются рекомендациями, а не стандартами, поэтому используются заглавные буквы.

Таблица 1.2.2 характеристики стандартов Wi-Fi

Стандарт	Примечание	Скорость	Частоты	Год принятия
IEEE 802.11	Изначальный	1 Мбит/с и 2 Мбит/с	2,4 ГГц и ИК	1997
IEEE 802.11a		54 Мбит/с,	5 ГГц	1999, выход продуктов в 2001
IEEE 802.11b	Улучшения к 802.11	5,5 и 11 Мбит/с		1999
IEEE 802.11c	Процедуры операций с мостами; включен в стандарт IEEE 802.1D			2001
IEEE 802.11d	Интернациональные роуминговые расширения			2001
IEEE 802.11e	Улучшения: QoS, включение packet bursting			2005
IEEE 802.11F	Inter-Access Point Protocol			2003
IEEE 802.11g	обратная совместимость с b	54 Мбит/с	2,4 ГГц	2003
IEEE 802.11h	Распределенный по спектру 802.11a для совместимости в Европе		5 GHz	2004
IEEE 802.11i	Улучшенная безопасность			2004
IEEE 802.11j	Расширения для Японии			2004
IEEE 802.11k	Улучшения измерения радио			

	ресурсов			
IEEE 802.11l	зарезервирован			
IEEE 802.11m	Поддержание эталона; обрезки			
IEEE 802.11n	Обратная совместимость с 802.11a/b/g	600 Мбит/с	2,4-2,5 или 5 ГГц	2009
IEEE 802.11o	зарезервирован			
IEEE 802.11p	WAVE - Wireless Access for the Vehicular Environment (Беспроводной Доступ для Транспортной Среды, такой как машины скорой помощи или пассажирский транспорт)			
IEEE 802.11q	зарезервирован			
IEEE 802.11r	Быстрый роуминг			
IEEE 802.11s	ESS Mesh Networking			
IEEE 802.11T	Wireless Performance Prediction (WPP, Предсказание Производительности Беспроводного Оборудования) - методы тестов и измерений			
IEEE 802.11u	взаимодействие с не-802 сетями (например, сотовые сети)			
IEEE 802.11v	Управление беспроводными сетями			
IEEE 802.11x	зарезервирован и не будет использоваться.			
IEEE 802.11y	дополнительный стандарт связи на расстояния до 5000 м на открытом пространстве.	3,65-3,70 ГГц.	54 Мбит/с	
IEEE 802.11w	Protected Management Frames (Защищенные Управляющие Фреймы)			

Рассмотрим основные рабочие стандарты Wi-Fi относительно рабочей скорости передачи данных и используемых рабочих частот.

Таблица 1.2.3 характеристики различных стандартов Wi-Fi

Стандарт	Скорость работы/рабочее расстояние	Рабочие частоты, ГГц	Примечание
802.11b	В закрытых помещениях: 30 м (11/5 Мбит/с), 91 м (1/0,5 Мбит/с). В открытых помещениях в пределах прямой видимости: 120 м (11/5 Мбит/с), 460 м (1/0,5 Мбит/с)	2,4 (2,4-2,4835)	Появился в 1999 г.

802.11g	В закрытых помещениях: 30 м (54/25 Мбит/с), 91 м (1/0,5 Мбит/с). В открытых помещениях в пределах прямой видимости: 120 м (54/25 Мбит/с), 460 м (1/0,5 Мбит/с)	2,4(2,4-2,4835)	Появился в 2003 г. Именно этот стандарт поддерживает большинство современных IP-видеокамер
802.11a	В закрытых помещениях: 12м (54/25 Мбит/с), 91 м (6/3 Мбит/с). В открытых помещениях в пределах прямой видимости: 30 м (54/25 Мбит/с), 305 м (6/3 Мбит/с)	5(5,15-5,350 и 5,725-5,825)	Появился в 1999 г. в России. Оборудование, работающее в этом частотном диапазоне, использовать не разрешено, поскольку его применяют для своих целей государственные службы
802.11n	200+/100 Мбит/с	2,4 или 5 ГГц	2009 г.

1.2.3 Стандарты сетей 802.11b/g/n

1.2.3.1 Оригинальный 802.11 MAC

Исходный стандарт 802.11 определяет два метода передачи на физическом уровне.

- Технология расширения спектра путем скачкообразной перестройки частоты (FHSS) в диапазоне 2,4 ГГц.
- Технология широкополосной модуляции с расширением спектра методом прямой последовательности (DSSS) в диапазоне 2,4 ГГц.

Обе эти 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 поддерживают скорости передачи 1 и 2 Мбит/с. Как следует из названия, устройства FHSS осуществляют скачкообразную перестройку частоты по некоторой предопределенной схеме. Устройства FHSS делят предназначенную для их работы полосу частот от 2,402 до 2,480 ГГц на 79 неперекрывающихся каналов. Ширина каждого из 79 каналов составляет 1 МГц, поэтому беспроводные локальные сети FHSS используют относительно высокую скорость передачи символов, 1 МГц, и намного меньшую скорость перестройки с канала на канал.

Последовательность перестройки частоты должна иметь следующие параметры: частота перескоков не менее 2,5 раз в секунду как минимум между 6-ю (6 МГц) каналами. Чтобы минимизировать число коллизий между перекрывающимися зонами покрытия, возможные последовательности перескоков должны быть разбиты на три набора последовательностей, длина которых 26

По сути, схема скачкообразной перестройки частоты обеспечивает неторопливый переход с одного возможного канала на другой таким образом, что после каждого скачка покрывается полоса частот, равная как минимум 6 МГц, благодаря чему в многосотовых сетях минимизируется возможность возникновения коллизий

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

В спецификации стандарта 802.11 оговорено использование и другого физического уровня — на основе технологии широкополосной модуляции с расширением спектра методом

прямой последовательности (DSSS). Как было указано в стандарте 802.11 разработки 1997 года, технология DSSS поддерживает скорости передачи 1 и 2 Мбит/с. В 1997 году рабочая группа ратифицировала стандарт 802.11b, позволяющий поддерживать скорости передачи 5,5 и 11 Мбит/с. Физический уровень DSSS стандарта 802.11b совместим с существующими WLAN стандарта 802.11. Подуровень PLCP технологии DSSS стандарта 802.11b такой же, как и для стандарта 802.11, лишь с дополнительными опциональными короткими преамбулой и заголовком.

Беспроводные локальные сети DSSS используют каналы шириной 22 МГц, благодаря чему многие WLAN могут работать в одной и той же зоне покрытия. Каналы шириной 22 МГц позволяют создать в диапазоне 2,4—2,483 ГГц три неперекрывающихся канала передачи.

Технология DSSS стандарта 802.11

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.

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 отбеленный 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 используют метод модуляции, при котором для передачи информации используется сигнал, спектр которого намного шире того, который необходим для передачи информации, и передается она с намного меньшей скоростью. Каждый бит заменяется или расширяется кодом, расширяющим полосу частот. Во многом благодаря кодированию (поскольку информация заменяется намного большим числом информационных битов) эта технология позволяет передавать информацию при малом соотношении сигнал/шум, обусловленным или помехами, или недостаточной мощностью передатчика. При использовании DSSS переданный сигнал, по сути, усиливается за счет применения расширяющей последовательности, совместно используемой передатчиком и приемником.

Беспроводные локальные сети типа DSSS особым образом кодируют данные, получая поток данных со скоростью 1 Мбит/с с канального уровня и преобразуя его в 11-мегагерцевый поток элементарных сигналов, или чипов (chip). Расширяющая спектр последовательность (ее еще называют расщепляющей (chipping) последовательностью или последовательностью Баркера), которая преобразует биты данных в элементарные сигналы, имеет длину 11 бит. В случае работы на скорости 1 и 2 Мбит/с один бит данных "расширяется" до 11 (двоичная 1 расширяется до значения 11111111111, а двоичный 0 — до значения 00000000000). "Расширенные" биты данных затем подаются на схему "ИЛИ" либо "исключающее ИЛИ" одновременно с расширяющей последовательностью, получившиеся в результате чипы преобразуются в символы и модулируются.

11-чиповая последовательность представляет один бит данных. Предположим, например, что расщепленная последовательность передается через беспроводную среду. В ходе передачи в нескольких частотных каналах на сигнал накладываются помехи. Поскольку передатчик расширил спектр передаваемого сигнала до 22 МГц, только несколько чипов последовательности окажутся подверженными их влиянию. Приемник сможет восстановить

исходную последовательность по полученным чипам. В качестве противоположного данному процессу можно рассматривать таковой получения необработанных данных; в этом случае часть данных из-за помех будет потеряна, и потребуется повторная их передача. При расширении спектра методом прямой последовательности все частоты канала используются для повышения пропускной способности канала и снижения задержек.

1.2.3.2 IEEE 802.11b

Стандарт 802.11b, появившийся в 1999 году, регламентировал правила использования высокоскоростной технологии DSSS (HR-DSSS), обеспечивающей скорость передачи в локальных беспроводных сетях ISM-диапазона 2,4 ГГц вплоть до 5,5 и 11 Мбит/с. При этом используется кодирование с использованием комплементарных кодов (complementary code keying, CCK) или технология двоичного пакетного сверточного кодирования (packet binary convolutional coding, PBCC). В технологии HR-DSSS используется та же схема организации каналов, что и в технологии DSSS, — полоса частот шириной 22 МГц, 11 каналов, 3 неперекрывающихся, ISM-диапазон 2,4 ГГц.

Модуляция ССК на подуровне PMD стандарта 802.11b

Хотя механизм расширения спектра, используемый для получения скоростей 5,5 и 11 Мбит/с с применением ССК, относится к методам, которые применяются для скоростей 1 и 2 Мбит/с, он по-своему уникален. В обоих случаях применяется метод расширения, но при использовании модуляции ССК расширяющий код представляет собой код из 8 комплексных чипов (complex chip), в то время как при работе со скоростями 1 и 2 Мбит/с применяется 11-разрядный код. 8-чиповый код определяется или 4, или 8 битами — в зависимости от скорости передачи данных. Скорость передачи чипов составляет 11 Мчип/с, т.е. при 8 комплексных чипах на символ и 4 или 8 битов на символ можно достигнуть скорости передачи данных 5,5 и 11 Мбит/с.

Технология двоичного пакетного сверточного кодирования (PBSS)

Как уже говорилось, стандарт HR-DSSS определяет также опциональный механизм модуляции для передачи данных со скоростью 5,5 и 11 Мбит/с. Эта технология отличается как от ССК, так и от DSSS стандарта 802.11. Вначале скремблированные биты PSDU передаются на двоичный сверточный кодер, работающий с эффективной степенью кодирования 1/2. Особый полускоростной кодер (particular half-rate encoder) имеет шесть линий задержки (delay), или запоминающих ячеек, и выдает 2 бита на каждый входной. Поскольку стандарт 802.11 рассчитан на использование фреймов и сверточные кодеры имеют память, все элементы задержки обнуляются с началом фрейма, а в его конец добавляется один октет нулей, чтобы обеспечить одинаковую помехоустойчивость для всех битов. Этот заключительный октет объясняет, почему вычисления длины слегка отличаются для ССК и PLCP. Затем закодированный поток бит пропускается через преобразователь символов (symbol mapper) BPSK, чтобы достичь скорости передачи данных 5,5 Мбит/с, или через преобразователь символов QPSK, чтобы реализовать передачу со скоростью 11 Мбит/с. (Здесь не применяется относительное кодирование.) Особое преобразование символов, используемое в данном случае, зависит от двоичного значения, s, поступающего от 256-битовой псевдослучайной последовательности.

1.2.3.3 IEEE 802.11g

Стандарт IEEE 802.1 lg, предложенный в июне 2003 года, определил технологию EPR как средство обеспечения скоростей передачи до 54 Мбит/с в диапазоне ISM 2,4 ГГц; он позаимствовал методы OFDM стандарта 802.11a. В противоположность стандарту 802.11a этот обеспечивает обратную совместимость со стандартом 802.11b, поскольку устройства,

соответствующие стандарту 802.1 lg, могут изменять скорость передачи данных до значений, меньших, чем регламентированы стандартом 802.11b. Определены три схемы модуляции: ERP-OFDM, ERP-PBCC и DSSS-OFDM. При использовании ERP-OFDM задействуются специально разработанные для нее механизмы, обеспечивающие скорость передачи 6, 9, 12, 18, 24, 36, 48, и 54 Мбит/с, из них обязательными являются скорости 6, 12 и 24 Мбит/с в дополнение к скоростям передачи данных 1, 2, 5,5 и 11 Мбит/с. Стандарт также позволяет опционально использовать режимы PBCC со скоростями 22 и 33 Мбит/с и также опционально режимы DSSS-OFDM со скоростями 6, 9, 12, 18, 24, 36, 48 и 54 Мбит/с.

Модуляция для беспроводных локальных сетей стандарта 802.11g

ERP-OFDM

Как уже говорилось, ERP-OFDM обеспечивает механизм для использования скоростей передачи данных стандарта 802.11a в диапазоне ISM таким образом, что обеспечивается обратная совместимость с технологиями DSSS и HR-DSSS. В дополнение к использованию модуляции OFDM стандарта 802.11a по схеме распределения частот диапазона 2,4 ГГц ERP-OFDM также устанавливает, что центральная частота передачи и тактовая частота символов определяются тем же генератором, который был опциональным для DSSS. Он использует канальный интервал длительностью 20 мкс, но она может быть уменьшена до 9 мкс, если выяснится, что в BSS находятся только устройства ERP.

ERP-PBCC

Для передачи данных с более высокими скоростями, 22 и 33 Мбит/с, технология двоичного пакетного сверточного кодирования (PBCC) использует тот же механизм, что и на меньших скоростях, 5,5 и 11 Мбит/с PBCC, но с использованием 8-PCK вместо QPCK и BPCK для достижения скорости 22 Мбит/с. Скорость 33 Мбит/с достигается за счет применения генератора с частотой 16,5 МГц вместо генератора с частотой 11 МГц.

Главное, что следует помнить относительно стандарта 802.1 lg, состоит в следующем. Он увеличивает поддерживаемые скорости передачи данных в диапазоне 2,4 ГГц до 54 Мбит/с способом, обеспечивающим обратную совместимость со старыми устройствами, соответствующими стандарту 802.11b. Если в локальной сети используются только устройства стандарта 802.11g, передача осуществляется с наивысшей возможной скоростью. Однако, если в нее вводятся устройства стандарта 802.11b, информация заголовков должна передаваться со скоростями стандарта 802.11b, чтобы их могли "понимать" эти старые устройства. Такое снижение скорости должно выполняться при всех передачах, независимо от того, происходят они между устройствами стандарта 802.11g или 802.11b. Конечным эффектом оказывается общее увеличение накладных расходов, но это — небольшая цена за обратную совместимость, обеспечиваемую стандартом 802.11g.

1.2.3.4 IEEE 802.11n

IEEE 802.11n — новейшая версия стандарта 802.11 для сетей Wi-Fi.

Этот стандарт был утверждён 11 сентября 2009.

Стандарт 802.11n повышает скорость передачи данных практически вчетверо по сравнению с устройствами стандартов 802.11g (максимальная скорость которых равна 54 МБит/с), при условии использования в режиме 802.11n с другими устройствами 802.11n. Теоретически 802.11n способен обеспечить скорость передачи данных до **480** Мбит/с. Устройства 802.11n работают в диапазонах 2,4 - 2,5 или 5,0 ГГц.

Кроме того, устройства 802.11n могут работать в трёх режимах:

- наследуемом (Legacy), в котором обеспечивается поддержка устройств 802.11b/g и 802.11a
- смешанном (Mixed), в котором поддерживаются устройства 802.11b/g, 802.11a и 802.11n
- «чистом» режиме — 802.11n (именно в этом режиме и можно воспользоваться преимуществами повышенной скорости и увеличенной дальностью передачи данных, обеспечиваемыми стандартом 802.11n).

Черновую версию стандарта 802.11n поддерживают многие современные сетевые устройства. Итоговая версия стандарта, которая была принята 11 сентября 2009 года, обеспечивает скорость до **600** Мбит/с, Многоканальный вход/выход, известный, как MIMO и большее покрытие.

Особенности стандарта

- **Два частотных диапазона**

Устройства стандарта 802.11n могут работать в одном из двух диапазонов — 2,4 или 5 ГГц. Это намного повышает гибкость их применения, позволяя отстраиваться от источников радиочастотных помех. При выборе подходящей системы ИТ-специалистам следует иметь в виду, что практически все клиенты 802.11n на основе CardBus и ExpressCard пока рассчитаны только на диапазон 2,4 ГГц, но несколько встраиваемых адаптеров и плат типоразмера mini-PCI способны поддерживать оба.

- **Каналы шириной 40 MHz**

Спецификация 802.11n предусматривает использование как стандартных каналов шириной 20 МГц, так и широкополосных — на 40 МГц с более высокой пропускной способностью. Проект её версии 2.0 рекомендует применять 40-мегагерцовые каналы только в диапазоне 5 ГГц, однако пользователи многих устройств такого типа получат возможность вручную переходить на них даже в диапазоне 2,4 ГГц.

- **MIMO**

Ключевой компонент стандарта 802.11n под названием MIMO (Multiple Input, Multiple Output — много входов, много выходов) предусматривает применение пространственного мультиплексирования с целью одновременной передачи нескольких информационных потоков по одному каналу, а также многолучевое отражение, которое обеспечивает доставку каждого бита информации соответствующему получателю с небольшой вероятностью влияния помех и потерь данных. Именно возможность одновременной передачи и приема данных определяет высокую пропускную способность устройств 802.11n.

- **Антенны**

Чаще всего стандартными считаются антенные конфигурации цепи для передачи и приёма информации 3 × 3 или 2 × 3, однако со временем устройства стандарта 802.11n станут поддерживать и другие варианты. В простых недорогих моделях будет реализована схема из одной передающей и двух принимающих цепей (по статистике абоненты потребляют гораздо больше данных, чем передают), тогда как пользователи, которым нужна очень большая скорость передачи данных, смогут приобрести старшие модели с конфигурацией антенн 4 × 4.

- **Обратная совместимость**

Разработчики спецификации 802.11n позаботились о том, чтобы компоненты на её базе сохраняли совместимость с устройствами стандарта 802.11b или 802.11g в диапазоне 2,4 ГГц и с устройствами 802.11a — в диапазоне 5 ГГц. В новых сетях 802.11n еще долгое время будет работать множество прежних беспроводных клиентов, так что при развертывании беспроводных ЛВС администратору следует обязательно предусмотреть их поддержку.

1.3 Основные элементы сети

Для построения беспроводной сети используются Wi-Fi адаптеры и точки доступа.

Адаптер представляет собой устройство, которое подключается через слот расширения PCI, PCMCI, CompactFlash. Существуют также адаптеры с подключением через порт USB 2.0. Wi-Fi адаптер выполняет ту же функцию, что и сетевая карта в проводной сети. Он служит для подключения компьютера пользователя к беспроводной сети. Благодаря платформе Centrino все современные ноутбуки имеют встроенные адаптеры Wi-Fi, совместимые со многими современными стандартами. Wi-Fi адаптерами, как правило, снабжены и КПК (карманные персональные компьютеры), что также позволяет подключать их к беспроводным сетям.

Точка доступа представляет собой автономный модуль со встроенным микрокомпьютером и приемно-передающим устройством.

Рис. 1.3.1. Wi-Fi адаптеры

Через точку доступа осуществляется взаимодействие и обмен информацией между беспроводными адаптерами, а также связь с проводным сегментом сети. Таким образом, точка доступа играет роль коммутатора.

Рис. 1.3.2. Точка доступа

1.3.1 Пропускная способность канала

Максимально возможная при определенных условиях скорость, при которой информация может передаваться по конкретному тракту связи, или каналу, называется пропускной способностью канала.

Существует четыре понятия, которые мы попытаемся связать воедино.

- Скорость передачи данных - скорость в битах в секунду (бит/с), с которой могут передаваться данные;

- Ширина полосы - ширина полосы передаваемого сигнала, ограничиваемая передатчиком и природой передающей среды. Выражается в периодах в секунду, или герцах (Гц);
- Шум. Средний уровень шума в канале связи;
- Уровень ошибок - частота появления ошибок. Ошибкой считается прием 1 при переданном 0 и наоборот.

1.4 Методы доступа к среде в беспроводных сетях

Одна из основных проблем построения беспроводных систем - это решение задачи доступа многих пользователей к ограниченному ресурсу среды передачи. Существует несколько базовых методов доступа (их еще называют методами уплотнения или мультиплексирования), основанных на разделении между станциями таких параметров, как пространство, время, частота и код. Задача уплотнения - выделить каждому каналу связи пространство, время, частоту и/или код с минимумом взаимных помех и максимальным использованием характеристик передающей среды.

- **Уплотнение с пространственным разделением**

Основано на разделении сигналов в пространстве, когда передатчик посылает сигнал, используя код c, время t и частоту f области s_i. То есть каждое беспроводное устройство может вести передачу данных только в границах определенной территории, на которой любому другому устройству запрещено передавать свои сообщения.

К примеру, если радиостанция вещает на строго определенной частоте на закрепленной за ней территории, а какая-либо другая станция в этой же местности также начнет вещать на той же частоте, слушатели радиопередач не смогут получить "чистый" сигнал ни от одной из этих станций. Другое дело, если радиостанции работают на одной частоте в разных городах. Искажений сигналов каждой радиостанции не будет в связи с ограниченной дальностью распространения сигналов этих станций, что исключает их наложение друг на друга.

Характерный пример - системы сотовой телефонной связи.

- **Уплотнение с частотным разделением (Frequency Division Multiplexing - FDM)**

Каждое устройство работает на определенной частоте, благодаря чему несколько устройств могут вести передачу данных на одной территории. Это один из наиболее известных методов, так или иначе используемый в самых современных системах беспроводной связи.

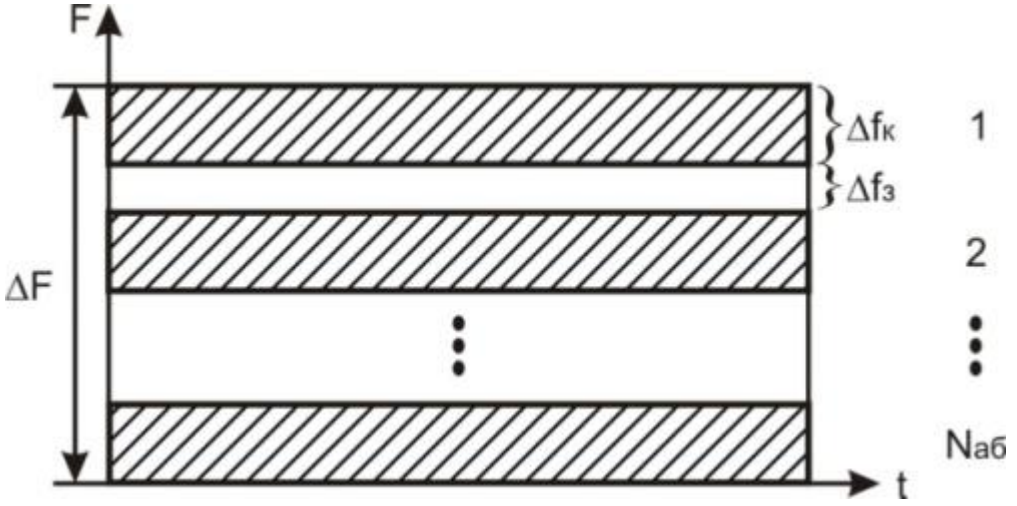


Рис. 1.4.1. Принцип частотного разделения каналов

Наглядная иллюстрация схемы частотного уплотнения - функционирование в одном городе нескольких радиостанций, работающих на разных частотах. Для надежной отстройки друг от друга их рабочие частоты должны быть разделены защитным частотным интервалом, который позволяет исключить взаимные помехи.

Эта схема, хотя и позволяет использовать множество устройств на определенной территории, сама по себе приводит к неоправданному расточительству обычно скудных частотных ресурсов, поскольку требует выделения своей частоты для каждого беспроводного устройства.

- **Уплотнение с временным разделением (Time Division Multiplexing - TDM)**

В данной схеме распределение каналов идет по времени, т. е. каждый передатчик транслирует сигнал на одной и той же частоте f области s, но в различные промежутки времени t_i (как правило, циклически повторяющиеся) при строгих требованиях к синхронизации процесса передачи.

Подобная схема достаточно удобна, так как временные интервалы могут динамично перераспределяться между устройствами сети. Устройствам с большим трафиком назначаются более длительные интервалы, чем устройствам с меньшим объемом трафика.

Основной недостаток систем с временным уплотнением - это мгновенная потеря информации при срыве синхронизации в канале, например из-за сильных помех, случайных или преднамеренных. Однако успешный опыт эксплуатации таких знаменитых TDM-систем, как сотовые телефонные сети стандарта GSM, свидетельствует о достаточной надежности механизма временного уплотнения.

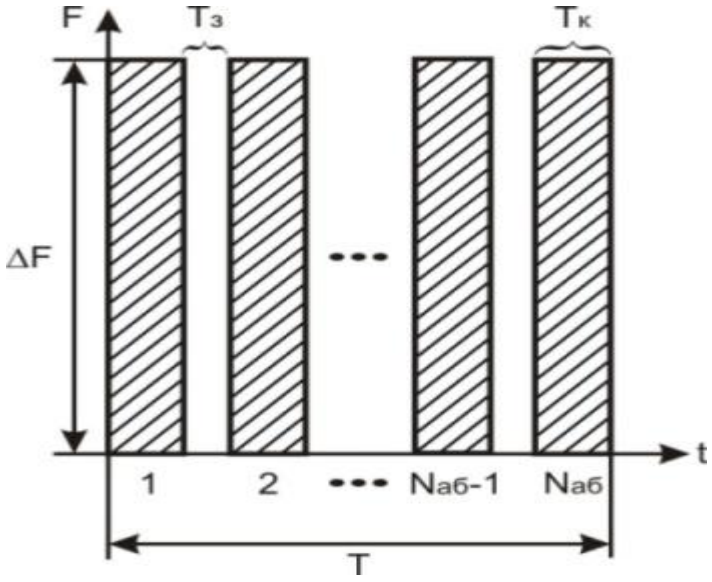


Рис. 1.4.2. Принцип временного разделения каналов

- **Уплотнение с кодовым разделением (Code Division Multiplexing - CDM)**

В данной схеме все передатчики транслируют сигналы на одной и той же частоте f, в области s и во время t, но с разными кодами C_i.

Именем основанного на CDM механизме разделения каналов (CDMA - CDM Access) даже назван стандарт сотовой телефонной связи IS-95a, а также ряд стандартов третьего поколения сотовых систем связи (cdma2000, WCDMA и др.).

В схеме CDM каждый передатчик заменяет каждый бит исходного потока данных на CDM-символ - кодовую последовательность длиной в 11, 16, 32, 64 и т. п. бит (их называют чипами). Кодовая последовательность уникальна для каждого передатчика. Как правило, если

для замены "1" в исходном потоке данных используют некий CDM-код, то для замены "0" применяют тот же код, но инвертированный.

Приемник знает CDM-код передатчика, сигналы которого должен воспринимать. Он постоянно принимает все сигналы и оцифровывает их. Затем в специальном устройстве (корреляторе) производится операция свертки (умножения с накоплением) входного оцифрованного сигнала с известным ему CDM-кодом и его инверсией. В несколько упрощенном виде это выглядит как операция скалярного произведения вектора входного сигнала и вектора с CDM-кодом. Если сигнал на выходе коррелятора превышает некий установленный пороговый уровень, приемник считает, что принял 1 или 0. Для увеличения вероятности приема передатчик может повторять посылку каждого бита несколько раз. При этом сигналы других передатчиков с другими CDM-кодами приемник воспринимает как аддитивный шум. Более того, благодаря большой избыточности (каждый бит заменяется десятками чипов), мощность принимаемого сигнала может быть сопоставима с интегральной мощностью шума. Сходства CDM-сигналов со случайным (гауссовым) шумом добиваются, используя CDM-коды, порожденные генератором псевдослучайных последовательностей. Поэтому данный метод еще называют методом расширения спектра сигнала посредством прямой последовательности (DSSS - Direct Sequence Spread Spectrum); о расширении спектра будет рассказано ниже.

Наиболее сильная сторона данного уплотнения заключается в повышенной защищенности и скрытности передачи данных: не зная кода, невозможно получить сигнал, а в ряде случаев - и обнаружить его присутствие. Кроме того, кодовое пространство несравненно более значительно по сравнению с частотной схемой уплотнения, что позволяет без особых проблем присваивать каждому передатчику свой индивидуальный код. Основной же проблемой кодового уплотнения до недавнего времени являлась сложность технической реализации приемников и необходимость обеспечения точной синхронизации передатчика и приемника для гарантированного получения пакета.

- **Механизм мультиплексирования посредством ортогональных несущих частот (Orthogonal Frequency Division Multiplexing - OFDM)**

Суть этого механизма: весь доступный частотный диапазон разбивается на достаточно много поднесущих (от нескольких сот до тысяч). Одному каналу связи (приемнику и передатчику) назначают для передачи несколько таких несущих, выбранных из множества по определенному закону. Передача ведется одновременно по всем поднесущим, т. е. в каждом передатчике исходящий поток данных разбивается на N субпотоков, где N - число поднесущих, назначенных данному передатчику.

Распределение поднесущих в ходе работы может динамически изменяться, что делает данный механизм не менее гибким, чем метод временного уплотнения.

Схема OFDM имеет несколько преимуществ. Во-первых, селективному замиранию будут подвержены только некоторые подканалы, а не весь сигнал. Если поток данных защищен кодом прямого исправления ошибок, то с этим замиранием легко бороться. Во-вторых, что более важно, OFDM позволяет подавить межсимвольную интерференцию. Межсимвольная интерференция оказывает значительное влияние при высоких скоростях передачи данных, так как расстояние между битами (или символами) мало. В схеме OFDM скорость передачи данных уменьшается в N раз, что позволяет увеличить время передачи символа в N раз. Таким образом, если время передачи символа для исходного потока составляет T_s, то период сигнала OFDM будет равен NT_s. Это позволяет существенно снизить влияние межсимвольных помех. При проектировании системы N выбирается таким образом, чтобы величина NT_s значительно превышала среднеквадратичный разброс задержек канала.

Технология расширенного спектра

Изначально метод расширенного спектра создавался для разведывательных и военных целей. Основная идея метода состоит в том, чтобы распределить информационный сигнал по широкой полосе радиодиапазона, что в итоге позволит значительно усложнить подавление или перехват сигнала. Первая разработанная схема расширенного спектра известна как метод перестройки частоты. Более современной схемой расширенного спектра является метод прямого последовательного расширения. Оба метода используются в различных стандартах и продуктах беспроводной связи.

- **Расширение спектра скачкообразной перестройкой частоты (Frequency Hopping Spread Spectrum - FHSS)**

Для того чтобы радиообмен нельзя было перехватить или подавить узкополосным шумом, было предложено вести передачу с постоянной сменой несущей в пределах широкого диапазона частот. В результате мощность сигнала распределялась по всему диапазону, и прослушивание какой-то определенной частоты давало только небольшой шум. Последовательность несущих частот была псевдослучайной, известной только передатчику и приемнику. Попытка подавления сигнала в каком-то узком диапазоне также не слишком ухудшала сигнал, так как подавлялась только небольшая часть информации.

В течение фиксированного интервала времени передача ведется на неизменной несущей частоте. На каждой несущей частоте для передачи дискретной информации применяются стандартные методы модуляции, такие как FSK или PSK. Для того чтобы приемник синхронизировался с передатчиком, для обозначения начала каждого периода передачи в течение некоторого времени передаются синхробиты. Так что полезная скорость этого метода кодирования оказывается меньше из-за постоянных накладных расходов на синхронизацию.

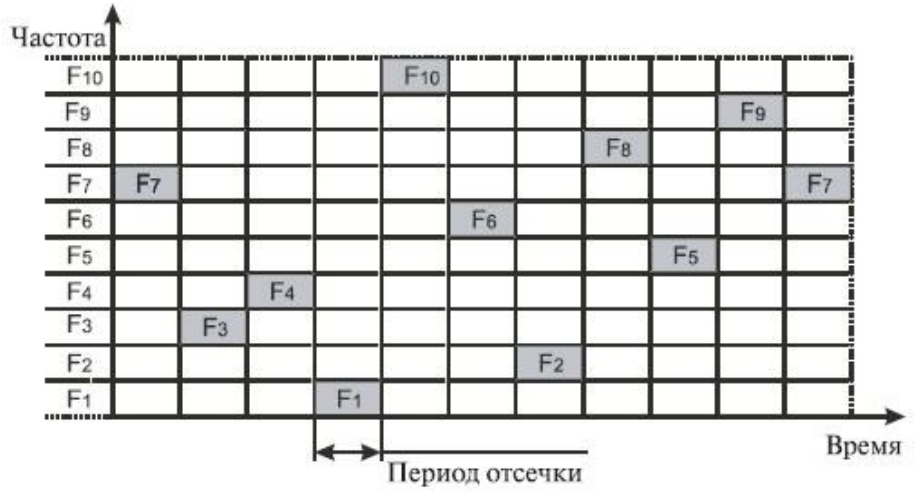


Рис. 1.4.3. Расширение спектра скачкообразной перестройкой частоты

Несущая частота меняется в соответствии с номерами частотных подканалов, вырабатываемых алгоритмом псевдослучайных чисел. Псевдослучайная последовательность зависит от некоторого параметра, который называют начальным числом. Если приемнику и передатчику известны алгоритм и значение начального числа, то они меняют частоты в одинаковой последовательности, называемой последовательностью псевдослучайной перестройки частоты.

Если частота смены подканалов ниже, чем скорость передачи данных в канале, то такой режим называют медленным расширением спектра, в противном случае мы имеем дело с быстрым расширением спектра.

Метод быстрого расширения спектра более устойчив к помехам, поскольку узкополосная помеха, которая подавляет сигнал в определенном подканале, не приводит к потере бита, так

как его значение повторяется несколько раз в различных частотных подканалах. В этом режиме не проявляется эффект межсимвольной интерференции, потому что ко времени прихода задержанного вдоль одного из путей сигнала система успевает перейти на другую частоту.

Метод медленного расширения спектра таким свойством не обладает, но зато он проще в реализации и сопряжен с меньшими накладными расходами.

Рис. 1.4.4. Соотношение между скоростью передачи данных и частотой смены подканалов

В FHSS подход к использованию частотного диапазона не такой, как в других методах кодирования - вместо экономного расходования узкой полосы делается попытка занять весь доступный диапазон. На первый взгляд это кажется не очень эффективным - ведь в каждый момент времени в диапазоне работает только один канал. Однако последнее утверждение не всегда справедливо - коды расширенного спектра можно использовать и для мультиплексирования нескольких каналов в широком диапазоне. В частности, методы FHSS позволяют организовать одновременную работу нескольких каналов путем выбора для каждого канала таких псевдослучайных последовательностей, чтобы в каждый момент времени каждый канал работал на своей частоте (конечно, это можно сделать, только если число каналов не превышает числа частотных подканалов).

Прямое последовательное расширение спектра (Direct Sequence Spread Spectrum - DSSS)

В методе прямого последовательного расширения спектра также используется весь частотный диапазон, выделенный для одной беспроводной линии связи. В отличие от метода FHSS, весь частотный диапазон занимается не за счет постоянных переключений с частоты на частоту, а за счет того, что каждый бит информации заменяется N-битами, так что тактовая скорость передачи сигналов увеличивается в N раз. А это, в свою очередь, означает, что спектр сигнала также расширяется в N раз. Достаточно соответствующим образом выбрать скорость передачи данных и значение N, чтобы спектр сигнала заполнил весь диапазон.

Цель кодирования методом DSSS та же, что и методом FHSS, - повышение устойчивости к помехам. Узкополосная помеха будет искажать только определенные частоты спектра сигнала, так что приемник с большой степенью вероятности сможет правильно распознать передаваемую информацию.

Код, которым заменяется двоичная единица исходной информации, называется расширяющей последовательностью, а каждый бит такой последовательности - чипом.

Соответственно, скорость передачи результирующего кода называют чиповой скоростью. Двоичный нуль кодируется инверсным значением расширяющей последовательности. Приемники должны знать расширяющую последовательность, которую использует передатчик, чтобы понять передаваемую информацию.

Количество битов в расширяющей последовательности определяет коэффициент расширения исходного кода. Как и в случае FHSS, для кодирования битов результирующего кода может использоваться любой вид модуляции, например BFSK.

Чем больше коэффициент расширения, тем шире спектр результирующего сигнала и выше степень подавления помех. Но при этом растет занимаемый каналом диапазон спектра. Обычно коэффициент расширения имеет значение от 10 до 100.

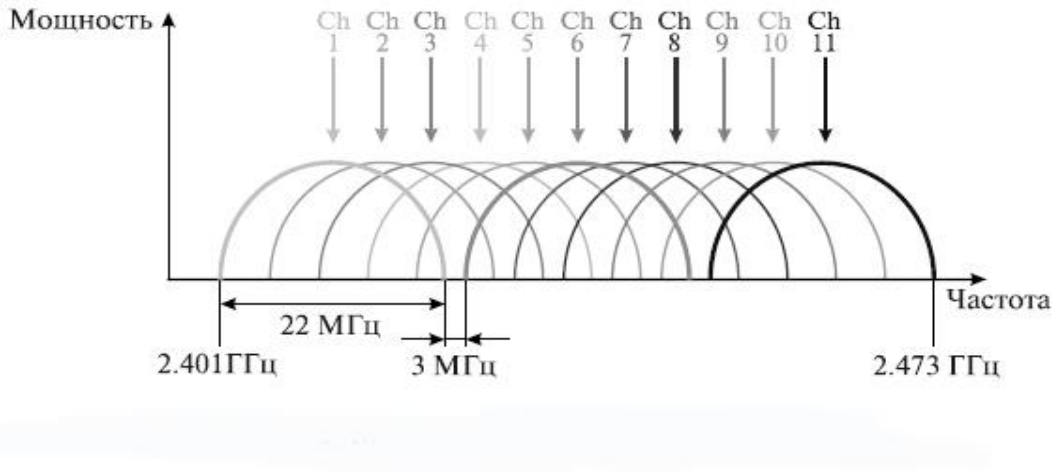


Рис. 1.4.5. Каналы, используемые в технологии DSSS

Беспроводные локальные сети DSSS используют каналы шириной 22 МГц, благодаря чему многие WLAN могут работать в одной и той же зоне покрытия. В Северной Америке и большей части Европы, в том числе и в России, каналы шириной 22 МГц позволяют создать в диапазоне 2,4- 2,483 ГГц три неперекрывающихся канала передачи.

1.4.1 Кодирование и защита от ошибок

Существует три наиболее распространенных орудия борьбы с ошибками в процессе передачи данных:

1. коды обнаружения ошибок;
2. коды с коррекцией ошибок, называемые также схемами прямой коррекции ошибок (Forward Error Correction - FEC);
3. протоколы с автоматическим запросом повторной передачи (Automatic Repeat Request - ARQ).

Код обнаружения ошибок позволяет довольно легко установить наличие ошибки. Как правило, подобные коды используются совместно с определенными протоколами канального или транспортного уровней, имеющими схему ARQ. В схеме ARQ приемник попросту отклоняет блок данных, в котором была обнаружена ошибка, после чего передатчик передает этот блок повторно. Коды с прямой коррекцией ошибок позволяют не только обнаружить ошибки, но и исправить их, не прибегая к повторной передаче. Схемы FEC часто используются в беспроводной передаче, где повторная передача крайне неэффективна, а уровень ошибок довольно высок.

I. Методы обнаружения ошибок

Методы обнаружения ошибок основаны на передаче в составе блока данных избыточной служебной информации, по которой можно судить с некоторой степенью вероятности о достоверности принятых данных.

Избыточную служебную информацию принято называть контрольной суммой, или контрольной последовательностью кадра (Frame Check Sequence, FCS). Контрольная сумма вычисляется как функция от основной информации, причем не обязательно путем суммирования. Принимающая сторона повторно вычисляет контрольную сумму кадра по известному алгоритму и в случае ее совпадения с контрольной суммой, вычисленной передающей стороной, делает вывод о том, что данные были переданы через сеть корректно. Рассмотрим несколько распространенных алгоритмов вычисления контрольной суммы, отличающихся вычислительной сложностью и способностью обнаруживать ошибки в данных.

- **Контроль по паритету**

Контроль по паритету представляет собой наиболее простой метод контроля данных. В то же время это наименее мощный алгоритм контроля, так как с его помощью можно обнаружить только одиночные ошибки в проверяемых данных. Метод заключается в суммировании по модулю 2 всех битов контролируемой информации. Нетрудно заметить, что для информации, состоящей из нечетного числа единиц, контрольная сумма всегда равна 1, а при четном числе единиц - 0. Например, для данных 100101011 результатом контрольного суммирования будет значение 1. Результат суммирования также представляет собой один дополнительный бит данных, который пересылается вместе с контролируемой информацией. При искажении в процессе пересылки любого бита исходных данных (или контрольного разряда) результат суммирования будет отличаться от принятого контрольного разряда, что говорит об ошибке. Однако двойная ошибка, например 110101010, будет неверно принята за корректные данные. Поэтому контроль по паритету применяется к небольшим порциям данных, как правило, к каждому байту, что дает коэффициент избыточности для этого метода 1/8. Метод редко применяется в компьютерных сетях из-за значительной избыточности и невысоких диагностических способностей.

- **Вертикальный и горизонтальный контроль по паритету**

Вертикальный и горизонтальный контроль по паритету представляет собой модификацию описанного выше метода. Его отличие состоит в том, что исходные данные рассматриваются в виде матрицы, строки которой составляют байты данных. Контрольный разряд подсчитывается отдельно для каждой строки и для каждого столбца матрицы. Этот метод обнаруживает значительную часть двойных ошибок, однако обладает еще большей избыточностью. Он сейчас также почти не применяется при передаче информации по сети.

- **Циклический избыточный контроль**

Циклический избыточный контроль (Cyclic Redundancy Check - CRC) является в настоящее время наиболее популярным методом контроля в вычислительных сетях (и не только в сетях; в частности, этот метод широко применяется при записи данных на гибкие и жесткие диски). Метод основан на рассмотрении исходных данных в виде одного многоразрядного двоичного числа. Например, кадр стандарта Ethernet, состоящий из 1024 байт, будет рассматриваться как одно число, состоящее из 8192 бит. Контрольной информацией считается остаток от деления этого числа на известный делитель R. Обычно в качестве делителя выбирается семнадцати- или тридцатитрехразрядное число, чтобы остаток от деления имел длину 16 разрядов (2 байт) или 32 разряда (4 байт). При получении кадра данных снова вычисляется остаток от деления на тот же делитель R, но при этом к данным

кадра добавляется и содержащаяся в нем контрольная сумма. Если остаток от деления на R равен нулю, то делается вывод об отсутствии ошибок в полученном кадре, в противном случае кадр считается искаженным.

Этот метод обладает более высокой вычислительной сложностью, но его диагностические возможности гораздо шире, чем у методов контроля по паритету. Метод CRC обнаруживает все одиночные ошибки, двойные ошибки и ошибки в нечетном числе битов. Метод также обладает невысокой степенью избыточности. Например, для кадра Ethernet размером 1024 байта контрольная информация длиной 4 байта составляет только 0,4%.

II. Методы коррекции ошибок

Техника кодирования, которая позволяет приемнику не только понять, что присланные данные содержат ошибки, но и исправить их, называется прямой коррекцией ошибок (Forward Error Correction - FEC). Коды, обеспечивающие прямую коррекцию ошибок, требуют введения большей избыточности в передаваемые данные, чем коды, которые только обнаруживают ошибки.

При применении любого избыточного кода не все комбинации кодов являются разрешенными. Например, контроль по паритету делает разрешенными только половину кодов. Если мы контролируем три информационных бита, то разрешенными 4-битными кодами с дополнением до нечетного количества единиц будут:

000 1, 001 0, 010 0, 011 1, 100 0, 101 1, 110 1, 111 0, то есть всего 8 кодов из 16 возможных.

Для того чтобы оценить количество дополнительных битов, необходимых для исправления ошибок, нужно знать так называемое расстояние Хемминга между разрешенными комбинациями кода. Расстоянием Хем-минга называется минимальное число битовых разрядов, в которых отличается любая пара разрешенных кодов. Для схем контроля по паритету расстояние Хемминга равно 2.

Можно доказать, что если мы сконструировали избыточный код с расстоянием Хемминга, равным n, такой код будет в состоянии распознавать (n-1)-кратные ошибки и исправлять (n-1)/2-кратные ошибки. Так как коды с контролем по паритету имеют расстояние Хемминга, равное 2, они могут только обнаруживать однократные ошибки и не могут исправлять ошибки.

Коды Хемминга эффективно обнаруживают и исправляют изолированные ошибки, то есть отдельные искаженные биты, которые разделены большим количеством корректных битов. Однако при появлении длинной последовательности искаженных битов (пульсации ошибок) коды Хемминга не работают.

Наиболее часто в современных системах связи применяется тип кодирования, реализуемый сверточным кодирующим устройством (Convolutional coder), потому что такое кодирование несложно реализовать аппаратно с использованием линий задержки (delay) и сумматоров. В отличие от рассмотренного выше кода, который относится к блочным кодам без памяти, сверточный код относится к кодам с конечной памятью (Finite memory code); это означает, что выходная последовательность кодера является функцией не только текущего входного сигнала, но также нескольких из числа последних предшествующих битов. Длина кодового ограничения (Constraint length of a code) показывает, как много выходных элементов выходит из системы в пересчете на один входной. Коды часто характеризуются их эффективной степенью (или коэффициентом) кодирования (Code rate). Вам может встретиться сверточный код с коэффициентом кодирования 1/2. Этот коэффициент указывает, что на каждый входной бит приходится два выходных. При сравнении кодов обращайте внимание на то, что, хотя коды с более высокой эффективной степенью кодирования позволяют передавать данные с более высокой скоростью, они, соответственно, более чувствительны к шуму.

В беспроводных системах с блочными кодами широко используется метод чередования блоков. Преимущество чередования состоит в том, что приемник распределяет пакет ошибок,

исказивший некоторую последовательность битов, по большому числу блоков, благодаря чему становится возможным исправление ошибок. Чередование выполняется с помощью чтения и записи данных в различном порядке. Если во время передачи пакет помех воздействует на некоторую последовательность битов, то все эти биты оказываются разнесенными по различным блокам. Следовательно, от любой контрольной последовательности требуется возможность исправить лишь небольшую часть от общего количества инвертированных битов.

III. Методы автоматического запроса повторной передачи

В простейшем случае защита от ошибок заключается только в их обнаружении. Система должна предупредить передатчик об обнаружении ошибки и необходимости повторной передачи. Такие процедуры защиты от ошибок известны как методы автоматического запроса повторной передачи (Automatic Repeat Request - ARQ). В беспроводных локальных сетях применяется процедура "запрос ARQ с остановками" (stop-and-wait ARQ).

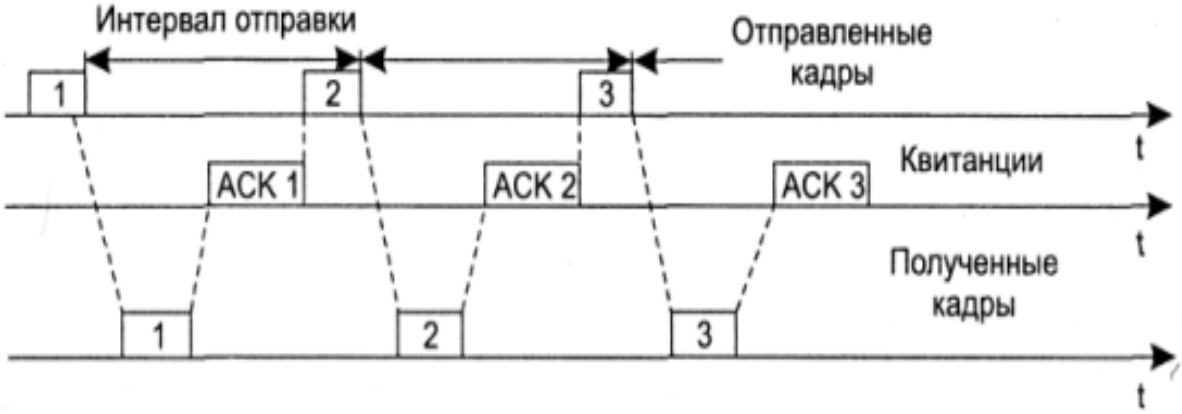


Рис. 1.4.6. Процедура запрос ARQ с остановками

В этом случае источник, пославший кадр, ожидает получения подтверждения (Acknowledgement - ACK), или, как еще его называют, квитанции, от приемника и только после этого посылает следующий кадр. Если же подтверждение не приходит в течение тайм-аута, то кадр (или подтверждение) считается утерянным и его передача повторяется.

1.5 Обзор систем шифрования

Механизмы шифрования основаны на алгоритмах, которые рандомизируют данные. Используются два вида шифров.

1. Поточный (групповой) шифр.
2. Блочный шифр.

Шифры обоих типов работают, генерируя ключевой поток (key stream), получаемый на основе значения секретного ключа. Ключевой поток смешивается с данными, или открытым текстом, в результате чего получается закодированный выходной сигнал, или зашифрованный текст. Названные два вида шифров отличаются по объему данных, с которыми они могут работать одновременно.

Поточный шифр генерирует непрерывный ключевой поток, основываясь на значении ключа. Например, поточный шифр может генерировать 15-разрядный ключевой поток для шифрования одного фрейма и 200-разрядный ключевой поток для шифрования другого. На рис. 2 проиллюстрирована работа поточного шифра. Поточные шифры - это небольшие и эффективные алгоритмы шифрования, благодаря которым нагрузка на центральный процессор оказывается небольшой. Наиболее распространенным является поточный шифр RC4, который и лежит в основе алгоритма WEP.

Блочный шифр, наоборот, генерирует единственный ключевой поток шифрования фиксированного размера. Открытый текст делится на блоки, и каждый блок смешивается с ключевым потоком независимо. Если блок открытого текста меньше, чем блок ключевого потока, первый дополняется с целью получения блока нужного размера. На рис. 3 проиллюстрирована работа блочного шифра. Процесс фрагментации, а также другие особенности шифрования с использованием блочного шифра вызывают повышенную, по сравнению с поточным шифрованием, нагрузку на центральный процессор. В результате производительность устройств, применяющих блочное шифрование, снижается.

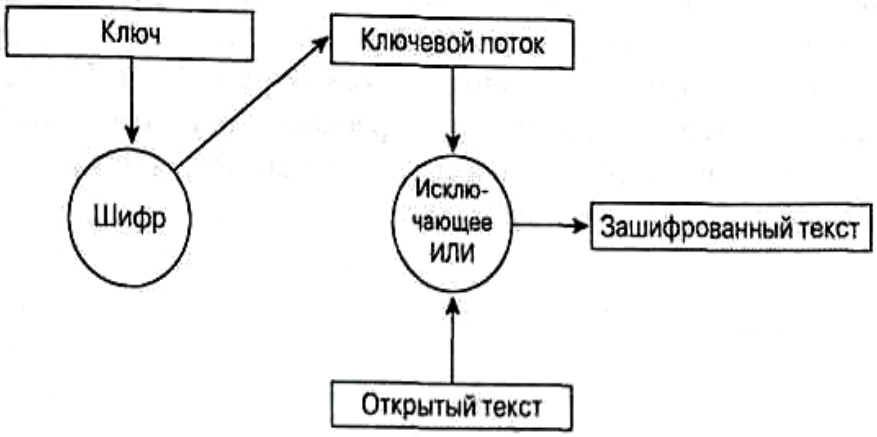


Рис. 1.5.1. Работа поточного шифра

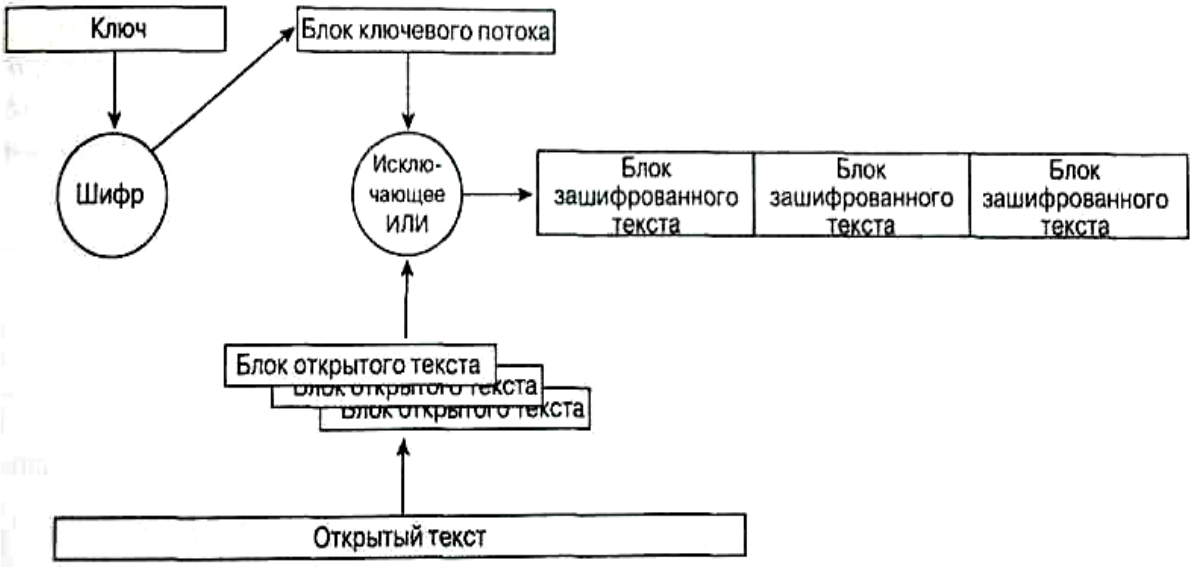


Рис. 1.5.2. Работа поточного блочное шифра.

Процесс шифрования, описанный для поточных и блочных шифров, называется режим шифрования с помощью книги электронных кодов (Electronic Code Book, ECB). Режим шифрования ECB характеризуется тем, что 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.

Некоторые методы шифрования позволяют решить эту проблему.

- Векторы инициализации (initialization vectors, IV).
- Режимы с обратной связью (feedback modes).

1.5.1 Векторы инициализации

Вектор инициализации — это номер, добавляемый к ключу, конечным результатом этого является изменение информации ключевого потока. Вектор инициализации связывается с ключом до того, как начнется генерация ключевого потока. Вектор инициализации все время изменяется, то же самое происходит с ключевым потоком. На рис. 1.5.3 показаны два сценария. Первый относится к шифрованию с использованием поточного шифра без применения вектора инициализации. В этом случае открытый текст DATA после смешения с ключевым потоком 12345 всегда преобразуется в зашифрованный текст AHGHE. Второй сценарий показывает, как тот же открытый текст смешивается с ключевым потоком, дополненным вектором инициализации для получения другого зашифрованного текста. Обратите внимание на то, что зашифрованный текст во втором случае отличается от такового в первом. Стандарт 802.11 рекомендует изменять вектор инициализации пофреймово (on a per-frame basis). Это означает, что если один и тот же фрейм будет передан дважды, весьма высокой окажется вероятность того, что зашифрованный текст будет разным.

- Шифрование с использованием поточного шифра без применения вектора инициализации.

- Шифрование с использованием поточного шифра и вектора инициализации

Рисунок 1.5.3 Шифрование и векторы инициализации.

1.5.2 Кодирование по стандарту 802.11 с использованием алгоритма WEP

Спецификация стандарта 802.11 предусматривает обеспечение защиты данных с использованием алгоритма WEP. 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. Алгоритм WEP был выбран главным образом потому, что он не требует объемных вычислений. Хотя персональные компьютеры с беспроводными сетевыми картами стандарта 802.11 сейчас широко распространены, в 1997 году ситуация была иной. Большинство из устройств, включаемых в беспроводные LAN, составляли специализированные устройства (application-specific devices, ASD). Примерами таких устройств могут служить считыватели штрих-кодов, планшетные ПК (tablet PC) и телефоны стандарта 802.11. Приложения, которые выполнялись этими специализированными устройствами, обычно не требовали большой вычислительной мощности, поэтому ASD оснащались слабенькими процессорами. 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, WEP использует 24-разрядный вектор инициализации, который добавляется к ключу перед выполнением обработки по алгоритму RC4. На рисунке 1.5.4 показан фрейм, зашифрованный по алгоритму WEP с использованием вектора инициализации.

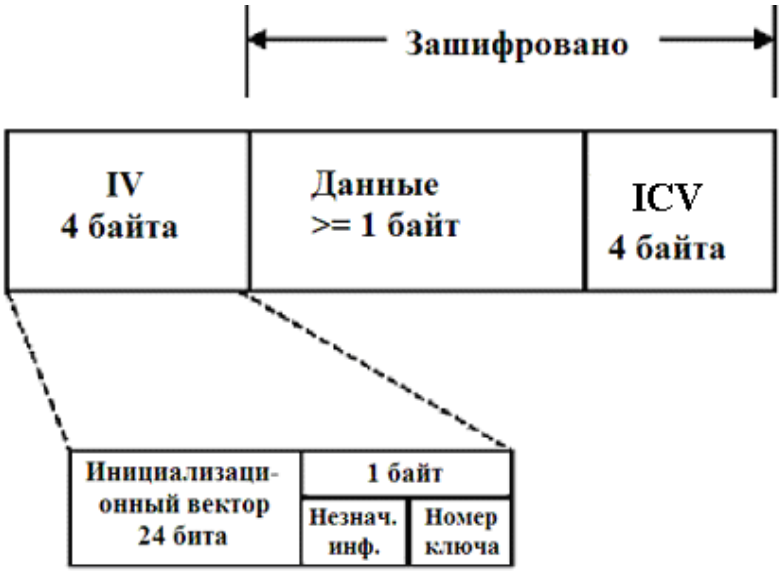


Рис. 1.5.4. Фрейм, зашифрованный по алгоритму WEP.

Вектор инициализации должен изменяться пофреймово во избежание IV-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 пофреимовые векторы инициализации в своих устройствах для беспроводных LAN.

Спецификация стандарта 802.11 требует, чтобы одинаковые WEP-ключи были сконфигурированы как на клиентах, так и на устройствах, образующих инфраструктуру сети. Можно определять до четырех ключей на одно устройство, но одновременно для шифрования отправляемых фреймов используется только один из них.

WEP-шифрование используется только по отношению к фреймам данных и во время процедуры аутентификации с совместно используемым ключом. По алгоритму WEP шифруются следующие поля фрейма данных стандарта 802.11.

- Данные или полезная нагрузка (payload).
- Контрольный признак целостности (integrity check value, ICV).

Значения всех остальных полей передаются без шифрования. Вектор инициализации должен быть послан незашифрованным внутри фрейма, чтобы приемная станция могла получить его и использовать для корректной расшифровки полезной нагрузки и ICV. На рис. 6 схематично представлен процесс шифрования, передачи, приема и расшифровки фрейма данных в соответствии с алгоритмом WEP.

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 результат в поле ICV. Значение поля ICV включается в часть фрейма, шифруемую по алгоритму WEP, так что его не могут просто так "увидеть" злоумышленники. Получатель фрейма дешифрует его, вычисляет значение ICV и сравнивает результат со значением поля ICV полученного фрейма. Если эти значения совпадают, фрейм считается подлинным, неподдельным. Если они не совпадают, такой фрейм отбрасывается. На рисунке 1.5.5 представлена диаграмма функционирования механизма ICV.

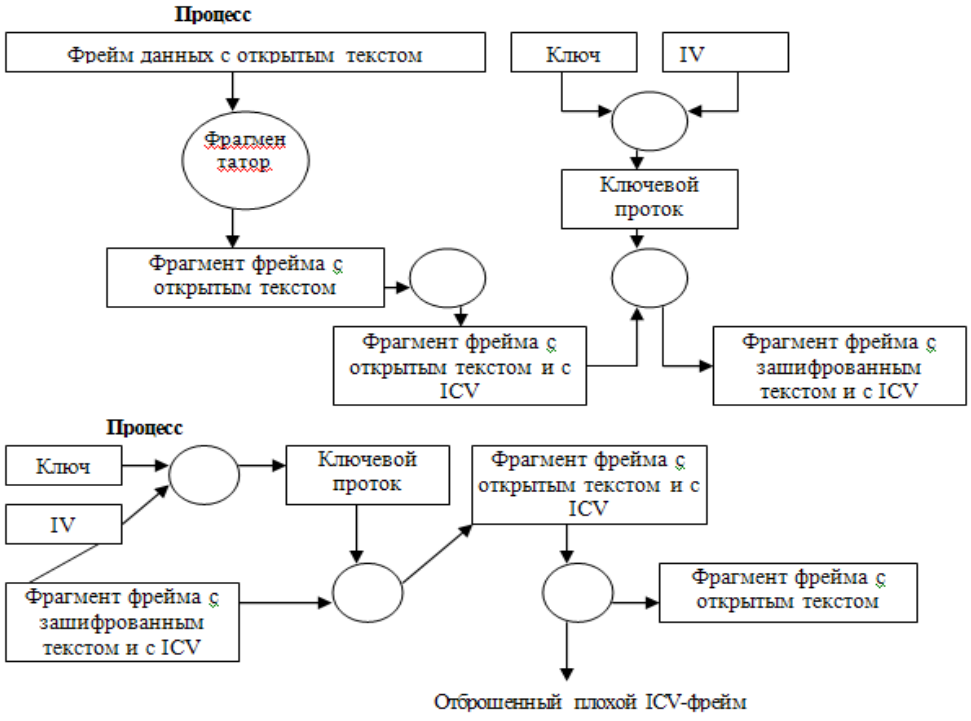


Рис. 1.5.5. Процесс шифрования и дешифрования

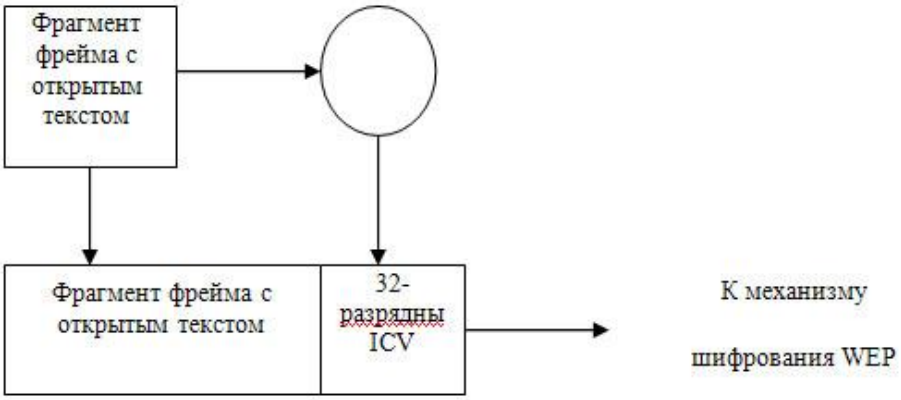


Рис. 1.5.6. Диаграмма функционирования механизма ICV

1.5.3 Шифрование по алгоритму AES.

Известно, что шифрование и аутентификация, проводимые в соответствии со стандартом 802.11, имеют слабые стороны. IEEE и WPA усилили алгоритм WEP протоколом TKIP и предлагают сильный механизм аутентификации по стандарту 802.11i, обеспечивающий защиту беспроводных LAN стандарта 802.11. В то же время IEEE рассматривает возможность усиления механизма шифрования. С этой целью IEEE адаптировал алгоритм AES для применения его по отношению к разделу, касающемуся защищаемых данных предлагаемого стандарта 802.11i. Компоненты WPA не обеспечивают поддержку шифрования по алгоритму AES. Однако последние версии WPA, возможно, будут реализованы в соответствии со стандартом 802.11i и для обеспечения взаимодействия будут поддерживать шифрование по алгоритму AES.

Алгоритм AES представляет собой следующее поколение средств шифрования, одобренное Национальным институтом стандартов и технологий (NIST) США. IEEE разработал режим AES, предназначенный специально для применения в беспроводных LAN. Этот режим называется режим счета сцеплений блоков шифра (Cipher Block Chaining Counter Mode, CBC-CTR) с контролем аутентичности сообщений о сцеплениях блоков шифра (Cipher Block Chaining Message Authenticity Check, CBC-MAC), все вместе это обозначается аббревиатурой AES-CCM. Режим CCM представляет собой комбинацию режима шифрования CBC-CTR и алгоритма контроля аутентичности сообщений CBC-MAC. Эти функции скомбинированы для обеспечения шифрования и проверки целостности сообщений в одном решении.

Алгоритм шифрования CBC-CTR работает с использованием счетчика для пополнения ключевого потока. Значение этого счетчика увеличивается на единицу после шифрования каждого блока. Такой процесс обеспечивает получение уникального ключевого потока для каждого блока. Фрейм с открытым текстом делится на 16-байтовые блоки. После шифрования каждого блока значение счетчика увеличивается на единицу, и так до тех пор, пока не будут зашифрованы все блоки. Для каждого нового фрейма счетчик переустанавливается.

Алгоритм шифрования CBC-MAC выполняется с использованием результата шифрования CBC по отношению ко всему фрейму, к адресу назначения, адресу источника и данным. Результирующий 128-разрядный выход усекается до 64 бит для использования в передаваемом фрейме.

CBC-MAC работает с известными криптографическими функциями, но имеет издержки, связанные с выполнением двух операций для шифрования и целостности сообщений. Этот

процесс требует серьезных вычислительных затрат и значительно увеличивает "накладные расходы" шифрования.

1.6 Защищенные LAN стандарта 802.11.

Промышленность преодолела слабые места в механизмах аутентификации и защиты сетей стандарта 802.11. Чтобы предоставить пользователям решения, обеспечивающие защищенность, масштабируемость и управляемость сетей, IEEE повысил защищенность сетей стандарта 802.11, разработав улучшенный механизм аутентификации и шифрования. Эти изменения были введены в проект стандарта 802.11i. На сегодняшний день проект 802.11i не утвержден как стандарт, поэтому Альянс Wi-Fi (Wi-Fi Alliance) собрал поднабор компонентов, соответствующих стандарту 802.11i, который получил название "защищенный доступ к Wi-Fi" (Wi-Fi Protected Access, WPA). В данном разделе подробно описаны стандарт 802.11i и компоненты WPA.

Многие ошибочно полагают, что WEP - это единственный компонент, обеспечивающий защиту беспроводных LAN. На самом деле защита беспроводных сетей имеет четыре составляющие.

1. Базовая аутентификация (authentication framework). Представляет собой механизм, который усиливает действие алгоритма аутентификации путем организации защищенного обмена сообщениями между клиентом, точкой доступа и сервером аутентификации.

2. Алгоритм аутентификации. Представляет собой алгоритм, посредством которого подтверждаются полномочия пользователя.

3. Алгоритм защиты данных. Обеспечивает защиту при передаче через беспроводную среду фреймов данных.

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

1.6.1 Базовая аутентификация.

Основой аутентификации стандарта 802.11 является служебный фрейм аутентификации стандарта 802.11. Этот служебный фрейм помогает реализовать алгоритмы открытой аутентификации и аутентификации с совместно используемым ключом, хотя сам по себе фрейм не обладает способностью аутентифицировать клиента. Поскольку о недостатках аутентификации стандарта 802.11 мы уже говорили, попробуем разобраться в том, что необходимо сделать для того, чтобы обеспечить проведение защищенной аутентификации в беспроводных LAN.

В стандарте 802.11 не определены основные компоненты, способные обеспечить эффективную аутентификацию (они перечислены ниже).

- Централизованная аутентификация, ориентированная на пользователя.
- Динамично шифруемые ключи.
- Управление зашифрованными ключами.
- Взаимная аутентификация.

Аутентификация, ориентированная на пользователя, чрезвычайно важна для обеспечения защиты сети. Аутентификация, ориентированная на устройства, подобная открытой аутентификации и аутентификации с совместно используемым ключом, не способна воспрепятствовать неавторизованным пользователям воспользоваться авторизованным устройством. Из этого следует, что при потере или 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.

Требование проводить аутентификацию, ориентированную на пользователя, имеет положительный побочный эффект: наличие отдельных ключей шифрования для каждого пользователя. Разновидности аутентификации, которые поддерживают создание динамических ключей шифрования, хорошо подходят для улучшения защиты беспроводных LAN и модели управления ими. Динамические ключи, индивидуальные для каждого пользователя, освобождают администратора сети от необходимости использования статически управляемых ключей. Ключи шифрования динамически назначаются и аннулируются, когда пользователь проходит процедуру аутентификации или выходит из сети. Для того чтобы удалить какого-либо пользователя из сети, достаточно аннулировать его учетную запись, и он потеряет возможность доступа к сети.

Взаимная аутентификация - это аутентификация двухсторонняя. Ее "двухсторонняя" природа обусловлена тем, что не только сеть аутентифицирует клиента, но и клиент аутентифицирует сеть. При открытой аутентификации и аутентификации с совместно используемым ключом точка доступа или сеть аутентифицирует клиента. Последний не знает наверняка, что подключился именно к той сети, к какой нужно, поскольку в стандарте 802.11 не предусмотрен механизм, позволяющий клиенту аутентифицировать сеть. В результате принадлежащая злоумышленнику точка доступа или клиентская станция может выдать себя за "законную" точку доступа и повредить данные на клиентской машине. На рисунке 1.6.1 представлены диаграммы, иллюстрирующие процессы односторонней и взаимной аутентификации.

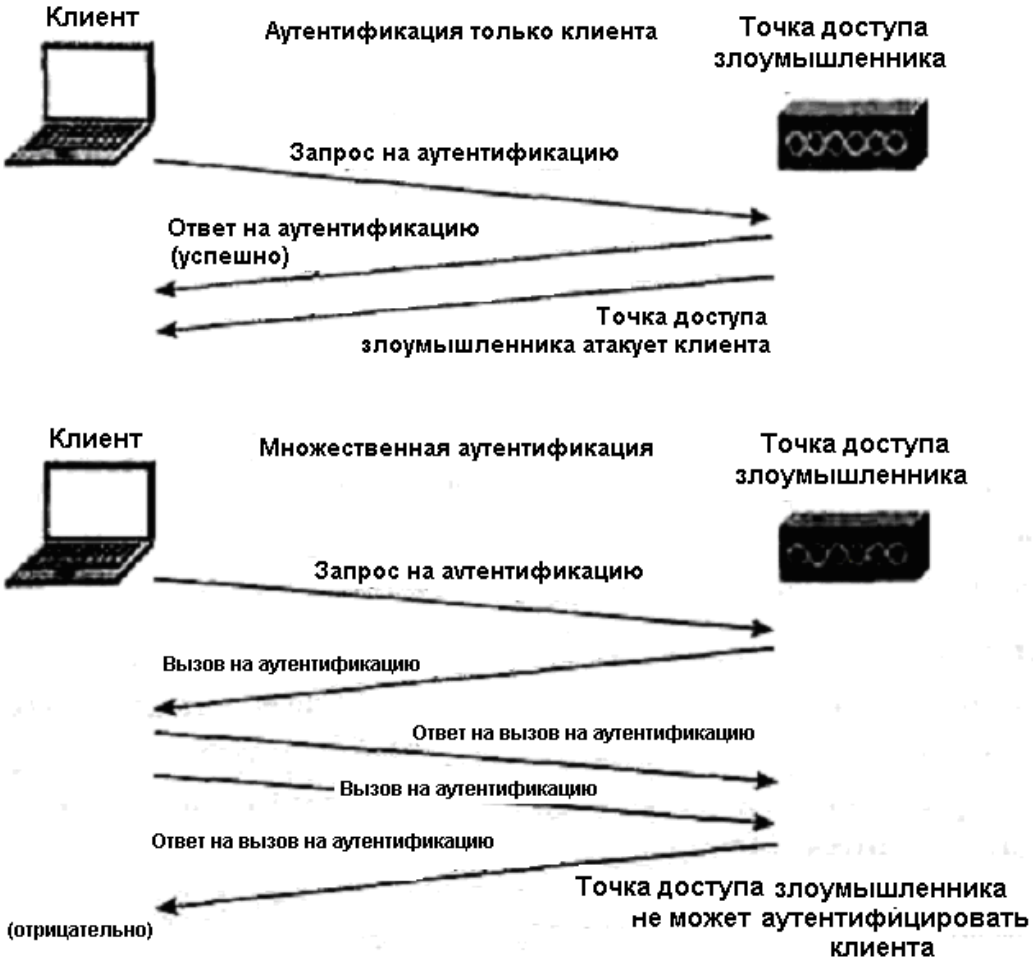


Рис. 1.6.1. Односторонняя и взаимная аутентификация.

IEEE начал борьбу с дефектами механизма аутентификации стандарта 802.11 с принятия базовой аутентификации, соответствующей стандарту 802.1X. Стандарт 802.1X представляет собой стандарт IEEE, который относится ко всем топологиям канального уровня серии стандартов 802 и позволяет наращивать его механизмы аутентификации до таковых, обычно реализуемых на более высоких уровнях. Стандарт 802.1X основан на принципах аутентификации, характерных для протокола типа "точка-точка" (Point-to-Point Protocol, PPP), и называется расширяемый протокол аутентификации (Extensible Authentication Protocol, EAP). Попросту говоря, стандарт 802.1X инкапсулирует сообщения для использования их на уровне 2. Стандарт 802.11i включает базовую аутентификацию стандарта 802.1X, требуя, чтобы она применялась для аутентификации пользователей. На рис. 1.6.2 представлен стандарт 802.1X в части алгоритма аутентификации и топологий канального уровня серии стандартов 802.

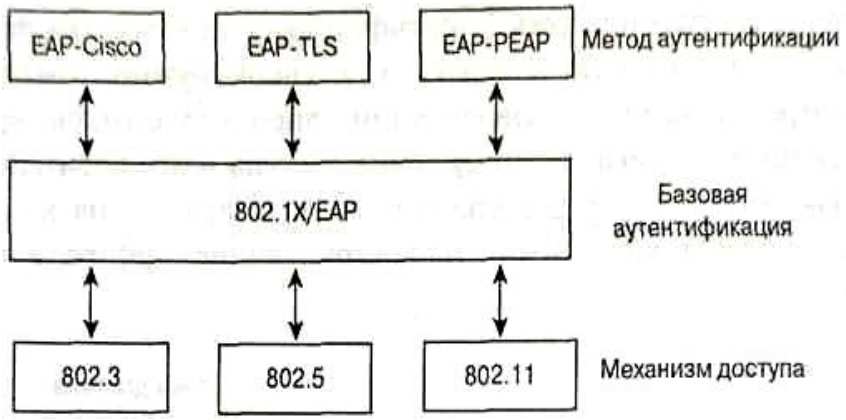


Рис. 1.6.2. Стандарт 802.1X и топологии канального уровня.

Протокол EAP (RFC 2284) и стандарт 802.1X не регламентируют использование особого алгоритма аутентификации. Администратор сети может применять соответствующую протоколу EAP разновидность аутентификации - или 802.1X, или EAP. Единственное требование - чтобы как клиент стандарта 802.11 (здесь он называется просителем (supplicant)), так и сервер аутентификации поддерживали алгоритм EAP-аутентификации. Такая открытая и расширяемая архитектура позволяет использовать базовую аутентификацию в различных условиях, и в каждой ситуации можно применять подходящую разновидность аутентификации.

Ниже приведены примеры типов EAP-аутентификации.

- EAP защиты транспортного уровня (EAP-transport layer security, EAP-PEAP). Работает аналогично протоколу защищенных сокетов (secure sockets layer, SSL). Взаимная аутентификация выполняется с использованием цифровых сертификатов на стороне сервера для создания SSL-туннеля для клиента, осуществляющего защищенную аутентификацию в сети.
- EAP-Message Digest 5 (EAP-MD5). Аналогично протоколу аутентификации с предварительным согласованием вызова (challenge handshake authentication protocol, CHAP), EAP-MD5 обеспечивает работу алгоритма односторонней аутентификации с использованием пароля.
- EAP-Cisco. EAP-аутентификация типа EAP-Cisco, которую называют также LEAP, была первой, определенной для применения специально в беспроводных LAN. EAP-Cisco — это алгоритм взаимной аутентификации с использованием пароля.

Аутентификация по стандарту 802.1X требует наличия трех составляющих.

1. Проситель. Размещается на стороне клиента беспроводной LAN.

2. Аутентификатор (authenticator). Размещается в точке доступа.
3. Сервер аутентификации. Размещается на сервере RADIUS.

Эти составляющие представляют собой программные компоненты, устанавливаемые на устройствах сети. С точки зрения стандарта 802.11 аутентификатор создает логический порт для устройства клиента, основанный на идентификаторе ассоциации (AID). Этот логический порт имеет два тракта прохождения данных: неконтролируемый и контролируемый. Неконтролируемый тракт прохождения данных позволяет проходить через сеть всему трафику аутентификации стандарта 802.1X. Контролируемый тракт прохождения данных блокирует обычный трафик сети до тех пор, пока не будет осуществлена успешная аутентификация клиента. На рис. 1.6.3 показаны логические порты аутентификатора стандарта 802.1X.

Рис. 1.6.3. Логические порты аутентификатора стандарта 802. 1X

1.6.2 Алгоритм аутентификации

Стандарт 802.11i и WPA обеспечивают механизм, поддерживающий работу алгоритма аутентификации с целью обеспечения связи между клиентом, точкой доступа и сервером аутентификации с использованием механизма базовой аутентификации стандарта 802.1X.

Ни стандарт 802.11i, ни WPA не регламентируют применение особого алгоритма аутентификации, но оба рекомендуют использовать алгоритм, который поддерживал бы взаимную аутентификацию, генерацию динамических ключей шифрования и аутентификацию пользователя. Примером такого алгоритма является алгоритм EAP-Cisco. Этот алгоритм, более известный как Cisco LEAP, представляет собой простой и эффективный алгоритм, разработанный специально для использования в беспроводных LAN.

Алгоритм EAP-Cisco является патентованным алгоритмом, который работает поверх алгоритма базовой открытой аутентификации. По этой причине детали алгоритма EAP-Cisco, касающиеся содержимого генерируемых вызова и ответа на вызов, а также распределения

ключей шифрования, не могут быть разглашены. Алгоритм EAP-Cisco перевыполняет требования, предъявляемые к защищенной аутентификации пользователя в беспроводной LAN, за счет применения следующих мер.

- Аутентификация, ориентированная на пользователя.
- Взаимная аутентификация.
- Динамические ключи шифрования.

Если какому-либо пользователю нужно запретить доступ к сети, достаточно удалить его учетную запись на централизованном сервере аутентификации. В результате пользователь не сможет успешно пройти процесс аутентификации, а его устройство - сгенерировать правильный динамический ключ шифрования.

1.6.3 Алгоритм защиты данных.

Уязвимость шифрования в WEP поставила производителей сетей стандарта 802.11 и исследователей IEEE в затруднительное положение. Как можно улучшить систему шифрования стандарта 802.11, не прибегая к замене всех точек доступа и сетевых карт клиентов?

IEEE ответил на этот вопрос, предложив являющийся частью стандарта 802.11i (и WPA) временный протокол целостности ключа (temporal key integrity protocol, TKIP).

Этот протокол использует многие основные функции WEP, чтобы оправдать инвестиции, сделанные клиентами в оборудование и инфраструктуру стандарта 802.11, но ликвидирует несколько слабых мест последнего, обеспечивая эффективное шифрование фреймов данных. Основные усовершенствования, внесенные протоколом TKIP, таковы.

Пофреймовое изменение ключей шифрования. WEP-ключ быстро изменяется, и для каждого фрейма он другой.

Контроль целостности сообщения (message integrity check, MIC). Обеспечивается эффективный контроль целостности фреймов данных с целью предотвращения проведения тайных манипуляций с фреймами и воспроизведения фреймов.

Атаки, использующие уязвимость слабых IV, основаны на накоплении нескольких фреймов данных, содержащих информацию, зашифрованную с использованием слабых IV. Простейшим способом сдерживания таких атак является изменение WEP-ключа, используемого при обмене фреймами между клиентом и точкой доступа, до того как атакующий успеет накопить фреймы в количестве, достаточном для вывода битов ключа.

IEEE адаптировала схему, известную как пофреймовое изменение ключа (per-frame keying). (Ее также называют изменение ключа для каждого пакета (per-packet keying) и частое изменение ключа пакета (fast packet keying).) Основной принцип, на котором основано пофреймовое изменение ключа, состоит в том, что IV, MAC-адрес передатчика и WEP-ключ обрабатываются вместе с помощью двухступенчатой функции перемешивания. Результат применения этой функции соответствует стандартному 104-разрядному WEP-ключу и 24-разрядному IV.

IEEE предложила также увеличить 24-разрядный вектор инициализации до 48-разрядного IV. В нижеследующих разделах объясняется, почему необходимо такое расширение IV. На рис. 18 представлен образец 48-разрядного IV и показано, как этот IV разбивается на части для использования при пофреймовом изменении ключа.

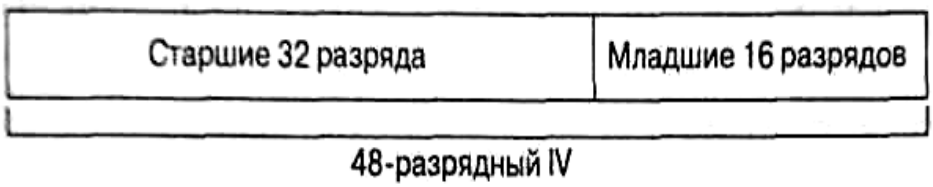


Рис. 1.6.4. Разбиение на части IV для использования при пофреймовом изменении ключа

Процесс пофреймового изменения ключа можно разбить на следующие этапы.

Базовый WEP-ключ (полученный в процессе аутентификации по стандарту 802.1X) перемешивается со старшими 32 разрядами 48-разрядного IV (32-разрядные числа могут принимать значения 0-4 294 967 295) и MAC-адресом передатчика. Результат этого действия называется ключ 1-й фазы (phase 1 key). Этот процесс позволяет занести ключ 1-й фазы в кэш и также напрямую поместить в ключ (рис. 19).

Ключ 1-й фазы снова перемешивается с IV и MAC-адресом передатчика (TA) для выработки значения пофреймового ключа.

Вектор инициализации (IV), используемый для передачи фрейма, имеет размер только 16 бит (16-разрядные числа могут принимать значения 0-65 535). Оставшиеся 8 бит представляют фиксированное значение, используемое как заполнитель.

Пофреймовый ключ используется для WEP-шифрования фрейма данных.

Когда 16-битовое пространство IV оказывается исчерпанным, ключ 1-й фазы отбрасывается и 32 старших разряда увеличиваются на 1. (Если значение IV первой фазы было равно 12, оно увеличивается до 13.)

Значение Пофреймового ключа вычисляется заново, как на этапе 2.

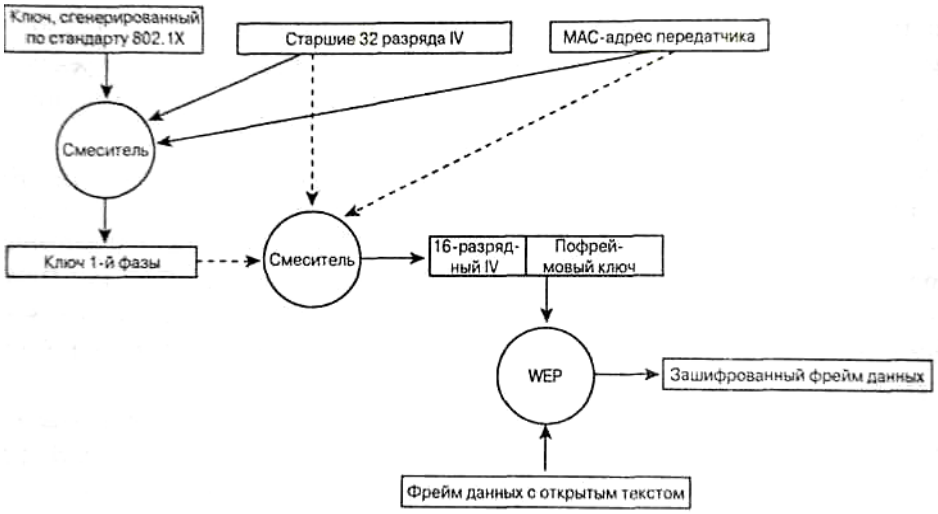


Рис. 1.6.5. Процесс Пофреймового изменения ключа

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-й фазы вычисляется заново путем увеличения старших 32 разрядов IV на 1 и повторного вычисления пофреймового ключа.

Этот алгоритм усиливает WEP до такой степени, что почти все известные сейчас возможности атак устраняются без замены существующего оборудования. Следует отметить, что этот алгоритм (и TKIP в целом) разработан с целью залатать бреши в системе аутентификации WEP и стандарта 802.11. Он жертвует слабыми алгоритмами, вместо того чтобы заменять оборудование. Следующее поколение оборудования стандарта 802.11 должно поддерживать TKIP, но WEP/TKIP будет постепенно свертываться в пользу алгоритма с большими возможностями шифрования, такого как усовершенствованный стандарт шифрования (advanced encryption standard, AES).

1.6.4 Целостность данных

В будущем для усиления малоэффективного механизма, основанного на использовании контрольного признака целостности (ICV) стандарта 802.11, будет применяться контроль целостности сообщения (MIC). Благодаря MIC могут быть ликвидированы слабые места защиты, способствующие проведению атак с использованием поддельных фреймов и жонглированием битами, рассмотренные ранее в. IEEE предложила специальный алгоритм, получивший название Michael (Майкл), чтобы усилить роль ICV в шифровании фреймов данных стандарта 802.11.

MIC имеет уникальный ключ, который отличается от ключа, используемого для шифрования фреймов данных. Этот уникальный ключ перемешивается с назначенным MAC-адресом и исходным MAC-адресом фрейма, а также со всей незашифрованной частью фрейма, несущей полезную нагрузку.

Меры противодействия MIC состоят в выполнении приемником следующих задач.

Приемник удаляет существующий ключ на ассоциирование.

Приемник регистрирует проблему как относящуюся к безопасности сети.

Ассоциированный клиент, от которого был получен ложный фрейм, не может быть ассоциирован и аутентифицирован в течение 60 секунд, чтобы замедлить атаку.

Если клиент получил ложный фрейм, то он отбрасывает все фреймы, не соответствующие стандарту 802.1X.

Такой клиент также запрашивает новый ключ.

Наше рассмотрение пофреймового назначения ключей и MIC касалось в основном ключа шифрования и ключа MIC. Но мы ничего не говорили о том, как ключи генерируются и пересылаются от клиента к точке доступа и наоборот. В следующем разделе мы и рассмотрим предлагаемый стандартом 802.11 механизм управления ключами.

1.6.5 Усовершенствованный механизм управления ключами

Алгоритмы аутентификации стандарта 802.11 и EAP могут обеспечить сервер RADIUS и клиента динамическими, ориентированными на пользователя ключами. Но тот ключ, который создается в процессе аутентификации, не является ключом, используемым для шифрования фреймов или проверки целостности сообщений. В стандарте 802.11i WPA для получения всех ключей используется так называемый мастер-ключ (master key). Клиент и точка доступа устанавливают динамический ключ (он называется парный мастер-ключ, или PMK, от англ. pairwise master key), полученный в процессе аутентификации по стандарту 802.1X. На основе этого ключа, а также MAC-адресов клиента и точки доступа генерируется парный переходный ключ (painvise transient key, PTK), на основе которого получают ключи для шифрования фреймов и проверки целостности сообщений.

Парный мастер-ключ (PMK) и парный переходный ключ (PTK) являются одноадресатными по своей природе. Они только шифруют и дешифруют одноадресатные фреймы, и предназначены для единственного пользователя. Широковещательные фреймы требуют отдельной иерархии ключей, потому что использование с этой целью одноадресатных ключей приведет к резкому возрастанию трафика сети. Точке доступа (единственному объекту BSS, имеющему право на рассылку широковещательных или многоадресатных сообщений) пришлось бы посылать один и тот же широковещательный или многоадресатный фрейм, зашифрованный соответствующими пофреймовыми ключами, каждому пользователю.

Широковещательные или многоадресатные фреймы используют иерархию групповых ключей. Групповой мастер-ключ (group master key, GMK) находится на вершине этой иерархии и выводится в точке доступа.

Групповой мастер-ключ, текстовая строка, MAC-адрес точки доступа и Gnonce (значение, которое берется из счетчика ключа точки доступа) объединяются и обрабатываются с помощью генератора ПСП, в результате чего получается 256-разрядный групповой пе-

реходный ключ (group transient key, GTK). GTK делится на 128-разрядный ключ шифрования широковещательных/многоадресатных фреймов, 64-разрядный ключ передачи MIC (transmit MIC key) и 64-разрядный ключ приема MIC (MIC receive key).

С помощью этих ключей широковещательные и многоадресатные фреймы шифруются и дешифруются точно так же, как с помощью одноадресатных ключей, полученных на основе парного мастер-ключа (PMK).

Групповые ключи удаляются и регенерируются каждый раз, когда какая-нибудь станция диассоциируется или деаутентнфицируется в BSS. Если происходит ошибка MIC, одной из мер противодействия также является удаление всех ключей с имеющей отношение к ошибке приемной станции, включая групповые ключи.

2 Применения Wi-Fi в системах видеонаблюдения

Беспроводное видеонаблюдение - одно из наиболее быстро развивающихся направлений в мире систем безопасности, использующееся для беспроводной передачи потоков видеоданных. Множество государственных учреждений и частных компаний постоянно используют новейшие разработки беспроводного видеонаблюдения, чтобы обеспечить свою безопасность и безопасность людей, которые в них работают, путем охраны внутренних и внешних территорий и помещений.

Видеонаблюдение встречается повсеместно - торговые центры, магазины, склады, различные учреждения, городские памятники архитектуры, места скопления людей, автомобилей. В интересах безопасности требуется оснащение системами беспроводного видеонаблюдения отдаленных мест, таких как водохранилища, атомные электростанции, аэропорты или продовольственные базы. Беспроводное видеонаблюдение может быть интегрировано как с IP-видеонаблюдением, так и с традиционными аналоговыми системами, путем оцифровки изображения. Это возможно благодаря использованию в качестве серверов или накопителей видеоинформации цифровых устройств, таких как видерегистраторы с функцией передачи данных по сети Ethernet.

Системы беспроводного видеонаблюдения могут обеспечивать безопасность различных объектов.

- Контроль безопасности портов и аэропортов.
- Внутренняя работу электростанций.
- Безопасность железных дорог.
- Контроль промышленных предприятий.

На схеме изображен принцип действия беспроводного видеонаблюдения, организованного с помощью Wi-Fi. Как и в случае с традиционным видеонаблюдением, здесь используется компьютер со специализированным программным обеспечением, которое является бесплатным. При этом плата видеозахвата не требуется, так как рассматриваются IP-камеры, изображение с которых изначально передается в цифровом формате.

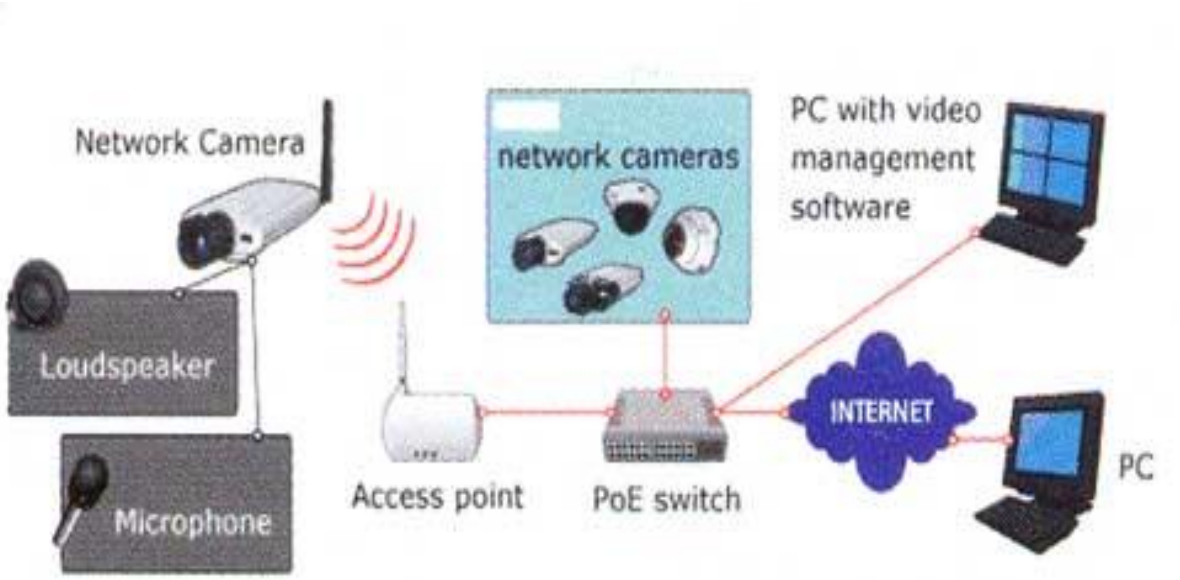


Рис. 2.1. Принцип действия беспроводного видеонаблюдения

На схеме видно, что видеокамеры получают питающее напряжение от блоков бесперебойного питания, расположенных в непосредственной близи от видеокамер. Таким образом, беспроводное видеонаблюдение подразумевает отсутствие кабелей между пунктом записи / наблюдения и видеокамерами, но система питания при этом функционирует с проводами.

2.1 Преимущества построения систем видеонаблюдения на базе IP-видеокамер

Среди достоинств Wi-Fi видеонаблюдения можно выявить следующие особенности:

- Высокое качество видеоизображения

В последнее время на рынке появилось значительное количество мегапиксельных IP-камер (1, 2, 3 и даже 5 мегапикселей). Мегапиксельные камеры формируют видеопотоки с достаточно хорошими скоростями обновления (например, 25 кадр/сек при двух мегапикселях или 50 кадр/сек при одном мегапикселе), что подразумевает более высокую информативность изображения, а значит и повышение уровня безопасности в целом.

- Высокая дальность применения при использовании направленных антенн

Использование дополнительных антенн дает возможность значительно увеличить зону действия систем беспроводного видеонаблюдения. Это происходит вследствие выноса антенны из помещения и подъема её относительно приемника/передатчика, а также благодаря коэффициенту усиления самой антенны. Так использование только одной направленной антенны в канале приемника увеличивает радиус действия системы в 4-6 раз, в зависимости от условий приема. Следует отметить, что при большой длине кабеля снижения от антенны к приемнику, используя кабель с большими потерями, можно лишиться всех преимуществ использования внешней антенны.

- Масштабируемость за счет применения ретрансляторов.

Использование ретрансляционного оборудования позволяет увеличить рабочее расстояние без прокладки кабельных линий.

- Возможность транслирования потока от нескольких камер по одной Wi-Fi сети.

Когда используется точка доступа, следует учитывать, что она представляет собой обычный концентратор. При нескольких подключениях видеокамер к одной точке полоса пропускания делится на количество подключенных пользователей. Теоретически ограничений на количество подключенных видеокамер нет, но на практике их число следует ограничивать, исходя из минимально необходимой скорости передачи данных для каждой камеры. Например, одна сетевая камера с разрешением VGA и скоростью 25 кадр/с при небольшом сжатии в самом популярном формате MPEG-4 занимает полосу в 2-2,5 Мбит/с. Это означает, что 10 камер отнимут максимум 25 Мбит/с, то есть точка доступа с полосой пропускания 54 Мбит/с (а с реальной скоростью передачи данных 25 Мбит/с) позволит без проблем принять сигнал от 10 Wi-Fi-видеокамер, а если брать в расчет видеокамеры с более современным сжатием H.264, то поток от камеры с тем же качеством займет около 0,5-1 Мбит/с. К одной точке доступа можно подключить и больше 25 видеокамер.

- Управление поворотными камерами

Оператор может наблюдать изображение с камеры, установленной в любой точке и управлять поворотным или фокусирующим механизмом точно так же, как если бы она была подключена к проводной сети.

- Надежность соединения

Правильный подбор оборудования, использование внешних узконаправленных антенн (которые, кстати, с помощью кабеля можно удалить от видеокамеры на расстояние до 30 м) и промежуточных точек доступа успешно решают эту проблему.

- Защищенность передачи данных

Защита видеоинформации в беспроводных IP-системах видеонаблюдения достигается несколькими способами. Ключевыми среди них являются: применение брандмауэров, использование паролей и шифрование. Брандмауэр работает как электронные "ворота", пропускающие зарегистрированных пользователей и запрещающие доступ неавторизованным лицам. Применение паролей позволяет не только ограничить доступ к системе видеонаблюдения, но и распределить права доступа персонала к определенным видеокамерам. А при шифровании попытки перехвата зашифрованных данных в IP-системе охранного видеонаблюдения становятся бессмысленными, если злоумышленник не знает уникального кода для расшифровки потока данных. Код, в свою очередь, устанавливается системным администратором.

- Легитимность использования Wi-Fi

Этот вопрос немного сложнее. Дело в том, что в России применение Wi-Fi без разрешения на использование частот от Государственной комиссии по радиочастотам (ГКРЧ) возможно для организации сети внутри зданий, закрытых складских помещений и производственных территорий. Для легального создания внеофисной беспроводной сети Wi-Fi (например, радиоканала между двумя соседними домами) необходимо получение разрешения на использование частот. При этом следует напомнить, что действует упрощенный порядок выдачи разрешений на использование радиочастот в полосе 2400-2483,5 МГц (стандарты 802.11b и g), для получения такого разрешения не требуется обращаться в ГКРЧ.

- Глушение сигнала

Такая опасность, действительно, существует. Но, во-первых, для того, чтобы полностью заглушить сигнал, нужен достаточно мощный источник, и, во-вторых, этот источник должен находиться очень близко к радиотракту. Однако даже в этом случае можно попытаться решить проблему с помощью мощных узконаправленных антенн.

- Вредность излучения

Мировая организация здравоохранения (World Health Organization) признала излучение Wi-Fi безвредным для здоровья человека. Так, например, излучение от устройств Wi-Fi в среднем в 10-20 раз ниже, чем от обычного сотового телефона.

- Экономическая целесообразность.

В отличие от традиционных систем, расширение которых фактически ведет к внушительным дополнительным затратам, использование IP-видео позволяет при расширении системы лишь добавлять IP-камеры или IP-видеосерверы. При наличии локальной вычислительной сети (ЛВС) дальнейшее расширение системы влечет за собой исключительно добавление IP-камер и не требует использования дополнительных линий. С другой стороны, программное обеспечение, которое применяется для записи IP-видео, как правило, рассчитано на дальнейшее расширение, то есть мы имеем дело лишь с закупкой соответствующих лицензий на запись необходимого количества видеоканалов.

2.2 Примеры существующих систем IP-видеонаблюдения

Приведем примеры различных вариантов построения систем видеонаблюдения с применением технологии Wi-Fi.

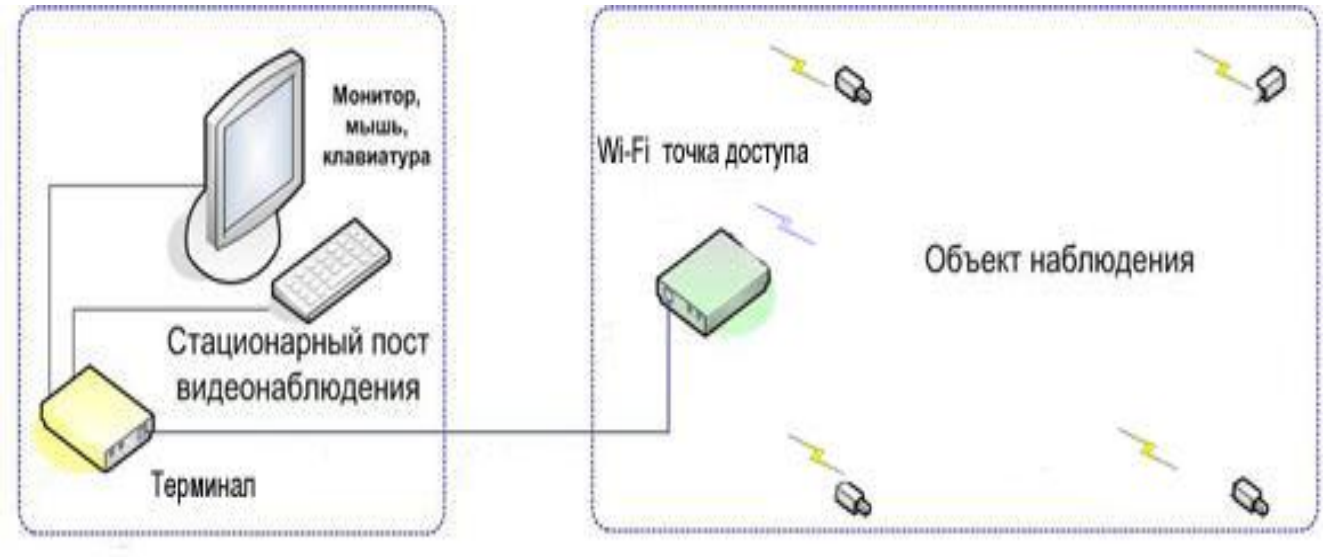


Рис. 2.2.1. Пример замкнутой системы видеонаблюдения

Состав системы:

- Wi-Fi точка доступа
- Терминал
- Камеры наблюдения

К Wi-Fi точке доступа подключается необходимое количество камер. Для обработки и отображения передаваемой от точки доступа информации использован терминал NetCore Vision. Малогабаритное устройство позволяет отображать на экране подключенного к нему стандартного SVGA монитора графическую информацию с разрешением 1024x768, а так же воспроизводить два канала звука. Использование данного терминала позволяет организовать пост наблюдения без использования персонального компьютера, что несет в себе неоспоримое преимущество - очень компактное решение, не имеет механических систем охлаждения, не требует технического обслуживания, низкое потребление электроэнергии, бесшумен.

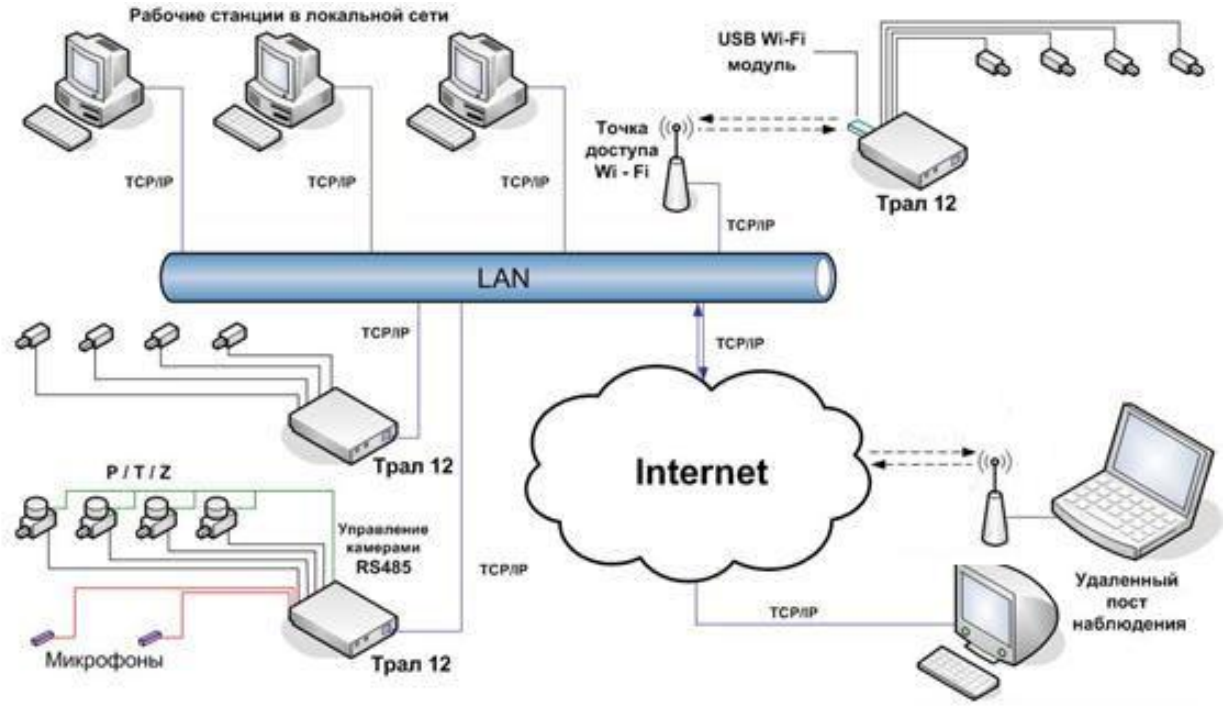


Рис. 2.2.2. Система видеонаблюдения интегрированная в локальную сеть учреждения

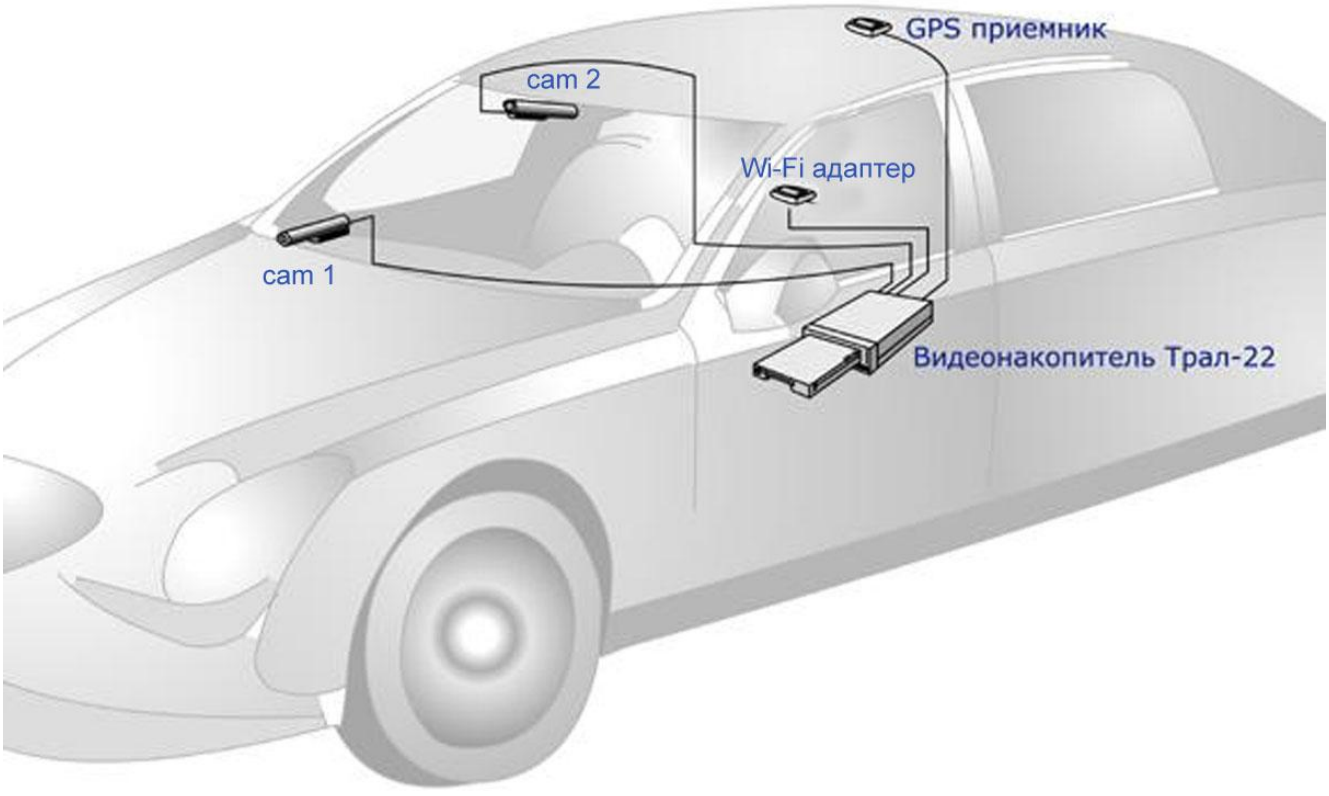


Рис. 2.2.3. Система видеонаблюдения в автомобиле

К видеонакопителю подключаются две камеры — одна курсовая, вторая направленная на водителя. Наряду с записью видео, производиться запись текущих географических координат поступающих от GPS приемника, установленного под лобовым стеклом автомобиля. Если

автомобиль находится в зоне действия Wi-Fi сети, возможен удаленный доступ к Тралу и его видеоархиву. Используя модель со съемным диском удобно производить просмотр всего видеоархива без извлечения видеонакопителя из автомобиля.

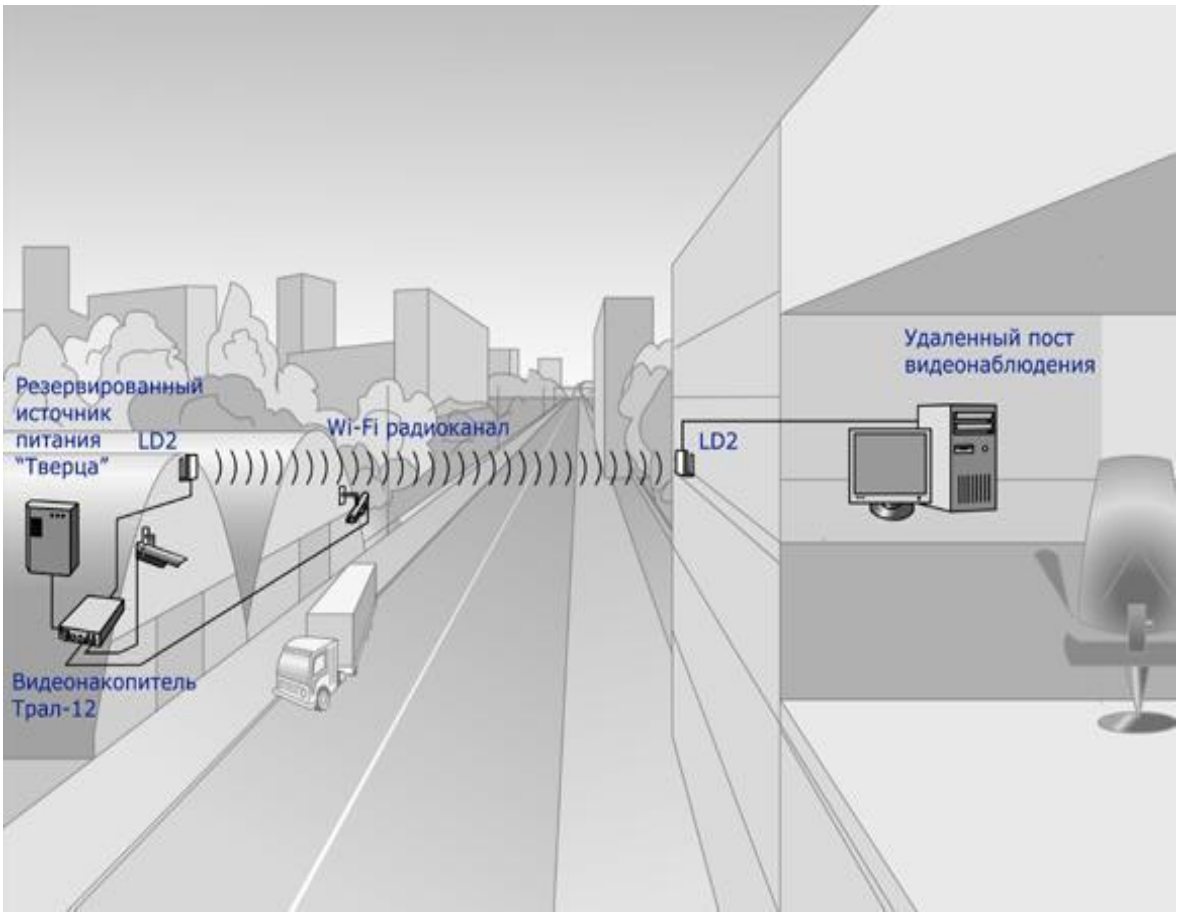


Рис. 2.2.4. Видеонаблюдение на территориально-распределенном объекте

В условиях, когда объект наблюдения и пост наблюдения находятся на значительном удалении друг от друга, возможно применение выносных направленных антенн беспроводной сети Wi-Fi. Направленные антенны обеспечивают устойчивый канал связи на расстоянии нескольких километров. Скорость обмена данными по радиоканалу позволяет работать с видеонакопителем нескольким пользователям.

2.3 Построение систем видеонаблюдения с использованием Wi-Fi

Источником видеосигнала для систем IP-видеонаблюдения являются цифровые камеры, на выходе которых аудио- и видеосигнал представлен в цифровом формате (IP-пакеты) с интерфейсом подключения в виде порта FastEthernet, который непосредственно подсоединяется к такому сетевому оборудованию, как коммутатор или маршрутизатор (в нашем случае – оборудование передачи данных по Wi-Fi). Это могут быть сетевые устройства, выделенные специально для систем наблюдения или совместно используемые для передачи всех корпоративных данных и подключения рабочих мест пользователей.

Схема системы видеонаблюдения с применением Wi-Fi показана на рисунке 2.3.1

Рис. 2.3.1. Схема системы видеонаблюдения, с применением Wi-Fi

В последнем случае может показаться, что безопасность системы видеонаблюдения зависит от действий любого пользователя компьютерной сети компании, и, если на месте пользователя окажется злоумышленник, он сможет безнаказанно нарушить ее работу. При правильном выборе и настройке сетевого оборудования доступ произвольного пользователя к данным и оборудованию системы IP-видеонаблюдения невозможен.

IP-камеры могут располагаться где угодно в пределах сети, связывающей их с сервером записи и клиентскими рабочими местами. IP-видео является идеальным решением тогда, когда сложно спрогнозировать, насколько система будет расширена в перспективе. Традиционные же системы видеонаблюдения хороши в тех ситуациях, когда количество камер заранее определено или планируется незначительное расширение системы. На объекте, где сложно заранее определить масштабы системы, IP-видео - однозначный выбор.

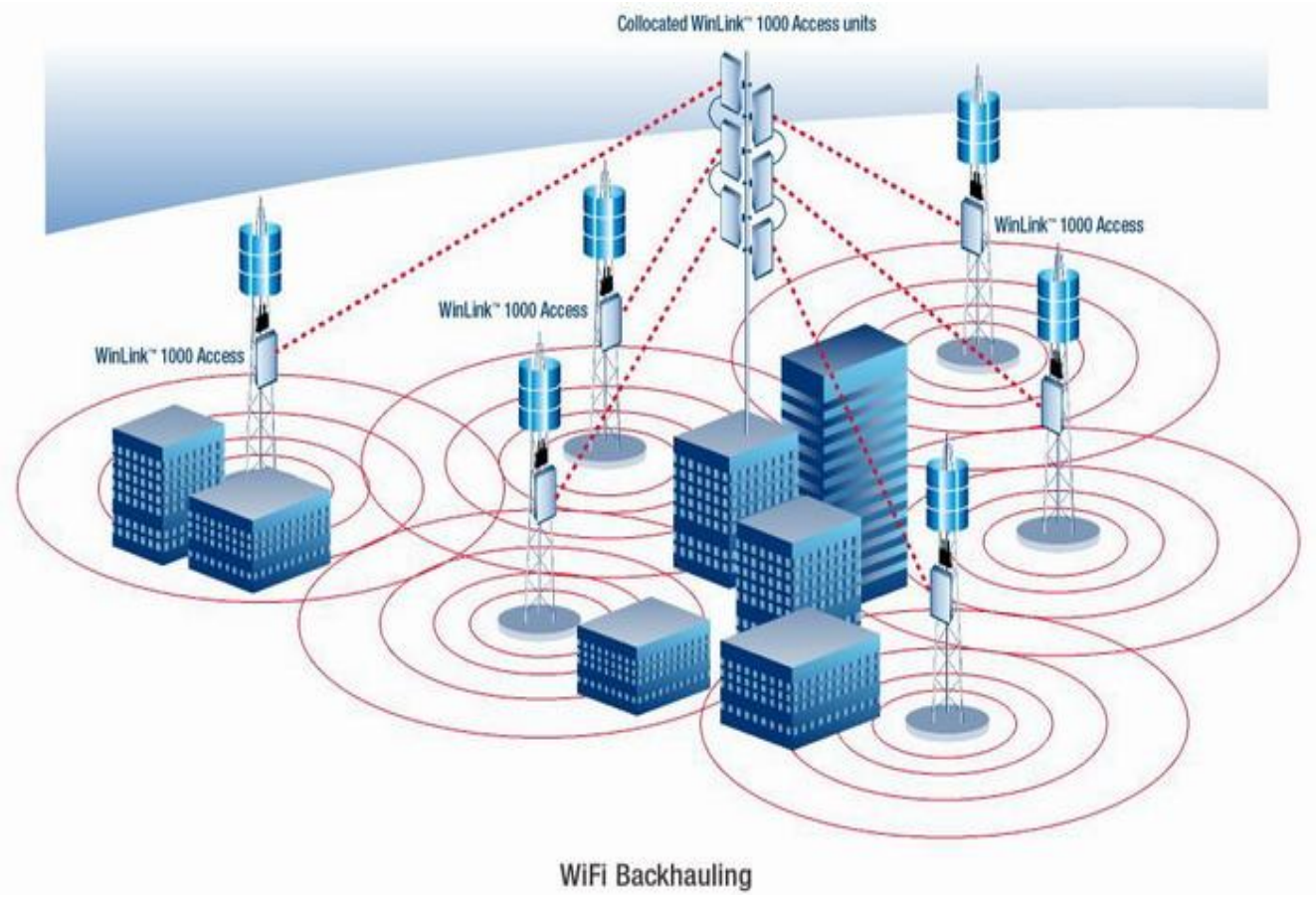


Рис. 2.3.2. Увеличение зоны покрытия при использовании системы ретрансляторов

Стандарт Wi-Fi не ограничивается малыми расстояниями и стенами помещений, а в открытых помещениях в прямой видимости он может работать на расстоянии почти 500 м. При использовании современных потоковых алгоритмов сжатия скорости 0,5 Мбит/с может оказаться вполне достаточно для передачи 1 канала видео приличного качества. А если учитывать, что это расстояние можно увеличивать с помощью направленных антенн и промежуточных точек доступа, то такое решение становится еще более интересным.

Для исключения падения производительности вашей беспроводной Wi-Fi сети все беспроводные клиенты должны поддерживать стандарт, на котором работает беспроводная точка доступа, а точке доступа принудительно указать режим работы.

Варианты использования антенн:

- Направленная антенна на приемнике - увеличение дальности в 4-6 раз
- Круговая антенна на приемнике - увеличение дальности в 2-3 раза
- Направленная антенна на передатчике и направленная антенна на приемнике - увеличение дальности в 5-10 раз

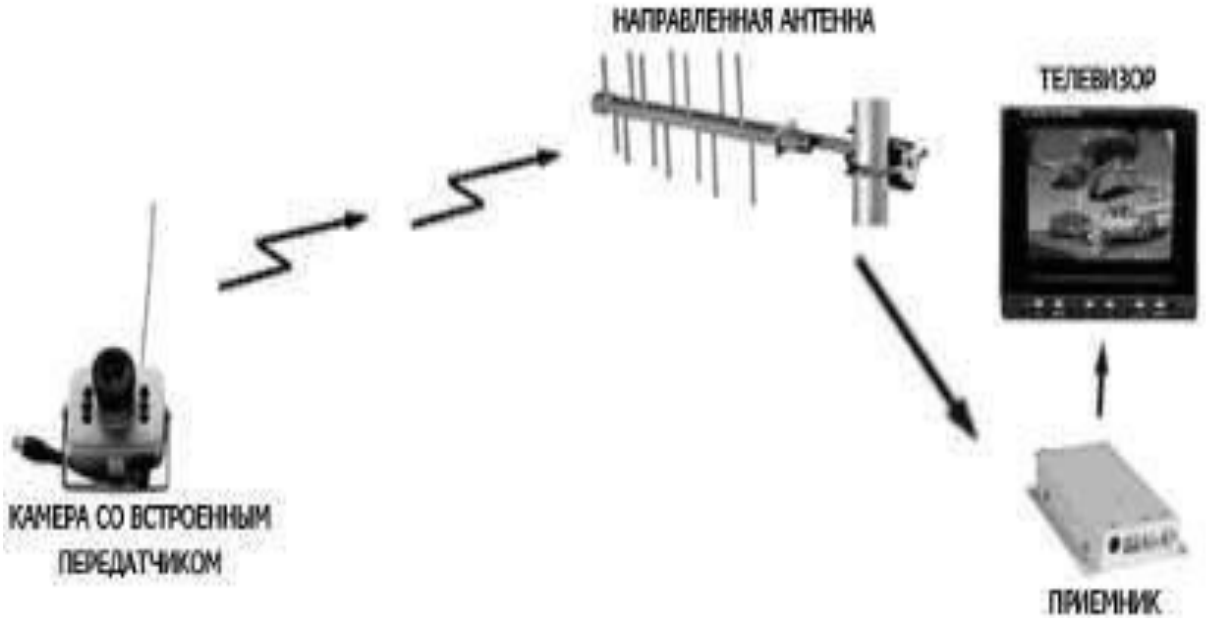


Рис. 2.3.3. Направленная антенна на приемнике

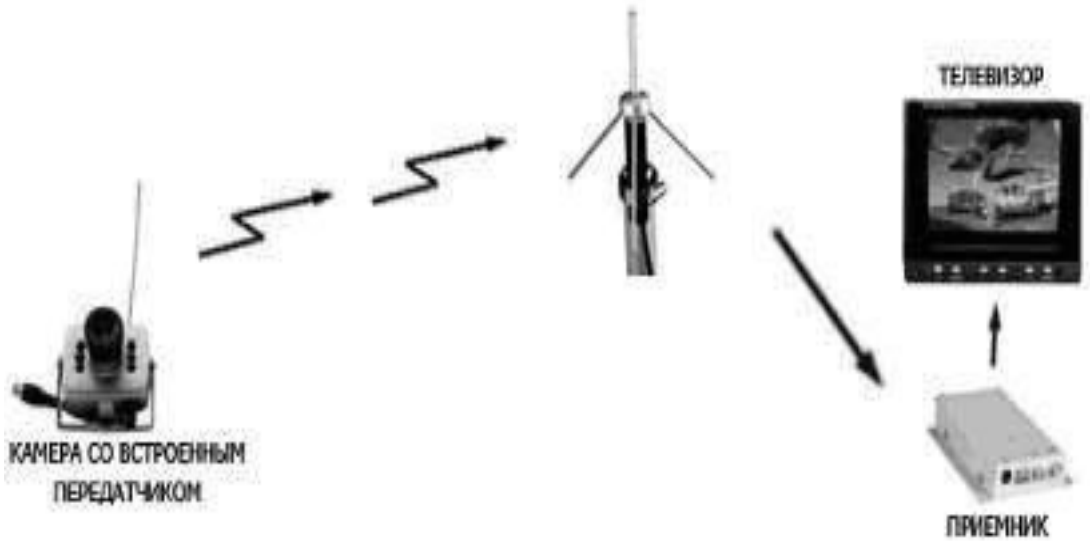


Рис. 2.3.4. Круговая антенна на приемнике

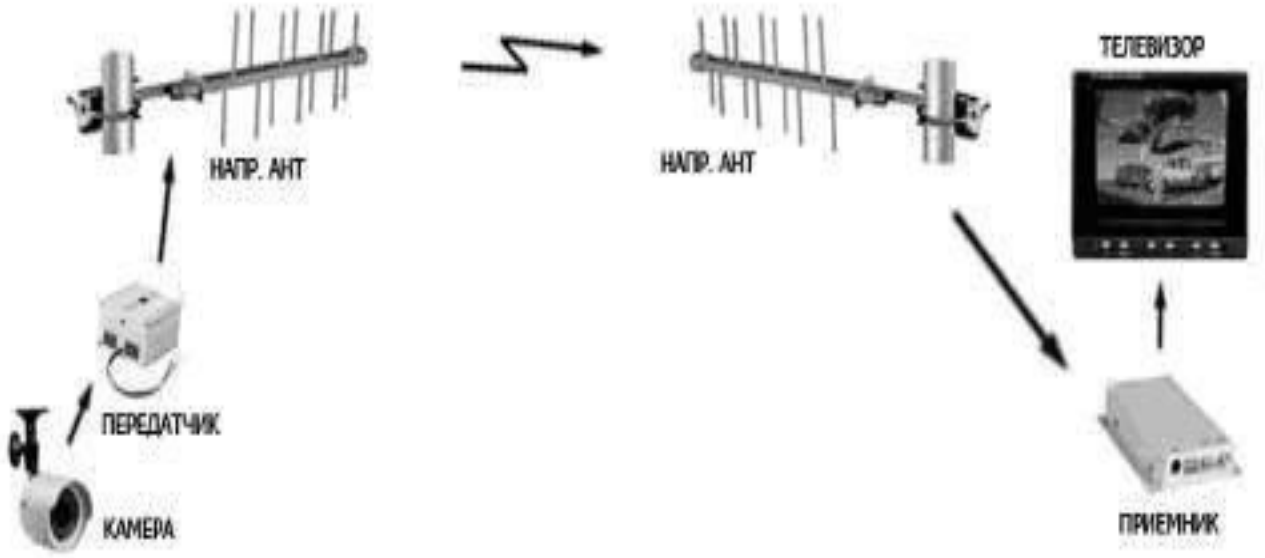


Рис. 2.3.5. Направленная антенна на передатчике и направленная антенна на приемнике

Итак, мы получили оцифрованный сигнал от камер, подключили камеры к сетевому оборудованию, а теперь будем использовать компьютерную сеть для передачи аудио- и видеоинформации непосредственно к посту видеонаблюдения. Этот пост может находиться как в 100м от объекта наблюдения, так и в 2000км от него. Замечательный показатель, который недостижим для традиционных аналоговых СВН. Однако нам он интересен с точки зрения масштабов IP-сети - от расстояний и количества объектов наблюдения зависит состав и конфигурация сетевого оборудования системы IP-видеонаблюдения и меры, необходимые для обеспечения ее безопасности. Это может быть один коммутатор, к которому подключены и камеры наблюдения, и компьютеры поста наблюдения, а также несколько маршрутизаторов и коммутаторов, обеспечивающих в совокупности передачу на значительные расстояния информации, поступающей от множества камер. Заметим, что в первом случае при использовании медного кабеля максимальное удаление камер от поста наблюдения составит 200м (ограничение стандарта FastEhernet).

В таблице 2.3.1 указаны расстояния, на которых (по "сдержанным" данным производителей IP-видеокамер) могут работать камеры со встроенными Wi-Fi-модулями стандарта 802.11 g.

Таблица 2.3.1 Дистанции работы Wi-Fi-IP-видеокамер в зависимости от типа антенны

Wi-Fi-IP-видеокамера	Точка доступа	Дистанция, м
Стандартная антенна внутри кожуха для установки вне помещения	Антенна для установки в помещении	10
Стандартная антенна внутри кожуха для установки вне помещения	Антенна для установки вне помещения	100
Внешняя антенна, подключенная к камере при помощи кабельного разъема	Антенна для установки вне помещения	300

2.4 Устройство IP-камер

Современная IP-камера представляет собой цифровое устройство, производящее видеосъемку, оцифровку, сжатие и передачу по компьютерной сети видеоизображения. Поэтому в состав ip-камеры входят следующие компоненты:

Таблица 2.4.1 Устройство ip-камеры

Компонент	назначение
ПЗС-матрица	В качестве фотоприемника в большинстве ip-камер применяется ПЗС-матрица (ПЗС, CCD – прибор с зарядовой связью) – прямоугольная светочувствительная полупроводниковая пластинка с отношением сторон 3 : 4, которая преобразует падающий на нее свет в электрический сигнал. ПЗС-матрица состоит из большого числа светочувствительных ячеек. Для того, чтобы повысить световую чувствительность ПЗС-матрицы, нередко формируют структуру, которая создает микролинзу перед каждой из ячеек. В технических параметрах ip-камеры обычно указывают формат ПЗС-матрицы (длина диагонали матрицы в дюймах), число эффективных пикселей, тип развертки (построчная или чересстрочная) и чувствительность.
Объектив	Объектив – это линзовая система, предназначенная для проецирования изображения объекта наблюдения на светочувствительный элемент камеры. Объектив является неотъемлемой частью ip-камеры, и от правильности его выбора и установки зависит качество видеоизображения, получаемого ip-камерой. Часто объектив входит в комплект поставки ip-камеры. Объективы характеризуются рядом важнейших параметров, таких как фокусное расстояние, относительное отверстие (F), глубина резкости, тип крепления (C, CS), формат.
Оптический фильтр	Оптические инфракрасные отсекающие фильтры, которые устанавливают в ip-камеры, представляют собой оптически точные плоскопараллельные пластинки, монтируемые сверху ПЗС-матрицы. Они работают как оптические низкочастотные фильтры с частотой среза около 700 нм, вблизи красного цвета. Они отсекают инфракрасную составляющую световых волн, обеспечивая тем самым правильную цветопередачу ip-камеры. Однако во многих черно-белых ip-камерах такие фильтры не используются, благодаря чему достигается более высокая чувствительность ip-камеры.
Плата видеозахвата	Плата видеозахвата (блок оцифровки) осуществляет преобразование аналогового электрического сигнала, сформированного матрицей, в цифровой формат. Процесс преобразования сигнала состоит из трех этапов: • Дискретизация; • Квантование; • Кодирование. **Дискретизация** – считывание амплитуды электрического сигнала через равные промежутки времени (период). Этот этап преобразования сигнала характеризуется частотой дискретизации. **Квантование** – это процесс представления результатов дискретизации в цифровой форме. Изменение уровня электрического сигнала за период дискретизации представляется в виде кодового слова из 8, 10 или 12 бит, которые дают соответственно 256, 1024 и 4096 уровней квантования. От числа уровней квантования зависит точность представления сигнала в цифровой форме. Кодирование. Помимо информации об изменении уровня сигнала, полученной на предыдущем этапе, в процессе кодирования формируются биты, сообщающие о конце синхроимпульса и начале нового кадра, а также дополнительные биты защиты от ошибок.
Блок компрессии (сжатия) видеоизображ	Блок компрессии выполняет сжатие оцифрованного видеосигнала в один из форматов сжатия (JPEG, MJPEG, MPEG-1/2/4, Wavelet). Благодаря сжатию сокращается размер видеокадра. Это необходимо для хранения и передачи видеоизображения по сети. Если локальная сеть, к которой подсоединена IP-

ения	камера, имеет ограниченную полосу пропускания, то во избежание переполнения сетевого трафика целесообразно сокращать объем передаваемой информации, снизив либо частоту передачи кадров по сети, либо разрешение кадров. Большинство форматов сжатия обеспечивает разумный компромисс между этими двумя способами решения проблемы передачи видео по сети. Известные на сегодняшний день форматы сжатия позволяют получить оцифрованный поток с полосой пропускания 64 Кб – 2 Мб (при такой полосе пропускания потоки видеоданных могут работать параллельно с другими потоками данных в сетях). Сжатие видеоизображения в IP-камере может быть представлено как аппаратно, так и программно. Программная реализация компрессии дешевле, однако, из-за высокой вычислительной емкости алгоритмов сжатия она малоэффективна, особенно когда требуется просматривать видеоизображение с ip-камеры в online режиме. Поэтому большинство ведущих производителей выпускают IP-камеры с аппаратной реализацией сжатия.
Центральный процессор и встроенный web-сервер	Центральный процессор является вычислительным ядром ip-камеры. Он осуществляет операции по выводу оцифрованного и сжатого видеоизображения, а также отвечает за выполнение функций встроенного web-сервера и управляющей программы для ip-камер.
ОЗУ	ОЗУ служит для хранения временных данных, которые генерируются при выполнении управляющих программ, и пользовательских скриптов. Многие интернет-камеры имеют так называемый видеобуфер. Это часть ОЗУ, зарезервированная для записи и временного хранения снятых ip-камерой видеокадров. Информация в видеобуфере обновляется циклически, т.е. новый кадр записывается вместо самого старого. Эта функция необходима, если ip-камера выполняет охранное видеонаблюдение, поскольку позволяет восстанавливать события, предшествующие и следующие за сигналом тревоги с подключенных к ip-камере охранных датчиков.
Флэш-память	Карта флэш-памяти позволяет обновлять управляющие программы для web-камер и хранить пользовательские HTML-страницы.
Сетевой интерфейс	После физического подключения к сети ip-камере присваивается IP-адрес. Благодаря встроенному программному обеспечению для web-сервера, FTP-сервера, FTP-клиента, e-mail клиента и др. ip-камера работает в ней как самостоятельное сетевое устройство. Это отличает ip-камеры от обычных компьютерных камер, которые требуют обязательного подключения к персональному компьютеру через USB. Кроме того, ip-камеры могут поддерживать работу с пользовательскими скриптами и JAVA-апплетами.
Тревожные порты	Тревожные входы/выходы служат для подключения датчиков тревоги. При срабатывании одного из датчиков генерируется сигнал тревоги, в результате чего процессор компонует набор кадров, записанных в видеобуфер до, после и в момент поступления сигнала тревоги. Этот набор кадров может отсылаться на заданный e-mail адрес или по FTP.
Дополнительные возможности и функции ip-камеры	
Детектор движения	Программный модуль, основной задачей которого является обнаружение перемещающихся в поле зрения веб-камеры объектов. Детектор движения не только обнаруживает перемещение в поле изображения, но и определяет габариты объекта и скорость его движения. В зависимости от задач видеонаблюдения, детектор движения настраивают на обнаружение перемещения объектов с предельной минимизацией ложных срабатываний (фильтрацией помех), задают гибкую логику обработки тревог (тревожная

	запись, интеграция с другим охранным оборудованием). Используя новые интеллектуальные алгоритмы программного обеспечения, могут распознавать номера машин, определять количество людей в кадре, анализировать уровень их агрессивности и т.д.
Защита паролем	Служит для ограничения прав доступа к ip-камере. По умолчанию видеоизображение с ip-камеры можно просматривать с любого сетевого компьютера, на котором установлен стандартный интернет-браузер, например, Internet Explorer. Однако можно ограничить число лиц с правами доступа к ip-камере, введя пароль на уровне пользователя. Многие ip-камеры поддерживают многоуровневую защиту паролем для разграничения прав доступа и администрирования.
Аудио регистратор/ спикер	Сетевые камеры обрабатывают аудиоинформацию непосредственно в камере, синхронизируя ее с видео или даже объединяя в тот же видеопоток и затем посылая по сети для контроля и/или записи. Звуковой канал может быть как одно-, так и двунаправленным, что позволяет не только получать, но и передавать звук на объект наблюдения.
Шифратор (программный / аппаратный)	IP камеры могут шифровать видео, посылаемое по сети, гарантируя, что видео поток не буден доступен для несанкционированного просмотра и вмешательства в него извне. Система может также устанавливать идентификацию подключения, используя сертификаты шифрования, с определенной сетевой камерой, таким образом устраняя возможность любого проникновения в линию связи. IP камера может добавлять зашифрованные "водяные знаки" в видео поток, данные с информацией относительно изображения, времени, местоположения, пользователей, тревог и т.д., чтобы обеспечить безопасность тракта передачи информации

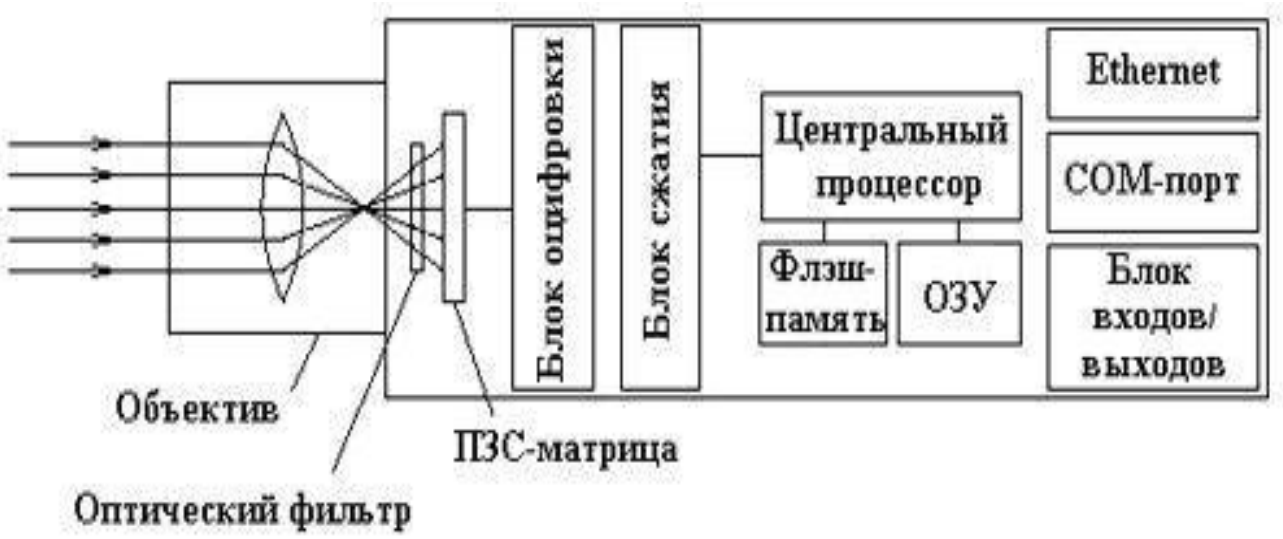


Рис. 2.4.1. Устройство IP-камеры

Видеокамеры характеризуются следующими параметрами:

- Формат (округленное значение диагонали матрицы в дюймах);

- Разрешающая способность (характеризует способность видеокамеры различать мелкие детали и удаленные предметы);
- Чувствительность или минимальная освещенность (характеризует способность видеокамеры наблюдать объекты при пониженной освещенности и даже в темноте, измеряется в люксах (лк));
- Борьба с изменениями освещенности (в составе видеокамеры имеется электронный затвор, который регулирует время накопления зарядов);
- Отношение сигнал/шум;
- Система автоматической регулировки усиления;
- Гамма-коррекция (указывает на то, что в видеокамере заведомо вводится нелинейная зависимость выходного видеосигнала от освещенности объекта для компенсации нелинейной зависимости яркости свечения кинескопа в видеомониторе от модулирующего напряжения);
- Компенсация встречной засветки;
- Баланс белого (является специфическим параметром цветных видеокамер, служит для правильной цветопередачи изображения на объекте при различных типах источника освещения);
- Напряжение питания (постоянный ток 12 В или сетевое напряжение 220 В);
- Диапазон рабочих температур;
- Конструктивное исполнение.

2.5 Общие сведения о VPN

Аббревиатура VPN расшифровывается как Virtual Private Network - "виртуальная частная сеть". Суть этой технологии в том, что при подключении к VPN серверу при помощи специального программного обеспечения поверх общедоступной сети в уже установленном соединении организуется зашифрованный канал, обеспечивающий высокую защиту передаваемой по этому каналу информации за счёт применения специальных алгоритмов шифрования.

В общем случае VPN - это объединение локальных сетей или отдельных машин, подключенных к сети общего пользования, в единую виртуальную (наложенную) сеть, обеспечивающую секретность и целостность передаваемой по ней информации (прозрачно для пользователей).

Использование технологии VPN необходимо там, где требуется защита корпоративной сети от воздействия вирусов, злоумышленников, просто любопытных, а также от других угроз, являющихся результатом ошибок в конфигурировании или администрировании сети.

Виртуальные частные сети (VPN), создаваемые на базе арендуемых и коммутируемых каналов связи сетей общего пользования (и, в первую очередь, Интернет), являются отличной альтернативой изолированным корпоративным сетям, причем, альтернативой, обладающей рядом несомненных преимуществ:

- низкая стоимость арендуемых каналов и коммуникационного оборудования;
- развитая топология сети (широкий географический охват);
- высокая надежность;
- легкость масштабирования (подключения новых сетей или пользователей);
- легкость изменения конфигурации;

• контроль событий и действий пользователей. Какими свойствами должна обладать VPN?

Можно выделить три фундаментальных свойства, превращающих наложенную корпоративную сеть, построенную на базе сети общего пользования, в виртуальную частную сеть:

• шифрование;
• аутентификация;
• контроль доступа.

Только реализация всех этих трех свойств позволяет защитить пользовательские машины, серверы предприятия и данные, передаваемые по физически незащищенным каналам связи, от внешних нежелательных вторжений, утечки информации и несанкционированных действий.

2.5.1 Классификация VPN

Классифицировать VPN решения можно по нескольким основным параметрам: 1. По типу используемой среды:

• *Защищенные VPN сети.* Наиболее распространённый вариант приватных частных сетей. С его помощью возможно создать надежную и защищенную подсеть на основе ненадёжной сети, как правило, Интернета. Примером защищенных VPN являются: IPSec, OpenVPN и PPTP.

• *Доверительные VPN сети.* Используются в случаях, когда передающую среду можно считать надёжной и необходимо решить лишь задачу создания виртуальной подсети в рамках большей сети. Вопросы обеспечения безопасности становятся неактуальными. Примерами подобных VPN решений являются: MPLS и L2TP. Корректнее сказать, что эти протоколы перекладывают задачу обеспечения безопасности на другие, например L2TP, как правило, используется в паре с IPSec.

2. По способу реализации:

• *VPN сети в виде специального программно-аппаратного обеспечения.* Реализация VPN сети осуществляется при помощи специального комплекса программно-аппаратных средств. Такая реализация обеспечивает высокую производительность и, как правило, высокую степень защищённости.

• *VPN сети в виде программного решения.* Используют персональный компьютер со специальным программным обеспечением, обеспечивающим функциональность VPN.

• *VPN сети с интегрированным решением.* Функциональность VPN обеспечивает комплекс, решающий также задачи фильтрации сетевого трафика, организации сетевого экрана и обеспечения качества обслуживания.

3. По назначению:

• *Intranet VPN.* Используют для объединения в единую защищенную сеть нескольких распределённых филиалов одной организации, обменивающихся данными по открытым каналам связи.

• *Remote Access VPN.* Используют для создания защищенного канала между сегментом корпоративной сети (центральным офисом или филиалом) и одиночным пользователем, который, работая дома, подключается к корпоративным ресурсам с домашнего компьютера или, находясь в командировке, подключается к корпоративным ресурсам при помощи ноутбука.

• *Extranet VPN.* Используют для сетей, к которым подключаются «внешние» пользователи (например, заказчики или клиенты). Уровень доверия к ним намного ниже, чем к сотрудникам компании, поэтому требуется обеспечение специальных «рубежей» защиты, предотвращающих или ограничивающих доступ последних к особо ценной, конфиденциальной информации.

4. По типу протокола:

Существуют реализации виртуальных частных сетей под *TCP/IP, IPX* и *AppleTalk.* Но на сегодняшний день наблюдается тенденция к всеобщему переходу на протокол *TCP/IP,* и абсолютное большинство VPN решений поддерживает именно его.

5. По уровню сетевого протокола:

По уровню сетевого протокола на основе сопоставления с уровнями эталонной сетевой модели ISO/OSI.

2.5.2 Построение VPN

Существуют различные варианты построения VPN. При выборе решения требуется учитывать факторы производительности средств построения VPN. Например, если маршрутизатор и так работает на пределе мощности своего процессора, то добавление туннелей VPN и применение шифрования/дешифрования информации могут остановить работу всей сети из-за того, что этот маршрутизатор не будет справляться с простым трафиком, не говоря уже о VPN. Опыт показывает, что для построения VPN лучше всего использовать специализированное оборудование, однако если имеется ограничение в средствах, то можно обратить внимание на чисто программное решение. Рассмотрим некоторые варианты построения VPN.

2.5.3 VPN на базе брандмауэров

Брандмауэры большинства производителей поддерживают туннелирование и шифрование данных. Все подобные продукты основаны на том, что трафик, проходящий через брандмауэр шифруется. К программному обеспечению собственно брандмауэра добавляется модуль шифрования. Недостатком этого метода можно назвать зависимость производительности от аппаратного обеспечения, на котором работает брандмауэр. При использовании брандмауэров на базе ПК надо помнить, что подобное решение можно применять только для небольших сетей с небольшим объемом передаваемой информации.

В качестве примера VPN на базе брандмауэра можно назвать Microsoft® Internet Security and Acceleration (ISA) Server 2006.

Функциональные возможности использования VPN в ISA Server 2006:

- политика брандмауэра, применяемая к соединениям VPN-клиентов;
- политика брандмауэра, применяемая к VPN-соединениям конфигурации узел-в-узел;
- VPN-карантин или временная изоляция;
- отображение пользователей для VPN-клиентов;
- поддержка клиентов SecureNAT для VPN-соединений;
- виртуальная частная сеть конфигурации «узел-в-узел» с применением туннельного режима протокола IPSec;
- публикация VPN-серверов по протоколу PPTP (Point-to-Point Tunneling Protocol, сквозной туннельный протокол);
- поддержка аутентификации секретным ключом Pre-shared Key для VPN-соединений по протоколу IPSec;
- улучшенная работа сервера имен для VPN-клиентов;
- мониторинг соединений VPN-клиентов.

2.5.4 VPN на базе маршрутизаторов

Другим способом построения VPN является применение для создания защищенных каналов маршрутизаторов. Так как вся информация, исходящая из локальной сети, проходит

через маршрутизатор, то целесообразно возложить на этот маршрутизатор и задачи шифрования.

Примером оборудования для построения VPN на маршрутизаторах является оборудование компании Cisco Systems. Начиная с версии программного обеспечения IOS 11.3, маршрутизаторы Cisco поддерживают протоколы L2TP и IPSec. Помимо простого шифрования проходящей информации Cisco поддерживает и другие функции VPN, такие как идентификация при установлении туннельного соединения и обмен ключами.

Для повышения производительности маршрутизатора может быть использован дополнительный модуль шифрования ESA. Кроме того, компания Cisco System выпустила специализированное устройство для VPN, которое так и называется Cisco 1720 VPN Access Router (маршрутизатор доступа к VPN), предназначенное для установки в компаниях малого и среднего размера, а также в отделениях крупных организаций.

2.5.5 VPN на базе программного обеспечения

Следующим подходом к построению VPN являются чисто программные решения. При реализации такого решения используется специализированное программное обеспечение, которое работает на выделенном компьютере, и в большинстве случаев выполняет роль proxy-сервера. Компьютер с таким программным обеспечением может быть расположен за брандмауэром.

Пример:

■ **OpenVPN** - свободная реализация технологии виртуальной частной сети (VPN) с открытым исходным кодом для создания зашифрованных каналов типа точка-точка или сервер-клиенты между компьютерами. Она позволяет устанавливать соединения между компьютерами находящимися за NAT-firewall без необходимости изменения его настроек. OpenVPN была создана Джеймсом Йонаном (James Yonan) и распространяется под лицензией GNU GPL.

2.5.6 VPN на базе сетевой ОС

■ В качестве VPN сервера можно использовать Windows NT Server 4.0, Windows 2000 Server, или Windows Server 2003/2008. Сам по себе сервер VPN очень прост. Это ничто иное, как усиленный Windows 2003/2008 Server, на котором запущены службы маршрутизации и удаленного доступа (Routing and Remote Access Services (RRAS)). После того, как произошла аутентификация входящего VPN соединения, сервер VPN просто работает как маршрутизатор, который предоставляет клиенту VPN доступ в частную сеть.

■ FreeBSD. VPN сервер реализуется на основе Multi-link PPP Daemon (MPD). MPD - это основанная на netgraph реализация PPP-протокола мультисвязи для FreeBSD. MPD спроектирован быть быстрым и гибким, обрабатывая конфигурацию и обращения в режиме пользователя, направляя пакеты данных напрямую в ядро.

2.5.7 VPN на базе аппаратных средств

Главное преимущество таких VPN - высокая производительность, поскольку быстродействие обусловлено тем, что шифрование в них осуществляется специализированными микросхемами.

Специализированные VPN-устройства обеспечивают высокий уровень безопасности, однако они дороги.

3. Фракталы и вейвлеты

Цифровые изображения занимают вес большую часть информационного мира. Развитие Интернета, наряду с доступностью все более мощных компьютеров и прогрессом в технологии производства цифровых камер, сканеров и принтеров, привели к широкому использованию цифровых изображений. Отсюда постоянный интерес к улучшению алгоритмов сжатия данных, представляющих изображения, Сжатие данных важно как для скорости передачи, так н эффективности хранения. Кроме многих видов коммерческого использования, технологии сжатия представляют также интерес для военных, например, приложения обработки данных телеметрии, полученных от перехватчиков ракет, или для архивного хранения данных об изображении местности для моделирования оборонительных действий. Решение проблемы сжатия изображения или в более общем смысле, кодирования изображения, использовало достижения и стимулировало развитие многих областей техники и математики.

Для начала приведем определение терминов относящихся к фрактал и вейвлет преобразованиям.

Фрактал (лат. fractus — дробленый, сломанный, разбитый) — сложная геометрическая фигура, обладающая свойством самоподобия, то есть составленная из нескольких частей, каждая из которых подобна всей фигуре целиком. В более широком смысле под фракталами понимают множества точек в евклидовом пространстве, имеющие дробную метрическую размерность (в смысле Минковского или Хаусдорфа), либо метрическую размерность, строго большую топологической.

Фрактал - это бесконечно самоподобная геометрическая фигура, каждый фрагмент которой повторяется при уменьшении масштаба.

Фрактал - самоподобное множество нецелой размерности.

Вейвлеты (от англ. wavelet), всплески (гораздо реже - вэйвлеты) - это математические функции, позволяющие анализировать различные частотные компоненты данных.

Однако это частное определение - в общем случае анализ сигналов производится в плоскости вейвлет-коэффициентов (масштаб - время - уровень) (Scale-Time-Amplitude). Вейвлет-коэффициенты определяются интегральным преобразованием сигнала. Полученные вейвлет-спектрограммы принципиально отличаются от обычных спектров Фурье тем, что дают четкую привязку спектра различных особенностей сигналов ко времени.

Следует отметить, что слово «фрактал» не является математическим термином и не имеет общепринятого строгого математического определения. Оно может употребляться, когда рассматриваемая фигура обладает какими-либо из перечисленных ниже свойств:

- Обладает нетривиальной структурой на всех шкалах. В этом отличие от регулярных фигур (таких, как окружность, эллипс, график гладкой функции): если мы рассмотрим небольшой фрагмент регулярной фигуры в очень крупном масштабе, он будет похож на фрагмент прямой. Для фрактала увеличение масштаба не ведёт к упрощению структуры, на всех шкалах мы увидим одинаково сложную картину.
- Является самоподобной или приближённо самоподобной.
- Обладает дробной метрической размерностью или метрической размерностью, превосходящей топологическую.

Многие объекты в природе обладают фрактальными свойствами, например, побережья, облака, кроны деревьев, кровеносная система и система альвеол человека или животных.

Фракталы, особенно на плоскости, популярны благодаря сочетанию красоты с простотой построения при помощи компьютера.

3.1 Вейвлетное сжатие

Вейвлетное сжатие - общее название класса методов кодирования изображений, использующих двумерное вейвлет-разложение кодируемого изображения или его частей. Обычно подразумевается сжатие с потерей качества.

Существенную роль в алгоритмах вейвлетной компрессии играет концепция представления результатов вейвлет-разложения в виде нуль-дерева (zero-tree).

Упорядоченные в нуль-дереве битовые плоскости коэффициентов вейвлет-разложения огрубляются и кодируются далее с использованием алгоритмов сжатия без потерь.

Суть метода

Вейвлетная компрессия в современных алгоритмах компрессии изображений позволяет значительно (до двух раз) повысить степень сжатия чёрно-белых и цветных изображений при сравнимом визуальном качестве по отношению к алгоритмам предыдущего поколения, основанным на дискретном косинусном преобразовании, таких, например, как JPEG.

3.2 Непрерывное вейвлет-преобразование

Непрерывное вейвлет-преобразование (англ. continuous wavelet transform, CWT) - вейвлет-преобразование, определяемое как

$$\gamma(\tau, s) = \int_{+\infty}^{-\infty} x(t) \frac{1}{\sqrt{s}} \psi^*\left(\frac{t-\tau}{s}\right) dt;$$

где τ представляет трансляцию, s представляет масштаб и ψ(t) — вейвлет-родитель (mother wavelet).

Изначальная функция может быть восстановлена с помощью обратного преобразования

$$x(t) = \frac{1}{C_\psi} \iint_{+\infty}^{-\infty} \gamma(\tau, s) \frac{1}{\sqrt{s}} \psi\left(\frac{t-\tau}{s}\right) dt \frac{ds}{|s|^2};$$

где

$$C_\psi = \int_{+\infty}^{-\infty} \frac{|\Psi(\varsigma)|^2}{|\varsigma|} d\varsigma$$

называется постоянной допустимости и Ψ — преобразование Фурье от ψ. Для того, чтобы обратное преобразование было успешным, постоянная допустимости должна соответствовать критерию допустимости

$C_\psi < +\infty$.

Также следует отметить, что критерий допустимости подразумевает, что Ψ(0) = 0, так что интеграл от вейвлета должен быть равен нулю.

Для работы с дискретными изображениями используется вариант вейвлет-преобразования, известный как алгоритм Малла, названный в честь его изобретателя Стефана Малла́ (фр. Stephane Mallat). Исходное изображение раскладывается на две составляющие — высокочастотные детали (состоящие в основном из резких перепадов яркости), и сглаженную уменьшенную версию оригинала. Это достигается применением пары фильтров, причём каждая из полученных составляющих вдвое меньше исходного изображения. Как правило, используются фильтры с конечным импульсным откликом, в которых пикселы, попавшие в небольшое «окно», умножаются на заданный набор коэффициентов, полученные значения суммируются, и окно сдвигается для расчёта следующего значения на выходе. Между вейвлетами и фильтрами есть тесная связь. Вейвлеты непосредственно не фигурируют в

алгоритмах, но если итерировать соответствующие фильтры на изображениях, состоящих из единственной яркой точки, то на выходе будут все отчётливей проступать вейвлеты.

Поскольку изображения двумерны, фильтрация производится и по вертикали, и по горизонтали. Этот процесс повторяется многократно, причём каждый раз в качестве входа используется сглаженная версия с предыдущего шага. Так как изображения «деталей» состоят обычно из набора резких границ, и содержат обширные участки где интенсивность близка к нулю. Если допустимо пренебречь некоторым количеством мелких деталей, то все эти значения можно просто обнулить. В результате получается версия исходного изображения, хорошо поддающаяся сжатию. Для восстановления оригинала снова применяется алгоритм Малла, но с парой фильтров, обратной к исходным.

Алгоритмы JPEG и MPEG, в отличие от вейвлетного, сжимают по отдельности каждый блок исходного изображения размером 8 на 8 пикселов. В результате, за счёт потери данных при сжатии, на восстановленном изображении может быть заметна блочная структура. При вейвлетном сжатии такой проблемы не возникает, но могут появляться искажения другого типа, имеющие вид «призрачной» ряби вблизи резких границ. Считается, что такие артефакты в среднем меньше бросаются в глаза наблюдателю, чем «квадратики», создаваемые JPEG.

Для работы с различными классами изображений могут использоваться различные фильтры. Возможно, поэтому всё ещё не существует единого стандарта для вейвлетного сжатия.

3.3 Фрактальное сжатие

Фрактальная архивация основана на том, что с помощью коэффициентов системы итерируемых функций изображение представляется в более компактной форме. В 1981 году Джон Хатчинсон опубликовал статью "Фракталы и самоподобие", в которой была представлена теория построения фракталов с помощью системы итерируемых функций (IFS, Iterated Function System).

Прежде чем рассматривать процесс архивации, разберем, как IFS строит изображение.

Строго говоря, IFS - это набор трехмерных аффинных преобразований, переводящих одно изображение в другое. Преобразованию подвергаются точки в трехмерном пространстве (x координата, y координата, яркость).

Наиболее наглядно этот процесс продемонстрировал сам Барнсли в своей книге "Фрактальное сжатие изображения". В ней введено понятие Фотокопировальной Машины, состоящей из экрана, на котором изображена исходная картинка, и системы линз, проецирующих изображение на другой экран. Каждая линза проецирует часть исходного изображения. Расставляя линзы и меняя их характеристики, можно управлять получаемым изображением. На линзы накладывается требование они должны уменьшать в размерах проектируемую часть изображения. Кроме того, они могут менять яркость фрагмента и проецируют не круги, а области с произвольной границей.

Существующие алгоритмы фрактального сжатия, как правило, придерживаются следующей схемы кодирования. Кодируемое изображение разбивается на множество неперекрывающихся блоков (ранговых областей), для каждого из которых, в пределах этого же изображения, ищется блок большего размера (домен), пикселы которого путём некоторого преобразования, задаваемого несколькими коэффициентами, переводились бы в пикселы ранговой области. При этом для поиска оптимального соответствия ранговых областей и

доменов необходим полный перебор вариантов, что влечёт за собой значительные вычислительные затраты. Из преобразований, переводящих домены в ранговые области, формируется отображение, переводящее изображение в изображение. При этом кодом изображения будут являться местоположение и размеры ранговых областей, а также коэффициенты преобразований, описывающих самоподобие внутри изображения. Количество бит, необходимых для описания кода, будет существенно меньше количества бит, необходимых для описания исходного изображения. Коэффициентом сжатия называется отношение битового представления изображения к битовому представлению кода. В известных фрактальных методах сжатия изображений значение этого коэффициента может достигать 100 при приемлемом качестве восстановления.

Для восстановления закодированного таким образом изображения используется принцип сжатых отображений, который гласит, что сжимающее отображение, действующее в полном метрическом пространстве, имеет единственную неподвижную точку. Отображение, действующее на полном метрическом пространстве изображений, формируется из преобразований, переводящих домены в ранговые области. Неподвижной точкой такого отображения (при условии, что оно является сжимающим) будет восстановленное полутоновое изображение.

Итак, пусть полутоновое изображение разбито на N ранговых областей R_i, для каждой из которых найден соответствующий домен D_i и преобразование w_i, задаваемое коэффициентами ($c_{i1},c_{i2},\ldots,c_{iK}$), такое что для каждого r$\hat{\imath}$ R_i существует d$\hat{\imath}$ D_i такое что $r=w_i(d)$. Причём преобразования w_i должны являться сжимающими, т.е. такими, что для всех d_l,dk$\hat{\imath}$ D_i выполняется

$$\|w_i(d_k) - w_i(d_i)\| \le s\|d_k - d_i\|;$$

где 0 £ s < 1. Из N преобразований w_i сформируем отображение W, переводящее изображения F_j в изображение F_{j+1}

$$F_{j+1} = W(F_j) = \bigcup_{i=1}^{N} w_i(F_j)$$

Следует учесть, что преобразования w_i действуют только на соответствующие домены D_i изображения F. Доказано, что если преобразования w_i являются сжимающими, то и отображение W также является сжимающим.

Для восстановления изображения, закодированного таким образом, нужно запустить итерационный процесс, используя в качестве стартового любое изображение F_0 (соответствующего размера). Согласно принципу сжатых отображений, отображение W будет иметь единственную неподвижную точку отображения (аттрактор), такую что F'=W(F'). Эта точка пространства изображений и будет восстановленным изображением, которое повторяет исходное с некоторой точностью. Задача построения оптимального кода изображения при использовании фрактального сжатия, как уже было сказано, требует значительных вычислительных затрат. Простейший путь ускорения вычислений заключается в использовании различных алгоритмов сужения поиска или вообще отказе от поиска. При использовании последнего алгоритма изображение разбивается на неперекрывающиеся квадратные блоки, каждый из которых разбит на четыре одинаковых квадратных подблока. Каждый блок является доменом для своих подблоков, а подблоки - ранговыми областями. Задача кодирования изображения в этом случае сводится к проверке подобия ранговой области домену, содержащему эту область. В случае отсутствия подобия соответствующий подблок снова разбивается на четыре квадратных "подподблока" и сам становится доменом для своих подблоков.

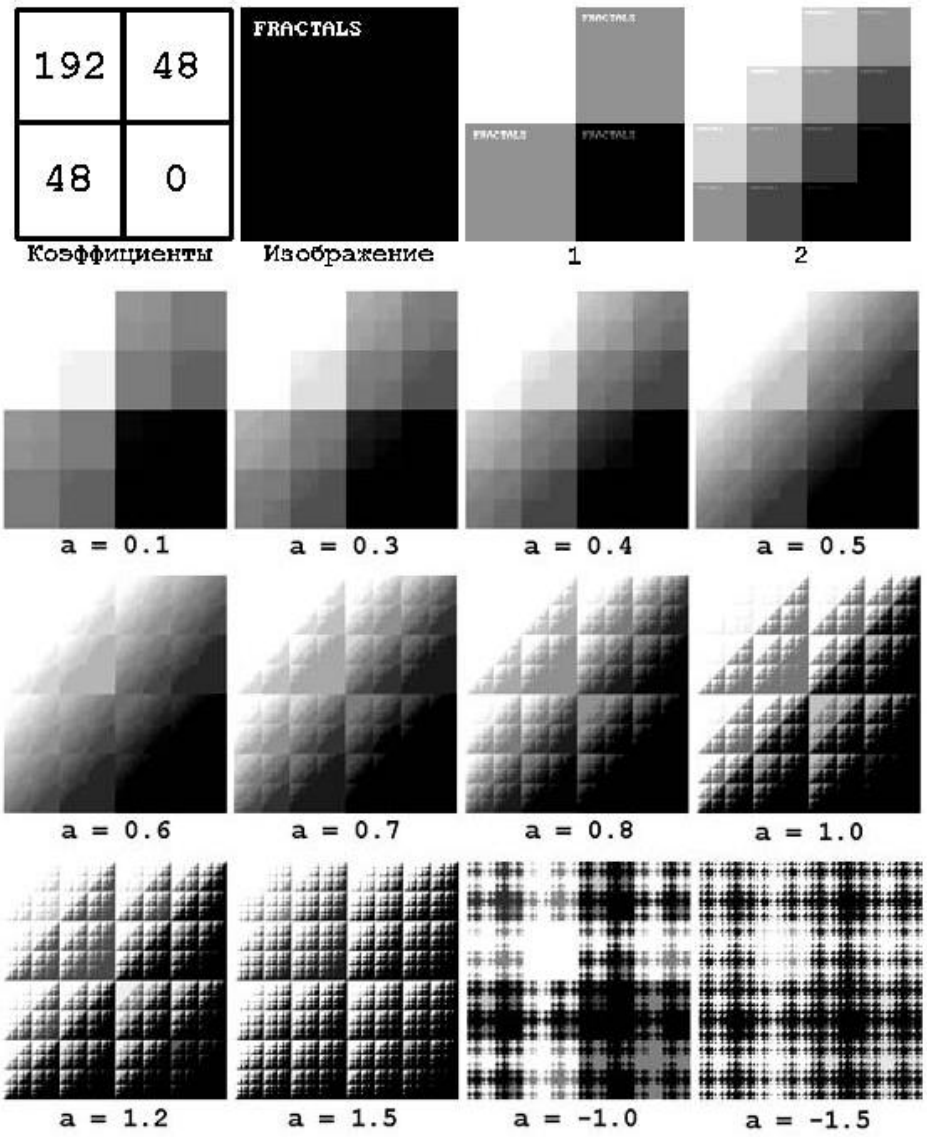


Рис. 3.3.1. Итерации восстановления изображения из кода

Процесс разбиений продолжается до тех пор, пока очередной подблок не будет состоять из одного пиксела.

В качестве примера построения фрактального изображения приведем общеизвестный треугольник Серпинского.

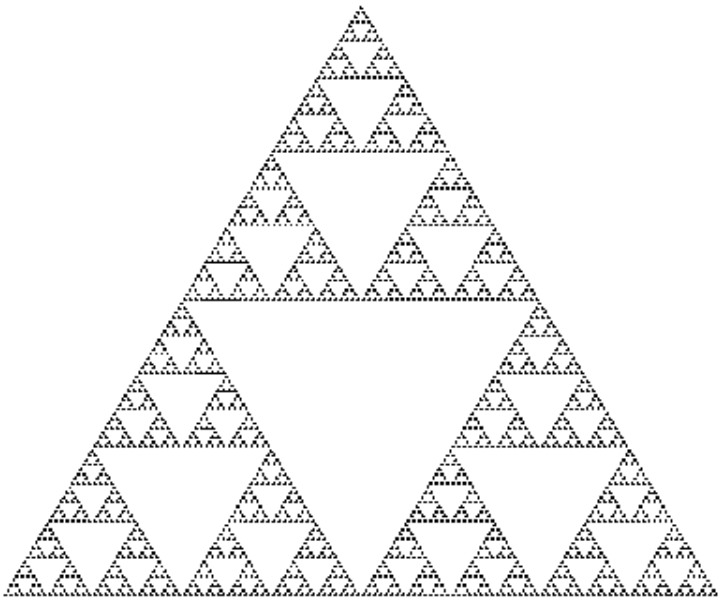


Рис. 3.3.2. Треугольник Серпинского

Алгоритмический шаг машины состоит в построении с помощью проецирования по исходному изображению нового. Утверждается, что на некотором шаге изображение перестанет изменяться. Оно будет зависеть только от расположения и характеристик линз и не будет зависеть от исходной картинки. Это изображение называется неподвижной точкой или аттрактором данной IFS. Collage Theorem гарантирует наличие ровно одной неподвижной точки для каждой IFS. Поскольку отображение линз является сжимающим, каждая линза в явном виде задает самоподобные области в нашем изображении. Благодаря самоподобию мы получаем сложную структуру изображения при любом увеличении.

Наиболее известны два изображения, полученных с помощью IFS треугольник Серпинского и папоротник Барнсли Первое задается тремя, а второе - питью аффинными преобразованиями (или, в нашей терминологии, линзами). Каждое преобразование задается буквально считанными байтами, в то время, как изображение, построенное с их помощью, может занимать и несколько мегабайт.

Становится понятно, как работает архиватор, и почему ему требуется так много времени. Фактически, фрактальная компрессия - это поиск самоподобных областей в изображении и определение для них параметров аффинных преобразований.

В худшем случае, если не будет применяться оптимизирующий алгоритм, потребуется перебор и сравнение всех возможных фрагментов изображения разного размера. Даже для небольших изображений при учете дискретности мы получим астрономическое число перебираемых вариантов. Даже резкое сужение классов преобразований, например, за счет масштабирования только в определенное число раз, не позволит добиться приемлемого времени. Кроме того, при этом теряется качество изображения. Подавляющее большинство исследований в области фрактальной компрессии сейчас направлены на уменьшение времени архивации, необходимого для получения качественного изображения.

3.4 Оценка потерь и способы их регулирования

До сих пор мы не затронули несколько важных вопросов. Например, что делать, если алгоритм не может подобрать для какого-либо фрагмента изображения подобный ему? Достаточно очевидное решение - разбить этот фрагмент на более мелкие и попытаться поискать для них. Однако понятно, что процедуру эту нельзя повторять до бесконечности, иначе количество необходимых преобразований станет так велико, что алгоритм перестанет быть алгоритмом компрессии. Следовательно, допускаются потери в какой-то части изображения.

Для фрактального алгоритма компрессии, как и для других алгоритмов сжатия с потерями, очень важны механизмы, с помощью которых можно будет регулировать степень сжатия и степень потерь. К настоящему времени разработан достаточно большой набор таких методов. Во-первых, можно ограничить количество преобразований, заведомо обеспечив степень сжатия не ниже фиксированной величины. Во-вторых, можно потребовать, чтобы в ситуации, когда разница между обрабатываемым фрагментом и наилучшим его приближением будет выше определенного порогового значения, этот фрагмент дробился обязательно (для него обязательно заводится несколько линз). Втретьих, можно запретить дробить фрагменты размером меньше, допустим, четырех точек. Изменяя пороговые значения и приоритет этих условий, можно очень гибко управлять коэффициентом компрессии изображения: от побитного соответствия, до любой степени сжатия.

3.5 Возможности масштабирования

IFS задает фрактальную структуру, сколь угодно близкую к нашему изображению. При внимательном рассмотрении процесса построения изображения с ее помощью становится понятно, что восстанавливаемое изображение может иметь любое разрешение.

На этапе архивации проводится распознавание изображения, и в виде коэффициентов хранится уже не растровая информация, а информация о структуре самого изображения. Именно это и позволяет при развертывании увеличивать его в несколько раз. Особенно впечатляют примеры, в которых при увеличении изображений природных объектов проявляются новые детали, действительно этим объектам присущие (например, когда при увеличении фотографии скалы она приобретает новые, более мелкие неровности).

Однако если изображение однородно (на фотографии только скала), то при увеличении получаются отличные результаты, однако, если сжимать изображение натюрморта, то предсказать, какие новые фрактальные структуры возникнут, очень сложно. Впрочем, вдвое-втрое можно увеличить практически любое изображение, при архивации которого задавалась небольшая степень потерь.

3.6 Сжатие видеопоследовательностей

Ещё одна проблема состоит в том, как эффективно использовать схожесть последовательных кадров при сжатии видео. В ранних алгоритмах, таких как Motion JPEG, этот фактор игнорировался, и кадры сжимались индивидуально. MPEG использует алгоритм сравнения блоков, который старается выделить участки, изменившиеся при смене кадра. Блоки же, которые не изменились, можно не сохранять. При третьем подходе, удобном для вейвлетного сжатия, время рассматривается как третье измерение массива данных, к которому применяется алгоритм Малла. Отсутствие перемещений проявляется в обнулении соответствующих деталей по временному направлению. Эксперименты показывают, что этот метод даёт хорошие результаты, хотя и требует больших вычислений.

Надо заметить, что вейвлет-преобразование само по себе ничего не сжимает. Оно лишь осуществляет препроцессинг изображения, после которого эффективность обычных методов сжатия резко возрастает, причём даже при использовании универсальных алгоритмов и программ (таких, как LZW и pkzip), не адаптированных к конкретной задаче. Впрочем, использование методов кодирования, учитывающих структуру вейвлет-преобразования, может существенно повысить степень сжатия. Один из широко используемых методов такого типа — метод нуль-дерева (англ. zero-tree compression). Он основан на предположении, что если некоторая область изображения не содержит нетривиальной информации на некотором уровне разрешения, то с большой вероятностью она не будет информативной и на более тонком уровне разрешения. Вейвлет-преобразование изображения можно хранить в виде дерева, корнем которого является сильно сглаженная версия оригинала, а ветви, представляющие отдельные блоки, обрываются на том уровне, где дальнейшая обработка не даёт заметного уточнения. Такое дерево можно с успехом сжать обычными методами типа хаффмановского или арифметического кодирования, которые используются почти во всех алгоритмах сжатия.

3.6 Реализации

Наиболее известный алгоритм вейвлетной компрессии — JPEG 2000. Вейвлет-компрессия используется также при кодировании в формат DjVu. Существует также множество нестандартизированных алгоритмов кодирования изображений и видео-последовательностей основанных на вейвлет-компрессии и предназначенных для специализированного применения. Например одними из самых известных алгоритмов, применяемых в системах видеонаблюдения является Motion Wavelet и 3D Wavelet. Вейвлет-преобразование в системах видеонаблюдения используется намного чаще по причине преимущества в качестве изображения каждого отдельного кадра видеозаписи. Профессиональное избыточное качество в системах видеонаблюдения необходимо для достоверного ретроспективного анализа событий по видеозаписям.

Формат сжатия MPEG 4

MPEG4 использует технологию так называемого фрактального сжатия изображений. Фрактальное (контурно-основанное) сжатие подразумевает выделение из изображения контуров и текстур объектов. Контуры представляются в виде т.н. сплайнов (полиномиальных функций) и кодируются опорными точками. Текстуры могут быть представлены в качестве коэффициентов пространственного частотного преобразования (например, дискретного косинусного или вейвлет-преобразования).

Диапазон скоростей передачи данных, который поддерживает формат сжатия видео изображений MPEG 4, гораздо шире, чем в MPEG 1 и MPEG 2. Формат сжатия видео изображений MPEG 4 поддерживает широкий набор стандартов и значений скорости передачи данных. MPEG 4 включает в себя методы прогрессивного и чересстрочного сканирования и поддерживает произвольные значения пространственного разрешения и скорости передачи данных в диапазоне от 5 кбит/с до 10 Мбит/с. В MPEG 4 усовершенствован алгоритм сжатия, качество и эффективность которого повышены при всех поддерживаемых значениях скорости передачи данных.

Варианты применения прогрессивных методов сжатия

На данный момент описанные выше методики сжатия видеоизображений широкого применения мало используются. Причин этому факту не видно как таковых. Возможно, патентные проблемы; возможно - неудачный маркетинг. Но факт остается фактом:

прогрессивная технология, использование которой могло бы сэкономить экзабайты дискового пространства и терабайты пропускной способности, не используется.

Нами предлагается использовать вейвлет и фрактал сжатие видеопоследовательностей по нескольким направлениям:

- Декодирование принимаемого изображения разрешением 640x480 в виде больших разрешений, таких как 860x640, или например 1024x768 используя свойство масштабируемости фрактального преобразование. Исключив из передаваемого ряда данных информацию о размере изображения производится увеличивающее декодирование видеоряда. С соответствующим сохранением качества и улучшением разрешающей способности графики применяемых в современных интерполяторах и аналогичными свойствами фрактал и вейвлет преобразований.
- Исключив из передаваемого ряда данных информацию о размере изображения производится увеличивающее декодирование видеоряда. С сохранением небольшой полосы пропускания соответствующей небольшим изображениям.
- Использование для передачи видеоизображения современных видео форматов применяющих технологию вейвлет и фрактал преобразования.
- Использование виртуальных вычислительных комплексов таких как LabVIEW и FMAQ Vision для обработки видеоизображения с использованием вейвлет и фрактал преобразований.

Варианты выбора способа и средств обработки видеоряда возможны любые из технологически приемлемых на данный момент развития тех уровня и возможностей.

Как вариант - распространение разных дополнений для сжатия интернет-трафика ведет к увеличению нагрузки на систему. Но нагрузка на систему не идет ни в какое сравнение с увеличением скорости и экономией трафика.

Технология мультикаст

Multicast (англ. групповая передача) — специальная форма широковещания, при которой копии пакетов направляются определённому подмножеству адресатов. Наряду с приложениями, устанавливающими связь между источником и одним получателем, существуют такие, где требуется, чтобы источник посылал информацию сразу группе получателей. В качестве таких приложений можно упомянуть дистанционное обучение, рассылку корпоративной информации, репликацию баз данных и информации веб-сайтов и многое другое. При традиционной технологии IP-адресации требуется каждому получателю информации послать свой пакет данных, то есть одна и та же информация передается много раз. Технология групповой адресации представляет собой расширение IP-адресации, позволяющее направить одну копию пакета сразу всем получателям. Множество получателей определяется принадлежностью каждого из них к конкретной группе. Рассылку для конкретной группы получают только члены этой группы.

Технология IP Multicast предоставляет ряд существенных преимуществ по сравнению с традиционным подходом. Например, добавление новых пользователей не влечет за собой необходимое увеличение пропускной способности сети. Значительно сокращается нагрузка на посылающий сервер, который больше не должен поддерживать множество двухсторонних соединений. Использование групповой адресации позволяет обеспечить доступ корпоративных пользователей к данным и сервисам, ранее недоступным, так как для их реализации с помощью обычной адресации потребовались бы значительные сетевые ресурсы.

В последнее время широкое распространение приобрели мультимедиа трансляции и видеоконференцсвязь. При использовании традиционной технологии пропускной способности существующих каналов хватает лишь для установления связи с очень ограниченным числом получателей. Групповая адресация снимает это ограничение и получателей может быть любое количество.

В настоящее время IP Multicast является широко поддерживаемым сетевым стандартом. Все современное сетевое программное обеспечение и аппаратное оборудование поддерживает этот стандарт. Для использования групповой IP-адресации необходима ее поддержка локальной сетью. Что касается глобальной сети, в некоторых случаях допустимо использование «туннелирования» для преодоления участков, эту адресацию не поддерживающих.

Для реализации групповой адресации в локальной сети необходимы: поддержка групповой адресации стеком протокола TCP/IP; программная поддержка протокола IGMP для отправки запроса о присоединении к группе и получении группового трафика; поддержка групповой адресации сетевой картой; приложение, использующее групповую адресацию, например видеоконференция. Для расширения этой возможности на глобальную сеть дополнительно необходима поддержка всеми промежуточными маршрутизаторами групповой

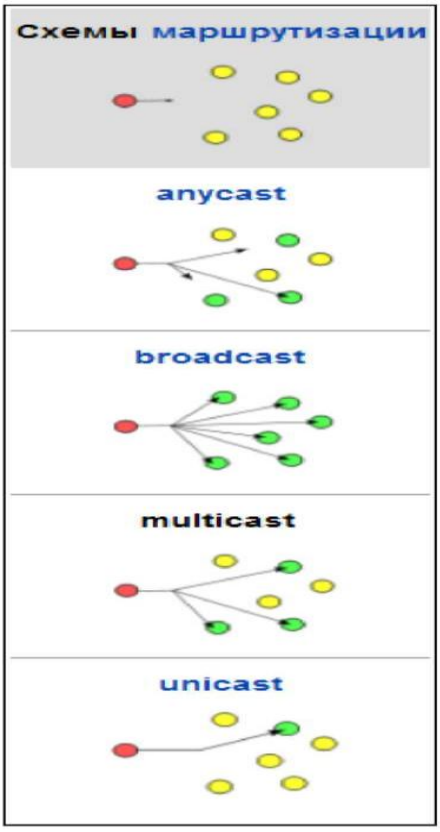


Рис. 3.3.3. Технология IP Multicast

адресации и пропускание группового трафика используемыми firewall-ами. В локальной сети можно добиться еще большей оптимизации, используя коммутаторы с фильтрацией группового трафика, автоматически настраивающиеся на передачу трафика только получателям.

Технология IP Multicast использует адреса с 224.0.0.0 до 239.255.255.255. Поддерживается статическая и динамическая адресация. Примером статических адресов являются 224.0.0.1 — адрес группы, включающей в себя все узлы локальной сети, 224.0.0.2 — все маршрутизаторы локальной сети. Диапазон адресов с 224.0.0.0 по 224.0.0.255 зарезервирован для протоколов маршрутизации и других низкоуровневых протоколов поддержки групповой адресации. Остальные адреса динамически используются приложениями.

Для определения членства сетевых устройств в различных группах локальной сети маршрутизатор использует протокол IGMP. Один из маршрутизаторов подсети периодически опрашивает узлы подсети, чтобы узнать, какие группы используются приложениями узлов. На каждую группу генерируется только один ответ в подсети. Для того, чтобы стать членом новой группы, узел получателя инициирует запрос на маршрутизатор локальной сети. Сетевой интерфейс узла-получателя настраивается на прием пакетов с этим групповым адресом. Каждый узел самостоятельно отслеживает свои активные групповые адреса, а когда отпадает необходимость состоять в данной группе, прекращает посылать подтверждения на IGMP-запросы. Результаты IGMP-запросов используются протоколами групповой маршрутизации для передачи информации о членстве в группе на соседние маршрутизаторы и далее по сети.

Основная идея групповой маршрутизации состоит в том, что маршрутизаторы, обмениваясь друг с другом информацией, строят пути распространения пакетов ко всем необходимым подсетям без дублирования и петель. Каждый из маршрутизаторов передает

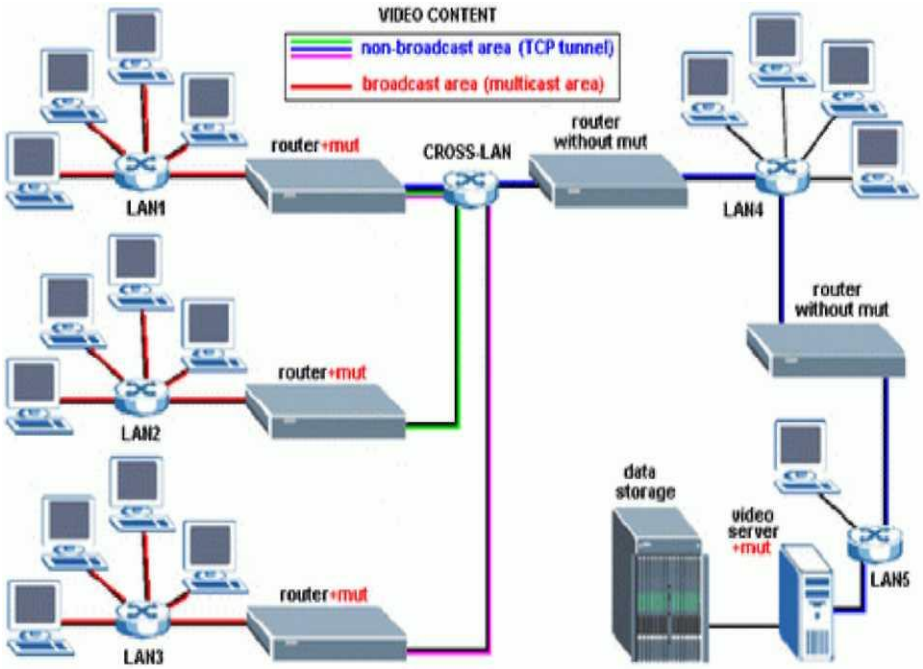


Рис. 2.7.2. Пример построения сети с использованием IP мультикаст

принимаемый пакет на один или несколько других маршрутизаторов, избегая тем самым повторной передачи одного и того же пакета по одному каналу и доставляя его всем получателям группы. Поскольку состав группы со временем может меняться, вновь появившиеся и выбывшие члены группы динамически учитываются в построении путей маршрутизации.

Преимущества построения систем видеонаблюдения на базе IP-видеокамер

Среди достоинств Wi-Fi видеонаблюдения можно выявить следующие особенности:

- Высокое качество видеоизображения

В последнее время на рынке появилось значительное количество мегапиксельных IP-камер (1, 2, 3 и даже 5 мегапикселей). Мегапиксельные камеры формируют видеопотоки с достаточно хорошими скоростями обновления (например, 25 кадр/сек при двух мегапикселях или 50 кадр/сек при одном мегапикселе), что подразумевает более высокую информативность изображения, а значит и повышение уровня безопасности в целом.

- Высокая дальность применения при использовании направленных антенн

Использование дополнительных антенн дает возможность значительно увеличить зону действия систем беспроводного видеонаблюдения. Это происходит вследствие выноса антенны из помещения и подъема её относительно приемника/передатчика, а также благодаря коэффициенту усиления самой антенны. Так использование только одной направленной антенны в канале приемника увеличивает радиус действия системы в 4-6 раз, в зависимости от условий приема. Следует отметить, что при большой длине кабеля снижения от антенны к приемнику, используя кабель с большими потерями, можно лишиться всех преимуществ использования внешней антенны.

- Масштабируемость за счет применения ретрансляторов.

Использование ретрансляционного оборудования позволяет увеличить рабочее расстояние без прокладки кабельных линий.

- Возможность транслирования потока от нескольких камер по одной Wi-Fi сети.

Когда используется точка доступа, следует учитывать, что она представляет собой обычный концентратор. При нескольких подключениях видеокамер к одной точке полоса пропускания делится на количество подключенных пользователей. Теоретически ограничений на количество подключенных видеокамер нет, но на практике их число следует ограничивать, исходя из минимально необходимой скорости передачи данных для каждой камеры. Например, одна сетевая камера с разрешением VGA и скоростью 25 кадр/с при небольшом сжатии в самом популярном формате MPEG-4 занимает полосу в 2-2,5 Мбит/с. Это означает, что 10 камер отнимут максимум 25 Мбит/с, то есть точка доступа с полосой пропускания 54 Мбит/с (а с реальной скоростью передачи данных 25 Мбит/с) позволит без проблем принять сигнал от 10 Wi-Fi-видеокамер, а если брать в расчет видеокамеры с более современным сжатием H.264, то поток от камеры с тем же качеством займет около 0,5-1 Мбит/с. К одной точке доступа можно подключить и больше 25 видеокамер.

- Управление поворотными камерами

Оператор может наблюдать изображение с камеры, установленной в любой точке и управлять поворотным или фокусирующим механизмом точно так же, как если бы она была подключена к проводной сети.

- Надежность соединения

Правильный подбор оборудования, использование внешних узконаправленных антенн (которые, кстати, с помощью кабеля можно удалить от видеокамеры на расстояние до 30 м) и промежуточных точек доступа успешно решают эту проблему.

- Защищенность передачи данных

Защита видеоинформации в беспроводных IP-системах видеонаблюдения достигается несколькими способами. Ключевыми среди них являются: применение брандмауэров, использование паролей и шифрование. Брандмауэр работает как электронные "ворота", пропускающие зарегистрированных пользователей и запрещающие доступ неавторизованным лицам. Применение паролей позволяет не только ограничить доступ к системе видеонаблюдения, но и распределить права доступа персонала к определенным видеокамерам. А при шифровании попытки перехвата зашифрованных данных в IP-системе охранного видеонаблюдения становятся бессмысленными, если злоумышленник не знает уникального кода для расшифровки потока данных. Код, в свою очередь, устанавливается системным администратором.

- Легитимность использования Wi-Fi

Этот вопрос немного сложнее. Дело в том, что в России применение Wi-Fi без разрешения на использование частот от Государственной комиссии по радиочастотам (ГКРЧ) возможно для организации сети внутри зданий, закрытых складских помещений и производственных территорий. Для легального создания внеофисной беспроводной сети Wi-Fi (например, радиоканала между двумя соседними домами) необходимо получение разрешения на использование частот. При этом следует напомнить, что действует упрощенный порядок выдачи разрешений на использование радиочастот в полосе 2400-2483,5 МГц (стандарты 802.11b и g), для получения такого разрешения не требуется обращаться в ГКРЧ.

- Глушение сигнала

Такая опасность, действительно, существует. Но, во-первых, для того, чтобы полностью заглушить сигнал, нужен достаточно мощный источник, и, во-вторых, этот источник должен находиться очень близко к радиотракту. Однако даже в этом случае можно попытаться решить проблему с помощью мощных узконаправленных антенн.

- Вредность излучения

Мировая организация здравоохранения (World Health Organization) признала излучение Wi-Fi безвредным для здоровья человека. Так, например, излучение от устройств Wi-Fi в среднем в 10-20 раз ниже, чем от обычного сотового телефона.

- Экономическая целесообразность.

В отличие от традиционных систем, расширение которых фактически ведет к внушительным дополнительным затратам, использование IP-видео позволяет при расширении системы лишь добавлять IP-камеры или IP-видеосерверы. При наличии локальной вычислительной сети (ЛВС) дальнейшее расширение системы влечет за собой исключительно добавление IP-камер и не требует использования дополнительных линий. С другой стороны, программное обеспечение, которое применяется для записи IP-видео, как правило, рассчитано на дальнейшее расширение, то есть мы имеем дело лишь с закупкой соответствующих лицензий на запись необходимого количества видеоканалов.

Схема лабораторного макета

С учетом поставленной задачи, а именно организовать макет системы IP-видеонаблюдения на основе технологии Wi-Fi , можно выделить следующие блоки, входящие в структурную схему:

- IP-видеокамеры;

- Сетевое оборудование;
- Компьютер поста видеонаблюдения;

Система коммутации и маршрутизации предназначена для транспортировки видеоданных и служебной информации внутри системы IP-видеонаблюдения. От нее требуется достаточная пропускная способность и защищенность.

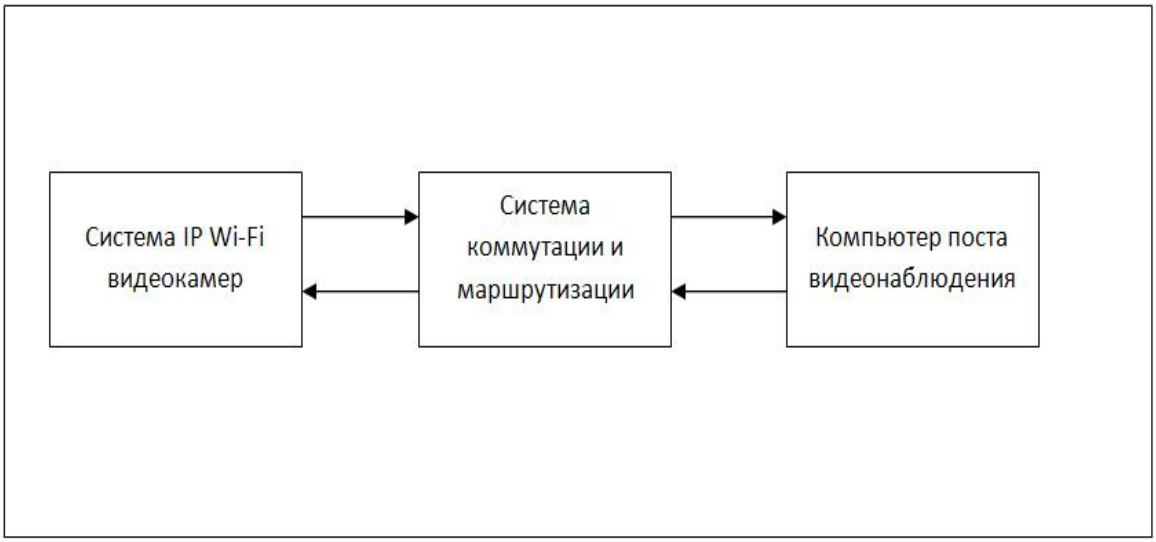


Рис. 3.5.1. Макет системы IP-видеонаблюдения

Компьютер поста видеонаблюдения должен быть оснащен удобным и доступным пользовательским интерфейсом. Также он должен обладать хорошими вычислительными мощностями, т.к. на него возлагается задача декомпрессии принимаемого видео. Пространство монитора должно вмещать области отображения от нескольких камер. На компьютере поста охраны должно быть установлено специализированное ПО, позволяющее транслировать видеоданные зарегистрированным пользователям из локальной сети.

Выбор оборудования

Критерии выбора видеокамеры для наружного наблюдения обуславливаются спецификой эксплуатации устройств - для четкого изображения в любое время суток особое значение приобретают разрешение, чувствительность устройства, его стойкость к низким и высоким температурам, взаимодействие оптики с посторонними источниками света, например, лампами освещения и т.д. Следует отметить, что для съемок в ночное время, как правило, устанавливается черно-белый режим, с ИК подсветкой.

Определим основные критерии выбора видеокамеры:

- Высокое качество изображения (разрешение, матрица с прогрессивной разверткой);
- Поддержка стандартов IEEE802.11b/g;
- Персональный беспроводной маршрутизатор;
- Сжатие видеопотока
- Функциональные возможности;
- Стоимость.

В качестве сетевого оборудования в моей системе выступает Wi-Fi router.

Таблица 3.6.1 Сравнение беспроводных IP-видеокамер.

Чувствительный элемент (ПЗС матрица)	1/4" (6мм)		1/3" (8мм)		Иная
Чувствительность	Отсутствие освещения	Минимальная освещенность	Стандартная освещенность		Хорошая освещенность
Объектив	встроенный		Съемный		
Угол обзора	90°	100°	110°	130°	150°
Разрешение видеокамеры	Более 15 уровней от 160x90 до 1280x1024 пикс.				
Формат сжатия	M-JPEG	MPEG-4	H.264	MPEG-2	HD
Видеопоток	параллельная передача	Выборочная передача	Одиночная передача		
Аудио	Встроенный микрофон		Подключаемый микрофон		
Беспроводное подключение	IEEE 802.11g	IEEE 802.11b	IEEE 802.11n	IEEE 802.11a	
Безопасность	Многоуровневая система парольной защиты	Фильтрация IP-адресов	HTTPS-кодирование	WEP 64/128 бит	WPA-PSK, TKIP / WPA2-PSK, AES
Многопользовательский доступ	одноадресная передача		многоадресная передача		
Подключение к сети	10BaseT	100BaseTX Ethernet	RJ-45	USB	Беспроводная передача данных
Сетевые протоколы	IPv4/v6, HTTP, TCP, ICMP, RTSP, RTP, UDP, IGMP, RTCP, SMTP, FTP, DHCP, UPnP, Bonjour, ARP, DNS, DynDNS, SOCKS, NTP и др.				

Выбор точки доступа был в основном по критерию надежности и поддержки стандартов, указанных в техническом задании. Технические характеристики представлены в таблице 3.6.2.

Таблица 3.6.2 Технические характеристики точки доступа.

Модель точки доступа	D-Link <DWL-G700AP> Wireless G Access Point
Частотный диапазон, ГГц	2,4-2,5 ГГц
Поддержка стандартов	IEEE 802.11g, IEEE 802.11b
Максимальная скорость передачи	54 Мбит/с
Тип оборудования	Точка доступа, мост
Внешняя антенна	1 антенна
Питание	Внешнее
Стоимость	1204 р

Нами используется модель видеокамеры Internet Camera Server TV-IP 110W
Параметры используемой видеокамеры приведены в таблице 3.6.3

Таблица 3.6.3 Технические характеристики точки доступа.

• Тип датчика	1/4" цветной CMOS-датчик
• Разрешение	640x480 pixel
• Объектив	Встроенный f: 6.0mm, F: 1.8
Video	
• Frame Rate	15fps@VGA, 30fps @ QVGA, 30fps @ QQVGA
• Compression	MJPEG
• Resolution	640x480,320x240,160x120
• Digital Zoom	4X
Беспроводная связь	
• Стандарты	IEEE B02,11Wg
• Скорость передачи данных	11g:54,48, 36,24,12,9 & 6 Mbps • 11Ь: 11,5.5, 2 & 1 Mbps
• Модульная аппаратура	8O2.11b. OFDM 802.11g. DESS
• Частота	2.4 - 2.4fl35GHz (ISMB)
• Антенна	Отсоединяемая разнесенная антенна, 2dBi {Разъем Reverse SMA)
• Шифрование	64/128 bits WEP (ASCII/HEX), WPA-PSK/WPA2-PSK (AES/TKIP)

Критерии оптимальности проектируемой системы

Для проектирования беспроводной системы видеонаблюдения, 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:

1. **Диапазон рабочих частот**. Данный параметр является особенно важным, поскольку система видеонаблюдения должна использовать аппаратуру, работающую в частотном диапазоне, разрешенном в РФ. 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, рассчитанного на работу в диапазоне 5 ГГц, не представляется возможным.

2. **Дальность действия радиосистемы.** Для обеспечения качественной связи видео 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

3. **Скорость передачи информации.** Требования к скорости передачи данных являются одними из основных. Из рассмотренных выше стандартов, оптимальным с точки зрения скорости, является стандарт передачи данных 802.11g, позволяющий передавать информацию со скорость до 54 Мбит/с.

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. Стандарт 802.11g наиболее приемлем, 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. В дальнейшем возможен переход на стандарт 802.11n по мере поступления оборудования на существующий рынок.

Оценка производительности системы

Не смотря на то, что все выпускаемое оборудование соответствует стандарту 802.11g, реальная пропускная способность при работе точки доступа с различным оборудованием оказывается различной.

Для тестирования будет применятся программный пакет **Traffic Meter 10.0.553**. 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 3.5.2. В помещении, где проводится тестирование, нет оборудования работающего в диапазоне 2.4 ГГц. Точки разнесены на 3 метра.

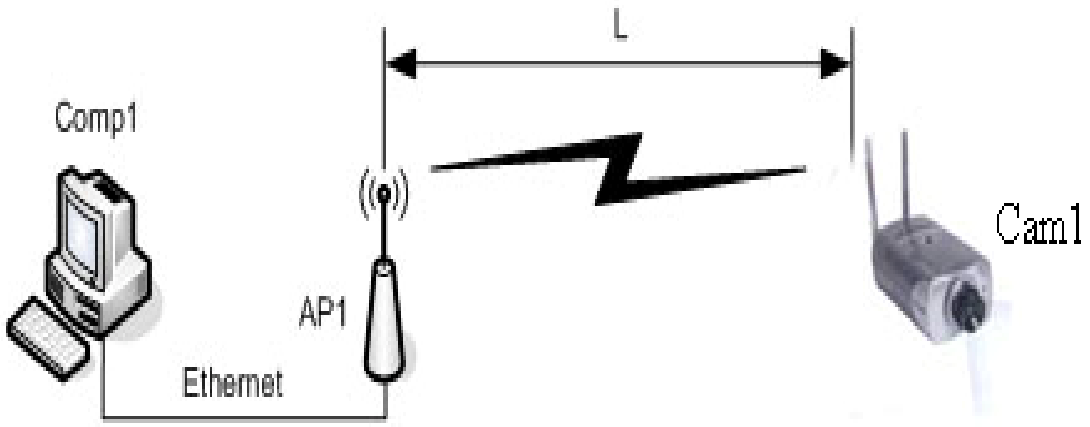


Рис. 3.5.2. Тестовый стенд для определения максимальной пропускной способности точки доступа.

Осуществляется передача трафика между узлами Comp1 и Cam1. В ходе тестирования направление передачи и количество потоков трафика будет меняться.

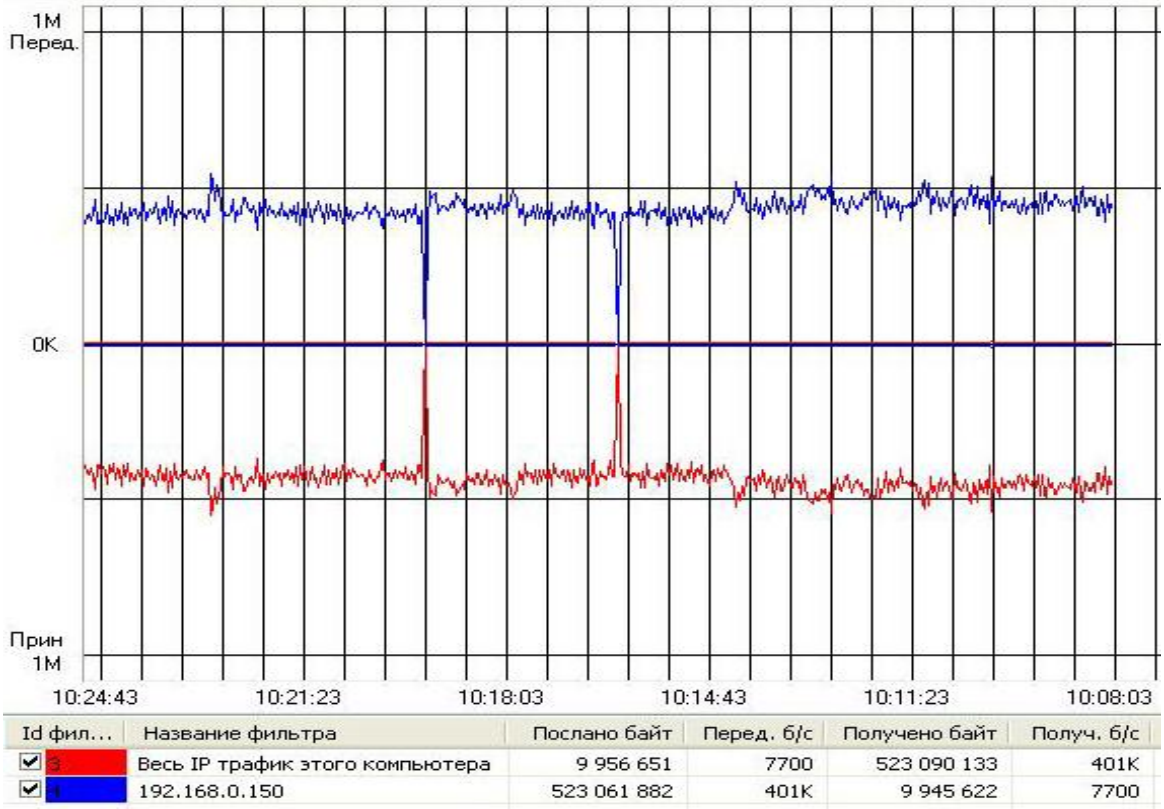
Оценка накладных расходов связанных с шифрованием

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).

При проведении тестирования будем использовать тестовый стенд, изображенный на рисунке 3.5.2.

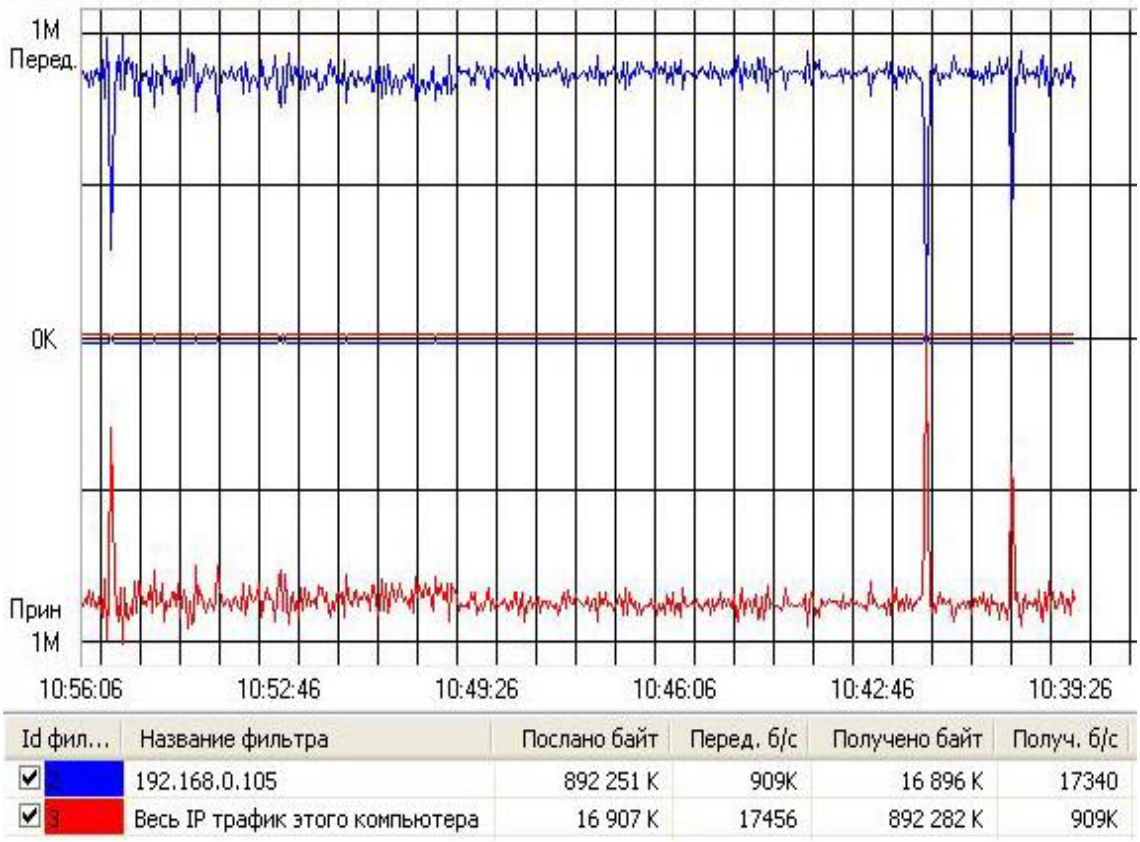
Результаты эксперимента.

Приведем некоторые из полученных данных: для сравнения измеряемого трафика параллельно ему мы отобразим весь интернет трафик тестового компьютера. Графическое представление нагрузки на сеть представлено в виде графиков для статичного изображения и динамичного изображения.



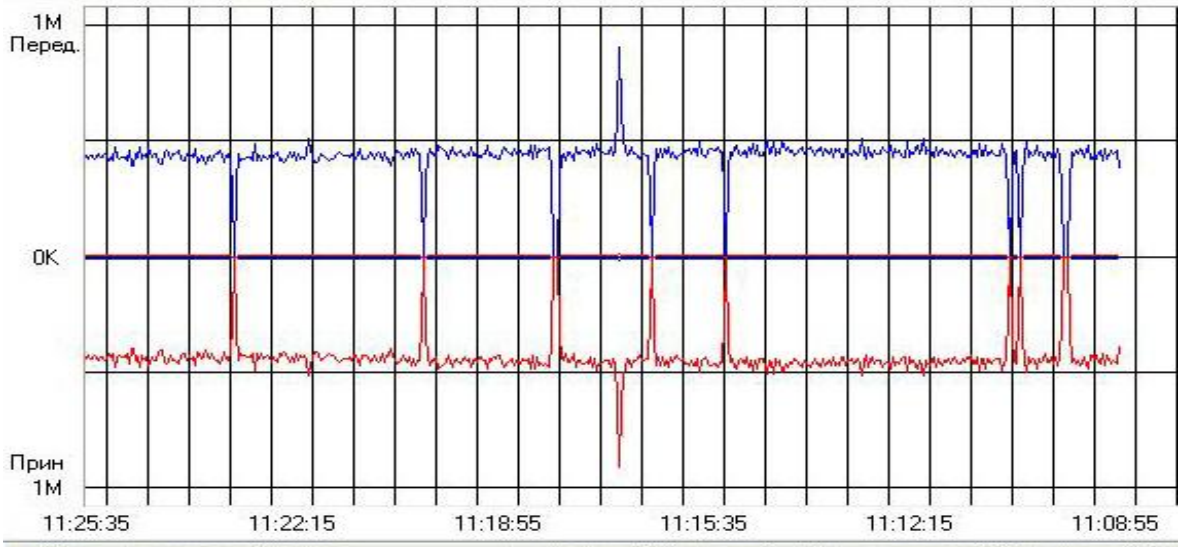
Id фил...	Название фильтра	Послано байт	Перед. б/с	Получено байт	Получ. б/с
3	Весь IP трафик этого компьютера	9 956 651	7700	523 090 133	401K
4	192.168.0.150	523 061 882	401K	9 945 622	7700

Рис. 3.5.3 Нагрузка на сеть при передаче статичного изображения



Id фил...	Название фильтра	Послано байт	Перед. б/с	Получено байт	Получ. б/с
	192.168.0.105	892 251 K	909K	16 896 K	17340
3	Весь IP трафик этого компьютера	16 907 K	17456	892 282 K	909K

Рис. 3.5.4. Нагрузка на сеть при передаче динамичного изображения



Id фил...	Название фильтра	Послано байт	Перед. б/с	Получено байт	Получ. б/с
	192.168.0.105	453 248 K	457K	8 675 K	9100
3	Весь IP трафик этого компьютера	8 685 K	9100	453 292 K	457K

Рис. 3.5.5. Неравномерность нагрузки на сеть при передаче изображения

Как мы можем наблюдать: в отличии от проводного видеонаблюдения в беспроводном возможны задержки передачи небольшой длительности, они компенсируются собственной памятью видеокамеры (16 Мбайт) что позволяет исключить потери видео длительностью до 30 секунд в результате помех на линии. Видео без потерь формируется в сервере хранения а на обзорном дисплее возможны задержки и искажения, так как ведется трансляция реального времени.

Проведем эксперимент, когда приемная и передающая точки разнесены в разные комнаты и разделены бетонной перегородкой толщиной 20 см.

Ухудшения качества изображения не наблюдается, но помеха вносит свое воздействие на передаваемый трафик и он становится неравномерным, что отображено на рисунке 3.5.6

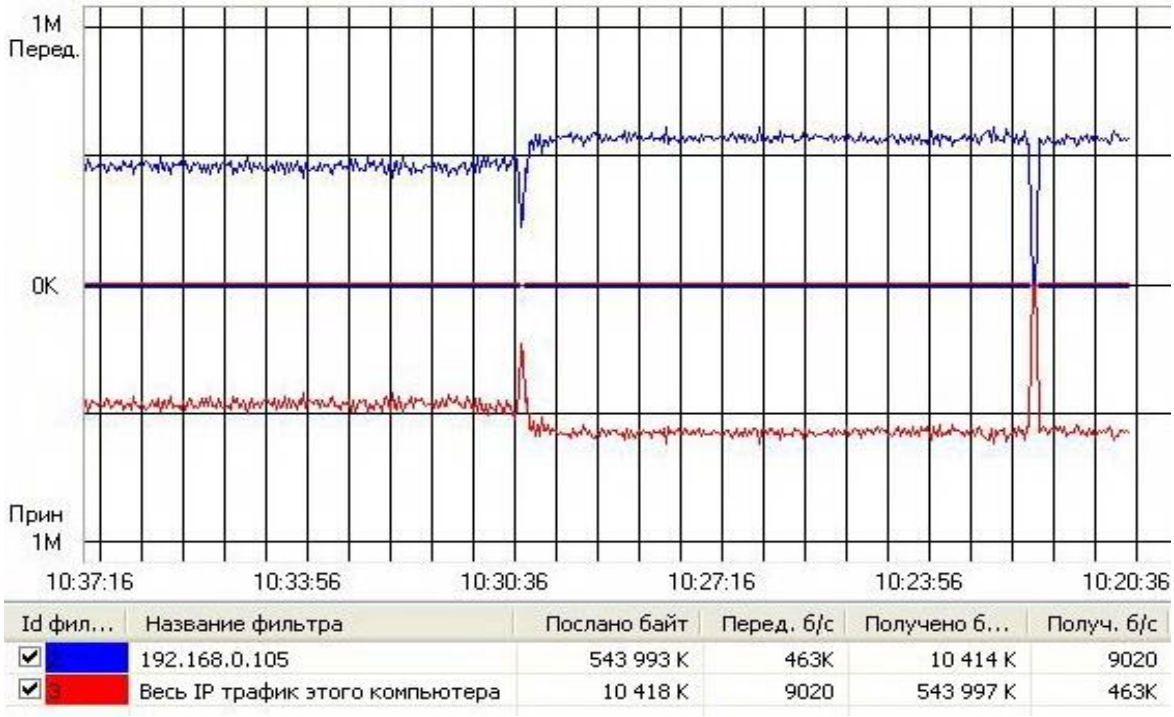


Рис. 3.9.4. Неравномерность нагрузки на сеть при передаче изображения из разных помещений.

Сравнив передачу видео при качестве **MPEG – 4 (640x480 / 25 к/с good quality)** расчетного, динамического изображения и статического изображения, мы можем сделать вывод: для неискаженной передачи для данной камеры необходимо иметь полосу пропускания 1Мбит/с. Уменьшение полосы ведет к искажению передаваемого видео сигнала.

4. Рекомендованная литература

1.Беспроводные сети Wi-Fi // http://www.INTUIT.ru

2.Дамьяновски В. CCTV. Библия видеонаблюдения. Цифровые и сетевые технологии.: Пер. с англ. - М.: ОАО «Ай-Эс-Эс-Пресс» 2006г - 406с.

3.Столлингс В. Беспроводные линии связи и сети.: Пер. с англ. - М.: Издательский дом «Вильямс», 2003. - 640 с.
4.Малухин А.А. Правда и мифы о Wi-Fi в ЛР-видеонаблюдении // http://www.daily.sec.ru

Лабораторная работа 3. Исследование системы IP-видеоконференций

1. Цель работы

Видеоконференция - это не просто видеотелефон. Видеоконференция - это компьютерная технология, которая позволяет людям видеть и слышать друг друга, обмениваться данными и совместно их обрабатывать в реальном режиме времени. Все это осуществимо благодаря специализированным системам видеоконференцсвязи (ВКС).

Для проведения сеансов видеоконференцсвязи необходимо выполнение двух важнейших условий: (а) Вы должны иметь соответствующее оборудование видеоконференцсвязи; (б) Вы должны иметь возможность соединиться с коллегой через любые каналы связи (в том числе и спутниковые), отвечающие требованиям видеоконференцсвязи.

По разным источникам 80…85 % информации человек воспринимает зрительно, поэтому видеоконференцсвязь оказывает неоценимую помощь человеку в жизни. В связи с этим применение видеоконференций в управлении, медицине, дистанционном обучении, системах безопасности и многих других областях приносит огромную пользу.

Конечно, даже видеоконференции никогда не заменят личного общения, но они позволяют добиться принципиально нового уровня общения людей, подчас разделенных многими тысячами километров. Ведь согласно многочисленным исследованиям, на слух человек воспринимает всего лишь десятую часть информации (как, например, при телефонном разговоре). А в случае, когда есть возможность следить за жестикуляцией и мимикой собеседника, КПД восприятия информации достигает 80…85 %.

Менеджеры компаний, использующие видеоконференции в повседневной жизни, утверждают, что системы видеоконференций резко сокращают временные и финансовые затраты фирмы на совещания, семинары, командировки их сотрудников и консультации.

2.Краткие теоретические сведения

В чем основные проблемы передачи аудио- и видеоинформации? Их две. Первая проблема состоит в том, что канал связи, по которому передается информация, должен быть достаточно скоростным, т.е. обладать высокой пропускной способностью. Обычные телефонные каналы вполне подходят для передачи аудиосигнала, но качественную передачу видеопотока они не обеспечивают (здесь правда существуют обходные пути - системы уплотнения каналов, но они применимы далеко не всегда). Эта проблема постепенно решается. Вспомним хотя бы, как медленно развивались локальные вычислительные сети в нашей стране. Сейчас же фактически во всех офисах существует локальная вычислительная сеть. А такая сеть уже вполне пригодна для организации высококачественной видеоконференции.

Вторая проблема - это проблема скорости обработки аудио- и видеопотока, т.е. кодирования передаваемых и декодирования получаемых данных. Дело в том, что в видеоконференциях используются специальные и весьма эффективные алгоритмы сжатия потока в десятки (а подчас и сотни!) раз. Можно сказать, что передаются не сами аудио- и видеосигналы, а только их важнейшие параметры, которые позволяют восстанавливать сигнал на приемном конце с приемлемым качеством. Если приемная сторона не успевает обрабатывать поток, то появляются пропущенные кадры, сбои в речевом канале, и т.п.

Направления применения видеоконференцсвязи

Видеоконференция применяется как средство оперативного принятия решения в той или иной ситуации; при чрезвычайных ситуациях; для сокращения командировочных расходов в территориально распределенных организациях; повышения эффективности; проведения судебных процессов с дистанционным участием осужденных, а также как один из элементов технологий телемедицины и дистанционного обучения.

Во многих государственных и коммерческих организациях видеоконференция приносит большие результаты и максимальную эффективность, а именно:

- снижает время на переезды и связанные с ними расходы;
- ускоряет процессы принятия решений в чрезвычайных ситуациях;
- сокращает время рассмотрения дел в судах общей юрисдикции;
- увеличивает производительность;
- решает кадровые вопросы и социально-экономические ситуации;
- предотвращает усталость и стресс;
- позволяет следить за состоянием рынка и быстро реагировать на его изменения;
- дает возможность принимать более обоснованные решения за счёт привлечения при необходимости дополнительных экспертов;
- быстро и эффективно распределяет ресурсы, и так далее.

Для общения в режиме видеоконференции абонент должен иметь терминальное устройство (кодек) видеоконференцсвязи, видеотелефон или иное средство вычислительной техники. Как правило в комплекс устройств для видеоконференцсвязи входит:

- центральное устройство — кодек с видеокамерой и микрофоном, обеспечивающего кодирование/декодирование аудио- и видео- информации, захват и отображение контента;
- устройство отображения информации и воспроизведения звука.

В качестве кодека может использоваться персональный компьютер с программным обеспечением для видеоконференций.

Большую роль в видеоконференции играют каналы связи, то есть транспортная сеть передачи данных. Для подключения к каналам связи используются сетевые протоколы IP или ISDN.

Существует два режима работы ВКС, которые позволяют проводить двусторонние (режим «точка-точка») и многосторонние (режим «многоточка») видеоконференции.

Как правило, видеоконференцсвязь в режиме «точка-точка» удовлетворяет потребности только на начальном этапе внедрения технологии, и довольно скоро возникает необходимость одновременного взаимодействия между несколькими абонентами. Такой режим работы называется «многоточечный» или многоточечной видеоконференцсвязью. Для реализации данного режима требуется наличие активации многоточечной лицензии в кодеке при условии, если устройство поддерживает данную функцию, либо специального видеосервера MCU (англ. *Multipoint Control Unit*), или программно-аппаратной системы управления.

Цель внедрения видеоконференцсвязи

Для внедрения видеоконференцсвязи руководителю (лицу, принимающему решения) организации необходимо определить главную цель применения: проведение совещаний, подбор персонала, оперативность при принятии решений, осуществление контроля, дистанционное обучение, консультация врачей, проведение судебных заседаний, допрос свидетелей и так далее. При этом необходимо учитывать основные правила видеоконференцсвязи:

- оборудование со стороны приёма/передачи должно быть одного производителя;
- гарантированная высокоскоростная услуга связи или выделенные каналы связи только для сеансов видеоконференций;

- стабильное и надёжное электропитание телекоммуникационного оборудования и видеоконференцсвязи;
- оптимальные шумо- и эхо- поглощающие особенности помещения в котором будет установлено оборудование видеоконференцсвязи;
- правильное расположение оборудования видеоконференцсвязи по отношению к световому фону помещения;
- корректная настройка телекоммуникационного оборудования и видеоконференцсвязи по обслуживанию качества услуги связи с приоритезацией передачи данных;
- компетентный обслуживающий технический персонал.

Основные категории и классы видеоконференцсвязи
Категории видеоконференцсвязи
Индивидуальные системы


Индивидуальные системы Polycom и Tandberg

Индивидуальные системы обеспечивают возможность индивидуального видеообщения пользователя в режиме реального времени, не покидая своего рабочего места. Конструктивно индивидуальные системы обычно выполняются в виде настольных терминалов либо виде программных решений.

Групповые системы

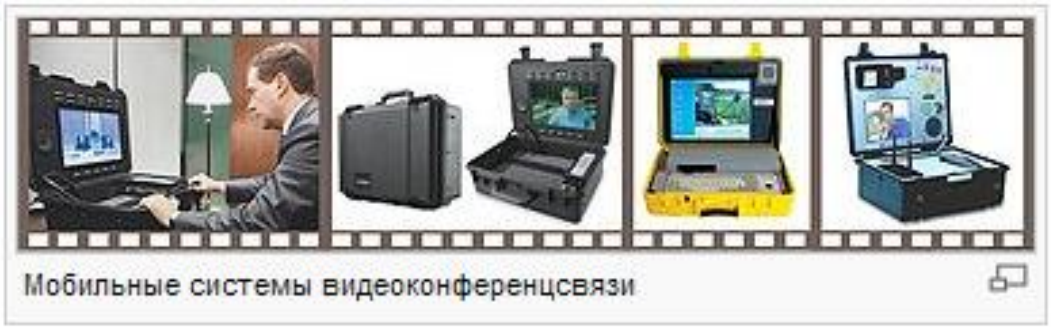

Групповые системы Polycom и Tandberg

Групповые системы предназначены для проведения групповых сеансов видеоконференцсвязи в переговорных (совещательных) комнатах. Групповая система способна превратить помещение любого размера в видеоконференц-студию для проведения интерактивных совещаний. К групповым системам относятся приставки видеоконференцсвязи (set-top) стандартного разрешения и с поддержкой высокой чёткости (High Definition). К этой же категории относятся и системы класса TelePresence (телеприсутствие), которые предоставляют собой комплекс средств, обеспечивающий максимальный эффект присутствия удалённых собеседников в одной комнате.

Отраслевые системы

Отраслевые системы — это системы, которые применяются непосредственно в определенной отрасли. Например, в медицинской отрасли очень часто применяют системы для проведения операций (телемедицина), в судебной системе — для проведения дистанционных кассационных и надзорных судебных процессов, в нефтегазовой, энергетической, строительной области для оперативности представления информации.

Мобильные системы



Мобильные системы — это компактные переносные системы видеоконференцсвязи для использования в удалённых районах и экстремальных условиях. Мобильные системы позволяют за короткое время организовать сеанс видеоконференцсвязи в нестандартных условиях. Данные системы обычно используются государственными органами, принимающими оперативные решения (военные, спасатели, врачи, службы экстренного реагирования). Типичный пример использования мобильных систем — организация ситуационного центра.

Административные системы

Административные системы представляют собой совокупность аппаратно-программных средств администрирования/управления многоточечными сеансами видеоконференцсвязи с использованием различного оконечного оборудования. К этой категории относятся сервера многоточечной видеоконференцсвязи (Multipoint Control Unit), а также программно-аппаратные системы управления (совокупность систем учёта, управления конфигурацией, безопасностью, производительностью и ошибками узлов, линий и оконечного оборудования видеоконференцсвязи).

Классы видеоконференцсвязи

Категории подразделяются на классы, которые включают в себя пять различных классов.

Программное решение

Программные решения устанавливаются на компьютер, оснащённый web-камерой и головной гарнитурой.

Программное решение видеоконференцсвязи

К данному классу относятся:

- Платные решения: Tandberg Movi, Polycom PVX, Meeting point 4.0, VideoPort SBS Plus, Tandberg See&Share и так далее.
- Бесплатные решения: Skype, NetMeeting, VC software, Ekiga, Earthlink beta, CU-SeeMe, Visitalk, Ivisit, HoneyQ, ICUII, ISPQ, VLVC, ooVoo, SightSpeedrvers, OpenH323 и другие.

Платные решения в отличие от бесплатных обычно обеспечивают более широкие функциональные возможности при проведении конференций (например, поддерживается большое число участников) и совместимость с аппаратными решениями видеоконференцсвязи различных производителей (благодаря использованию открытых стандартов SIP и H.323).

Общие ограничения программных решений:

- предназначены только для индивидуального использования (невозможно использовать в переговорных комнатах для проведения групповых сеансов видеоконференцсвязи);
- высокая нагрузка на центральный процессор ПК.

Видеоконференции стандартного качества

Групповые системы Polycom и Tandberg стандартного качества

Видеоконференции стандартного качества (англ. Standard Definition) подразумевают поддержку четырёх стандартных видеоразрешений: SQCIF (128x96), QCIF (176x144), CIF (352x288) и 4CIF (704x576) на скоростях передачи данных от 64 Кбит/с до 768 Кбит/с.

Разрешения SQCIF и QCIF изначально были введены для медленных каналов связи (от 64 Кбит/с) и в настоящее время практически не используются. Разрешение CIF поддерживается на скоростях от 256 Кбит/с. Самое высокое стандартное разрешение 4CIF доступно на скоростях от 384 Кбит/с.

Примечание — минимальные значения скоростей передачи данных для того или иного разрешения могут варьироваться в зависимости от производителя оборудования.

Видеоконференции высокой чёткости

Класс высокой четкости (англ. High Definition или англ. HD) появился в связи с выпуском на рынок систем ВКС с более высоким разрешением, чем 4CIF, то есть разрешение HD (1280x720), которое требует в несколько раз больше пикселей для построения изображения по сравнению со стандартной видеоконференцсвязью, и, соответственно, для её передачи необходима более высокая скорость.

Появлению видеоконференции высокой чёткости способствовало несколько факторов:

- в западных странах начался массовый переход на цифровое телевидение, в результате которого мониторы, фотоаппараты, камеры стали поддерживать технологии высокой четкости;
- в дополнение к H.323 был ратифицирован стандарт сжатия видео H.264, обеспечивающий более эффективный алгоритм сжатия громоздких файлов для передачи видео по сети, в том числе беспроводной;
- одновременно с этим на рынок было выпущено новое поколение высокопроизводительных специализированных процессоров для обработки видео.

Термин High Definition никаким стандартом не определяется. Он появился как маркетинговое понятие, подразумевающее передачу видеоизображения с разрешением выше 4CIF и его сопровождение более качественным звуком. Качество изображения уровня HD может быть получено при ширине канала не менее 1 Мбит/с. При отсутствии необходимой полосы пропускания технология HD позволяет адаптироваться под существующий канал связи, то есть если полосы пропускания недостаточно для поддержки качества HD, то система

видеоконференцсвязи не откажется работать, а просто автоматически подберёт соответствующую скорость работы стандартного качества.

Телеприсутствие


Телеприсутствие

Телеприсутствие (англ. TelePresence) — технология проведения сеансов видеоконференцсвязи, обеспечивающая максимально возможный эффект присутствия. Практически это и есть совокупность класса видеоконференции высокой чёткости в комплексе с другим оборудованием.

Небольшие отличия от оборудования видеоконференцсвязи высокой чёткости:

- повышенная четкость изображения;
- улучшенное качество передачи звука, достигаемое благодаря высокой частоте дискретизации (до 22 кГц) и объёмному звучанию;
- увеличенная пропускная способность канала связи.

Благодаря технологии телеприсутствия стали доступными следующие возможности:

- воспроизведение малейших эмоциональных проявлений собеседника;
- масштабирование изображения до размеров реального человека;
- маскировка технологических деталей (видеокамер, микрофонов, рамок телевизионных матриц) и так далее.

Ситуационные/диспетчерские центры


Ситуационные центры Российской Федерации

Ситуационные/диспетчерские центры (англ. Situation and Control Centers) или комнаты предназначены для лиц, принимающих решения и могут быть использованы в различных областях деятельности.

Ситуационные и диспетчерские центры предоставляют возможность:

- экспресс-анализа текущего положения;

- моделирования сценариев возможных событий;
- экспертной оценки принимаемых решений и их оптимизации;
- выбора наиболее эффективного управленческого воздействия на ту или иную ситуацию и так далее.

Организация каналов связи

Основную роль в видеоконференции играют каналы связи между абонентами. Рассмотрим несколько методов организации каналов связи для видеоконференций.

В сети Интернет

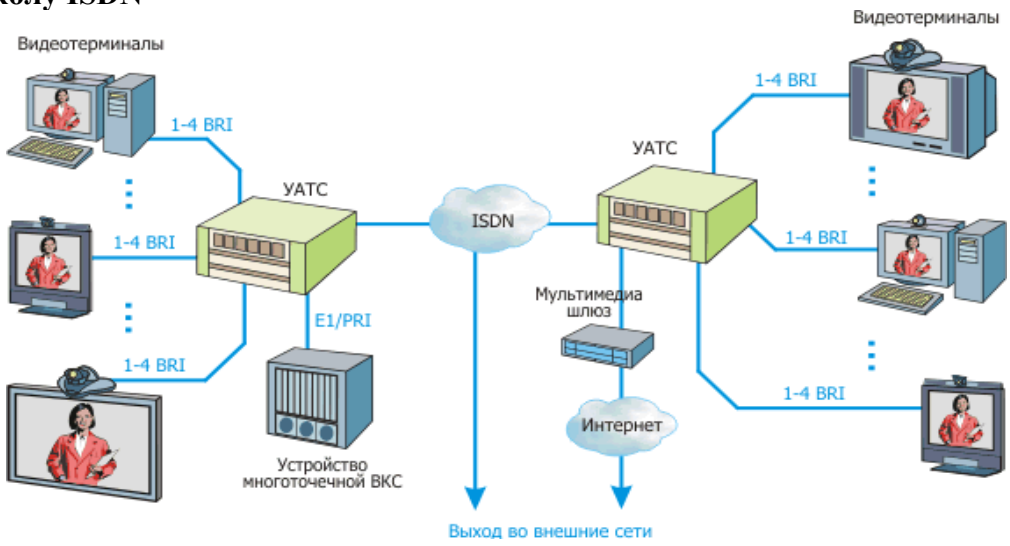
Самый простой и дешевый метод организации видеоконференцсвязи через Интернет. Однако о качестве сеанса связи в данном случае говорить не приходится, так как интернет не является гарантированным каналом передачи аудио- и видео- данных. Плюс к этому добавляется и проблема безопасности видеоконференции, то есть она может стать «общественным достоянием». Для организации видеоконференцсвязи через Интернет требуется иметь статические IP-адреса и каналы связи с пропускной способностью не менее 512 кБит/с в обе стороны (для исходящего и входящего трафика).

Для проведения сеанса ВКС потребуется задать в оборудовании следующие параметры:

- статический IP-адрес вашей системы ВКС;
- шлюз сети провайдера;
- маску подсети;
- статический IP-адрес системы ВКС, с которой осуществляется соединение.

Немного сложнее настраивается связь по протоколу инкапсуляции видовой маршрутизации GRE (англ. *Generic Routing Encapsulation*). Протокол принадлежит к сетевому уровню. Он может инкапсулировать другие протоколы, а затем осуществлять маршрутизацию всего набора до места назначения. В данном случае обеспечивается минимальная защита видеотрафика в сети интернет, что позволяет предотвратить основное число «неопытных» вторжений в информационное облако видеоконференцсвязи. Тот же принцип заложен и в протоколе IPsec.

По протоколу ISDN



Аббревиатура ISDN (англ. *Integrated Services Digital Network*) расшифровывается как цифровая сеть с интеграцией услуг. Цифровые сети с интегральными услугами относятся к сетям, в которых основным режимом связи является режим коммутации каналов, а данные обрабатываются в цифровой форме. Данная услуга не очень распространена в России. Один из самых крупных проектов развития сети является сеть делового обслуживания «Искра-2», которая основывается на существующей аналоговой телефонной сети общего пользования.

Необходимо отметить, что ISDN имеет ряд преимуществ по сравнению с традиционными аналоговыми сетями, но вот по сравнению с новыми телекоммуникационными технологиями передачи данных имеет ряд критичных недостатков:

- тяжело отследить, на каком участке произошел сбой связи;
- низкая оперативность восстановления каналов связи;
- небольшая распространенность на территории РФ;
- всего несколько операторов связи поддерживают данную технологию;
- сравнительно высокая стоимость применения услуги связи при межрегиональном соединении.

Видеоконференция (англ. *videoconference*) — это область информационной технологии, обеспечивающая одновременно двухстороннюю передачу, обработку, преобразование и представление интерактивной информации на расстояние в реальном режиме времени с помощью аппаратно-программных средств вычислительной техники.

Взаимодействие в режиме видеоконференций также называют сеансом видеоконференцсвязи.

Видеоконференцсвязь (сокращенное название ВКС) — это телекоммуникационная технология интерактивного взаимодействия двух и более удаленных абонентов, при которой между ними возможен обмен аудио- и видеоинформацией в реальном масштабе времени с учетом передачи управляющих данных.

Зачем нужна видеосвязь?

В соответствии с исследованиями психологов, в процессе телефонного разговора в среднем воспринимается около 20% информации, в ходе личного общения - 80%, а в ходе сеанса видеосвязи - 60%. То есть если к общению собеседников по звуковому (аудиальному)

каналу добавляется визуальный невербальный язык (жесты, мимика и т.п), то у собеседников повышается эффективность восприятия информации.

Как видно по своим психофизиологическим параметрам видеосвязь достаточно близка к личному общению и намного превосходит возможности телефонной связи. Однако для того, чтобы обеспечить эффективное применение видеосвязи в бизнесе, мало только видеть и слышать одного собеседника. Необходима возможность организации конференций с несколькими участниками, возможность обмена дополнительной информацией (презентации, документы, изображения с дополнительных видеокамер и др.). Режим работы, обеспечивающий все это, называется видеоконференция, а сама технология одновременной передачи видео, голоса и данных — видеоконференцсвязь.

Где используют видеосвязь и видеоконференции?

Технология видеосвязи сегодня во всем мире позиционируется в первую очередь как эффективное средство для оптимизации бизнес-процессов, в том числе для сокращения числа деловых командировок, экономии на представительских, транспортных и накладных расходах.

В настоящее время видеоконференцсвязь уже не такая дорогая технология как несколько лет тому назад и позволить ее себе могут не только большие, но и довольно ограниченные в средствах компании. В отечественных условиях, применение видеосвязи и видеоконференций оптимально в следующих случаях:

- Там, где стоимость рабочего времени руководства (а для него в первую очередь и внедряются эти системы) настолько высока, что тратить время и силы на переезды является непозволительной роскошью для эффективного управления компанией.

Как показывают западные исследования, за свою жизнь среднестатистический менеджер проводит 3 года в самолете, 2 года в дороге в аэропорт и из него, 23 месяца в ожидании своего рейса, 11 месяцев в ожидании пересадки с рейса на рейс и 3 месяца в поиске места для парковки.

- Там, где нужно добиться высокой обучаемости, быстрого усвоения материала и где требуется передать эмоции докладчика.

Зарубежные исследования показывают:	***Отечественные специалисты идут дальше:***
• *«…обучаемость на 200% выше…»* • *«…материал усваивается на 40% быстрее…»* • *«...материал усваивается на 38% лучше...»* • *«...убедительность докладчика на 43% выше…»* • *«…55% влияния от процесса коммуникаций обеспечивает мимика и 38% голос…»*	*7 «Лучше 1 раз увидеть, чем 100 раз услышать».* *8 «…при телефонном разговоре можно передать только десятую часть транслируемой информации…»* *9 «..невербальные формы общения – мимика и жесты – несут до 80 % информации…»*

1. Там, где существует объективная необходимость быстрого принятия решений: зачастую для принятия решения недостаточно иметь только «сухие цифры» или переговорить по телефону, нужно посмотреть своему собеседнику в глаза.
2. При объективной необходимости одновременного личного присутствия в нескольких местах одновременно. Если нужно немедленно собрать в одном (пусть и виртуальном)

совещании многочисленных и крайне занятых руководителей и экспертов различного уровня, причем зачастую расположенных в различных географических точках.

Кратко суммировать вышеизложенное можно так: «Видеоконференция позволяет экономить время и необходима там, где реальная стоимость этого времени по разным причинам высока».

Основную роль в видеоконференции играют каналы связи между абонентами. Рассмотрим несколько методов организации каналов связи для видеоконференций.

Методы организации каналов связи

В сети Интернет

Самый простой и дешевый метод организации видеоконференцсвязи через Интернет. Однако о качестве сеанса связи в данном случае говорить не приходится, так как интернет не является гарантированным каналом передачи аудио- и видео- данных. Плюс к этому добавляется и проблема безопасности видеоконференции, то есть она может стать «общественным достоянием». Для организации видеоконференцсвязи через Интернет требуется иметь статические IP-адреса и каналы связи с пропускной способностью не менее 512 кБит/с в обе стороны (для исходящего и входящего трафика).

Для проведения сеанса ВКС потребуется задать в оборудовании следующие параметры:

- статический IP-адрес вашей системы ВКС;
- шлюз сети провайдера;
- маску подсети;
- статический IP-адрес системы ВКС, с которой осуществляется соединение.

Немного сложнее настраивается связь по протоколу инкапсуляции видовой маршрутизации GRE (англ. *Generic Routing Encapsulation*). Протокол принадлежит к сетевому уровню. Он может инкапсулировать другие протоколы, а затем осуществлять маршрутизацию всего набора до места назначения. В данном случае обеспечивается минимальная защита видеотрафика в сети интернет, что позволяет предотвратить основное число «неопытных» вторжений в информационное облако видеоконференцсвязи. Тот же принцип заложен и в протоколе IPsec.

По протоколу ISDN

Аббревиатура ISDN (англ. *Integrated Services Digital Network*) расшифровывается как цифровая сеть с интеграцией услуг. Цифровые сети с интегральными услугами относятся к сетям, в которых основным режимом связи является режим коммутации каналов, а данные обрабатываются в цифровой форме. Данная услуга не очень распространена в России. Один из самых крупных проектов развития сети является сеть делового обслуживания «Искра-2», которая основывается на существующей аналоговой телефонной сети общего пользования.

Необходимо отметить, что ISDN имеет ряд преимуществ по сравнению с традиционными аналоговыми сетями, но вот по сравнению с новыми телекоммуникационными технологиями передачи данных имеет ряд критичных недостатков:

- тяжело отследить, на каком участке произошел сбой связи;
- низкая оперативность восстановления каналов связи;
- небольшая распространенность на территории РФ;
- всего несколько операторов связи поддерживают данную технологию;

- сравнительно высокая стоимость применения услуги связи при межрегиональном соединении.

По технологии IP VPN MPLS

Услуга связи по технологии IP VPN MPLS сегодня является одной из самых надежных и дешевых для организации видеоконференций через Интернет. Этому способствует:

- VPN (англ. *Virtual Private Network*) — виртуальная частная сеть, то есть обобщённое название технологий, позволяющих обеспечить одно или несколько сетевых соединений (логическую сеть) поверх другой сети.
- MPLS (англ. *Multiprotocol Label Switching*) — мультипротокольная коммутация по меткам, то есть механизм передачи данных, который эмулирует различные свойства сетей с коммутацией каналов поверх сетей с коммутацией пакетов.

Технология IP VPN MPLS по степени защищенности используемой среды относится к доверительной зоне. Она используется в случаях, когда передающую среду можно считать надёжной и необходимо решить лишь задачу создания виртуальной подсети в рамках большей сети.

Так как нас в большей степени интересует построение ВКС на основе технологии VPN, то рассмотрим ее более подробно.

Виртуальные частные сети

В случаях построения территориально распределенных систем IP-видеонаблюдения или вынужденного использовании небезопасных участков телекоммуникационных сетей операторов связи (таких, где нет возможности реализовать меры защиты) необходимо использовать оборудование с поддержкой шифрования передаваемых по сети данных. А именно оборудование с поддержкой технологии виртуальных частных сетей (VPN).

VPN (Virtual Private Network) – зашифрованный или инкапсулированный процесс коммуникации, который безопасным образом передает данные из одной точки в другую; безопасность этих данных обеспечена устойчивой технологией шифрования, и передаваемые данные проходят через открытую, незащищенную, маршрутизируемую сеть.

Цель VPN-технологий состоит в максимальной степени обособления потоков данных одного предприятия от потоков данных всех других пользователей публичной сети. Обособленность должна быть обеспечена в отношении параметров пропускной способности потоков и в конфиденциальности передаваемых данных. Таким образом, основными задачами технологий VPN являются обеспечение в публичной сети гарантированного качества обслуживания для потоков пользовательских данных, а также защита их от возможного несанкционированного доступа (НСД) или разрушения.

VPN-технологии обеспечивают:

- защиту (конфиденциальность, подлинность и целостность) передаваемой по сетям информации;
- защиту внутренних сегментов сети от НСД со стороны сетей общего пользования;
- контроль доступа в защищаемый периметр сети;
- сокрытие внутренней структуры защищаемых сегментов сети;
- идентификацию и аутентификацию пользователей сетевых объектов;
- централизованное управление политикой корпоративной сетевой безопасности и настройками VPN-сети;

- криптографическую защиту данных, передаваемых по каналам связи сетей общего пользования между защищаемыми сегментами сети;
- безопасный доступ пользователей VPN к ресурсам сетей общего пользования.

Интерес пользователей к данной технологии обусловлен следующими факторами:

1. низкой стоимостью эксплуатации за счет использования сетей общего пользования вместо собственных или арендуемых линий связи;
2. практически не ограниченной масштабируемостью;
3. простотой изменения конфигурации и наращивания корпоративной сети (КС);
4. «прозрачностью» для пользователей и приложений.

Компания Check Point предлагает выделить четыре основных вида VPN:

- Интрасеть (Intranet VPN);
- VPN клиент/сервер (Client/server VPN);
- Экстрасеть (Extranet VPN);
- Удаленный доступ (Remote Access VPN).

Интрасеть VPN позволяет объединить в единую защищенную сеть несколько распределенных филиалов одной организации, взаимодействующих по открытым каналам связи.

VPN клиент/сервер обеспечивает защиту передаваемых данных между двумя узлами (не сетями) КС. Особенность данного варианта в том, что VPN строится между узлами, находящимися, как правило, в одном сегменте сети, например, между рабочей станцией и сервером.

Экстрасеть строится в том случае, если к КС подключаются так называемые пользователи «со стороны», уровень доверия к которым намного ниже, чем к своим сотрудникам.

Виртуальная частная сеть с удаленным доступом позволяет мобильным пользователям получать доступ к КС своей компании. Данный вариант отличается тем, что удаленный пользователь, как правило, не имеет статического адреса.

Туннелирование в виртуальных частных сетях.

VPN состоит из каналов глобальной сети, защищенных протоколов и маршрутизаторов. Для объединения удаленных локальных вычислительных сетей (ЛВС) в VPN используются так называемые виртуальные выделенные каналы. Для организации подобных соединений применяется механизм туннелирования, или инкапсуляции.

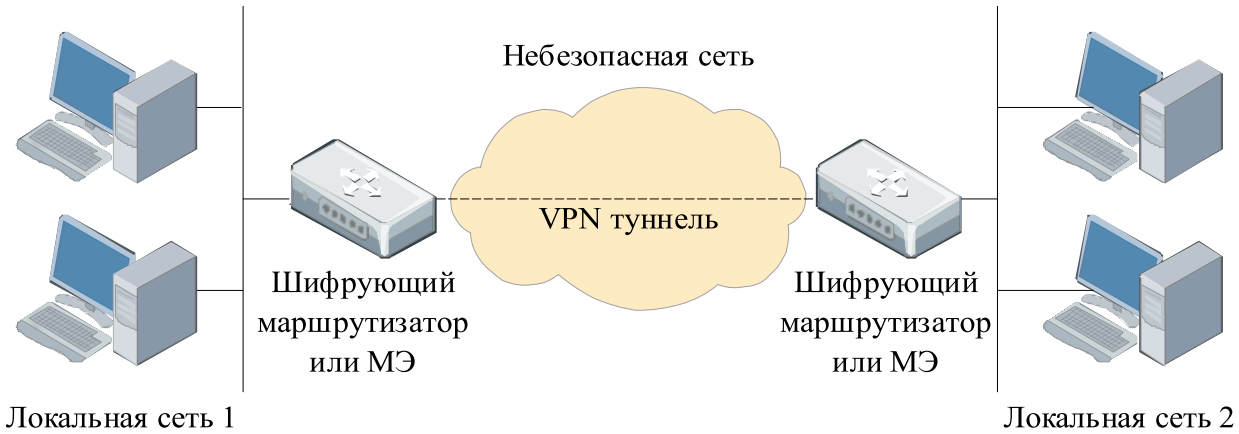


Рис. 2.1. Структура VPN

При туннелировании пакет протокола более низкого уровня помещается в поле данных пакета протокола более высокого или такого же уровня. Например, при туннелировании кадр Ethernet может быть размещен в пакете IP, а пакет IPX — в пакете IP. Возможен и такой вариант: пакет IP размещается в пакете IP.

Туннель создается двумя пограничными устройствами, которые размещаются в точках входа в публичную сеть. Инициатор туннеля инкапсулирует пакеты ЛВС (в том числе пакеты немаршрутизируемых протоколов) в IP-пакеты, содержащие в заголовке адреса инициатора и терминатора туннеля. Терминатор туннеля извлекает исходный пакет. Естественно, при подобной передаче требуется решать проблему конфиденциальности и целостности данных, что не обеспечивается простым туннелированием. Конфиденциальность передаваемой корпоративной информации достигается шифрованием (алгоритм одинаков на обоих концах туннеля).

Особенностью туннелирования является то, что эта технология позволяет зашифровать исходный пакет целиком, вместе с заголовком, а не только его поле данных. Исходный пакет зашифровывают полностью, вместе с заголовком, и этот зашифрованный пакет помещают в другой, внешний пакет с открытым заголовком. Для транспортировки данных по «опасной» сети используются открытые поля заголовка внешнего пакета, а при прибытии внешнего пакета в конечную точку защищенного канала из него извлекают внутренний пакет, расшифровывают и используют его заголовок для дальнейшей передачи уже в открытом виде по сети, не требующей защиты. При этом для внешних пакетов используются адреса пограничных маршрутизаторов, установленных в этих двух точках, а внутренние адреса конечных узлов содержатся во внутренних пакетах в защищенном виде

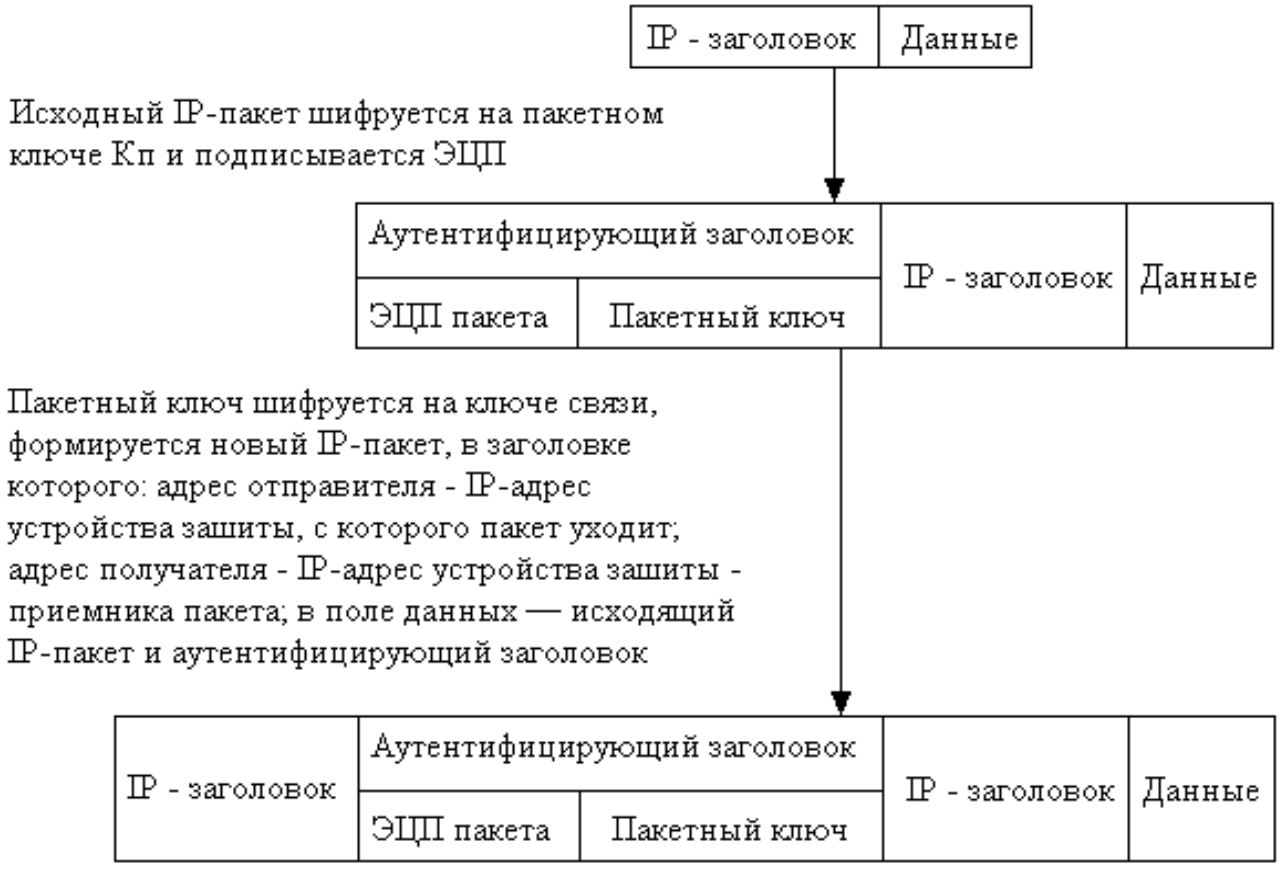


Рис. 2.2. Туннелирование пакетов

VPN-агенты, т.е. средства, реализующие VPN, автоматически шифруют всю исходящую информацию (и соответственно расшифровывают всю входящую). Они также следят за ее целостностью с помощью электронной цифровой подписи (ЭЦП) или имитовставок (криптографическая контрольная сумма, рассчитанная с использованием ключа

шифрования). Поскольку информация, циркулирующая в Internet, представляет собой множество пакетов протокола IP, VPN-агенты работают именно с ними.

Перед отправкой IP-пакета VPN-агент действует следующим образом.

- Из нескольких поддерживаемых им алгоритмов шифрования и ЭЦП по IP-адресу получателя выбирает нужный для защиты данного пакета, а также ключи. Если же в его настройках такого получателя нет, то информация не отправляется. Генерирует и добавляет в пакет ЭЦП отправителя или имитовставку.
- Шифрует пакет (целиком, включая заголовок).
- Проводит инкапсуляцию, т.е. формирует новый заголовок, где указывается адрес вовсе не получателя, а его VPN-агента. Эта полезная дополнительная функция позволяет представить обмен между двумя сетями как обмен между двумя компьютерами, на которых установлены VPN-агенты. Всякая полезная для злоумышленника информация, например, внутренние IP-адреса, ему уже недоступна.

При получении IP-пакета выполняются обратные действия.

- Заголовок содержит сведения о VPN-агенте отправителя. Если таковой не входит в список разрешенных в настройках, то информация просто отбрасывается. То же самое происходит при приеме пакета с намеренно или случайно поврежденным заголовком.
- Согласно настройкам выбираются алгоритмы шифрования и ЭЦП, а также необходимые криптографические ключи.
- Пакет расшифровывается, затем проверяется его целостность. Если ЭЦП неверна, то он отбрасывается.
- Пакет в его исходном виде отправляется настоящему адресату по внутренней сети.

Все операции выполняются автоматически. Сложной в технологии VPN является только настройка VPN-агентов.

VPN-агент может находиться непосредственно на защищаемом ПК, что полезно для мобильных пользователей, подключающихся к Internet из разных мест. В этом случае он обезопасит обмен данными только того компьютера, на котором установлен.

Возможно совмещение VPN-агента с маршрутизатором (в этом случае его называют криптографическим) IP-пакетов. Ведущие мировые производители в последнее время выпускают маршрутизаторы со встроенной поддержкой VPN, например Express VPN от Intel, который шифрует все проходящие пакеты по алгоритму Triple DES.

Как видно из описания, VPN-агенты создают каналы между защищаемыми сетями, которые обычно называют туннелями. Они «прорыты» от одной сети к другой; циркулирующая внутри информация спрятана от чужих глаз.

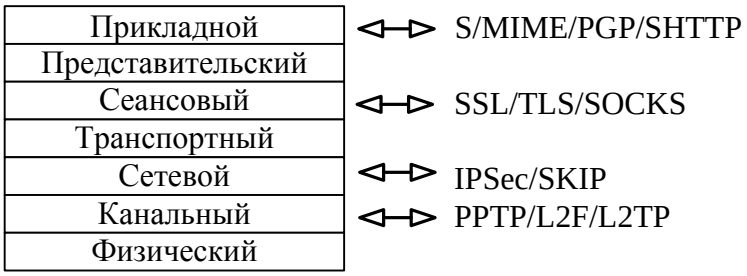
Кроме того, все пакеты фильтруются в соответствии с настройками. Таким образом, все действия VPN-агентов можно свести к двум механизмам: созданию туннелей и фильтрации проходящих пакетов.

Совокупность правил создания туннелей, которая называется «политикой безопасности», записывается в настройках VPN-агентов. IP-пакеты направляются в тот или иной туннель или отбрасываются после того, как будут проверены:

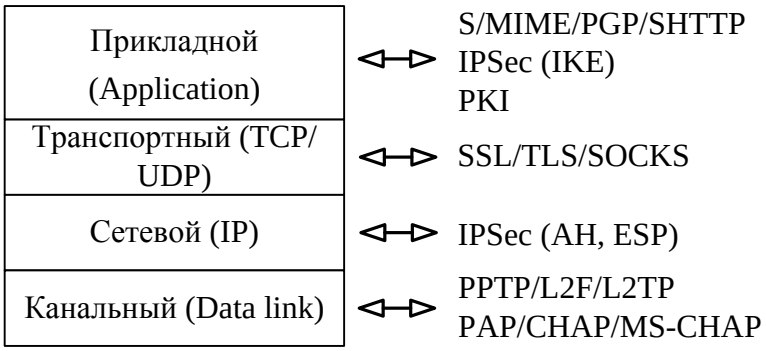
- IP-адрес источника (для исходящего пакета — адрес конкретного компьютера защищаемой сети);
- IP-адрес назначения;
- протокол более высокого уровня, которому принадлежит данный пакет (например, TCP или UDP);
- номер порта, с которого или на который отправлена информация (например, 1080).

Уровни защищенных каналов.

Важной характеристикой стандартов защищенного канала является уровень модели взаимодействия открытых систем OSI, на котором работают протоколы данного стандарта.



а)



б)

Рис. 2.3. Уровни защищенных каналов

Чем ниже по стеку расположены средства защищенного канала, тем проще их сделать прозрачными для приложений и прикладных протоколов. Хотя протоколы защиты данных могут работать практически на любом уровне стека протоколов, обычно к средствам VPN относят только те протоколы, которые полностью прозрачны для приложений и сетевых служб. Поэтому к средствам VPN, как правило, относят протоколы трех уровней: канального, сетевого и транспортного, и эти уровни называют соответственно VPN-уровнями. Такие же средства, как протоколы SSL, TLS или SOCKS, прозрачностью не обладают. По этой причине некоторые специалисты не относят их (и другие непрозрачные протоколы) к средствам VPN.

К протоколам построения VPN канального уровня относятся:

- протокол PPTP (Point-to-Point Tunneling Protocol), разработанный Microsoft совместно с компаниями Ascend Communications, 3Com/Primary Access, Ecl-Telematics и US Robotics,
- протокол L2F (Layer-2 Forwarding) компании Cisco Systems,
- протокол L2TP (Layer-2 Tunneling Protocol), объединивший оба вышеназванных протокола.

Однако эти протоколы, в отличие от IPSec, нельзя назвать полнофункциональными (например, PPTP не определяет метод шифрования).

Протоколы PPTP, L2F и L2TP объединяет то, что они представляют собой протоколы туннелирования канального уровня, которые инкапсулируют кадры канального протокола в протокол сетевого уровня. С помощью последнего данные затем передаются по составной сети. Кроме того, эти протоколы близки также и тем, что их главная область применения — решение задачи защищенного многопротокольного удаленного доступа к ресурсам КС через публичную сеть, в первую очередь через Internet. Так как практически любое клиентское ПО использует сегодня для удаленного доступа стандартный протокол канального уровня PPP, то

и протоколы PPTP, L2F и L2TP основаны на инкапсуляции кадров PPP в пакеты сетевого уровня. В таком качестве используется прежде всего IP, но возможно применение и других сетевых протоколов, таких как IPX или DECnet.

Хотя все три протокола часто относят к протоколам образования защищенного канала, строго говоря, этому определению соответствует только PPTP, обеспечивающий как туннелирование, так и шифрование данных. Протоколы L2F и L2TP являются только протоколами туннелирования, а функции защиты данных (шифрование, аутентификация, целостность) в них не поддерживаются. Предполагается, что при их применении защита туннелируемых данных будет выполняться с помощью некоторого третьего протокола, например, IPSec.

Возможность построения VPN на оборудовании и ПО различных производителей достигается внедрением некоторого стандартного механизма. Таким механизмом выступает протокол Internet Protocol Security (IPSec). Он описывает все стандартные методы VPN и определяет методы идентификации при инициализации туннеля, методы шифрования в конечных точках туннеля и механизмы обмена и управления ключами шифрования между этими точками. Правда, этот протокол ориентирован исключительно на IP-протокол.

IPSec – это система открытых стандартов, которая имеет на сегодня четко очерченное ядро и в то же время позволяет достаточно просто дополнять ее новыми протоколами, алгоритмами и функциями. Этому способствует ее открытое построение, включающее все новые достижения в области криптографии. Осенью 1998 г. были приняты пересмотренные спецификации RFC на все основные компоненты IPSec, а совместная работа этих компонентов описана в стандарте RFC 2401 «Security Architecture for the Internet Protocol». По сравнению с первыми версиями стандартов IPSec, принятых в 1996 г., пересмотренные в 1998 г. спецификации стали более конкретными. Например, применение IKE (Internet Key Exchange, протокол обмена ключами Internet) снимает большую степень неопределенности при управлении ключами, отличавшую первую версию стандартов IPSec.

IPSec решает следующие основные задачи установления и поддержания защищенного соединения:

- аутентификацию пользователей или компьютеров при инициации защищенного соединения;
- шифрование и аутентификацию передаваемых данных между конечными точками соединения;
- автоматическое снабжение конечных точек секретными ключами, необходимыми для работы протоколов аутентификации и шифрования данных.

Для решения поставленных задач система IPSec использует протоколы трех типов:

1. протокол обмена ключами Internet IKE (Internet Key Exchange), предназначенный для первоначального этапа установки соединения и определяющий способ инициализации защищенного канала, а также процедуры обмена и управления секретными ключами в рамках защищенного соединения, методы шифрования и др.;
2. протокол AH (Authentication Header), который обеспечивает целостность и аутентификацию источника данных в передаваемых пакетах, а также опционально — защиту от ложного воспроизведения пакетов (в заголовке AH данные пакета не шифруются);
3. протокол ESP (Encapsulation Security Payload), обеспечивающий шифрование, аутентификацию и целостность передаваемых данных, и опционально — защиту от ложного воспроизведения пакетов (данные и заголовок шифруются в соответствии с этим протоколом).

Для шифрования данных в IPSec может быть применен любой симметричный алгоритм шифрования, использующий секретные ключи. Проверка целостности и аутентификация данных выполняются с помощью вычисления хэш-кода данных.

Наиболее известным протоколом защищенного канала, работающим на сеансовом уровне модели OSI, является протокол Secure Socket Layer (SSL), разработанный компанией Netscape Communications. В январе 1999 г. на смену версии SSL 3.0 пришел протокол Transport Layer Security (TLS), который является стандартом Internet. TLS базируется на SSL, и различия между SSL 3.0 и TLS 1.0 не слишком существенны (хотя и достаточны для того, чтобы эти протоколы не были совместимыми). Основные свойства протокола SSL, описанные ниже, применимы и к TLS.

Преимуществом SSL является то, что он независим от прикладного протокола. Протоколы приложения, такие как HTTP, FTP, TELNET и т.д., могут работать поверх протокола SSL совершенно прозрачно. Протокол SSL может согласовывать алгоритм шифрования и сеансовый ключ, а также аутентифицировать сервер до того, как приложение примет или передаст первый байт данных. Все протокольные прикладные данные передаются зашифрованными с гарантией конфиденциальности.

Несмотря на то, что протокол SSL может использоваться для создания защищенного канала между любыми приложениями, наиболее широко он используется протоколом HTTP (режим HTTPS).

Целью протокола TLS (Transport Layer Security) является обеспечение конфиденциальности и целостности данных при связи двух приложений.

TLS состоит из двух основных протоколов:

- TLS Handshake Protocol (протокол установления соединения, или протокол диалога) — выполняет двустороннюю аутентификацию и обмен ключевой информацией; предназначен для создания защищенной сессии;
- TLS Record Protocol (протокол записи) — обеспечивает шифрование и контроль целостности передаваемых данных.

На нижнем уровне, работающем поверх транспортного протокола (например, TCP), размещается протокол записей TLS. Этот протокол обеспечивает безопасность соединений, которые имеют два основных свойства.

Соединение является конфиденциальным. Для шифрования данных используется симметричная криптография (например, DES, RC4 и т.д.). Ключи для шифрования генерируются независимо для каждого соединения и базируются на секретном коде, получаемом с помощью другого протокола (такого, как протокол диалога TLS). Протокол записей может использоваться и без шифрования.

Соединение является надежным. Процедура передачи сообщения включает в себя проверку целостности с помощью вычисления MAC. Для расчета MAC используются хэш-функции (например, SHA, MD5 и т.д.). Протокол записей может работать и без MAC, но в этом режиме он применяется только в случае, когда другой протокол использует протокол записей в качестве транспортного при выяснении параметров безопасности.

Протокол SOCKS разработан в 1990 г. Дэвидом Кобласом для организации посредничества при взаимодействии между клиент-серверными приложениями на сеансовом уровне модели OSI. Изначально данный протокол разрабатывался только для перенаправления запросов к серверам со стороны клиентских приложений, а также возврата этим приложениям полученных ответов. Однако даже лишь перенаправление запросов и ответов между клиент-серверными приложениями уже позволяет реализовать функцию трансляции сетевых IP-адресов (Network Address Translation — NAT). При замене для исходящих пакетов внутренних IP-адресов отправителей одним IP-адресом шлюза топология внутренней сети скрыта от внешних пользователей, что усложняет НСД. Трансляция сетевых адресов, помимо повышения безопасности, позволяет расширить внутреннее адресное пространство сети за счет возможности поддержки собственной системы адресации, не согласованной с адресацией во внешней сети.

VPN и МЭ благодаря протоколу SOCKS могут организовать безопасное взаимодействие и обмен информацией между разными сетями. Кроме того, SOCKS позволяет реализовать безопасное управление этими системами на основе унифицированной стратегии. Следует отметить, что если на основе протоколов канального и сетевого уровня защищенные виртуальные каналы формируются между разными парами взаимодействующих сторон, то на основе протокола SOCKS могут создаваться защищенные туннели для каждого приложения и сеанса в отдельности.

Виды решений

Сегодня на рынке сосуществуют две технологии обеспечивающие возможность видеосвязи и проведения видеоконференций - программные и аппаратные. И у тех и у других свои достоинства и недостатки.

Программные решения для видеосвязи и видеоконференций

Программные решения для видеосвязи и видеоконференций требуют для своей работы персонального компьютера с подключенной к нему вебкамерой и гарнитурой. Эти программы бывают бесплатные (Skype и др.) и платные. Их основные достоинства:

- минимальные первоначальные вложения (камера+гарнитура);
- возможность проведения видеоконференций с несколькими участниками (поддерживают не все программы);
- низкая цена (или бесплатность).

Основные недостатки программных решений для видеосвязи:

- низкое качество видеоизображения (низкое разрешение и низкая частота кадров);
- резкое ухудшение качества если используется режим видеоконференция;
- очень высокая загрузка ПК, делающая не комфортной параллельную работу за ПК.

Аппаратные решения для видеосвязи и видеоконференций

Аппаратные решения для общения по видеосвязи и видеоконференций стоят заметно дороже программных, зато они лишены всех их недостатков. Аппаратные решения для видеосвязи обеспечивают телевизионное (включая HD) качество передачи изображения, поддерживают подключение различных внешних источников видеосигнала, обеспечивают стабильную работу и имеют массу других достоинств, речь о которых пойдет ниже.

Рынки программных и аппаратных решений для видеосвязи и видеоконференций имеют разную аудиторию. Программные решения дешевы, но они жестко привязаны к ПК и серьезно отстают по массе показателей, в первую очередь по качеству. Программные решения нельзя использовать для инсталляций в переговорных комнатах и конференц-залах, они не поддерживают автоматическое наведение видеокамеры на голос, не позволяют подключать дополнительные камеры и выводить изображение на несколько дисплеев; они также плохо интегрируются с системами озвучивания (эхо и шумоподавления, АРУ) и управления (например, Crestron) конференц-залов.

Программное решение для видеоконференций не поставишь руководителю высшего звена, низкокачественная видеосвязь - это просто не солидно. В-третьих, любое программное решение привязано к ПК и к операционной системе, что сказывается на надежности и стабильности видеосвязи.

Рынки программных и аппаратных решений для проведения видеоконференций имеют разную аудиторию. Первые годятся пока лишь для первичной, тестовой эксплуатации внутри компании.

В свою очередь аппаратные решения для видеосвязи уже сегодня используют как адекватную замену бизнес командировкам, совещаниям руководителей высшего звена, выездным семинарам, тренингам и многому другому.

Групповая видеосвязь и видеоконференция

Для организации групповых видеоконференций в которых участвуют несколько сторон (групп), в каждой из которых может быть по несколько участников используют - групповые системы видеоконференцсвязи.

Системы групповой видеосвязи обычно устанавливают в отдельных помещениях, например, в переговорных комнатах или конференц-залах. Их непременный атрибут — большой плазменный/ЖК телевизор или проектор для отображения участников видеоконференции.

Основное назначение групповых систем ВКС — обеспечить комфортную видеосвязь или видеоконференцсвязь группы людей с удаленными собеседниками. В общем случае такой системе приходится решать две задачи. Первая заключается в видеосъемке одних участников видеоконференции и передаче их изображения (вместе со звуком от микрофона) другим. Вторая состоит в отображении картинки на одном или нескольких ТВ (мониторах) и выводе звука на динамики телевизора или акустические колонки (через звукоусиливающую аппаратуру). Чтобы все это обеспечить групповые системы ВКС должны обладать большой вычислительной мощностью для обработки голосовой и видеоинформации в режиме реального времени (особенно в случае HD качества видео), и поэтому они представляют собой сложные, с инженерной точки зрения и довольно дорогостоящие продукты.

Групповые системы для видеоконференций можно разделить на системы начального уровня и системы бизнес-класса. Первые предназначены для подключения к минимально необходимому для работы аудио/видеооборудованию и поддерживают в основном соединение «точка-точка» (то есть видеосвязь между двумя участниками или двумя группами участников). Вторые, как правило, более производительны, поддерживают высокоскоростные соединения и способны автоматически наводить камеру на говорящего. С помощью встроенного сервера видеоконференцсвязи они позволяют организовать многопользовательские (многосторонние) видеоконференции и обладают широким набором сетевых интерфейсов и аудио/видеопортов.

Принадлежность оборудования для групповых видеоконференций к тому или иному классу вовсе не означает, что одно обеспечивает общение более высокого качества, нежели другое. Выбор конкретного класса определяется задачами, которые возлагают на систему видеосвязи. Например, если в компании требуется наладить видеосвязь между несколькими отделениями (офисами), но в многосторонних конференциях нет нужды, то использовать системы бизнес-уровня не имеет смысла.

Пример наиболее часто используемой структуры корпоративной сети видеосвязи для малого и среднего бизнеса приведена на рисунке ниже.

Рис 5.1. Схема многопользовательской ВКС

Центральная групповая система ВКС со встроенным MCU располагается в центральном офисе компании. Она обеспечивает проведение видеоконференций. Эта система соединена с другими крупными офисами, где установлены групповые системы ВКС начального уровня, и/или личные персональные терминалы видеосвязи сотрудников. Такая структура корпоративной сети видеосвязи позволяет, с одной стороны, организовывать все виды видеоконференций, а с другой — экономить на групповых терминалах.

В техническом описании любой групповой системы предназначенной для организации видеосвязи и проведения видеоконференций можно встретить длинный перечень поддерживаемых стандартов: видеокодеки, аудиокодеки, стандарты совместной работы с данными, связи и управления. Между тем, большая часть приводимых в описаниях характеристик не имеет практического значения.

Практическая часть

Выбор решений

Одним из важнейших критерием выбора будет являться окрытость исходного кода. Т.к. програмное решение будет внедряться в образовательной среде, то факт открытости исходного кода благотворно скажется на развитии навыков работы с подобными системами, благотворно скажется на процессе доработки под нужды учебного процесса. На данный момент вышеописанным требованиям удовлетворяет только OpenMeetings.

OpenMeetings является бесплатным сервером веб-конференций, где можно организовывать захват экрана любого участникии передать его любому участнику, совместный доступ к документам, чат, разговоры и трансляции через веб-камеру с участниками. Широкая поддержка "комьюнити". Широкая языковая поддержка. Строится на основе браузера.

Система подробно продокументирована.

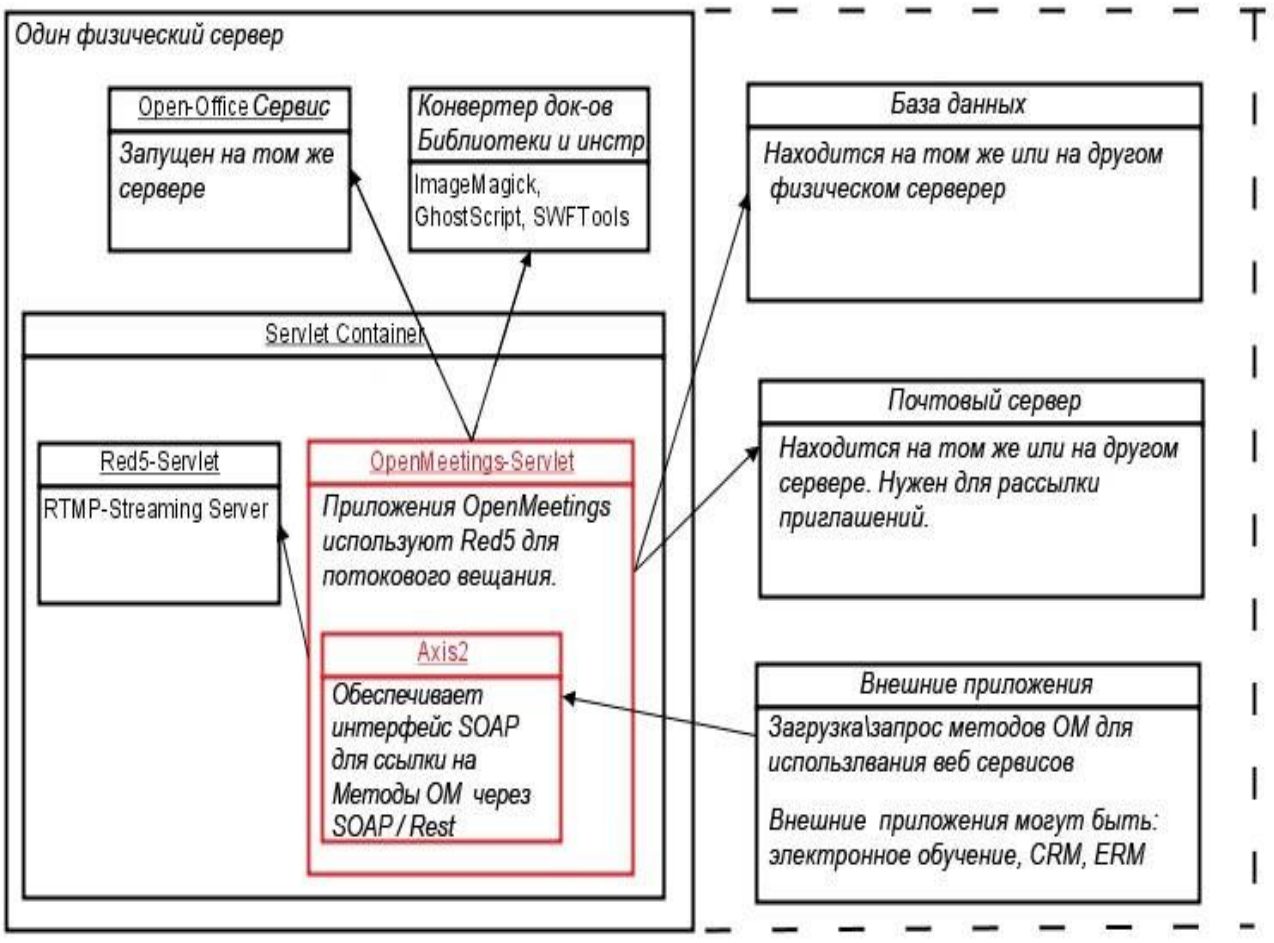
Архитектура OpenMeetings

* Client OpenLaszlo http://www.openlaszlo.org
* Server (Remoting and Streaming) Red5 http://www.osflash.org/red5
* Xuggler http://www.xuggle.com
* Persistent Layer: Hibernate http://www.hibernate.org
* Database: !MySQL or Postgres, or any other with a Hibernate-Dialect (full-list)
* DocumentConverter: OpenOffice http://www.openoffice.org and JOD (http://www.artofsolving.com/opensource/jodconverter),

for help in installing see: OpenOfficeConverter

* ImageConverter: http://www.imagemagick.org

* Axis2, see available/planned Services at SoapMethods



Установка OpenMeetings

http://www.gentoo-wiki.info/OpenMeetingshttp://docs

.google.com/Doc?id=dcbbhg8d_3
4d3xkczg8

Установка сервера видеосовещаний

Данная инструкция содержит перечень необходимых шагов, необходимых для установки сервера видеосовещаний на сервер. Предполагается, что шаги выполняет специалист надлежащей квалификации, то есть системный администратор или специалист по установке сервера видеосовещаний. Предварительные условия Предполагается, что перед началом установки выполнены следующие условия:

- предоставлен сервер с предустановленной ОС Debian GNU/Linux 5.0 (Lenny) (для настроек требуется логин и парольадминистратора);
- в операционной системе создана учётная запись для работы сервера видеосовещаний (предоставлены логин ипароль);
- создана учётная запись и реквизиты SMTP сервера (для рассылки приглашений на конференции);
- предоставлены реквизиты LDAP сервера (например, ActiveDirectory).

Установка дополнительных пакетов Установить следующие пакеты ПО из стандартного дистрибутива и сети Интернет:

- среду исполнения java 6 (sun-java6-jre);
- инструмент преобразования swftools;
- офисный пакет Openoffice.org в следующем составе: openoffice.org3, openoffice.org3-writer, openoffice.org3-calc,openoffice.org3-impress, openoffice.org3-draw, openoffice.org3-ru openoffice.org3-dict-ru, openoffice.org3-math.
- базу данных mysql (пакеты mysql-server-5.0, mysql-client-5.0, php5-mysql, phpmyadmin);
- веб сервер apache (пакеты apache2, apache2-utils, libapache2-mod-php5filter);
- средства удалённого доступа (openssh-server, openssh-blacklist, openssh-blacklist-extra);
- пакеты с вспомогательными утилитами для конфигурирования и мониторинга состояния системы: ferm (упрощеннаянастройка iptables), monit (контроль работоспособности демонов).

Конфигурация сети, настройка сетевого фильтра и удалённого доступа

Подключить сервер к сети, соблюдая следующие требования:

- обеспечить полосу пропускания сети 128 кбит/сек на каждого потенциального участника конференции (например,1,3 Мбит на 10 участников);
- обеспечить время прохождения пакетов (ping) от каждой из точек до сервера менее 80 мс.

Настроить у сервера статический IP-адрес, доступный для всех участников конференции.

- В случае использования сервера видеоконференции в локальной сети IP-адрес сервера может принадлежать только этой сети.
- Для доступа из сети Интернет сервер должен иметь внешний статический адрес, доступный для пользователей сети Интернет.
- входящий 22 tcp – ssh, используется для удалённой настройки сервера. назначение порта может быть изменено.

- прописывание учётной записи (логин, пароль) в установочный файл openmeetings/conf/hibernate.cfg.xml;
- запись цвета, названия и URL организации в openmeetings/config.xml;
- прописывание учётной записи и конфигурации LDAP в openmeetings/conf/om_ldap.cfg.

Схемы подключения сервера Ниже приведены схемы включения в локальную сеть организации сервера видеосовещаний. Существуют две основные схемы подключения:

- Сервер устанавливается в демилитаризованной зоне (DMZ).
- Сервер устанавливается в общей локальной сети.

Для того, чтобы подключаемый сервер был виден из сети Интернет необходимо дополнить конфигурацию роутера. Например, для роутера Cisco 2821 неободимо добавить в кнфигурацию следующие команды

ip nat inside source static tcp <local_ip> 1935 <global_ip> 1935 route-map <filter> extendableip nat inside source static tcp <local_ip> 5080 <global_ip> 5080 route-map <filter> extendableip nat inside source static tcp <local_ip> 8088 <global_ip> 8088 route-map <filter> extendable

В списках доступа надо разрешить соединения на соответствующие порты <global_ip>.

Конфигурация LDAP

Для конфигурации параметров LDAP необходимо иметь некий базовый уровень познаний в этой области, например, ознакомиться с материалами по проекту OpenLDAP: http://www.openldap.org/doc/admin24/intro.html#What is LDAP. Дляпроверки правильности вводимых данных и работоспособности сервера LDAP нужна утилита JXplorer (http://www.jxplorer.org):используя её, можно зайти на сервер LDAP и проверить параметры соединения.

Настройка LDAP в OpenMeetings включает два шага:

- Укажите путь к установочному файлу в закладке Администрирование->Конфигурация администратором OpenMeetings (параметр ldap_config_path). По указанному пути должен лежать файл, пример которого находится вopenmeetings/conf/om_ldap.cfg.
- Установите в установочном файле следующие поля:

ldap_conn_url – сервер:порт LDAP,ldap_admin_dn – distinguished name (DN) пользователя с правами на обращение к серверу LDAP,ldap_passwd – пароль пользователя сервера LDAP,ldap_search_base – в какой ветви осуществлять поиск введенных данных,field_user_principal – с каким полем записи сервера сравнивать введённые данные.

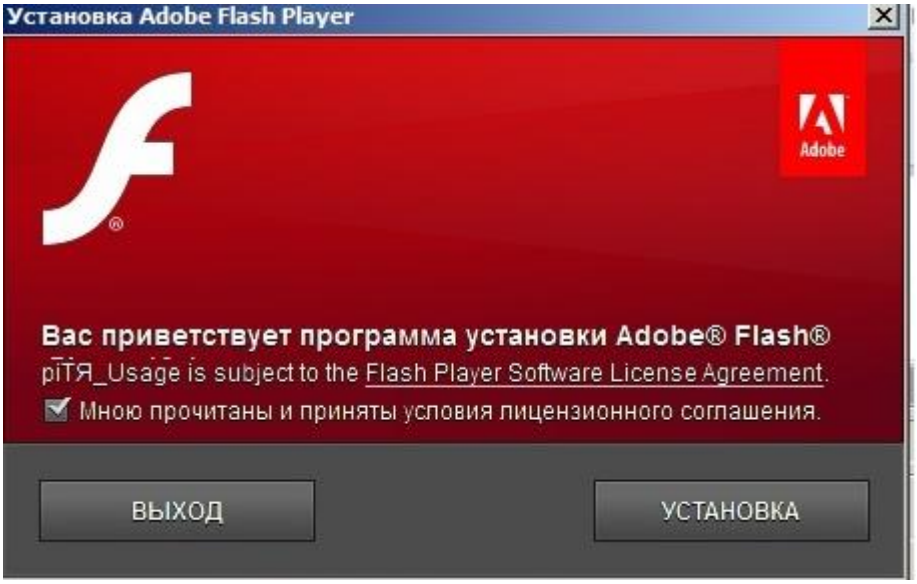
Если файл составлен правильно, и данные верны, то после перезапуска сервера видеосовещаний для авторизации пользователей будет в первую очередь использоваться LDAP, затем локальная таблица пользователей.

ПРИЛОЖЕНИЕ

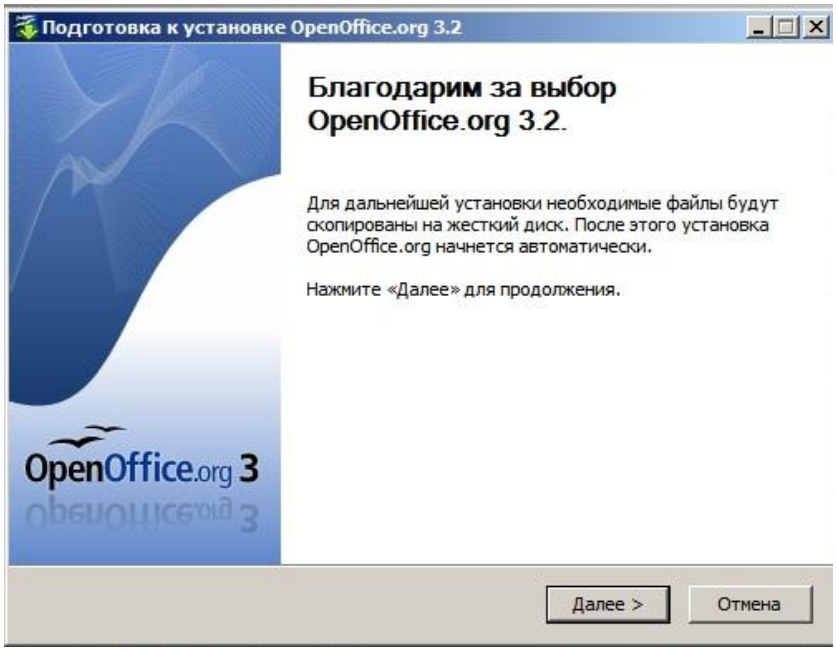
Набор пакетов для развертывания сервера видеоконференции Openmeetings:

ffmpeg.exe
flashplayer10_1_p3_plugin_022310.exe
ImageMagick-6.6.0-0-Q16-windows-dll.exe
OOo_3.2.0_Win32Intel_install_wJRE_ru.exe
openmeetings_1_1_r2905.zip
postgresql-8.4.2-1-windows.exe
sox-14.3.0-win32.zip
swftools-2010-02-06-1900.exe

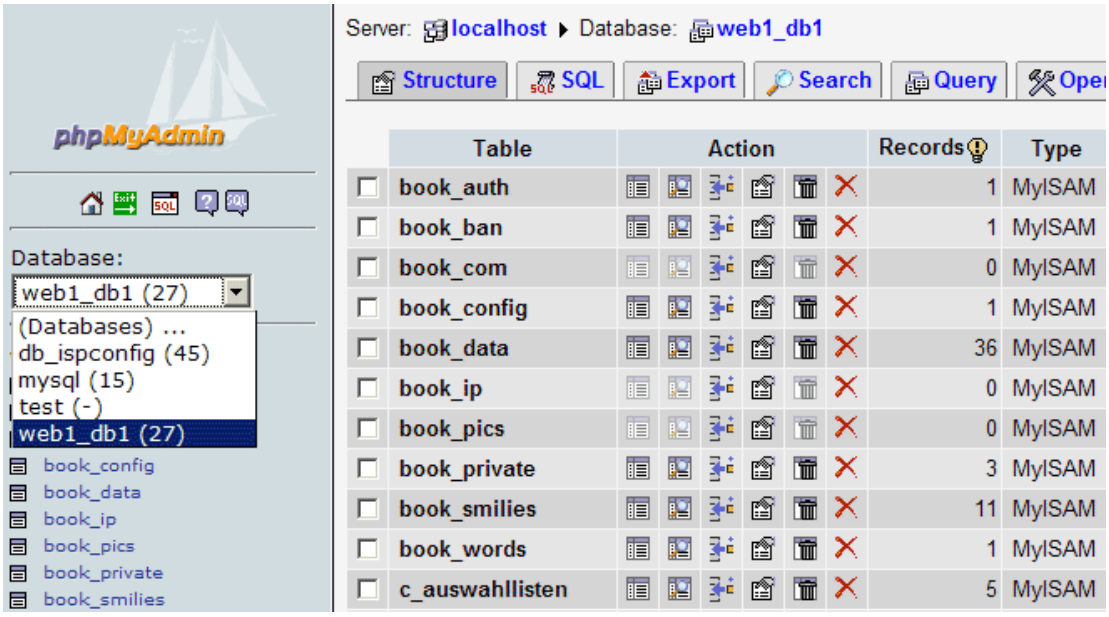
Методика развертывания сервера видеоконференции Openmeetings: Устанавливаем вспомогательные пакеты необходимые для работы Openmeeting:
1. Запустить flashplayer10_1_p3_plugin_022310.exe, нажать установка



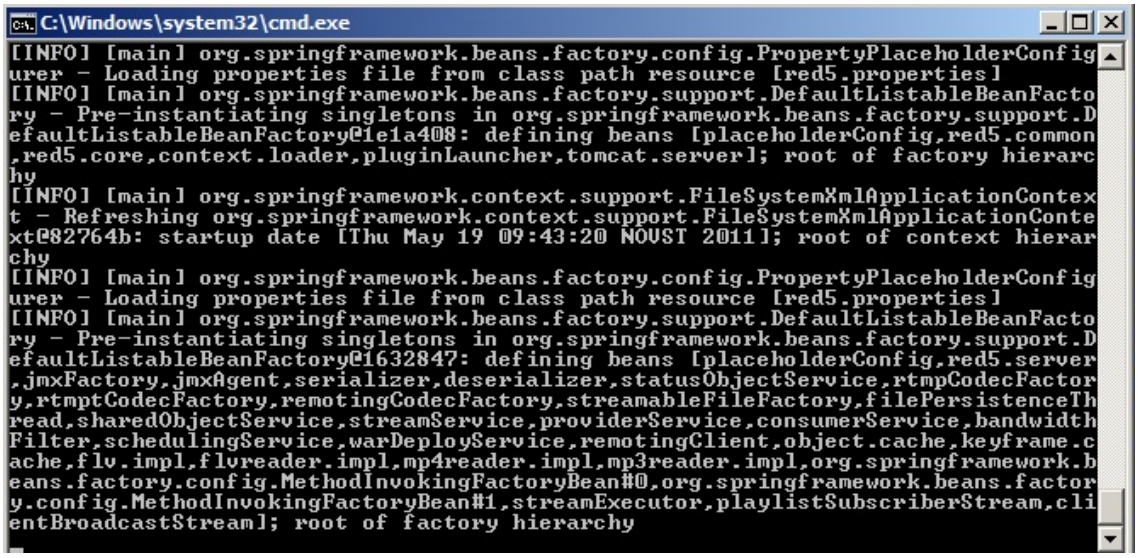
2. Запустить ImageMagick-6.6.0-0-Q16-windows-dll.exe, нажать «Next», «Next», «Next»
3. Запустить установку пакета OOo_3.2.0_Win32Intel_install_wJRE_ru.exe (OpenOffice), выбирайте полную установку. В том числе установится Java JDK 1.6 необходимая для работы openview.



1. Создать папку ffmpeg в например и скопировать туда файл ffmpeg.exe
5. Распаковать sox-14.3.0-win32.zip в например .
6. Установить MySQL и создать базу Openmeetings



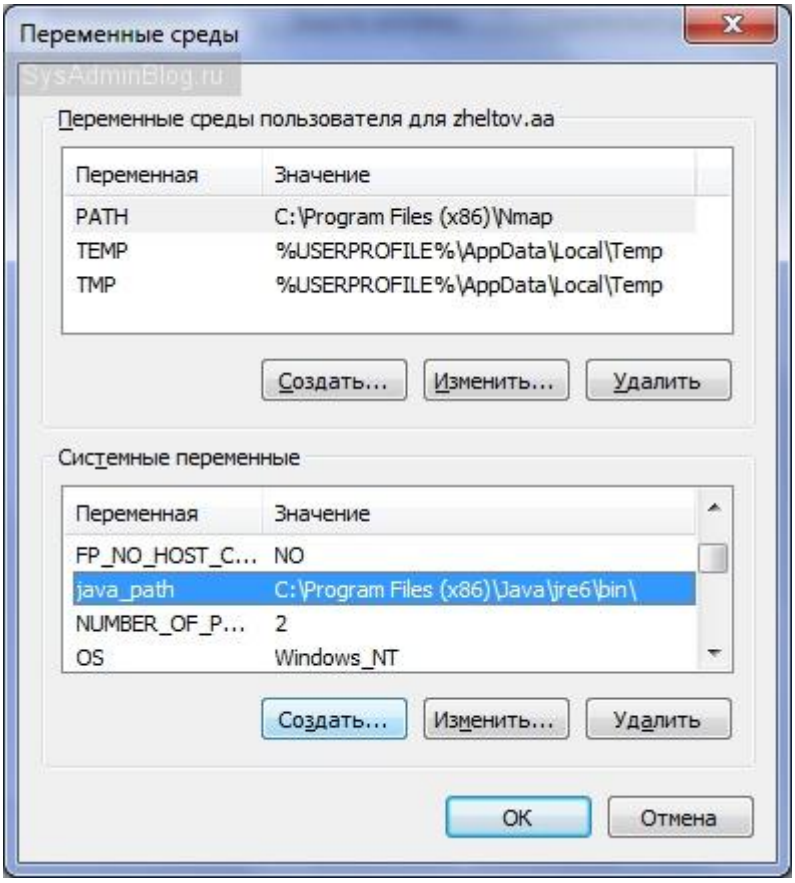
7. Распаковываем openmeetings_1_1_r2905.zip и запускаем red5.bat



8. Копируем \webapps\openmeetings\conf\postgres_hibernate.cfg.xml в \webapps\openmeetings\conf\hibernate.cfg.xml
9. Редактируем файл \webapps\openmeetings\conf\hibernate.cfg.xml, указываем параметры авторизации СУБД

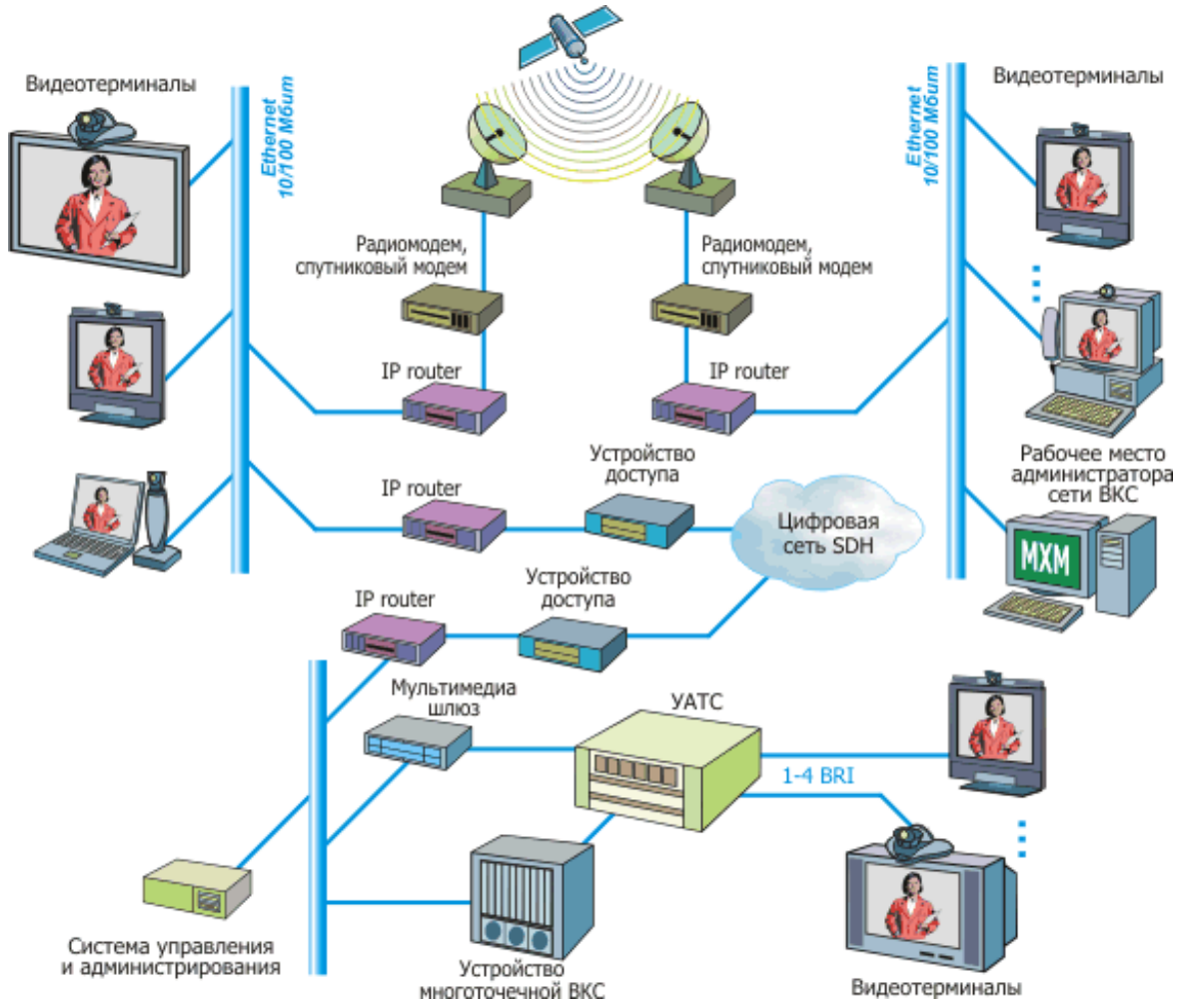
```
<!-- a SessionFactory instance listed as /jndi/name -->
<session-factory>

    <!-- User / Password -->
    <property name="connection.username">root</property>
    <property name="connection.password"></property>

    <!-- Database Settings -->
    <property name="connection.driver_class">com.mysql.jdbc.Driver</property>
    <!-- for performance reasons changed to MyISAM from org.hibernate.dialect.MySQLInnoDBDialect -->
    <property name="dialect">org.openmeetings.app.hibernate.utils.MySQL5MyISAMDialect</property>
    <property name="connection.url">jdbc:mysql://localhost/openmeetings?
autoReconnect=true&amp;useUnicode=true&amp;createDatabaseIfNotExist=true&amp;characterEncoding=utf-8</property>
```

10. Создаем переменную окружение JAVA_PATH с путем до java, в нашем случае «C:\Program Files\Java\jre6»



11. Перегружаем сервер
12. Открываем адрес http://servername:5080/openmeetings/install
13. Указываем свои настройки и пути до установленных пакетов swftools, ffmpeg, ImageMagick, sox и жмем Install
Сервер готов!

По технологии IP VPN MPLS



Услуга связи по технологии IP VPN MPLS сегодня является одной из самых надежных и дешевых для организации видеоконференций через Интернет. Этому способствует:

- VPN (англ. *Virtual Private Network*) — виртуальная частная сеть, то есть обобщённое название технологий, позволяющих обеспечить одно или несколько сетевых соединений (логическую сеть) поверх другой сети.
- MPLS (англ. *Multiprotocol Label Switching*) — мультипротокольная коммутация по меткам, то есть механизм передачи данных, который эмулирует различные свойства сетей с коммутацией каналов поверх сетей с коммутацией пакетов.

Технология IP VPN MPLS по степени защищенности используемой среды относится к доверительной зоне. Она используется в случаях, когда передающую среду можно считать надёжной и необходимо решить лишь задачу создания виртуальной подсети в рамках большей сети.

Протоколы организации видеоконференцсвязи

В 1990 году был одобрен первый международный стандарт в области видеоконференцсвязи - спецификация H.320 для поддержки видеоконференций по ISDN.

Затем ITU одобрил еще целую серию рекомендаций, относящихся к видеоконференцсвязи. Эта серия рекомендаций, часто называемая H.32x, помимо H.320, включает в себя стандарты H.321-H.324, которые предназначены для различных типов сетей.
Во второй половине 90-х годов интенсивное развитие получили IP сети и Интернет. Они превратились в экономичную среду передачи данных и стали практически повсеместными. Однако, в отличие от ISDN, IP сети плохо приспособлены для передачи аудио и видеопотоков. Стремление использовать сложившуюся структуру IP сетей привело к появлению в 1996 году стандарта H.323 (Visual Telephone Systems and Terminal Equipment for Local Area Networks which Provide a Non-Guaranteed Quality of Service, Видеотелефоны и терминальное оборудование для локальных сетей с негарантированным качеством обслуживания). В 1998 году была одобрена вторая версия этого стандарта H.323 v.2 (Packet-based multimedia communication systems, Мультимедийные системы связи для сетей с коммутаций пакетов), в сентябре 1999 года была одобрена третья версия рекомендаций, 17 ноября 2001 года была одобрена четвертая версия стандарта H.323 . Сейчас H.323 - один из важнейших стандартов из этой серии. H.323 - это рекомендации ITU-T для мультимедийных приложений в вычислительных сетях, не обеспечивающих гарантированное качество обслуживания (QoS). Такие сети включают в себя сети пакетной коммутации IP и IPX на базе Ethernet, Fast Ethernet и Token Ring.

Рекомендации H.323 предусматривают:

- Управление полосой пропускания
- Возможность взаимодействия сетей
- Платформенную независимость
- Поддержку многоточечных конференций
- Поддержку многоадресной передачи
- Стандарты для кодеков
- Поддержку групповой адресации

Управление полосой пропускания

Передача аудио- и видеоинформации весьма интенсивно нагружает каналы связи, и, если не следить за ростом этой нагрузки, работоспособность критически важных сетевых сервисов может быть нарушена. Поэтому рекомендации H.323 предусматривают управление полосой пропускания. Можно ограничить как число одновременных соединений, так и суммарную полосу пропускания для всех приложений H.323. Эти ограничения помогают сохранить необходимые ресурсы для работы других сетевых приложений. Каждый терминал H.323 может управлять своей полосой пропускания в конкретной сессии конференции. См. решения VCON для управления полосой пропускания

Межсетевые конференции

Рекомендации H.323 предлагают средство соединения участников видеоконференции в разнородных сетях (например, IP и ISDN, IP и PSTN).

Платформенная независимость

H.323 не привязан ни к каким технологическим решениям, связанным с оборудованием или программным обеспечением. Взаимодействующие между собой приложения могут создаваться на основе разных платформ, с разными операционными системами.

Поддержка многоточечных конференций

Рекомендации H.323 позволяют организовывать конференцию с тремя или более участниками. Многоточечные конференции могут проводиться как с использованием центрального MCU (устройства многоточечной конференции), так и без него.

Поддержка многоадресной передачи

H.323 поддерживает многоадресную передачу в многоточечной конференции, если сеть поддерживает протокол управления групповой адресацией (такой, как IGMP). При многоадресной передаче один пакет информации отравляется всем необходимым адресатам без лишнего дублирования. Многоадресная передача использует полосу пропускания гораздо более эффективно, поскольку всем адресатам - участникам списка рассылки отправляется ровно один поток. См. VCON Interactive Multicast

Стандарты для кодеков

Рекомендация	H.320	H.321	H.322	H.323 V1/V2	H.324
Год принятия	1990	1995	1995	1996/1998	1996
Сеть	Узко-полосная ISDN	Широко-полосная ISDN, ATM LAN	Сеть с коммутацией пакетов и гаранти-рованным качеством обслуживания (isoEthernet)	Сеть с коммутацией пакетов и негаранти-рованным качеством обслуживания (Ethernet)	Аналоговые телефонные сети общего назначения (PSTN или POTS)
Видео	H.261 H.263	H.261 H.263	H.261 H.263	H.261 H.263	H.261 H.263
Аудио	G.711 G.722 G.728	G.711 G.722 G.728	G.711 G.722 G.728	G.711 G.722 G.728 G.723 G.729	G.723
Мультиплекси-рование	H.221	H.221	H.221	H.225.0	H.223
Управление	H.230 H.242	H.242	H.242 H.230	H.245	H.245
Поддержка многоточечных конференций	H.231 H.243	H.231 H.243	H.231 H.243	H.323	-
Обмен данными	T.120	T.120	T.120	T.120	T.120
Сетевой интерфейс	I.400	AAL I.363 AJM I.361 PHY I.400	I.400 & TCP/IP	TCP/IP	V.34 Модем

H323 устанавливает стандарты для кодирования и декодирования аудио- и видеопотоков с целью обеспечения совместимости оборудования разных производителей. Вместе с тем стандарт достаточно гибок. Существуют требования, выполнение которых обязательно, и существуют опциональные возможности, в случае использования которых также

необходимо строго следовать стандарту. Помимо этого, производитель может включать в мультимедийные продукты и приложения дополнительные возможности, если они не противоречат обязательным и опциональным требованиям стандарта.

Совместимость

Участники конференции хотят общаться друг с другом, не заботясь о вопросах совместимости между собой. Рекомендации H323 поддерживают выяснение общих возможностей оборудования конечных пользователей и устанавливают наилучшие из общих для участников конференции протоколов кодирования, вызова и управления.

Гибкость

H323 конференция может включать участников, конечное оборудование которых обладает различными возможностями. Например, один из участников может использовать терминал лишь только с аудио- возможностями, в то время как остальные участники конференции могут обладать возможностями передачи/приема также видео и данных.

Базовая архитектура стандарта H.323

В число "объектов" H.323, как они названы в стандарте, включаются терминалы, мультимедиа шлюзы, устройства управления многоточечными конференциями и контроллеры зоны (Gatekeeper).

Терминал (Terminal) - оконечное мультимедийное (голос, видео, данные) устройство, предназначенное для участия в конференции
Мультимедиа шлюз (Gateway) - устройство, предназначенное для преобразования мультимедийной и управляющей информации при сопряжении разнородных сетей.
Устройство управления многоточечными конференциями (Multipoint Control Unit - MCU) - предназначено для организации конференций с участием трех и более участников
Контроллер зоны (Gatekeeper, Привратник, Конференц-менеджер) - рекомендуемое, но не обязательное устройство, обеспечивающее сетевое управление и исполняющее роль виртуальной телефонной станции.

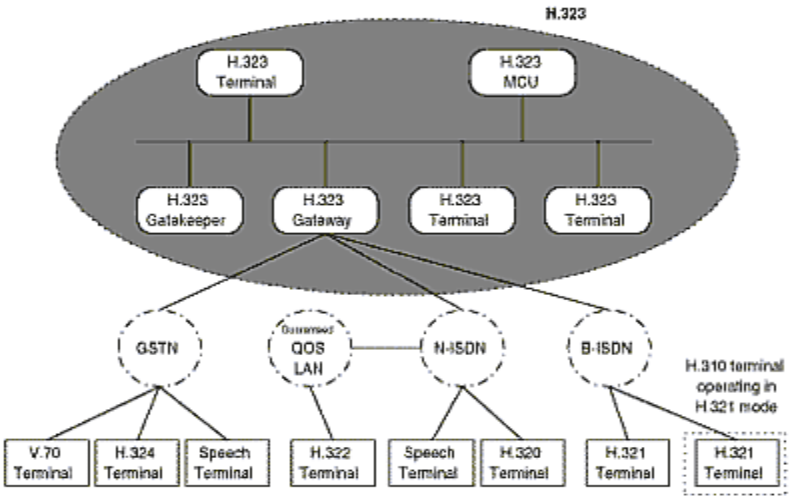


Рис.1. Базовая архитектура стандарта H.323

Терминалы H.323

Под терминалом стандарт понимает оборудование конечных точек сети, которое позволяет пользователям общаться друг с другом в реальном времени.

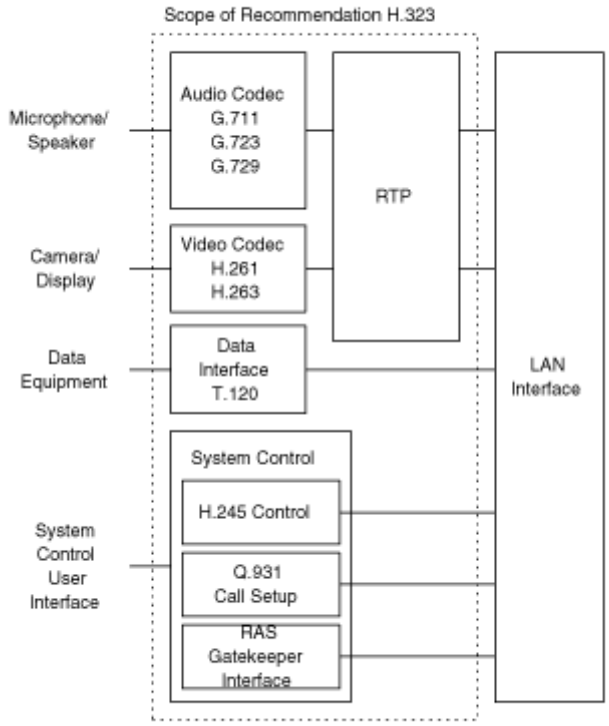


Рис.2. Структура терминала H.323.

Терминалы должны поддерживать протоколы H.245 - согласование параметров соединения, Q.931 - для установления соединения и согласования параметров этого соединения, канал RAS (Registration/Admission/Status) взаимодействия с контроллером зоны (Gatekeeper), протокол RTP/RTCP для работы с потоками аудио и видео пакетов, протокол G.711 для сжатия аудиопотока.
Согласно рекомендациям, для терминала H.323 опциональной является поддержка видеокодеков, протокола T.120, и возможностей MCU.

Видеовозможности терминалов H.323

Несмотря на то, что стандарт считает функции видео необязательными, все терминалы с видеовозможностями должны поддерживать кодек H.261, опционально возможна поддержка H.263.
H.263 является развитием кодека H.261, видеокартинка, полученная с помощью кодека H.263 обладает лучшим качеством, поскольку используется полупиксельная технология предсказания движения. Кроме того, используемое кодирование по Хаффману оптимизировано для работы с более низкими скоростями передачи.
Определено пять стандартных форматов кадров:

Табл.2. Форматы кадров H.261 и H.263

Формат кадра	**Размер в пикселях**	**H.261**	**H.263**
sub-QCIF	128x96	не определено	обязательно
QCIF	176x144	обязательно	обязательно
CIF	352x288	возможно	возможно
4CIF	702x576	не определено	возможно
16CIF	1408x1152	не определено	возможно

.

Мультимедиа шлюз (Gateway) H.323

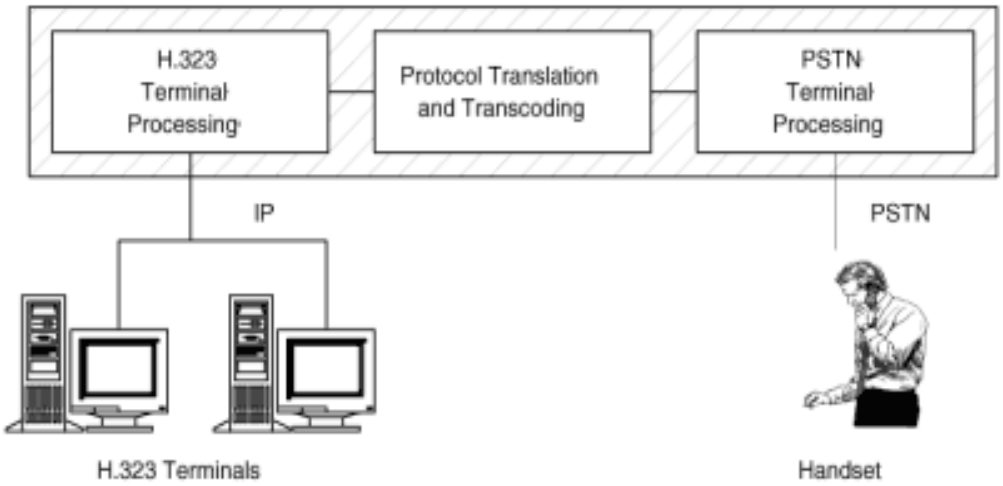


Рис.3. Мультимедиа шлюз H.323/PSTN.

Согласно H.323, мультимедиа шлюз - это опциональный элемент в конференции H.323. Он может выполнять много различных функций. Типичной его функцией являются задача преобразования форматов протоколов передачи (например, H.225.0 и H.221). Обычно мультимедиа шлюзы используются для поддержки взаимодействия между разнородными сетями. На Рис.3. показан шлюз H.323/PSTN.

Контроллер зоны (Gatekeeper, Привратник, Конференц-менеджер)

Это рекомендуемое, но не обязательное устройство, обеспечивающее сетевое управление и исполняющее роль виртуальной телефонной станции.

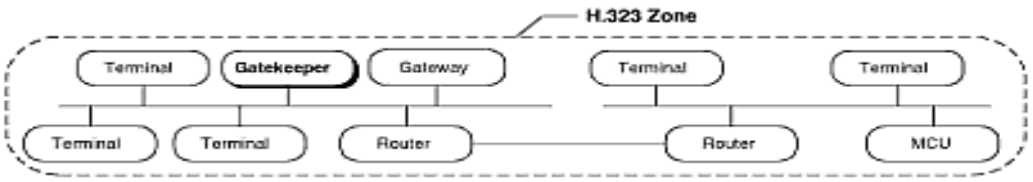


Рис.4. Контроллер зоны (Gatekeeper)

Основными функциями контроллера зоны являются:

- Управление и адресация вызовов
- Обеспечение основными типами обслуживания, такими как телефонный справочник и сервисом, характерным для УАТС (передача и перенаправление вызовов и т.д.)
- Управление использованием полосы пропускания приложениями H.323 таким образом, чтобы обеспечить качество обслуживания (QoS).
- Управление общим использованием сетевых ресурсов
- Системное администрирование и обеспечение безопасности

Несмотря на то, что Рекомендации H.323 определяют контроллер зоны как необязательный компонент, без него невозможно воспользоваться мощным и разнообразным спектром услуг, предусмотренных создателями стандарта H.323 для приложений IP-телефонии и мультимедийных телеконференций.

- **Устройство управления многоточечной конференцией (Multipoint Control Units (MCU))**

Устройство MCU предназначено для поддержки конференции между тремя и более участниками. В этом устройстве должен присутствовать контроллер Multipoint Controller (MC), и, возможно, процессоры Multipoint Processors (MP). Контроллер MC поддерживает протокол H.245 и предназначен для согласования параметров обработки аудио- и видеопотоков между терминалами. Процессоры занимаются коммутированием, микшированием и обработкой этих потоков.

Конфигурация многоточечной конференции может быть централизованной, децентрализованной, гибридной и смешанной.

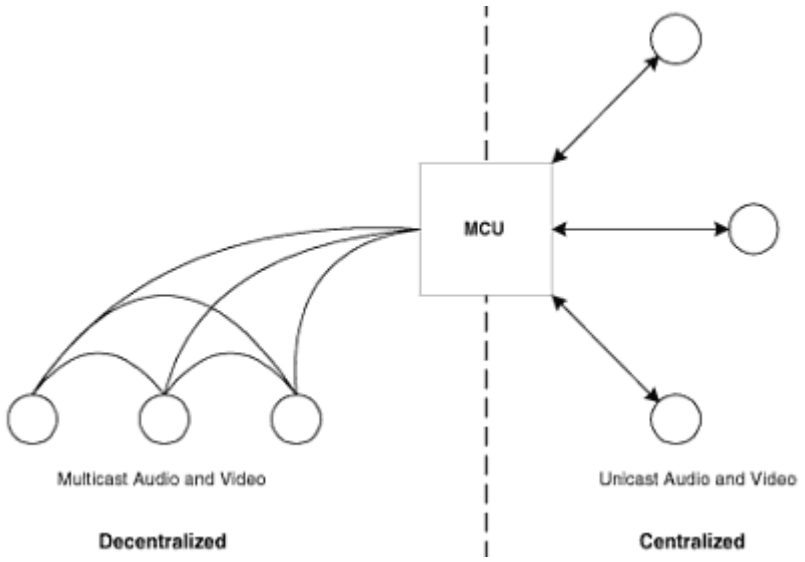


Рис. 5. Схемы централизованной и децентрализованной организаций конференции в H.323.

Централизованная многоточечная конференция требует наличия устройства MCU. Каждый терминал обменивается с MCU потоками аудио, видео, данными и командами управления по схеме "точка-точка". Контроллер MC, используя протокол H.245, определяет возможности каждого терминала. Процессор MP формирует

необходимые для каждого терминала мультимедийные потоки и рассылает их. Кроме того, процессор может обеспечивать преобразования потоков от различных кодеков с различными скоростями данных.
Децентрализованная многоточечная конференция использует технологию групповой адресации. Участвующие в конференции H.323 терминалы осуществляют многоадресную передачу мультимедиа потока остальным участникам без посылки на MCU. Передача контрольной и управляющей информации осуществляется по схеме "точка-точка" между терминалами и MCU. В этом случае контроль многоточечной рассылки осуществляется контроллером MC.
Гибридная схема организации конференцсвязи является комбинацией двух предыдущих. Участвующие в конференции H.323 терминалы осуществляют многоадресную передачу только аудио- или только видеопотока остальным участникам без посылки на MCU. Передача остальных потоков осуществляется по схеме "точка-точка" между терминалами и MCU. В этом случае задействуются как контроллер, так и процессор MCU.

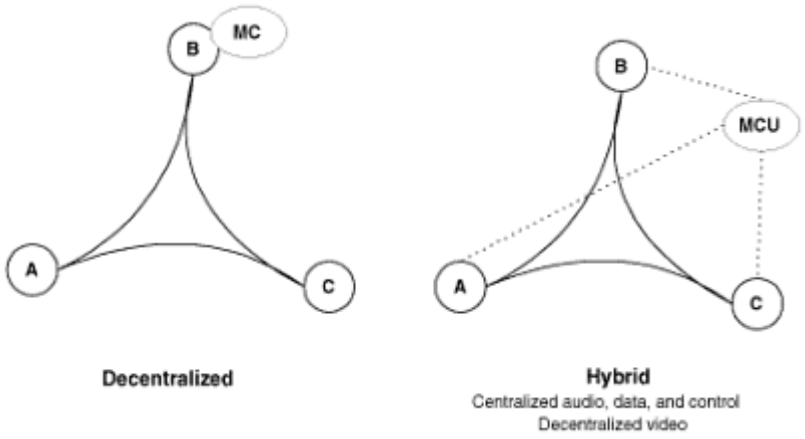


Рис. 6. Схемы децентрализованной и смешанной организаций конференции в H.323.

В смешанной схеме организации конференцсвязи одна группа терминалов может работать по централизованной схеме, а другая группа - по децентрализованной.

- **Тенденции развития рекомендаций H.323**

H.323 v.2

Во второй версии H.323 v.2 рекомендаций были устранены недостатки предыдущей версии. Были усовершенствованы существующие протоколы: Q.931, H.245 и H.225, а также введен ряд новых. Основные преимущества новой версии стандарта заключаются в добавлении функций безопасности, установки быстрого вызова, некоторых дополнительных сервисов и интеграции протоколов H.323 и T.120.

- Функции безопасности (H.235) включают в себя обеспечение аутентификации (механизм, который подтверждает то, что участники конференции именно те, за которых они себя выдают), целостности

(механизм, подтверждающий то, что переданные пакеты не были искажены), криптографическую защиту передаваемой информации от несанкционированного доступа.

- Функция Fast Call Setup решает имевшуюся в первой версии проблему, когда после прохождения звонка одного абонента другому могла быть задержка в прохождении аудио и видеопотоков.
- Протокол T.120 был интегрирован и в первую версию рекомендаций H.323, однако сценарии установки звонка были довольно сложны. Во второй версии рекомендаций H.323 эта проблема решается следующим образом: стандарт требует, чтобы оборудование конечных пользователей, поддерживающее одновременно и T.120, и H.323, управлялось звонками по H.323. Более того, согласно второй версии рекомендаций T.120 является опциональной частью конференции H.323 и возможности действий по T.120 отдаются на усмотрение каждого устройства в H.323 конференции по отдельности.

H.323 v.3

В третьей версии H.323 v.3 рекомендаций было введено несколько новых возможностей. Прежде всего они касаются дополнений к основному документу и рекомендациям H.225.0, внося усовершенствования в архитектуру стандарта. Среди них можно выделить:

- Более эффективное использование ранее установленных сигнальных соединений, в частности, между мультимедиа шлюзом и контроллером зоны
- Возможность переадресации вызова при установленном соединении
- Повышено удобство получения информации об абонентах (Caller ID).
- Сигнальная информация включает в себя информацию о языке абонента, что расширяет возможности обработки вызова.
- Предложен механизм, облегчающий добавление новых кодеков.
- Механизм сигнализации может теперь использовать UDP транспорт, вместо TCP, что существенно для конференций с большим числом участников.
- Введено понятие упрощенного терминала (Simple Endpoint Type - SET). Такие терминалы могут поддерживать только незначительную часть рекомендаций H. 323, тем не менее обеспечивая проведение аудиосвязи с другими H.323 терминалами.
- Введена возможность SNMP - управления оборудованием видеоконференцсвязи.
- Информационная база управления (MIB) описывается документом H.341.

H.323 v.4

Четвертая версия рекомендаций H.323 v.4 принята 17 ноября 2000 года. Туда внесено много изменений с целью повышения надежности, мобильности и гибкости систем видеоконференций. Новые возможности, касающиеся мультимедиа шлюзов и

устройств многоточечной конференции, направлены на повышение качества организации и проведения конференции с большим числом участников. Перечислим некоторые из нововведений.

- Новые механизмы повышения устойчивости работы H.323 конференции.
- Декомпозиция структуры мультимедиа шлюза с целью отделения модуля управления от исполнительных устройств.
- Возможность мультиплексирования аудио и видео в одном RTP потоке.
- Модификация процесса регистрации на контроллере зоны с целью облегчить регистрацию большого числа участников конференции.
- Совершенствование механизмов распределения нагрузки и повышения устойчивости работы контроллеров зоны
- Для терминалов H.323 предусматриваются способы выделения реально необходимой полосы пропускания как для обычной, так и для групповой адресации.

Системы управления видеоконференцсвязью

Существует общемировое правило — чем больше сеть, тем сложнее сетью становится управлять. Для обеспечения надежности и повышения отказоустойчивости и безопасности сетей видеоконференции используются технологии, получившие название системы управления сетями.

В понятие системы управления сетями видеоконференций должны входить

Обработка и анализ ошибок — обеспечение необходимыми инструментами для обнаружения сбоев и отказов сетевых и терминальных устройств, определения их причин и принятия действий по восстановлению работоспособности.

- Управление конфигурацией — отслеживание и настройка конфигурации сетевого аппаратно-программного обеспечения.
- Учет — измерение использования и доступности сетевых ресурсов.
- Управление производительностью — измерение производительности сети, сбор и анализ статистической информации о поведении сети для ее поддержания на приемлемом уровне как для оперативного управления сетью, так и для планирования ее развития.
- Управление безопасностью — контроль доступа к оборудованию и сетевым ресурсам с ведением журналов доступа для обнаружения, предотвращения и пресечения несанкционированного доступа.

К основным системам управления видеоконференции относят:

- **Tandberg:** Tandberg Management Suite (TMS).
- **Polycom:** Polycom Converged Management Application (CMA); Distributed Media Application (DMA); Global Management System (GMS); PathNavigator.
- **Emblaze-VCON:** Media eXchange Manager (MXM).
- **Codian:** Codian Management Platform (CMP); Codian Director; Codian Scheduller.

Производители аппаратных и программных решений для видеоконференций
Зарубежные производители

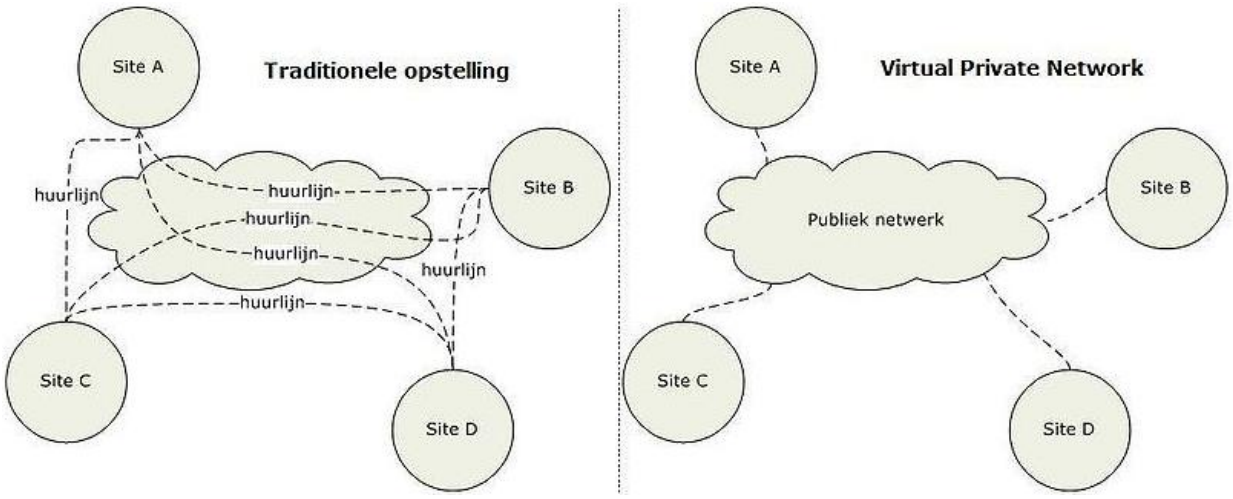
- Polycom (США), аппаратные и программные решения

- Tandberg (Норвегия), аппаратные и программные решения
- Sony (Япония), аппаратные решения
- Aethra (Италия), аппаратные решения
- Codian (Англия), аппаратные и программные решения
- LifeSize (США), аппаратные решения
- Vidyo (США), программные решения
- RadVision (Израиль), аппаратные и программные решения
- Emblaze-VCON (Израиль), аппаратные и программные решения
- AddPac (Корея), аппаратные решения
- Huawei Technologies (Китай), аппаратные решения
- Cisco Systems (США), аппаратные решения
- Scotty (Англия), аппаратные решения
- e-works (Италия), программные решения
- ARTA Software (Казахстан), программные решения

Российские производители

- ВидеоПорт, программные решения
- ВидеоМост, программные решения
- DiViSy, программные решения
- Vidicor, аппаратно-программные решения
- Mototelecom Videomeeting System, программные решения

VPN (англ. *Virtual Private Network* — виртуальная частная сеть) — обобщённое название технологий, позволяющих обеспечить одно или несколько сетевых соединений (логическую сеть) поверх другой сети (например, Интернет). Несмотря на то, что коммуникации осуществляются по сетям с меньшим неизвестным уровнем доверия (например, по публичным сетям), уровень доверия к построенной логической сети не зависит от уровня доверия к базовым сетям благодаря использованию средств криптографии (шифрованию, аутентификация, инфраструктуры публичных ключей, средствам для защиты от повторов и изменения передаваемых по логической сети сообщений).



Уровни реализации

Обычно VPN развёртывают на уровнях не выше сетевого, так как применение криптографии на этих уровнях позволяет использовать в неизменном виде транспортные протоколы (такие как TCP, UDP).

Пользователи Microsoft Windows обозначают термином VPN одну из реализаций виртуальной сети — PPTP, причём используемую зачастую *не* для создания частных сетей.

Чаще всего для создания виртуальной сети используется инкапсуляция протокола PPP в какой-нибудь другой протокол — IP (такой способ использует реализация PPTP — Point-to-Point Tunneling Protocol) или Ethernet (PPPoE) (хотя и они имеют различия). Технология VPN в последнее время используется не только для создания собственно частных сетей, но и некоторыми провайдерами «последней мили» для предоставления выхода в Интернет.

При должном уровне реализации и использовании специального программного обеспечения сеть VPN может обеспечить высокий уровень шифрования передаваемой информации. При правильной настройке всех компонентов технология VPN обеспечивает анонимность в Сети.

Структура VPN

VPN состоит из двух частей: «внутренняя» (подконтрольная) сеть, которых может быть несколько, и «внешняя» сеть, по которой проходит инкапсулированное соединение (обычно используется Интернет). Возможно также подключение к виртуальной сети отдельного компьютера. Подключение удалённого пользователя к VPN производится посредством сервера доступа, который подключён как к внутренней, так и к внешней (общедоступной) сети. При подключении удалённого пользователя (либо при установке соединения с другой защищённой сетью) сервер доступа требует прохождения процесса идентификации, а затем процесса аутентификации. После успешного прохождения обоих процессов, удалённый пользователь (удаленная сеть) наделяется полномочиями для работы в сети, то есть происходит процесс авторизации.

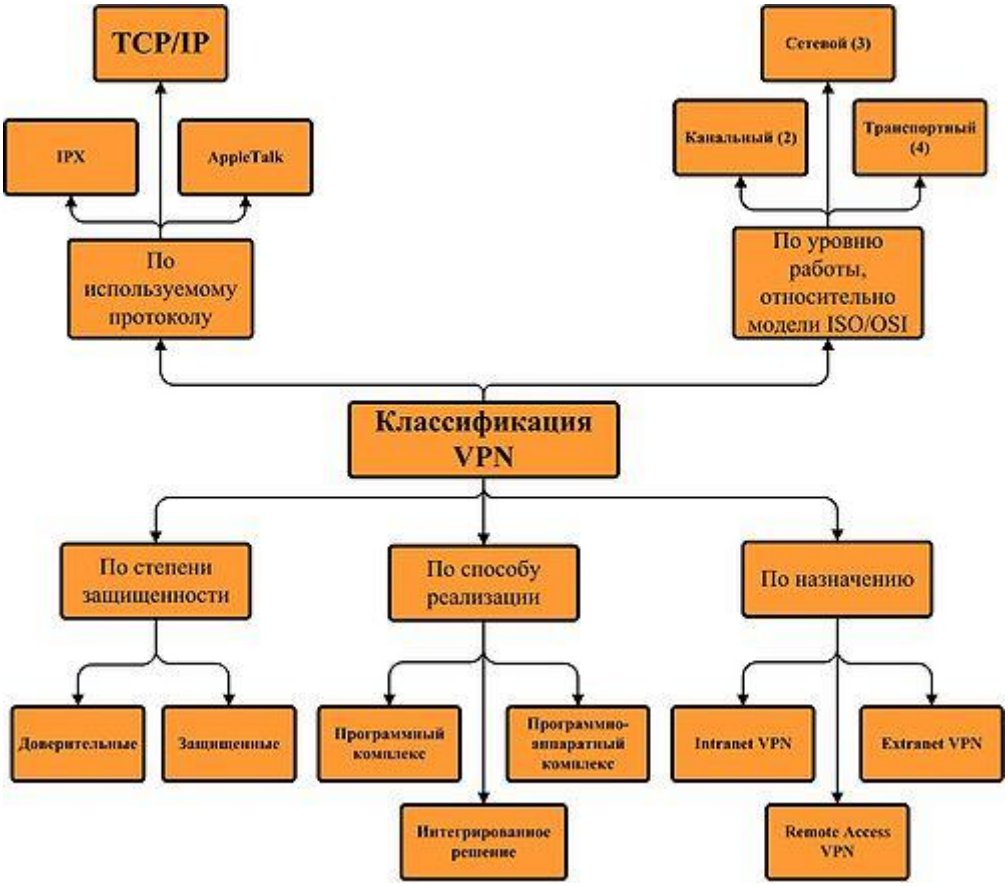
Примеры VPN

- IPSec (IP security) — часто используется поверх IPv4.
- PPTP (point-to-point tunneling protocol) — разрабатывался совместными усилиями нескольких компаний, включая Microsoft.
- PPPoE (PPP (Point-to-Point Protocol) over Ethernet)
- L2TP (Layer 2 Tunnelling Protocol) — используется в продуктах компаний Microsoft и Cisco.
- L2TPv3 (Layer 2 Tunnelling Protocol version 3).
- OpenVPN SSL VPN с открытым исходным кодом, поддерживает режимы PPP, bridge, point-to-point, multi-client server

Многие крупные провайдеры предлагают свои услуги по организации VPN-сетей для бизнес-клиентов.

Классификация VPN

Классификация VPN



Классифицировать VPN решения можно по нескольким основным параметрам:

По степени защищенности используемой среды
Защищённые

Наиболее распространённый вариант виртуальных частных сетей. С его помощью возможно создать надежную и защищенную на основе ненадёжной сети, как правило, Интернета. Примером защищённых VPN являются: IPSec, OpenVPN и PPTP.

Доверительные

Используются в случаях, когда передающую среду можно считать надёжной и необходимо решить лишь задачу создания виртуальной подсети в рамках большей сети. безопасности становятся неактуальными. Примерами подобных VPN решений являются: Multi-protocol label switching (MPLS) и L2TP (Layer 2 Tunnelling Protocol). (точнее сказать, что эти протоколы перекладывают задачу обеспечения безопасности на другие, например L2TP, как правило, используется в паре с IPSec).

По способу реализации
В виде специального программно-аппаратного обеспечения

Реализация VPN сети осуществляется при помощи специального комплекса программно-аппаратных средств. Такая реализация обеспечивает высокую производительность и, как правило, высокую степень защищённости.

В виде программного решения

Используют персональный компьютер со специальным программным обеспечением, обеспечивающим функциональность VPN.

Интегрированное решение

Функциональность VPN обеспечивает комплекс, решающий также задачи фильтрации сетевого трафика, организации сетевого экрана и обеспечения качества обслуживания.

По типу протокола

Существуют реализации виртуальных частных сетей под TCP/IP, IPX и AppleTalk. Но на сегодняшний день наблюдается тенденция к всеобщему переходу на протокол TCP/IP, и абсолютное большинство VPN решений поддерживает именно его. Адресация в нём чаще всего выбирается в соответствии со стандартом RFC5735, из диапазона Приватных сетей TCP/IP

По уровню сетевого протокола

По уровню сетевого протокола на основе сопоставления с уровнями эталонной сетевой модели ISO/OSI.

Шифрование

Шифрование с использованием протокола MPPE (Microsoft Point-to-Point Encryption)

Метод MPPE (Microsoft Point-to-Point Encryption) используется для шифрования данных в подключениях удаленного доступа на базе протокола PPP (Point-to-Point Protocol) или подключениях к виртуальной частной сети (VPN — virtual private network) по протоколу PPTP (Point-to-Point Tunneling Protocol). Поддерживаются схемы шифрования MPPE с 128-разрядным ключом (усиленная), с 56-разрядным ключом и с 40-разрядным ключом (стандартная). MPPE обеспечивает безопасность данных для подключений PPTP между VPN-клиентом и VPN-сервером.

MPPE требует использования ключей шифрования, генерируемых в процессе проверки подлинности по протоколу MS-CHAP (Microsoft Challenge Handshake Authentication Protocol), MS-CHAP v2 (Microsoft Challenge Handshake Authentication Protocol версии 2) или EAP-TLS (Extensible Authentication Protocol-Transport Level Security).

Чтобы включить шифрование данных с использованием MPPE на подключениях VPN, необходимо активизировать проверку подлинности по протоколу MS-CHAP, MS-CHAP v2 или EAP-TLS. Все эти методы проверки подлинности генерируют ключи, используемые в процессе шифрования.

Шифрование с использованием протокола IPSec (Internet Protocol security)

IPSec — это набор служб защиты и протоколов безопасности, основанных на средствах криптографии. Этот протокол представляет одно из наиболее перспективных направлений развития средств защиты сетей. Так как протокол IPSec не требует изменения приложений или протоколов, он легко развертывается в существующих сетях.

IPSec обеспечивает проверку подлинности на уровне компьютера и шифрование данных для подключений VPN, использующих протокол L2TP. Согласование IPSec между локальным компьютером и VPN-сервером, использующим L2TP, выполняется перед установкой подключения L2TP. Это согласование защищает и пароли, и данные.

При взаимодействии с IPSec протокол L2TP использует стандартные методы проверки подлинности на базе PPP, такие как EAP, MS-CHAP, MS-CHAP v2, CHAP, SPAP и PAP.

Тип шифрования определяется так называемым сопоставлением безопасности IPSec. Сопоставление безопасности — это набор атрибутов, состоящий из адреса назначения, протокола безопасности и уникального идентификатора, называемого индексом параметров безопасности. Поддерживаются следующие алгоритмы шифрования:
• DES (Data Encryption Standard), использующий 56-разрядный ключ;
• 3DES (Triple DES), использующий три 56-разрядных ключа и предназначенный для среды с высоким уровнем безопасности.

По назначению

Intranet VPN

Используют для объединения в единую защищённую сеть нескольких распределённых филиалов одной организации, обменивающихся данными по открытым каналам связи.

Remote Access VPN

Используют для создания защищённого канала между сегментом корпоративной сети (центральным офисом или филиалом) и одиночным пользователем, который, работая дома, подключается к корпоративным ресурсам с домашнего компьютера, корпоративного ноутбука, смартфона или интернет-киоска.

Extranet VPN

Используют для сетей, к которым подключаются «внешние» пользователи (например, заказчики или клиенты). Уровень доверия к ним намного ниже, чем к сотрудникам компании, поэтому требуется обеспечение специальных «рубежей» защиты, предотвращающих или ограничивающих доступ последних к особо ценной, конфиденциальной информации.

Internet VPN

Используется для предоставления доступа к интернету провайдерами, обычно в случае если по одному физическому каналу подключаются несколько пользователей.

Client/Server VPN

Он обеспечивает защиту передаваемых данных между двумя узлами (не сетями) корпоративной сети. Особенность данного варианта в том, что VPN строится между узлами, находящимися, как правило, в одном сегменте сети, например, между рабочей станцией и сервером. Такая необходимость очень часто возникает в тех случаях, когда в одной физической сети необходимо создать несколько логических сетей. Например, когда надо разделить трафик между финансовым департаментом и отделом кадров, обращающихся к серверам, находящимся в одном физическом сегменте. Этот вариант похож на технологию VLAN, но вместо разделения трафика, используется его шифрование.

Skype

Skype (произносится «скайп») — бесплатное проприетарное программное обеспечение с закрытым кодом, обеспечивающее шифрованную голосовую связь через Интернет между компьютерами (VoIP), а также платные услуги для связи с абонентами обычной телефонной сети.

Программа также позволяет совершать конференц-звонки (до 25 голосовых абонентов, включая инициатора), видеозвонки (в т.ч. видеоконференции до 10 абонентов), а также обеспечивает передачу текстовых сообщений и файлов.

Технология

В отличие от многих других программ IP-телефонии, для передачи данных Skype использует P2P-архитектуру. Каталог пользователей Skype распределён по компьютерам пользователей сети Skype, что позволяет сети легко масштабироваться до очень больших размеров (в данный момент более 100 миллионов пользователей, 15—20 миллионов онлайн) без дорогой инфраструктуры централизованных серверов.

Кроме того, Skype может маршрутизировать звонки через компьютеры других пользователей. Это позволяет соединяться друг с другом пользователям, находящимися за NAT или брандмауэром, однако создаёт дополнительную нагрузку на компьютеры и каналы пользователей, подключённых к Интернету напрямую.

Единственным центральным элементом для Skype является сервер идентификации, на котором хранятся учётные записи пользователей и резервные копии их списков контактов. Центральный сервер нужен только для установки связи. После того как связь установлена, компьютеры пересылают голосовые данные напрямую друг другу (если между ними есть прямая связь) или через Skype-посредник (суперузел — компьютер, у которого есть внешний IP-адрес и открыт TCP-порт для Skype). В частности, если два компьютера, находящиеся внутри одной локальной сети, установили между собой Skype-соединение, то связь с Интернетом можно прервать и разговор будет продолжаться вплоть до его завершения пользователями или какого-либо сбоя связи внутри локальной сети.

Благодаря используемым Skype кодекам (алгоритмам сжатия данных) SVOPC (16 кГц), AMR-WB (16 кГц), G.729 (8 кГц) и G.711 (ранее использовались также ILBC и ISAC) и при достаточной скорости интернет-соединения (30—60 кбит/с) в большинстве случаев качество звука сопоставимо с качеством обычной телефонной связи.

При установке соединения между ПК данные шифруются при помощи AES-256, для передачи ключа которого, в свою очередь, используется 1024-битный ключ RSA. Открытые ключи пользователей сертифицируются центральным сервером Skype при входе в систему с использованием 1536- или 2048-битных сертификатов RSA.

VoIP-протокол Skype закрыт и используется только оригинальным программным обеспечением Skype. При помощи API к его функциям могут получать доступ программы сторонних разработчиков.

Официально подтверждённых разработчиком случаев расшифровки и/или перехвата данных в Skype не зафиксировано, и большинство спецслужб выражают по этому поводу недовольство. Однако правоохранительные органы Австрии на встрече с провайдерами в местном Министерстве внутренних дел сообщили, что провели «законный перехват IP-трафика» 25 июня 2008 года. Аналогичное заявление прозвучало и от представителя органов внутренних дел Австралии. Также, благодаря утечке информации, стало известно о разработке фирмой Digitask программы перехвата онлайн-коммуникаций по заказу одного из министерств Баварии, а компания FaceTime разработала сканер защищённых IM-сообщений Skype. Кроме того, о наличии решений для прослушивания Skype объявили власти Швейцарии и ФСБ.

Для стабильного использования видеосвязи необходима скорость интернет-соединения более 200 кбит/с и желательна тактовая частота процессора не менее 1 ГГц.

Чат

Skype позволяет пользователям общаться с помощью голоса и более традиционным способом с помощью текстовых сообщений (IM-чата). Голосовой чат позволяет как разговаривать с одним пользователям, так и устраивать конференц-связь. Он использует собственные кодеки. Skype-чат позволяет устраивать групповые чаты, посылать смайлики, хранить историю.

Также предоставляются обычные для IM-чатов возможности — профили пользователя, индикаторы состояния (статус) и так далее.

Попытки запрета Skype

Комиссия по телекоммуникациям и информационным технологиям Российского союза промышленников и предпринимателей (РСПП) готовит рекомендации по запрету в России Skype. Интересы связистов-участников РСПП ясны: благодаря наличию Skype, миллионы пользователей Интернета в России имеют возможность обойти существующие высокие тарифы на международную телефонную связь. Кроме того, инициаторы запрета и ФСБ утверждают, что Skype трудно подслушивать из-за отсутствия его подключения к СОРМ.

В Белоруссии все звонки по сети фиксированной связи должны проходить через государственного оператора, а использование других международных сетей, включая Skype, считается нарушением законодательства.

Крупнейшая европейская телекоммуникационная компания Deutsche Telekom заявила, что будет блокировать Skype при попытке использования ее с iPhone.

Доступ к Skype может быть заблокирован аппаратными средствами. Подобные решения есть у Verso Technologies и Cisco Systems. В частности, ими пользуется крупнейший китайский провайдер China Telecom. До марта 2010 года аналогичным образом Skype блокировали в ОАЭ.

В ответ на попытки запрета Skype его разработчики начали внедрять в программу средства маскировки трафика для обхода блокировки VoIP. Кроме того, Skype может работать внутри анонимной сети I2P, подвергаясь при этом дополнительному многоуровневому шифрованию и анонимизации, также Skype может работать с прокси-серверами, VPN и Tor, что практически сводит на нет эффективность его блокировки.

Критика

- Skype практически невозможно прослушать, за что его критикуют спецслужбы многих стран. В то же время сам сервис не раз обвинялся в шпионаже в пользу США и Китая.

- Одним из недостатков Skype считается использование проприетарного протокола, несовместимого с открытыми стандартами (такими, как SIP или H.323). Однако оператор российской сети Sipnet сумел наладить взаимодействие со Skype.

- В процессе работы Skype генерирует типичный для P2P-сетей и неизбежный постоянный трафик, который может достигать гигабайта в месяц. Решением данной проблемы может быть запрет в файрволе входящих соединений для Skype. В версии для платформы Windows эту функцию также можно отключить редактированием реестра.

- На конференции Black Hat Europe 2006, посвящённой вопросам информационной безопасности, был представлен анализ Skype. Среди прочего, там были отмечены:

    - интенсивное использование антиотладочных приёмов и обфусцированного кода;
    - постоянная передача данных (даже в ситуациях, когда сама программа находится в режиме ожидания);
    - использование 3G-сетей.

- Крис Касперски активно критикует Skype:

Skype — это чёрный ящик с многоуровневой системой шифрования, напичканной антиотладочными приёмами исполняемого файла, считывающий с компьютера конфиденциальную информацию и передающий её в сеть по закрытому протоколу. Последний обходит брандмауэры и сурово маскирует свой трафик, препятствуя его блокированию. Всё это превращает Skype в идеального переносчика вирусов, червей и дронов, создающих свои собственные распределённые сети внутри Skype-сети. …
Skype активно изучается в хакерских лабораториях и security-организациях по всему миру, и большинство исследователей единодушно сходятся во мнении, что Skype — это дьявольски хитрая программа, написанная бесспорно талантливыми людьми в стиле Black Magic Art. Skype не брезгует грязными трюками, создающими огромные проблемы.

- К версии Skype под Linux высказываются претензии о том, что им читаются файлы, содержащие пароли.

- В феврале 2007 стало известно об ошибке, в результате которой Skype создаёт в каталоге для временных файлов файл 1.com, который позволяет считывать информацию из BIOS. Согласно информации из официального блога, это было вызвано использовавшейся в подключаемом модуле Skype Extras Manager системы безопасности, изготовленной фирмой EasyBits Software, которая таким образом получала серийный номер материнской платы для однозначной идентификации компьютера. Данная система не используется в версиях 3.0.0.216 и старше.

- Как и любая сеть, работающая по принципу P2P, Skype подвержен вирусным эпидемиям. Уже известны случаи распространения вредоносных программ, перехватывающих и записывающих разговоры в Skype.

- Не существует линукс-версии Skype для 64-битной архитектуры. На официальном сайте Skype есть архив для Ubuntu x64, но это ложь, он использует 32-битные библиотеки.

Openmeetings

Сервис Openmeetings предназначен для организации индивидуальных и групповых вебинаров в режиме реального времени с передачей видео и аудио сигналов между участниками. Для работы с сервисом могут быть использованы различные широко распространенные интернет-браузеры (см. Тех.требования) в стандартной конфигурации. Никакого специализированного программного обеспечения на рабочей станции участника не требуется.
Различные режимы работы позволяют организовать вебинары различного вида — лекции (публичное вещание лекции одного участника-модератора), диспуты и диалоги (публичное вещание ведения диалога между двумя участниками), конференции (публичное вещание общения всех участников между собой). В данном случае под публичным вещание подразумевается просмотр и прослушивание всеми остальными участниками вебинара.

Технические требования к рабочей станции участника
На момент написания данного документа работа сервиса Openmeetings была протестирована на рабочих станциях с операционными системами:
•Microsoft Windows XP SP3;
•Microsoft Windows Vista;
•Microsoft Windows 7 Basic edition.
В качестве интернет-браузеров были использованы следующие программы:

•Microsoft Internet Explorer 8 (версия 8.0.6001.18702);
•Mozilla Firefox (версия 3.6.6);
•Opera (версия 10.54, сборка 3423);
•Google Chrome (версия 5.0.375.86);
•Apple Safari (версия 4.0.4, сборка 531.21.10).
Для работы сервиса на рабочую станцию участника необходимо установить бесплатный флэш-проигрыватель Shockwave Flash, который можно скачать по адресу - http://get.adobe.com/ru/flashplayer/ На момент написания этого документа его версия — 10.1. Данный проигрыватель работает во всех, перечисленных выше, браузерах.
Для работы с сервисом используются TCP-порты 5080 и 1935. Компьютер участника должен иметь возможность организовать подключения на указанные порты сервера с сервисом Openmeetings. Если ваша локальная сеть защищена файрволом или доступ в интернет ограничивается прокси-сервером, то необходимо в правилах этих сервисов обеспечить доступ рабочих станций участников на указанные порты по адресам — 217.113.126.170 (интернет) и 10.128.67.1 (ТМС). Инициатором данных соединений всегда выступает рабочая станция участника.

Для прослушивания аудиоинформации (голоса ведущего) необходимо наличие подключенных к рабочей станции участника аудио-колонок или наушников. Если участник будет являться ведущим вебинара, то также необходимо наличие подключенного микрофона и желательно наличие подключенной веб-камеры.

Регистрация
Перед любым использованием сервиса Openmeetings участник должен зарегистрироваться на данном сервисе. При регистрации каждый участник получает на сервисе учетную запись, идентифицируемую индивидуальными логином и паролем данного участника. На Рисунок 1 показан экран Регистрации/Входа участника. Он появляется при входе на сервис. Для регистрации участник должен нажать указанную на рисунке кнопку «Регистрация».
После нажатия кнопки «Регистрация» на экране появится форма учетной записи участника, которую необходимо заполнить - Рисунок 2.
Поля «Имя» и «Фамилия» заполняются на русском языке с заглавной буквы.
В поле «Пользователь» участник должен придумать и вписать свой логин на английском языке — это имя будет использоваться участником при входе на сервис. В логине помимо букв латинского алфавита допускается использовать символы «-» и «_», а также цифры.

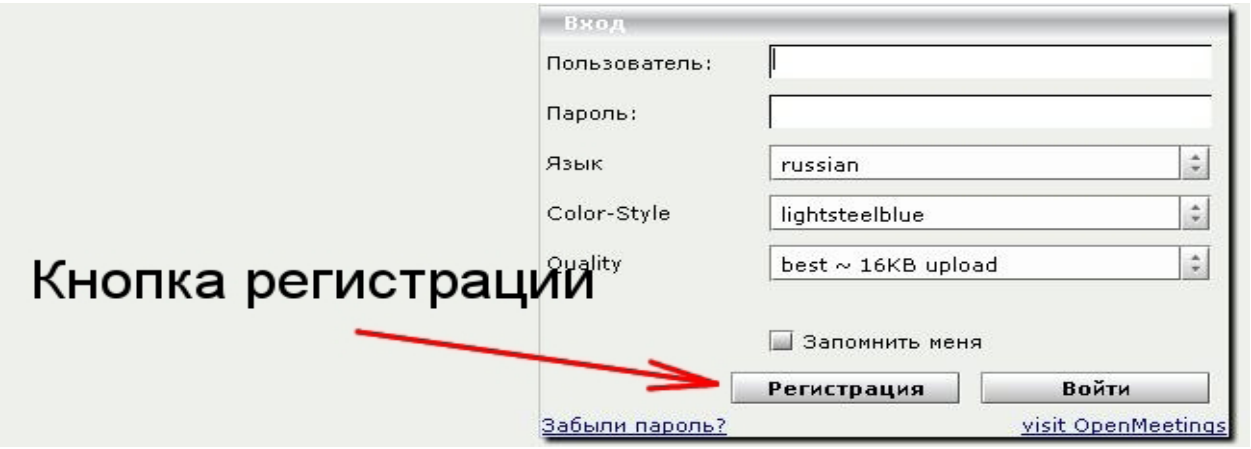


Рисунок 1: Первый экран - регистрация участника.

В случае, если логин, введенный участником, уже существует в базе учетных записей сервиса, на экран будет выдано соответствующее сообщение и участнику необходимо будет придумать и ввести другой логин.
В поля «Пароль» и «Повторить» участник должен внести свой пароль. Пароль должен удовлетворять следующим условиям — могут быть использованы буквы латинского алфавита и цифры. Длинна пароля должна быть не менее 7 символов, из которых минимум 5 — буквы и минимум 2 — цифры. Такие жесткие требования к паролю связаны в первую очередь с тем, что сервис Openmeetings является публичным и доступ к нему со стороны интернет не ограничен.
В поле «E-Mail» необходимо внести адрес электронной почты участника. На момент написания этого документа это поле не используется при работе сервиса. В будущем на адрес, указанный в этом поле, участнику будут высылаться приглашения на вебинары данного сервиса и уведомления об зменениях в порядке работы.

В поле «Страна» участник, с помощью кнопки в правой части поля, должен выбрать значение «Russian Federation», как показано на рисунке.

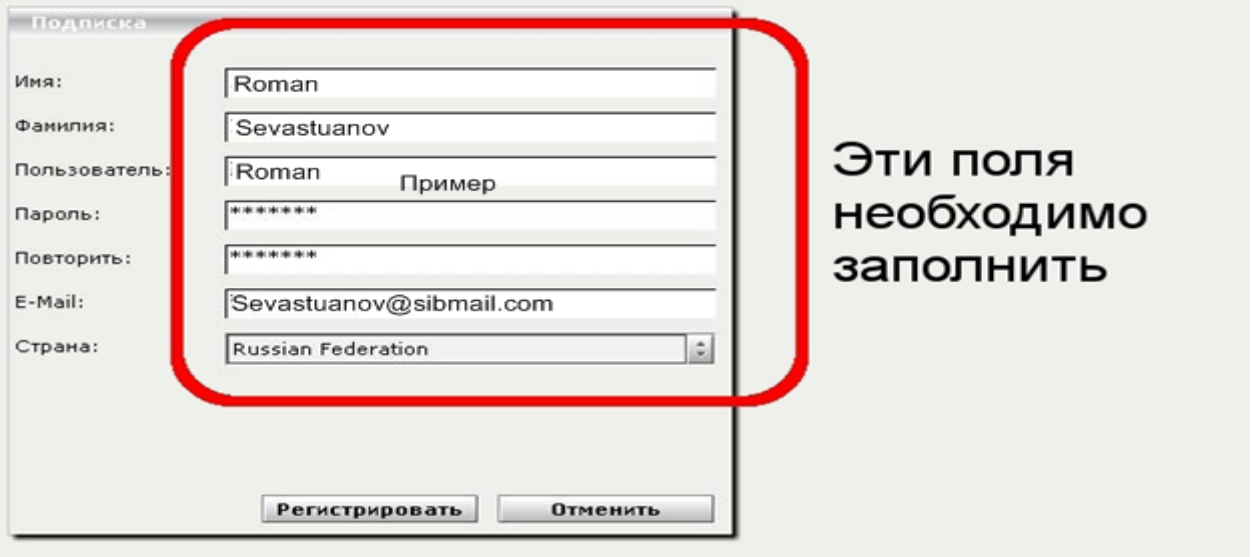
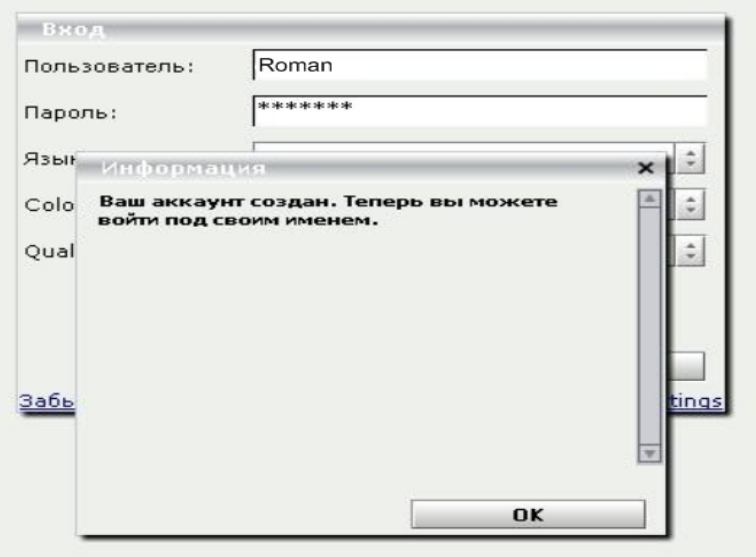


Рисунок 2: Форма регистрации участника.

После заполнения всех полей регистрационной формы и нажатия кнопки «Регистрировать» в ее нижней части, на экране появится сообщение о создании учетной записи - Рисунок 3. После нажатия кнопки «ОК» в нижней части этого сообщения регистрацию можно считать законченной и участник может войти в сервис.
Процес регистрации — однократная процедура. Однажды зарегистрировавшись, участник в дальнейшем может входить под своими логином и паролем для работы с сервисом.
Вся информация кроме логина, внесенная участником в регистрационную форму, может быть в дальнейшем изменена им при редактировании профиля своей учетной записи. Никакая информация из профиля учетной записи участника не будет использована кроме как для использования функций сервиса Openmeetings.



Вход

После регистрации участник может войти под своими логином и паролем на сервис. Для этого необходимо ввести свои логин и пароль, указанные при регистрации, в поля «Логин» и «Пароль» окна входа — Рисунок 4.

В поле «Язык» кнопкой в правой части поля необходимо установить значение «russian».

Поле «Color-Style» определяет цветовое оформление сервиса в вашем интернет-браузере.

Поле «Quality» определяет качество изображения на экране интернет-браузера и одновременно регулирует объем потребляемого участником трафика при работе с сервисом. Оно может принимать два значения: «best» (лучшее) со средним потреблением 16 Килобайт в секунду и «medium» (среднее) со средним потреблением 10 Килобайт в секунду. Выбрать необходимое значение участник может кнопкой в правой части поля.

После заполнения всех полей и нажатия кнопки «Войти» в нижней части окна участник попадет на главную страницу сервиса.

Рисунок 4. Окно входа на сервис

Подключение к вебинару

Главная страница сервиса Openmeetings выглядит, как показано на Рисунок 5.

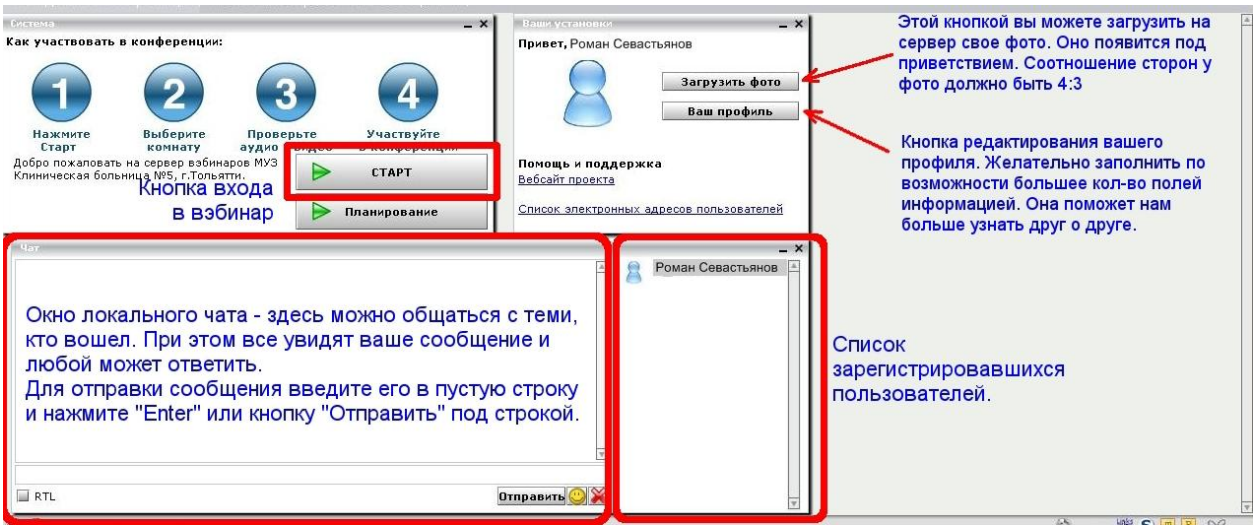


Рисунок 5.

На этой странице присутствуют окно «Система» (слева вверху) со схемой использования сервиса и кнопкой «СТАРТ» для входа в вебинар, окно «Ваши установки» (справа вверху) с кнопками загрузки вашего фото и редактирования полей профиля учетной записи и окно «Чат» с полями чата и вошедших участников.
До начала вебинара можно задавать вопросы в чате. При этом все, кто находится в списке справа от окна чата, увидят ваш вопрос и любой может ответить.

Для входа непосредственно в вебинар необходимо нажать кнопку «СТАРТ». После ее нажатия на экране появится окно входа в вебинар — Рисунок 6.

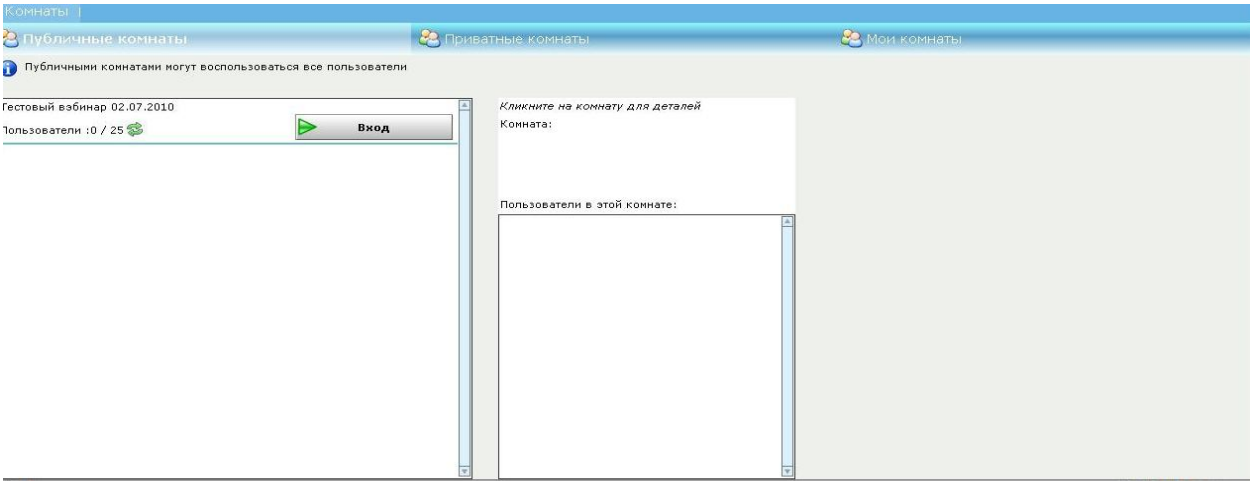
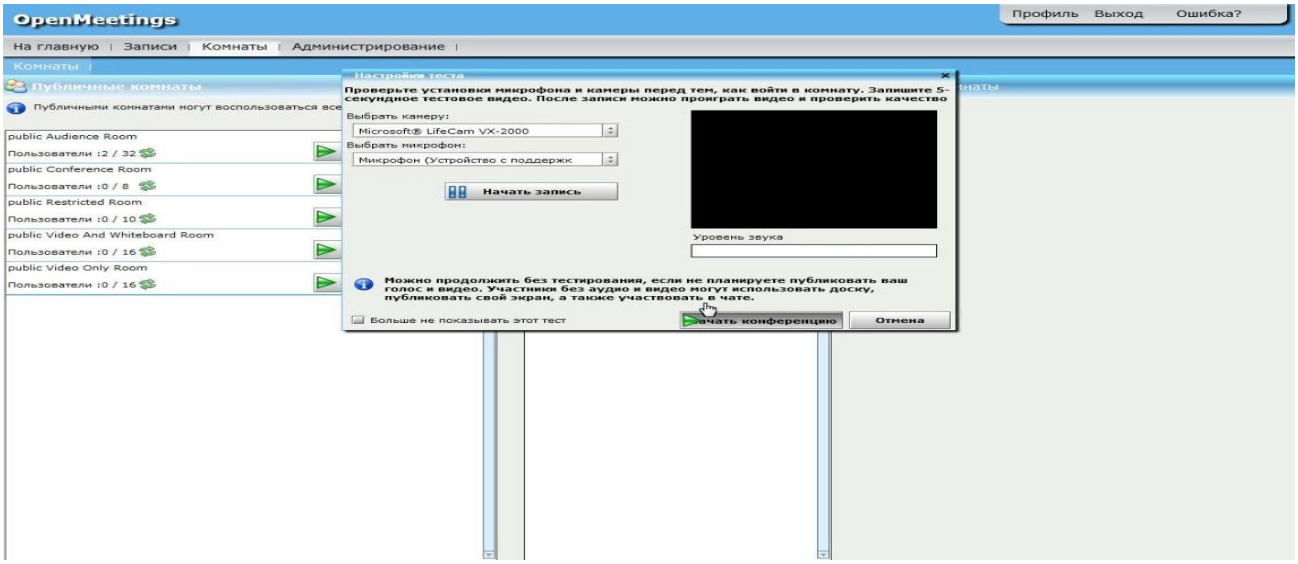
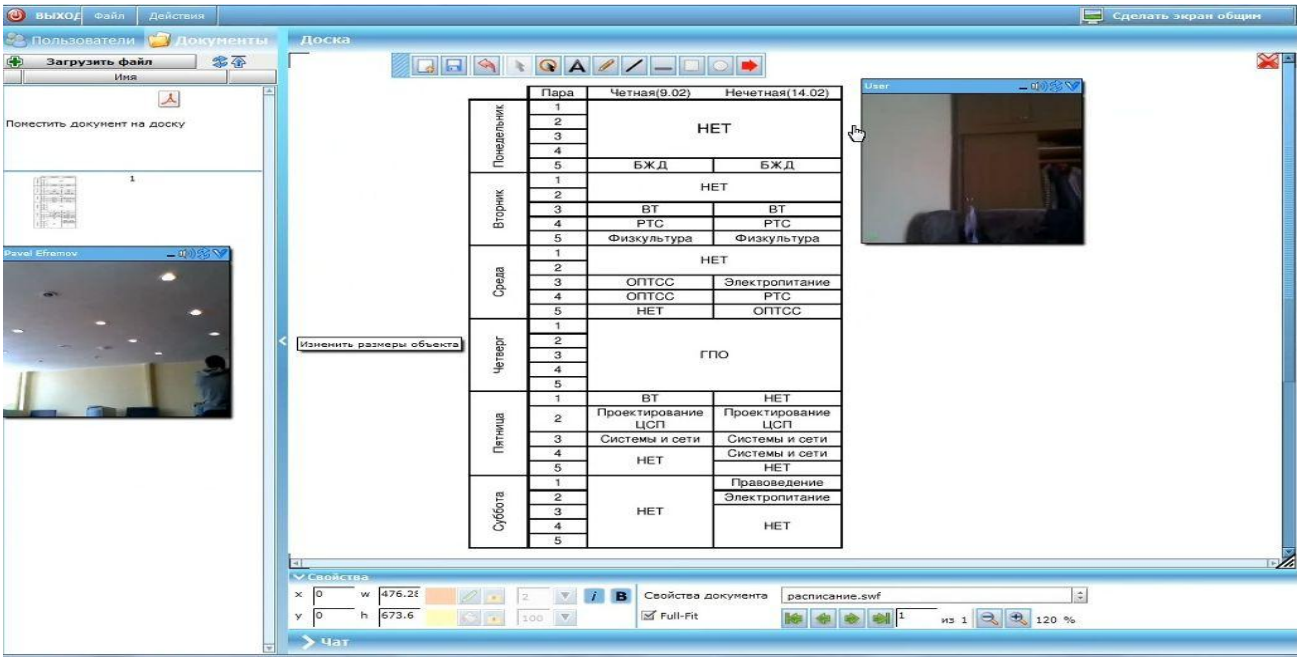


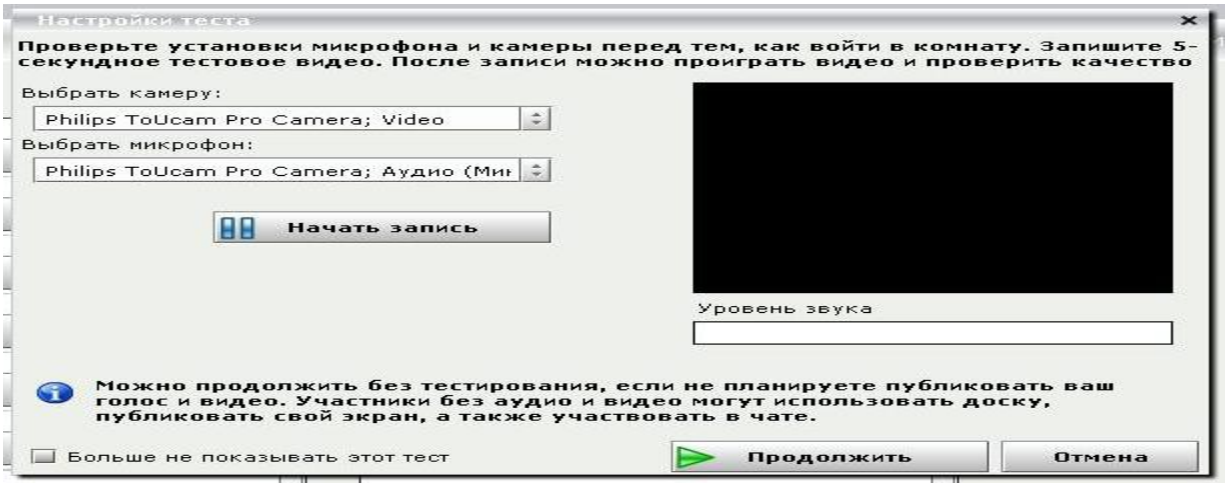
Рисунок 6.

На момент написания данного документа на старнице вебинаров был единственный «Тестовый вебинар». Нажав кнопку «Вход» напротив названия вебинара участник подключится к этому вебинару.



При подключении сервис попытается определить наличие подключенных к рабочей станции участника веб-камеры и микрофона. При этом на экране появится окно выбора источников видео и аудиосигналов.





Если у участника нет источников видео и аудиосигналов, то можно просто нажать кнопку «Продолжить».

Если же участник желает использовать вэб-камеру и микрофон, то он должен выбрать в соответствующих полях «Выбрать камеру:» и «Выбрать микрофон:» свои источники сигналов, а затем проверить их работу, нажав кнопку «Запись». При этом в черном квадрате появится изображение с выбранной камеры, а в поле «Уровень звука» под ним — уровень сигнала с микрофона — Рисунок 8. Сервер сделает трехсекундную запись изображения и звука, которую затем можно проиграть нажав кнопку «ПРОИГРАТЬ». При этом в окне должно появиться записанное изображение, а в динамиках или наушниках — звук.

Если выбранные вами камера и микрофон работают, то можно нажать кнопку «Продолжить» и войти в вебинар. В противном случае нужно выбрать другой источник для камеры и микрофона и попробовать еще раз.

После входа в вебинар участник увидит на экране следующий запрос использования выбранных им камеры и микрофона - Рисунок 9. При этом в поле «Изменить Published Devices» можно установить одно из следующих значений:

•«Аудио и видео» - изображение с камеры и микрофона участника буду передаваться на сервер Openmeetings и транслироваться им всем остальным участникам вебинара;

•«Только аудио» - звук с микрофона участника будут передаваться на сервер и транслироваться им всем участниками вебинара;

•«Только видео» - изображение с камеры участника будет передваться на сервер и транслироваться им всем участникам вебинара;

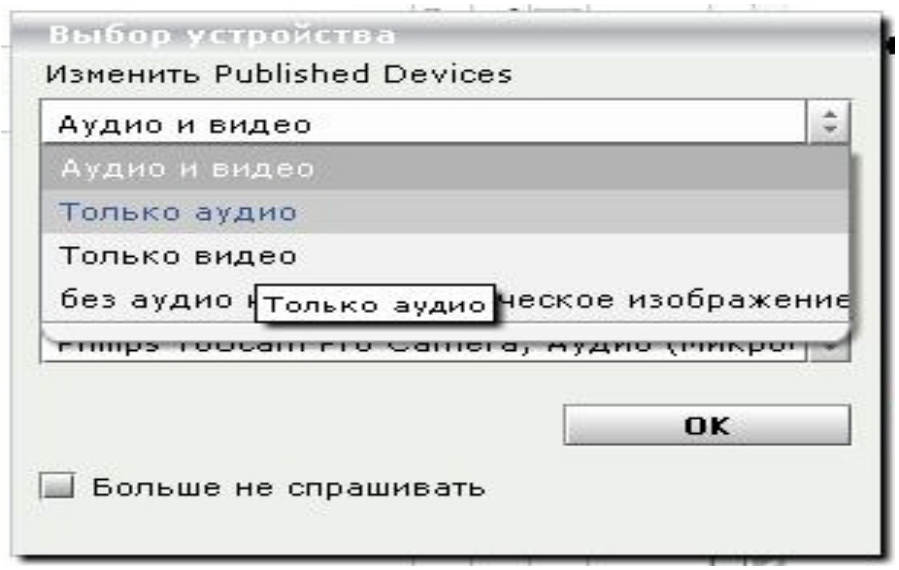
•«Без аудио и видео» - камера и микрофон участника не будут использоваться сервисом Openmeetings.

Если вы не являетесь ведущим вебинара и не планируете им стать в процессе его проведения, то рекомендуется выбирать режим «Без аудио и видео». Это позволит снизить нагрузку на сервер и уменьшить размер транслируемых им данных, уменьшив таким образом загрузку каналов доступа в интернет самого сервера и участников вебинара.

Основной экран вебинара состоит из трех окон — окна «Участников вебинара/документов», окна «Чата» и окна «Доски» - Рисунок 10.

В окне «Участников вебинара/документов» отображается список участников или документов, используемых («прикрепленных») в данном вебинаре.

В окне «Чата» все участники вебинара могут писать сообщения и читать ответы на них других участников.



В окне «Доски» ведущий может разместить материалы вебинара, а также выполнять несложные рисунки.

4.Рекомендуемая литература

1.Преимущества создания систем видеонаблюдения на базе IP / А.А. Виталисов // Системы безопасности. – 2007. - №4. с. 34.
2.http://code.google.com/p/openmeetingshttp://wiki.auditory.ru/w/list
3.http://code.google.com/p/openmeetings/wiki/InstallationDebian
4.http://www.teleportservice.ru/htm/benefits_05.htm
5.http://www.mefeedia.com/entry/openmeetings-basic-installation/8604209
6.http://vk.it-sfera.com.ua/242.html
7.http://sysadminblog.ru/blog/manual/1.html
8.http://videoconference.com.ru/
9.VPN и IPSec на пальцах [Электронный документ] / Dru Lavigne. —
11.http://www.nestor.minsk.by/sr/2005/03/050315.html
12.Мобильные комплексы видеоконференцсвязи, журнал «Connect! Мир Связи», 10.2009

Лабораторная работа 4. Исследование транспортной сети связи на основе технологии IP-телефонии

1.Цель работы

IP-телефония , исследуемая в работе, предназначена для организации передачи речи и данных между сотрудниками организации, в целях использования новых для традиционной телефонии сервисов и приложений

2. Краткие теоретические сведения

Термин «IP-телефония» постоянно на слуху. Многие сетевые специалисты считают эту технологию очень важным этапом эволюции телекоммуникаций. Средства IP-телефонии используют протокол IP для передачи речи по сети передачи данных, преобразуя при этом обычный аналоговый речевой сигнал в цифровой.

Технология IP-телефонии является революционной, поскольку объединяет два очень разных мира: мир телефонных сетей, которые должны функционировать очень надежно, и мир сетей передачи данных, эпизодические отказы которых в ряде случаев вполне допустимы. Кроме того, сети передачи данных быстро развиваются, поскольку требования к их пропускной способности постоянно растут.

Техническое решение, объединяющее эти два мира, должно быть надежным в работе, экономически эффективным, широкополосным (обеспечить высокую скорость передачи данных) и способным к быстрой эволюции одновременно. Создать систему, соответствующую этим требованиям, совсем непросто.

Под IP-телефонией понимается технология, позволяющая использовать сеть с коммутацией IP-пакетов, в частном случае – Интернет, в качестве средства организации ведения телефонных разговоров и передачи факсов в режиме реального времени между удаленными абонентами. IP-телефония является одним из наиболее сложных и системных приложений компьютерной телефонии. Термин IP-телефония буквально – обеспечение телефонных переговоров с использованием протокола межсетевого взаимодействия (Internet Protocol).

Внедрение IP-телефонии существенно изменяет подход к обеспечению телефонной связи. Для телефонии с начала века используются коммутируемые каналы с гарантированной полосой пропускания, чем и обеспечивается беспрерывная связь. В IP-телефонии используется коммутация пакетов. Принципиально разница состоит в следующем. В традиционно обеспечиваемой телефонной связи каждому абоненту в монопольное распоряжение выделяется линия связи. При коммутации пакетов несколько пользователей одновременно используют один и тот же канал. Уплотняя трафик путем разбиения на пакеты непрерывного разговора и эффективно заполняя ими доступный канал, можно существенно понизить стоимость использования дорогого цифрового канала для каждого отдельного пользователя.

Конечный пользователь IP-телефонии не только сохранит имеющиеся преимущества телефонной сети общего пользования, которые включают широкий диапазон услуг, простоту использования, надежность и качество голоса, но и получит следующие дополнительные преимущества:

- Существенно низкие цены на междугородние и международные переговоры ;
- IP- телефония одновременно поддерживает голос и данные, удовлетворяя требованиям конвергенции. Это означает, что клиенты получат дополнительные преимущества от экономии в развитии, возможные за счет использования единой сети, а также за счет

того, что объемы трафика и шаблоны быстро сменяются от данных к голосу, и наоборот и это защищает клиента;

- Феноменальная мобильность пользователя, которую обеспечивает сеть IP-телефонии: звонки и факсы автоматически перенаправляются в любую точку мира, пользователи будут иметь доступ к одному и тому же набору услуг вне зависимости от того, где и как они подключаются к сети. Эта распределенная структура обеспечивает прекрасную гибкость и делает возможным отсутствие привязки к месту предоставления услуги;
- Новый набор устройств доступа, от традиционных телефонов и факсов до компьютеров;
- Доступ к новым услугам (голосовая почта, конференцсвязь, передача факса и др.) через открытый интерфейс архитектуры на базе IP, что обеспечивает совместимость для широкого спектра разработчиков приложений;
- Возможность настройки набора услуг.

Связь через IP получается дешевле по ряду причин. Во-первых, в IP-телефонии используются широко распространенные (и дешевые) сети с коммутацией пакетов, (в отличие от более дорогостоящих сетей с коммутацией каналов, применяемых в традиционной телефонии). Во-вторых, благодаря использованию голосовых кодеков достигается существенное сжатие речевой информации. Так, при передаче голосового потока в системах цифровой телефонии требуется канал 64 кБит/с (ISDN). В системах IP-телефонии, при использовании наиболее популярных на сегодняшний день кодеков, требуется гораздо меньшая пропускная способность (6-13 кБит/с).

Наряду с провайдерами IP-телефонии Интернет-провайдеры также могут занять определенную нишу на рынке услуг IP-телефонии, так как существующая у них IP-инфраструктура дает хорошие возможности для внедрения услуг голосовой связи.

Для Интернет-провайдеров услуга Интернет-телефонии обеспечивает следующие преимущества:

- Сбережение капитальных вложений за счет использования открытых компьютерных платформ;
- Снижение эксплутационных расходов как результат предоставления разнообразия услуг на единой сети;
- Множество услуг может быть доступно через единственный канал с пользователем, что означает больше прибыли в расчете на одного пользователя.

С появлением IP-телефонии в рядах операторов дальней связи началась легкая паника. В результате традиционные телефонисты вынуждены были сами заняться IP-технологиями и, надо отдать им должное, довольно быстро преуспели в этом, используя IP-решения как минимум для создания резервных каналов для пропуска трафика на случай перегрузок или аварий, что позволило получать им дополнительную прибыль.

На страницах отечественных и зарубежных телекоммуникационных журналах в последнее время развернулась дискуссия по поводу определения места и роли IP-телефонии в дальнейшем развитии средств передачи речи. Взгляды сторон, участвующих в дискуссии, резко противоположны.

Одни из них утверждают, что будущее принадлежит только протоколу IP, их главный тезис «Все по IP, IP по всему». Сейчас даже появилось понятие «айпизм», которое подразумевает универсальность применения данной технологии для передачи любых видов информации (голоса, данных, видео) и замену всех других сетей на сеть с пакетной коммутацией на базе протокола IP. Часто приходится слышать, что дни традиционной телефонии с коммутацией каналов сочтены и через 10-15 лет от нее уже ничего не останется.

Сторонники противоположных взглядов указывают на то, что, несмотря на большие темпы роста объема трафика IP-телефонии за последние годы, его доля в США составляет около одного процента от трафика классической телефонии, а во всем мире и того меньше. Даже с

учетом всех оптимистических прогнозов операторы сетей связи и в перспективе будут получать основную прибыль от предоставления услуг телефонных сетей с коммутацией каналов. Аргументами в пользу этих доводов являются существующие проблемы с обеспечением требуемого качества передачи речи по публичным каналам Интернет, сравнительно меньшая надежность существующих IP-сетей, трудность управления такими сетями.

Похоже истина где-то посередине. Действительно, IP-телефония – не панацея для решения всех телекоммуникационных проблем. Но в тоже время ее использование позволяет предлагать пользователям совершенно новые, невозможные для традиционной телефонии сервисы и приложения. Да и сам фактор экономии затрат на телефонную связь играет не последнюю роль даже с учетом более низкого, но приемлемого, качества передачи разговора. Все это говорит о том, что технология IP-телефонии по большому счету выгодна всем: и пользователям, и операторам сетей, и производителям оборудования.

«Классические» телефонные сети основаны на технологии коммутации каналов, которая для каждого телефонного разговора требует выделенного физического соединения. Следовательно, один телефонный разговор представляет собой одно физическое соединение телефонных каналов. В этом случае аналоговый сигнал шириной 3,1 кГц передается на ближайшую АТС, где он мультиплексируется по технологии временного разделения с сигналами, которые поступают от других абонентов, подключенных к этой АТС. Далее групповой сигнал передается по сети межстанционных каналов. Достигнув АТС назначения, сигнал демультиплексируется и доходит до адресата. Основным недостатком телефонных сетей с коммутацией каналов является неэффективное использование полосы канала - во время пауз в речи канал не несет никакой полезной нагрузки.

Переход от аналоговых к цифровым технологиям стал важным шагом для возникновения современных цифровых телекоммуникационных сетей. Одним из таких шагов в развитии цифровой телефонии стал переход к пакетной коммутации. В сетях пакетной коммутации по каналам связи передаются единицы информации, которые не зависят от физического носителя. Такими единицами могут быть пакеты, кадры или ячейки (в зависимости от протокола), но в любом случае они передаются по разделяемой сети (рисунок 3.1), более того - по отдельным виртуальным каналам, не зависящим от физической среды. Каждый пакет идентифицируется заголовком, который может содержать информацию об используемом им канале, его происхождении (то есть об источнике или отправителе) и пункте назначения (о получателе или приемнике).

В сетях на основе протокола IP все данные - голос, текст, видео, компьютерные программы или информация в любой другой форме - передаются в виде пакетов. Любой компьютер и терминал такой сети имеет свой уникальный IP-адрес, и передаваемые пакеты маршрутизируются к получателю в соответствии с этим адресом, указываемом в заголовке. Данные могут передаваться одновременно между многими пользователями и процессами по одной и той же линии. При возникновении проблем IP-сети могут изменять маршрут для обхода неисправных участков. При этом протокол IP не требует выделенного канала для сигнализации.

Процесс передачи голоса по IP-сети состоит из нескольких этапов [1].

На первом этапе осуществляется оцифровка голоса. Затем оцифрованные данные анализируются и обрабатываются с целью уменьшения физического объема данных, передаваемых получателю. Как правило, на этом этапе происходит подавление ненужных пауз и фонового шума, а также компрессирование.

На следующем этапе полученная последовательность данных разбивается на пакеты и к ней добавляется протокольная информация - адрес получателя, порядковый номер пакета на случай, если они будут доставлены не последовательно, и дополнительные данные для

коррекции ошибок. При этом происходит временное накопление необходимого количества данных для образования пакета до его непосредственной отправки в сеть.

Извлечение переданной голосовой информации из полученных пакетов также происходит в несколько этапов. Когда голосовые пакеты приходят на терминал получателя, то сначала проверяется их порядковая последовательность. Поскольку IP-сети не гарантируют время доставки, то пакеты со старшими порядковыми номерами могут прийти раньше, более того, интервал времени получения также может колебаться. Для восстановления исходной последовательности и синхронизации происходит временное накопление пакетов. Однако некоторые пакеты могут быть вообще потеряны при доставке, либо задержка их доставки превышает допустимый разброс. В обычных условиях приемный терминал запрашивает повторную передачу ошибочных или потерянных данных. Но передача голоса слишком критична ко времени доставки, поэтому в этом случае либо включается алгоритм аппроксимации, позволяющий на основе полученных пакетов приблизительно восстановить потерянные, либо эти потери просто игнорируются, а пропуски заполняются данными случайным образом.

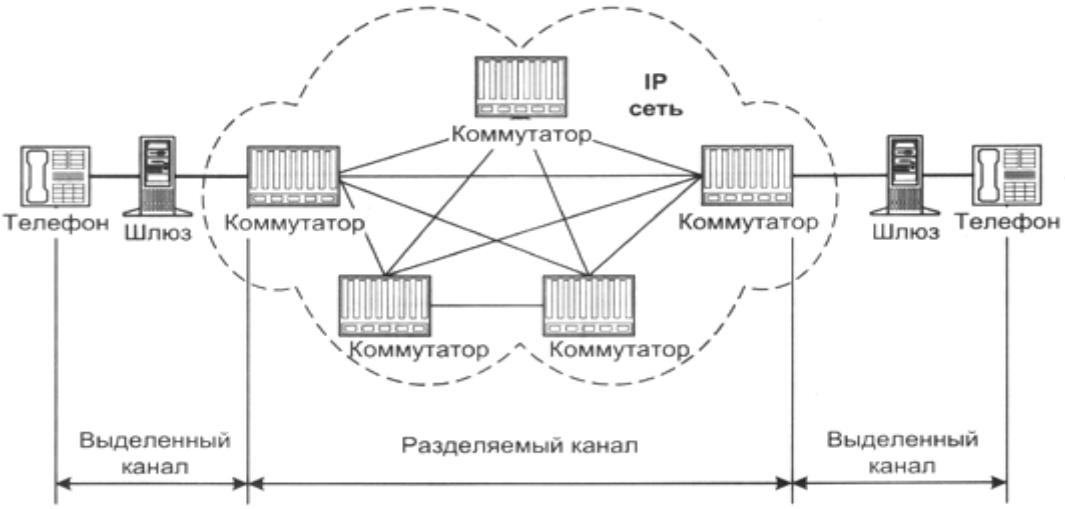


Рис. 1. Соединение в сети с коммутацией пакетов

Полученная таким образом (не восстановленная) последовательность данных декомпрессируется и преобразуется непосредственно в аудио-сигнал, несущий голосовую информацию получателю.

Таким образом, с большой степенью вероятности, полученная информация не соответствует исходной (искажена) и задержана (обработка на приёмной и передающей сторонах требует промежуточного накопления). Однако в некоторых пределах избыточность голосовой информации позволяет мириться с такими потерями.

Абонент, оплативший полосу 64 кбит/с, использует канал в среднем лишь на 25 %. Значит, оператор способен продать имеющийся у него ресурс в четыре раза большему числу пользователей, не перегружая свою сеть. Это выгодно обеим сторонам – и клиенту, и продавцу, - поскольку оператор увеличивает свои доходы и уменьшает абонентскую плату за счёт снижения издержек.

В настоящее время, в IP-телефонии существует два основных способа передачи голосовых пакетов по IP-сети:

- через глобальную сеть Интернет (Интернет-телефония);
- использую сети передачи данных на базе выделенных каналов (IP-телефония);

В первом случае, полоса пропускания напрямую зависит от загруженности сети Интернет пакетами, содержащими данные, голос, графику, а значит, задержки при прохождении пакетов могут быть самыми разными. При использовании же выделенных каналов исключительно для голосовых пакетов можно гарантировать фиксированную (или почти фиксированную) скорость передачи. Ввиду широкого распространения сети Интернет особый интерес вызывает реализация системы Интернет-телефонии, хотя в этом случае качество телефонной связи оператором не гарантируется.

Для того чтобы осуществить междугородную (международную) связь с помощью телефонных серверов, оператор услуги должны иметь по серверу в тех местах, куда и откуда планируются звонки. Стоимость такой связи на порядок меньше стоимости телефонного звонка по обычным телефонным линиям.

Общий принцип действия телефонных серверов Интернет-телефонии таков: с одной стороны, сервер связан с телефонными линиями и может соединиться с любым телефоном мира. С другой стороны, сервер связан с Интернетом и может связаться с любым компьютером в мире. Сервер принимает стандартный телефонный сигнал, оцифровывает его (если он исходно не цифровой), значительно сжимает, разбивает на пакеты и отправляет через Интернет по назначению с использованием протокола IP. Для пакетов, приходящих из сети на телефонный сервер и уходящих в телефонную линию, операция происходит в обратном порядке. Обе составляющие операции (вход сигнала в телефонную сеть и его выход из телефонной сети) происходят практически одновременно, что позволяет обеспечить полнодуплексный разговор. На основе этих базовых операций можно построить много различных конфигураций. Например, звонок «телефон-компьютер» или «компьютер-телефон» может обеспечивать один телефонный сервер. Для организации связи телефон (факс)-телефон (факс) нужно два сервера.

С точки зрения масштабируемости (если отвлечься от проблем с неконтролируемым ухудшением качества при росте нагрузки на сеть) IP-телефония представляется вполне законченным решением. Во-первых, поскольку соединение на базе протокола IP может начинаться (и заканчиваться) в любой точке сети от абонента до магистрали. Соответственно, IP-телефонию в сети можно вводить участок за участком, что, кстати, на руку и с точки зрения миграции, так как ее можно проводить «сверху вниз», «снизу вверх» или по любой другой схеме. Для решений IP-телефонии характерна определенная модульность: количество и мощность различных узлов - шлюзов, gatekeeper («привратников» - так в терминологии VoIP именуются серверы обработки номерных планов) - можно наращивать практически независимо, в соответствии с текущими потребностями.

Межсетевой протокол IP

В настоящее время наиболее эффективная передача потока любых дискретных (цифровых) сигналов, в том числе и несущих речь (голос), обеспечивается цифровыми сетями электросвязи, в которых реализована пакетная технология IP [2].

Протокол IP – основной протокол сетевого уровня, позволяющий реализовывать межсетевые соединения.

Следует подчеркнуть, что протокол IP реализуется не только в глобальной сети Интернет, для которой он был первоначально разработан, он может быть применен и в других цифровых телекоммуникационных сетях.

Основным сдерживающим фактором на пути масштабного внедрения IP-телефонии является отсутствие в протоколе IP механизмов обеспечения гарантированного качества услуг, что делает его пока не самым надежным транспортом для передачи голосового трафика. Протокол IP обрабатывает каждый IP-пакет как независимую единицу, не имеющую связи ни с какими другими IP-пакетами. Сам протокол IP не гарантирует доставку пакетов, а также время их доставки, что вызывает такие проблемы, как «рваный голос» и просто

провалы в разговоре. В протоколе IP нет механизмов, обычно применяемых для увеличения достоверности конечных данных: отсутствует квитирование – обмен подтверждениями между отправителем и получателем, нет процедуры упорядочения, повторных передач или других подобных функций. Если во время продвижения пакета произошла какая-либо ошибка, то протокол IP по своей инициативе ничего не предпринимает для исправления этой ошибки. Например, если на промежуточном маршрутизаторе пакет был отброшен по причине истечения времени жизни или из-за ошибки в контрольной сумме, то модуль IP не пытается заново послать испорченный или потерянный пакет. Все вопросы обеспечения надежности доставки данных по составной сети в стеке TCP/IP решает протокол TCP, работающий непосредственно над протоколом IP.

IP-адрес

Администратор сети присваивает оконечным устройствам IP-адреса в соответствии с тем, к каким IP-сетям они подключены. Старшие биты 4-х байтного IP-адреса определяют номер IP-сети. Оставшаяся часть IP-адреса – номер узла (хост-номер). IP-адрес узла идентифицирует точку доступа модуля IP к сетевому интерфейсу, а не устройство. Существует 5 классов IP-адресов, отличающихся количеством бит в сетевом номере и хост-номере. Класс адреса определяется значением его первого октета.

В таблице 1 приведено соответствие классов адресов значениям первого октета и указано количество возможных IP-адресов каждого класса.

Адреса класса A предназначены для использования в больших сетях общего пользования. Они допускают большое количество номеров узлов. Адреса класса B используются в сетях среднего размера, например, сетях университетов и крупных компаний. Адреса класса C используются в сетях с небольшим числом компьютеров. Адреса класса D используются при обращениях к группам устройств, а адреса класса E зарезервированы на будущее.

Таблица 1. Характеристики классов адресов

Класс	Диапазон значений первого октета	Возможное количество сетей	Возможное количество узлов
A	1-126	126	16777214
B	128-191	16382	65534
C	192-223	2097150	254
D	224-239	-	2**28
E	240-247	-	2**27

Некоторые IP-адреса являются выделенными и трактуются по-особому.

Виды соединений в сети IP-телефонии

Сети IP-телефонии предоставляют возможности для вызовов четырех основных типов:

1. «От телефона к телефону». Вызов идет с обычного телефонного аппарата к АТС, на один из выходов которой подключен шлюз IP-телефонии, и через IP-сеть доходит до другого шлюза, который осуществляет обратные преобразования.
2. «От компьютера к телефону». Мультимедийный компьютер, имеющий программное обеспечение IP-телефонии, звуковую плату (адаптер), микрофон и акустические системы, подключается к IP-сети или к сети Интернет, и с другой стороны шлюз IP-телефонии имеет соединение через АТС с обычным телефонным аппаратом.
3. «От компьютера к компьютеру». В этом случае соединение устанавливается через IP-сеть между двумя мультимедийными компьютерами, оборудованными аппаратными или программными средствами для работы с IP-телефонией.

4. «От WEB браузера к телефону». С развитием сети Интернет стал возможен доступ и к речевым услугам. Например, на WEB странице некоторой компании в разделе «Контакты» размещается кнопка «Вызов», нажав на которую можно осуществить речевое соединение с представителем данной компании без набора телефонного номера. Стоимость такого звонка для вызывающего пользователя входит в стоимость работы в сети Интернет [2].

Следует отметить, что в соединениях 1 и 2 типов вместо телефонных аппаратов могут быть включены факсимильные аппараты, и в этом случае сеть IP-телефонии должна обеспечивать передачу факсимильных сообщений.

Описание основных протоколов систем IP-телефонии

Стандарт H.323

Набор рекомендаций МСЭ-Т H.323 определяет сетевые компоненты, протоколы и процедуры, позволяющие организовать мультимедиа-связь в пакетных сетях, в том числе в ЛВС Ethernet. Они определяют порядок функционирования абонентских терминалов в сетях с разделяемым ресурсом, не гарантирующих качества обслуживания QoS. H.323-совместимые устройства могут применяться для телефонной связи (IP-телефония), передачи звука и видео (видеотелефония), а также звука, видео и данных (мультимедийные конференции).

В связи с появлением множества аппаратно-программных средств организации телефонной связи по протоколу IP потребовалось внести изменения в спецификации H.323, так как эти средства зачастую оказывались несовместимыми друг с другом. В частности, понадобилось обеспечить взаимодействие телефонных устройств на базе ПК и обычных телефонов для сетей, функционирующих по принципу коммутации каналов. Стандарт H.323 входит в семейство рекомендаций H.32x, описывающих порядок организации мультимедиа-связи в сетях различных типов:

- H.320 - узкополосные цифровые коммутируемые сети, включая -ISDN;
- H.321 - широкополосные сети ISDN и ATM;
- H.322 - пакетные сети с гарантированной полосой пропускания;
- H.324 - телефонные сети общего пользования (ТфОП).

Одна из основных целей разработки стандарта H.323 - обеспечение взаимодействия с другими типами сетей мультимедиа-связи (рисунок 1). Данная задача реализуется с помощью шлюзов, осуществляющих трансляцию сигнализации и форматов данных. Стандарт H.323 позволяет создать надежные решения для организации коммуникаций по ненадежным сетям с переменной задержкой. При условии соответствия стандарту устройства с различными возможностями могут и взаимодействовать друг с другом. Например, терминалы с видеосредствами могут участвовать в аудиоконференции. В совокупности с другими стандартами МСЭ-Т на мультимедийную связь и телеконференции рекомендации H.323 применимы для любых видов соединений - от многоточечных до соединений «точка-точка». [1]. Основные компоненты этого стандарта приведены в таблица 2.

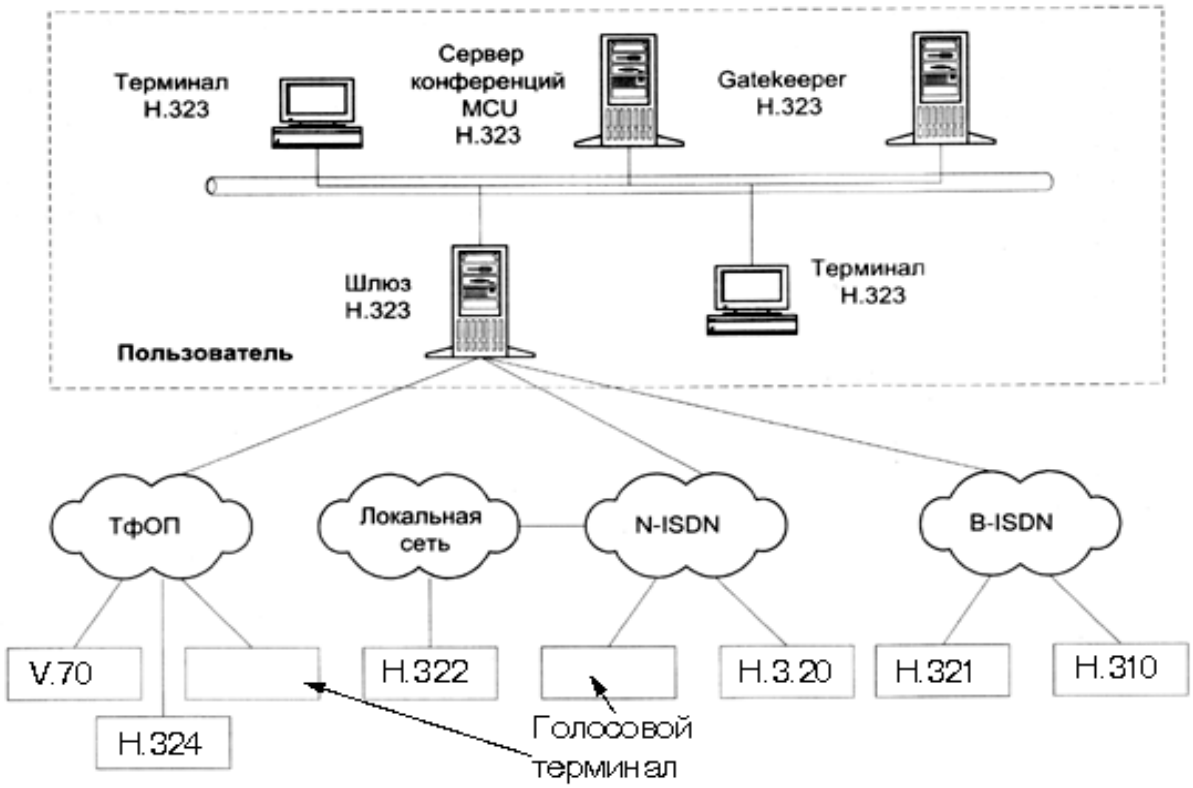


Рис. 2. Конфигурация сети на базе стандарта H.323

Стандарт H. 323 определяет также порядок взаимодействия с оконечными устройствами других стандартов. Наиболее часто такая задача возникает при сопряжении телефонных сетей с коммутацией пакетов и коммутацией каналов. Сети стандарта H.323 совместимы и с другими типами H.32x-сетей. Межсетевое взаимодействие различных H.32x-сетей определяет рекомендация H.246. На следующем этапе развития IP-телефонии к спецификациям H.323, соответствующим нижним уровням эталонной модели взаимодействия открытых систем (ЭМВОС), будут добавлены новые. Они зафиксируют возможности обеспечения классов (class-of-service, CoS) и качества обслуживания (quality-of-service, QoS), т. е. услуг, относящихся, соответственно, ко второму (канальному) и третьему (сетевому) уровням [1].

Таблица 2. Основные компоненты стандарта H.323

Рекомендация	Описание
H.225	Определяет сообщения по управлению вызовом, включая сигнализацию и регистрацию, а также пакетизацию и синхронизацию потоков мультимедийных данных
H.245	Определяет сообщения для открытия и закрытия каналов для передачи потоков мультимедийных данных, а также другие команды и запросы
H.261	Видеокодек для аудиовизуальных сервисов на каналах P x 64 кбит/с
H.263	Описывает новый видеокодек для передачи видео по обычным телефонным сетям
G.711	Аудио кодек, 3,1 кГц на 48, 56, и 64 кбит/с

G.722	Аудио кодек, 7 кГц на 48, 56, и 64 кбит/с
G.728	Аудио кодек, 3,1 кГц на 16 кбит/с
G.723	Аудио кодек, для режимов 5,3 и 6,3 кбит/с
G.729	Аудио кодек

Архитектура системы на базе стандарта H.323

Стандарт H.323 разработан Сектором стандартизации телекоммуникаций Международного союза электросвязи (МСЭ-Т) и содержит описание терминальных устройств, оборудования и сетевых служб, предназначенных для осуществления мультимедийной связи в сетях с коммутацией пакетов. Терминальные устройства и сетевое оборудование стандарта H.323 могут передавать данные, речь и видеоинформацию в масштабе реального времени. В стандарте H.323 не определены: сетевой интерфейс, физическая среда передачи информации и транспортный протокол, используемый в сети. Сеть, через которую осуществляется связь между терминалами H.323, может представлять собой сегмент или множество сегментов со сложной топологией. Терминалы H.323 могут быть интегрированы в персональные компьютеры или реализованы как автономные устройства. Поддержка речевого обмена – обязательная функция для устройства стандарта H.323.

В рекомендации H.323 описываются четыре основных компонента:

- терминал;
- привратник;
- шлюз;
- устройство управления конференциями.

Все перечисленные компоненты реализованы в так называемые зоны H.323. Одна зона состоит из привратника и нескольких конечных точек, причем привратник управляет всеми конечными точками своей зоны. Для обеспечения большей надежности одну "зону" могут обслуживать несколько привратников, тогда один из них называется "главным", а остальные - "альтернативными". Зоной может быть и вся сеть поставщика услуг IP-телефонии или ее часть, охватывающая отдельный регион [3].

Терминалы H.23

Терминал представляет собой оконечное устройство пользователя сети IP-телефонии, которое обеспечивает двустороннюю речевую (мультимедийную связь) с другим терминалом H.323, шлюзом или устройством управления конференциями.

Шлюзы H.323

Шлюз IP-телефонии реализует передачу речевого трафика по сетям с маршрутизацией пакетов IP по протоколу H.323. Основное назначение шлюза – преобразование речевой информации, поступающей со стороны ТфОП, в вид, пригодный для передачи по сетям с маршрутизацией пакетов IP. Кроме того, шлюз преобразует сигнальные сообщения систем сигнализации DSS1 и ОКС7 в сигнальные сообщения H.323 и производит обратное преобразование в соответствии с рекомендацией ITU H.246.

Привратник

Основной управляющий элемент сети H.323, координирующий и контролирующий работу всех ее устройств. Привратник выполняет следующие функции:

- преобразовывает адреса-псевдонимы в транспортные адреса;
- контролирует доступ в сеть на основании авторизации вызовов;
- контролирует полосу пропускания;
- управляет зонами.

Причем привратник осуществляет вышеперечисленные функции в отношении терминалов, шлюзов и устройств управления, зарегистрированных в нем. Помимо управления и

централизованного разрешения имен абонентов, привратники также могут предоставлять дополнительные возможности, например, выполнять функции прокси-сервера для сигнальных и медиаданных.

Устройство управления конференциями (MCU)

Устройство управления конференциями состоит из одного обязательного элемента – контроллера конференций (MCU – Multipoint Control Unit), и, кроме того, может включать в себя один или более процессоров для обработки пользовательской информации. Контроллер может быть физически совмещен с привратником, шлюзом или устройством управления конференциями, а последнее, в свою очередь, может быть совмещено со шлюзом или привратником.

Устройство управления конференциями обеспечивает возможность организации связи между тремя или более участниками. Рекомендация H.323 предусматривает три вида конференции: децентрализованная, централизованная и смешанная.

Первый тип требует, чтобы все участники конференции пересылали многоадресные (групповые) сообщения всем остальным. Для этого требуется более сложное терминальное оборудование, и управлять такой конференцией не очень удобно. Большинство производителей предлагают централизованные системы. При их использовании конечные узлы передают сигнал системе MCU, которая и обеспечивает его рассылку.

Все терминалы, участвующие в конференции, устанавливают соединение с MCU. Сервер управляет ресурсами конференции, согласовывает возможности терминалов по обработке звука и видео, определяет аудио- и видеопотоки, которые необходимо направлять по многим адресам.

Сигнализация по стандарту H.323

Для обеспечения широкомасштабного внедрения IP-телефонии одним из самых важных факторов является обеспечение совместимости систем разных фирм. Достижение совместимости возможно только на базе стандартных протоколов сигнализации. Протоколы сигнализации обеспечивают установление, администрирование и завершение сеанса связи между конечными точками (пользователями), однозначно идентифицируемыми заданной схемой адресации. Понятие «сигнализация» относится ко всей информации, связанной с вызовами и необходимой для их установления, маршрутизации, мониторинга и завершения, как на физическом, так и на логическом уровне [1].

В традиционной телефонии вызывающий пользователь набирает номер нужного ему абонента, а телефонная сеть использует его для маршрутизации вызова. Процедура управления вызовами делится на три фазы: установление соединения, передача речи и данных и разъединение. Сообщения системы сигнализации инициируют и завершают эти фазы, а стандартные контрольные сигналы и (или) записанные голосовые сообщения информируют абонента о характере прохождения его вызова.

Во всех современных сетях с коммутацией каналов система сигнализации основана на семействе ОКС №7. Они обеспечивают обмен сообщениями, которые необходимы для маршрутизации вызовов, резервирования ресурсов, трансляции адресов, установления соединений, управления ими, выставления счетов. Кроме того, на Взаимоувязанной сети связи Российской Федерации используется еще много других систем сигнализации (аналоговых и цифровых).

По сравнению с сигнализацией в обычных телефонных сетях сигнализация IP-телефонии должна обладать более широкими возможностями в силу специфики конечных узлов. Они могут иметь самые разные характеристики в части требуемой полосы пропускания, кодирования/декодирования аудиосигналов, передачи данных и т.д., и для установления сеанса связи между ними необходимо убедиться в совместимости этих характеристик.

Еще один важный вопрос, связанный с сигнализацией в IP-телефонии – контроль доступа к сети. В обычной телефонной сети общего пользования (ТФОП) абонент подключается к АТС

через фиксированный местный шлейф, поэтому идентифицировать его телефонный аппарат очень просто. В сети IP-телефонии все гораздо сложнее, поскольку существует множество разных способов доступа к ней: с обычного телефона через ТФОП, по модемному соединению через сервер удаленного доступа, через ЛВС и территориально распределенную сеть и т.д. Кроме этого, пользователи могут перемещаться между различными сетями, таким образом, абонента нельзя идентифицировать по используемой им линии доступа.

Для эффективного контроля доступа оператор должен аутентифицировать каждого пользователя, запрашивающего услугу. С увеличением числа операторов IP-телефонии требуются также средства контроля над трафиком на границе между их сетями. Такие средства должны осуществлять контроль доступа и использованием сетевых ресурсов и выполнением соглашений по качеству обслуживания. При их отсутствии оператору может оказаться проблематичным гарантировать пользователю определенный класс обслуживания, если его трафик частично проходит через сеть другого оператора.

Рекомендация Международного союза электросвязи (МСЭ-Т) H.323 определяет основы процесса передачи аудио, видео и данных по сетям с коммутацией пакетов, например по сетям IP. В ней описаны объекты, необходимые для мультимедийной связи, их функции и способы взаимодействия, в частности алгоритмы формирования пакетов, сжатия аудио- и видеоинформации. Кроме того, рекомендация H.323 нацелена на решение задач администрирования конечных пользователей, адресации, контроля над использованием полосы пропускания сети и сетевых объектов [3].

Семейство протоколов H.323 включает в себя три основных протокола:

- протокол RAS (Registration, Admission, Status) – протокол взаимодействия оконечного оборудования с привратником;
- протокол H.225 – протокол управления соединениями;
- протокол управления логическими каналами H.245.

Для переноса сигнальных сообщений H.225 и управляющих сообщений H.245 используется протокол с установление соединения и с гарантированной доставкой информации – TCP. Сигнальные сообщения RAS переносятся с протоколом с негарантированной доставкой информации – UDP. Для переноса речевой и видеоинформации используется протокол передачи информации в реальном времени – RTP. Контроль переноса пользовательской информации производится протоколом RTCP.

Протокол RAS – этот протокол применяется для передачи служебных сообщений между терминалами и контроллером зоны (привратником) H.323. RAS-сообщения служат для регистрации терминалов, допуска их к сеансу связи, изменения используемой полосы пропускания, информирования о состоянии сеанса и его прекращении. В отсутствии привратника протокол RAS не задействуется.

С помощью сигнализации RAS должно осуществляться:

- нахождение привратника, на котором возможна регистрация оконечного оборудования;
- регистрация оконечного устройства у привратника;
- контроль доступа оконечного оборудования к сетевым ресурсам;
- определение местоположения оконечного оборудования в сети;
- изменение полосы пропускания в процессе обслуживания вызова;
- опрос и индикация текущего состояния оконечного оборудования;
- оповещение привратника об освобождении полосы пропускания, ранее занимавшейся оборудованием.

Выполнение первых трех процедур, предусмотренных протоколом RAS, является начальной фазой установления соединения с использованием сигнализации H.323. Далее следует фаза сигнализации H.225.0 (Q.931) и обмен управляющими сообщениями H.245.

Разъединение происходит в обратной последовательности: в первую очередь закрывается управляющий канал H.245 и сигнальный канал H.225.0, после чего по каналу RAS, после чего по каналу RAS привратник оповещается об освобождении ранее занимавшейся оконечным оборудованием полосы пропускания.

Для переноса сообщений протокола RAS используется протокол негарантированной доставки информации UDP. В связи с этим ITU-T рекомендовал передавать повторно те сообщения RAS, получение которых не было подтверждено в течение установленного промежутка времени. Оконечное оборудование или привратник, не имеющие возможности в текущий момент времени ответить на полученный запрос, могуи передавать сообщения RIP (Request in Progress) для индикации того, что запрос находится в стадии обработки. При приеме сообщения RIP привратник и оконечное оборудование должны перезапустить свои таймеры.

Важно отметить, что в сети без привратника сигнальный канал RAS вообще не используется.

Сигнальный канал H.225.0 – рекомендация, в которой международным союзом электросвязи специфицированы процедуры управления соединениями в сетях H.323. Данные процедуры предусматривают использование в базовом процессе обслуживания вызова ряда сигнальных сообщений Q.931, причем должен быть реализован симметричный обмен сигнальными сообщениями. Это требование не распространяется на взаимодействие шлюза с сетью с коммутацией каналов.

Транспортировку сигнальных сообщений обеспечивает протокол TCP. В соответствии с рекомендацией H.323 для каждого нового вызова открывается отдельный сигнальный канал. В сетях, не имеющих привратника, открывается сигнальный канал H.225.0, непосредственно связывающий вызывающее оконечное оборудование с вызываемым. В этом случае вызывающий пользователь должен знать транспортный адрес сигнального канала оборудования вызываемого пользователя.

Ниже приведены наиболее часто используемые сигнальные сообщения:

- Сообщение Setup передается вызывающим оборудованием с целью установить соединение.
- Сообщение Call Proceeding передается вызывающему оборудованию, чтобы известить его о том, что вызов принят к обслуживанию.
- Сообщение Alerting передается вызывающему оборудованию и информирует его о том, что вызываемое оборудование не занято и что пользователю подается сигнал о входящем вызове.
- Сообщение Connect передается вызывающему оборудованию и информирует его о том, что вызываемый пользователь принял входящий вызов. Сообщение Connect может содержать транспортный адрес управляющего канала H.245.
- Сообщение Release Complete передается вызывающим или вызываемым оборудованием с целью завершить соединение. Это сообщение передается только в том случае, когда открыт сигнальный канал.
- Сообщение Q.932 Facility используется для обращения к дополнительным услугам в соответствии с Рекомендациями ITU H.450.x.

Управляющий канал H.245

В рекомендации ITU-T H.245 определен ряд независимых процедур, которые должны выполняться для управления информационными каналами. К ним относятся процедуры:

- определения ведущего и ведомого устройств;
- обмена данными о функциональных возможностях
- открытия и закрытия однонаправленных логических каналов
- открытия и закрытия двунаправленных логических каналов

- закрытия логических каналов
- определения задержки, возникающей при передаче информации от источника к приемнику и в обратном направлении
- выбора режима обработки информации
- сигнализации по петле, создаваемой для целей технического обслуживания оборудования

Для выполнения вышеуказанных процедур между оконечными устройствами или между оконечным оборудованием и устройством управления конференциями или привратником организуется управляющий канал H.245. При этом оконечное оборудование должно открывать один (и только один) управляющий канал для каждого соединения, в котором оно участвует. Терминалы, устройства управления конференциями, шлюзы и привратники могут участвовать одновременно в нескольких соединениях и, следовательно, открывать несколько управляющих каналов.

Перенос управляющей информации H.245 осуществляется протоколом TCP по нулевому логическому каналу, который должен быть постоянно открытым с момента организации канала H.245 и вплоть до его ликвидации. Следует отметить, что нормальные процедуры открытия и закрытия логических каналов, для управления нулевым логическим каналом не применяются.

По управляющему каналу H.245 передаются сообщения четырех категорий: запросы, ответы, команды и индикации. Получив сообщение-запрос, оборудование должно выполнить определенное действие и немедленно передать обратно сообщение-ответ. Получив сообщение-команду, оборудование также должно выполнить определенное действие, но отвечать на команду не должно. Сообщение-индикация служить для того, чтобы информировать о чем-либо получателя, но не требует от него ни ответа, ни каких бы то ни было действий.

Протокол инициирования сеансов связи – SIP

Принципы протокола SIP

За годы работы с протоколом H.323 накоплен большой опыт использования, который позволил выявить как его положительные черты, так и недостатки, которые были учтены при разработке протокола SIP.

Протокол инициирования сеансов – Session Initiation Protocol (SIP) является протоколом прикладного уровня и предназначается для организации, модификации и завершения сеансов связи: мультимедийных конференций, телефонных соединений и передачи данных. Пользователи могут принимать участие в существующих сеансах связи, приглашать других пользователей и быть приглашенными ими к новому сеансу связи. Приглашения могут быть адресованы определенному пользователю, группе пользователей или всем пользователям [3].
Протокол SIP разработан группой MMUSIC (Multiparty Multimedia Session Control) комитета IETF (Internet Engineering Task Force), а спецификации протокола представлены в документе RFC 2543. В основу протокола рабочая группа MMUSIC заложила следующие принципы:

- *Персональная мобильность пользователей.*
  Пользователи могут перемещаться без ограничений в пределах сети, поэтому услуги связи должны предоставляться им в любом месте этой сети. Пользователю присваивается уникальный идентификатор, а сеть предоставляет ему услуги связи вне зависимости от того, где он находится. Для этого пользователь с помощью специального сообщения – REGISTER – информирует о своих перемещениях сервер определения местоположения.
- *Масштабируемость сети.*
  Она характеризуется, в первую очередь, возможностью увеличения количества элементов сети при ее расширении. Серверная структура сети, построенной на базе протокола SIP, в полной мере отвечает этому требованию.

- *Расширяемость протокола.*
  Она характеризуется возможностью дополнения протокола новыми функциями при введении новых услуг и его адаптации к работе с различными приложениями.
  Расширение функций протокола SIP может быть произведено за счет введения новых заголовков сообщений. При этом, если SIP-серевер принимает сообщения с неизвестными ему полями, то он просто игнорирует их и обрабатывает лишь те поля, которые он знает.
  Для расширения возможностей протокола SIP могут быть также добавлены и новые типы сообщений.
- *Интеграция в стек существующих протоколов Internet, разработанных IETF.*
  Протокол SIP является частью глобальной архитектуры мультимедиа, разработанной комитетом IETF. Эта архитектура включает в себя также протокол резервирования ресурсов (Resource Reservation Protocol - RSVP), транспортный протокол реального времени (Real-Time Transport Protocol - RTP), протокол передачи потоковой информации в реальном времени (Real-Time Streaming Protocol - RTSP). Однако функции протокола SIP не зависят ни от одного из этих протоколов.
- *Взаимодействие с другими протоколами сигнализации.*
  Протокол SIP может быть использован совместно с протоколом H.323. Возможно даже взаимодействие протокола SIP с системами сигнализации ТфОП – DSS1 и ОКС7. Для упрощения такого взаимодействия сигнальные сообщения протокола SIP могут переносить не только специфический SIP-адрес, но и телефонный номер формата E.164 или любого другого формата [6].

Интеграция протокола SIP с IP-сетями

Одной из важнейших особенностей протокола SIP является его независимость от транспортных технологий. Но, в то же время, предпочтение отдается технологии маршрутизации пакетов IP и протоколу UDP. При этом, правда, необходимо создать дополнительные механизмы для надежной доставки сигнальной информации. К таким механизмам относятся повторная передача информации при ее потере, подтверждение приема и др.

Здесь же следует отметить то, что сигнальные сообщения могут переноситься не только протоколом транспортного уровня UDP, но и протоколом TCP. Протокол UDP позволяет быстрее, чем TCP, доставлять сигнальную информацию (даже с учетом повторной передачи неподтвержденных сообщений), а также вести параллельный поиск местоположения пользователей и передавать приглашения к участию в сеансе связи в режиме многоадресной рассылки.

По сети с маршрутизацией пакетов IP может передаваться пользовательская информация практически любого вида: речь, видео и данные, а также любая их комбинация, называемая мультимедийной информацией. При организации связи между терминалами пользователей необходим механизм обмена информацией о том, какие сервисы может использовать вызываемая\вызывающая стороны. Для этой цели используется протокол SDP (Session Description Protocol) - протокол описания сессии. Данный протокол позволяет определить, какие звуковые (видео и другие) кодеки и иные возможности может использовать удаленная сторона.

Для передачи речевой информации комитет IETF предлагает использовать протокол RTP (Real-time Transport Protocol, протокол транспортировки в реальном времени). Таким образом, сам протокол SIP непосредственного участия в передаче голосовых, видео и других данных не принимает, он отвечает только за установление связи (по протоколам SDP, RTP и др.), поэтому под SIP-телефонией понимается не передача голоса по протоколу SIP, а передача голоса с использованием протокола SIP. Использование протокола SIP предоставляет новые

возможности установления соединений (а также возможность беспроблемного расширения данных возможностей), а не непосредственной передачи голосового и других видов трафика.

В глобальной информационной сети Интернет уже довольно давно функционирует экспериментальный участок Mbone, который образован из сетевых узлов, поддерживающих режим многоадресной рассылки мультимедийной информации. Важнейшей функцией Mbone является поддержка мультимедийных конференций, а основным способом приглашения участников к конференции стал протокол SIP. Протокол SIP дает возможность присоединения новых участников к уже существующему сеансу связи, т.е двусторонний сеанс может перейти в конференцию.

Предназначенный для инициации сеансов протокол SIP обеспечивает определение адреса пользователя и установления соединения с ним. Кроме этого, он служит основой для применения других протоколов, реализующих функции защиты, аутентификации, описания канала мультимедийной связи и т.д. [3].

Адресация

Для взаимодействия между собой приложения используют SIP адрес, очень напоминающий адрес электронной почты (SIP URL) . Адреса SIP имеют только UA. Все остальные компоненты (Proxy, Redirect, Registrar) идентифицируются только IP адресами и номерами портов (например, по умолчанию SIP сервер использует 5060 порт).

Синтаксис SIP адреса следующий:
sip:userid@hostname, где userid - username или e.164 адрес (телефонный номер), hostname - домен, хост или IP адрес.

Кроме того, в SIP адрес могут входить дополнительные параметры (пароли, номера портов и тому подобное).

Архитектура сети SIP

SIP использует обычные текстовые сообщения и очень напоминает HTTP протокол (практически базируется на нем). Архитектура сети SIP базируется на клиент-серверном взаимодействии.

Стандартными элементами в SIP-сети являются:

1. User Agent: по протоколу SIP устанавливаются соединения "клиент-сервер". Клиент устанавливает соединения, а сервер принимает вызовы, но так обычно телефонный аппарат (или программный телефон) может как устанавливать, так и принимать звонки, то получается что он одновременно играет роль и клиента и сервера (хотя в реализации протокола это не является обязательным критерием) - в этом случае его называют User Agent (UA) или терминал.

В составе UA выделяются две логические составляющие:

- агент-клиент (UAC - user agent client) - посылает запросы и получает ответы;
- агент-сервер (UAS - user agent server) - принимает запросы и посылает ответы.

Ввиду того, что большинству устройств необходимо как передавать, так и принимать данные, в реальных устройствах присутствует как UAC, так и UAS.

2. Прокси-сервер: прокси-сервер принимает запросы и производит с ним некоторые действия (например, определяет местоположение клиента, производит переадресацию или перенаправление вызова и др.). Он также может устанавливать собственные соединения. Зачастую прокси-сервер совмещают с сервером определения местоположения (Register-сервер), в таком случае его называют Registrar-сервером.

3. Сервер определения местоположения или сервер регистрации (Register): данный вид сервера служит для регистрации пользователей. Регистрация пользователя производится для определения его текущего IP-адреса, для того чтобы можно было произвести вызов user@IP-адрес. В случае если пользователь переместится в другое место и/или не имеет определенного

IP-адреса, его текущий адрес можно будет определить после того, как он зарегистрируется на сервере регистрации. Таким образом, клиент останется доступен по одному и тому же SIP-адресу вне зависимости от того, где на самом деле находится.

4. Сервер переадресации: обращается к серверу регистрации для определения текущего IP-адреса пользователя, но в отличие от прокси-сервера только "переадресует" клиента, а не устанавливает собственные соединения [7].

В результате SIP архитектура выглядит следующим образом:

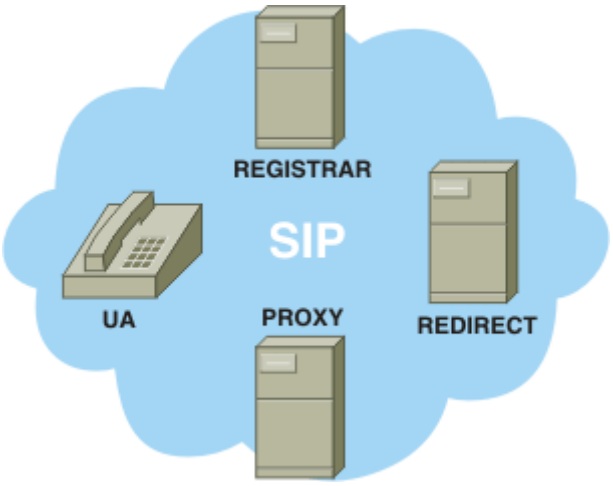


Рис. 3. Архитектура сети на базе протокола SIP

Сигнализация на основе протокола SIP

При организации мультимедийного сеанса используется два основных метода для нахождения и информирования заинтересованных участников:

- Уведомление о сеансе с использованием разных средств – электронной почты, новостных групп, WEB-страниц или специального протокола SAP (Session Announcement Protocol);
- Приглашение к участию в сеансе с помощью протокола SIP.

Ниже приведена на рисунке 4.8 схема сигнализации по протоколу SIP.

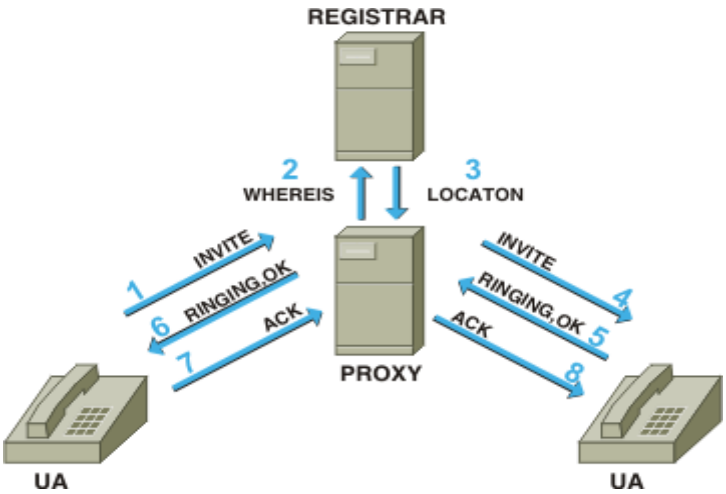


Рис. 4. Схема сигнализации по протоколу SIP

Обработка вызовов осуществляется сервером SIP, который может работать в режиме непосредственного установления связи или в режиме переадресации. В обоих режимах сервер принимает запросы на определение местоположения нужного пользователя, но если в первом режиме он сам доводит вызов до адресата, то во втором – возвращает адрес конечного пункта запрашиваемому клиенту [7].

В протоколе SIP определены два вида сигнальных сообщений – запрос и ответ.

Они имеют текстовый формат (кодировка символов согласно RFC 2279) и базируются на протоколе HTTP. В запросе указываются процедуры, вызываемые для выполнения требуемых операций, а в ответе – результаты их выполнения. Определены шесть процедур:

- INVITE - вызывает адресата для установления связи. С помощью этого сообщения адресату передаются виды поддерживаемых сервисов (которые могут быть использованы инициатором сеанса), а также виды сервисов, которые желает передавать инициатор связи;
- ACK - сообщение, подтверждающее согласие адресата установить соединения. В этом сообщении могут быть переданы окончательные параметры сеанса связи (окончательно выбираются виды сервисов и их параметры которые будут использованы);
- Cancel – прекращает поиск пользователя;
- BYE - запрос завершения соединения;
- Register - данным запросом пользователь идентифицирует свое текущее местоположение;
- OPTIONS - запрос информации о функциональных возможностях терминала (применяется в случае, если эти данные нужно получить до установления соединения, то есть до фактического обмена данной информацией с помощью запросов INVITE и ACK).

Вызывающий UA должен знать постоянный адрес абонента, а прокси-сервер осуществит поиск и приглашение к сеансу связи. Текущий адрес знать не обязательно. Кроме того, UA должен предварительно выяснить IP адрес прокси-сервера (например заданный в конфигурации). Также может осуществляться взаимодействие непосредственно между клиентскими приложениями (UA) без участия серверов. Для этого вызывающий UA должен знать текущий адрес вызываемого абонента.

Протокол управления шлюзами – MGCP

Рабочая группа MEGACO комитета IETF разработала протокол управления шлюзами - Media Gateway Control Protocol (MGCP). При разработке протокола рабочая группа MEGACO опиралась на принцип декомпозиции, согласно которому шлюз разбивается на отдельные функциональные блоки:

- транспортный шлюз - Media Gateway, который выполняет функции преобразования речевой информации, поступающей со стороны ТфОП с постоянной скоростью, в вид, пригодный для передачи по сетям с маршрутизацией пакетов IP: кодирование и упаковку речевой информации в пакеты RTP/UDP/IP, а также обратное преобразование;
- устройство управления - Call Agent, выполняющее функции управления шлюзом;
- шлюз сигнализации - Signaling Gateway, который обеспечивает доставку сигнальной информации, поступающей со стороны ТфОП, к устройству управления шлюзом и перенос сигнальной информации в обратном направлении.

Таким образом, весь интеллект функционально распределенного шлюза размещается в устройстве управления, функции которого, в свою очередь, могут быть распределены между несколькими компьютерными платформами. Шлюз сигнализации выполняет функции STP - транзитного пункта системы сигнализации по общему каналу - ОКС7. Транспортные шлюзы

выполняют только функции преобразования речевой информации. Одно устройство управления обслуживает одновременно несколько шлюзов. В сети может присутствовать несколько устройств управления. Предполагается, что эти устройства синхронизованы между собой и согласованно управляют шлюзами, участвующими в соединении.

Одно из основных требований, предъявляемых к протоколу MGCP, состоит в том, что устройства, реализующие этот протокол, должны работать в режиме без сохранения информации о последовательности транзакций между устройством управления и транспортным шлюзом, т.е. в устройствах не требуется реализации конечного автомата для описания этой последовательности. Однако это не относится к последовательности состояний соединений, сведения о которых хранятся в устройстве управления. Протокол MGCP использует принцип master/slave (ведущий/ведомый), причем устройство управления шлюзами является ведущим, а транспортный шлюз - ведомым устройством, выполняющим команды, поступающие от устройства управления. Такое решение обеспечивает масштабируемость сети и простоту эксплуатационного управления этой сетью через устройство управления шлюзами.

Основной недостаток этого подхода - незаконченность стандартов. Функциональные блоки распределенных шлюзов, разработанные разными фирмами-производителями телекоммуникационного оборудования, практически несовместимы. Функции устройства управления шлюзами точно не определены. Не стандартизированы механизмы переноса сигнальной информации от шлюза сигнализации (Signalling Gateway) к устройству управления и в обратном направлении. К недостаткам можно отнести также отсутствие стандартизированного протокола взаимодействия между устройствами управления. Кроме того, протокол MGCP, являясь протоколом управления шлюзами, не предназначен для управления соединениями с участием терминального оборудования пользователей (IP-телефонами). Это означает, что в сети, построенной на базе протокола MGCP, для управления терминалами должен присутствовать привратник или сервер SIP [3].

Обеспечение качества IP-телефонии

Показатели качества IP-телефонии

Традиционные телефонные сети коммутируют электрические сигналы с гарантированной полосой пропускания, достаточной для передачи сигналов голосового спектра. При фиксированной пропускной способности передаваемого сигнала цена единицы времени связи зависит от удаленности и расположения точек вызова и места ответа.

Сети с коммутацией пакетов не обеспечивают гарантированной пропускной способности, поскольку не обеспечивают гарантированного пути между точками связи.

IP-телефония является одной из областей передачи данных, где важна динамика передачи сигнала, которая обеспечивается современными методами кодирования и передачи информации, а также увеличением пропускной способности каналов, что приводит к возможности успешной конкуренции IP-телефонии с традиционными телефонными сетями [1].

Основными составляющими качества IP-телефонии являются:

- Качество речи, которое включает:
  - *диалог* – возможность пользователя связываться и разговаривать с другим пользователем в реальном времени и полнодуплексном режиме;
  - *разборчивость* – чистота и тональность речи;
  - *эхо* – слышимость собственной речи;
  - *уровень* – громкость речи.
- Качество сигнализации, включающее:
  - *установление вызова* – скорость успешного доступа и время установления соединения;

- *завершение вызова* – время отбоя и скорость разъединения;
- *DTMF* – определение и фиксация сигналов многочастотного набора номера.

Факторы, которые влияют на качество IP-телефонии, могут быть разделены на две категории:

- Факторы качества IP- сети:
  - *максимальная пропускная способность* – максимальное количество полезных и избыточных данных, которая она передает;
  - *задержка* – промежуток времени, требуемый для передачи пакета через сеть;
  - *джиттер* - задержка между двумя последовательными пакетами;
  - *потеря пакета* – пакеты или данные, потерянные при передачи через сеть.
- Факторы качества шлюза:

- *требуемая полоса пропускания* - различные кодеки требуют различную полосу. Например, кодек G.723 требует полосы 16,3 кбит/с для каждого речевого канала;
- *задержка* - время, необходимое цифровому сигнальному процессору DSP или другим устройствам обработки для кодирования и декодирования речевого сигнала;
- *буфер джиттера* - сохранение пакетов данных до тех пор, пока все пакеты не будут получены, и можно будет передать в требуемой последовательности для минимизации джиттера;
- *потеря пакетов* - потеря пакетов при сжатии и/или передаче в оборудовании IP-телефонии;
- *подавление эхо* — механизм для подавления эхо, возникающего при передаче по сети;
- *управление уровнем* - возможность регулировать громкость речи.

Влияние сети на показатели качества IP-телефонии

Задержка

Задержка создает неудобство при ведении диалога, приводит к перекрытию разговоров и возникновению эхо. Эхо возникает в случае, когда отраженный речевой сигнал вместе с сигналом от удаленного конца возвращается опять в ухо говорящего. Эхо становится трудной проблемой, когда задержка в петле передачи больше, чем 50 мс. Так как эхо является проблемой качества, системы с пакетной коммутацией речи должны иметь возможность управлять эхо и использовать эффективные методы эхоподавления.

Затруднение диалога и перекрытие разговоров становятся серьезным вопросом качества, когда задержка в одном направлении передачи превышает 250 мс. Можно выделить следующие источники задержки при пакетной передаче речи из конца в конец. [1]

- Задержка накопления (иногда называется алгоритмической задержкой): эта задержка обусловлена необходимостью сбора кадра речевых отсчетов, выполняемая в речевом кодере. Величина задержки определяется типом речевого кодера и изменяется от небольших величин (0,125 мкс) до нескольких миллисекунд. Например, стандартные речевые кодеры имеют следующие длительности кадров:
  G.729 CS-ACELP (8 кбит/с) – 10 мс
  G.723.1 – Multi Rate Coder (5,3; 6,3 кбит/с) – 30 мс.
- Задержка обработки: процесс кодирования и сбора закодированных отсчетов в пакеты для передачи через пакетную сеть создает определенные задержки. Задержка кодирования или обработки зависит от времени работы процессора и используемого типа алгоритма обработки.
- Сетевая задержка: задержка обусловлена физической средой и протоколами, используемыми для передачи речевых данных, а также буферами, используемыми для удаления джиггера пакетов на приемном конце. Сетевая задержка зависит от емкости сети и процессов передачи пакетов в сети.

Время задержки при передачи речевого сигнала можно отнести к одному из трех уровней:

- первый уровень до 200 мс – отличное качество связи. Для сравнения, в телефонной сети общего пользования допустимы задержки до 150-200 мс;
- второй уровень до 400 мс – считается хорошим качеством связи. Но если сравнивать с качеством связи по сетям ТФОП, то разница будет видна. Если задержка постоянно удерживается на верхней границе 2-го уровня (на 400 мс), то не рекомендуется использовать эту связь для деловых переговоров;
- третий уровень до 700 мс – считается приемлемым качеством связи для ведения неделовых переговоров. Такое качество связи возможно также при передаче пакетов по спутниковой связи.

Качество Интернет-телефонии попадает под 2-3 уровни, провайдеры IP-телефонии, работающие по выделенным каналам попадают под 1-2 уровни. Также необходимо учитывать задержки при кодировании/декодировании голосового сигнала. Средние суммарные задержки при использовании IP-телефонии обычно находятся в пределах 150-250 мс.

Джиттер

Когда речь или данные разбиваются на пакеты для передачи речи через IP-сеть, пакеты часто прибывают в пункт назначения в различное время и в разной последовательности. Это создает разброс времени доставки пакетов (джиттер). Джиттер приводит к специфическим нарушениям передачи речи, слышимым как трески и щелчки.

Для того, чтобы компенсировать влияние джиттера, в терминалах используется так называемый джиттер-буфер. Этот буфер хранит в памяти прибывшие пакеты в течение времени, определяемого ее емкостью (длиной). Пакеты, прибывшие слишком поздно, когда буфер заполнен, отбрасываются. Интервалы между пакетами восстанавливаются на основе значений временных меток RTP-пакетов. В функции джиттер-буфера входит и восстановление исходной очередности следования пакетов, если при транспортировки по сети они оказались «перепутаны».

Слишком короткий буфер будет приводить к слишком частым потерям «опоздавших» пакетов, а слишком длинный – к неприемлемо большой дополнительной задержке. Обычно предусматривается динамическая подстройка длины буфера в течение всего времени существования соединения [3].

Потеря пакетов

Потерянные пакеты в IP-телефонии нарушают речь и создают искажения тембра. В существующих IP-сетях все голосовые данные. При пиковых нагрузках и перегрузках голосовые кадры будут отбрасываться, как и кадры данных. Однако кадры данных не связаны со временем, и отброшенные пакеты могут быть успешно переданы путем повторения. Потеря голосовых пакетов, в свою очередь, не может быть восполнена таким способом и в результате произойдет неполная передача информации. Предполагается, что потеря до 5% пакетов незаметна, а свыше 10-15% - недопустима. Причем данные величины существенно зависят от алгоритмов компрессии/декомпрессии [1].

Существенно, что потеря большой группы пакетов приводит к необратимым локальным искажениям речи, тогда как потери одного, двух, трех пакетов можно пытаться компенсировать.

Взаимосвязь методов обеспечения качества IP-телефонии, показателей качества сети и качества вызова представлена на рисунке 5.

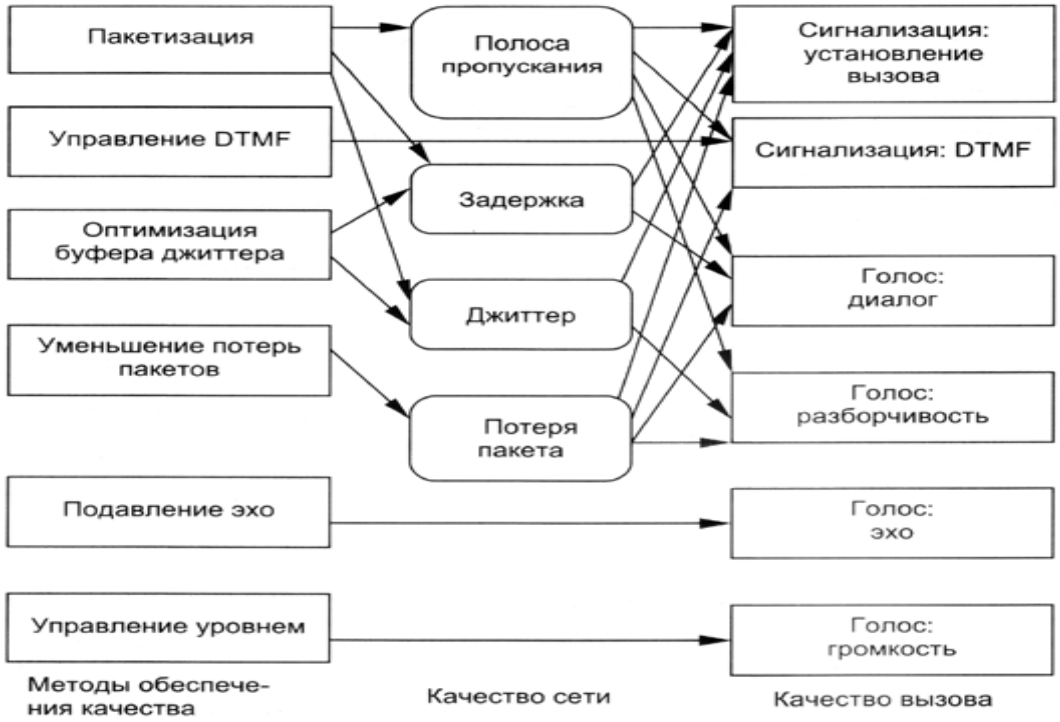


Рис. 5. Схема обеспечения качества IP-телефонии

Безопасность IP-телефонии

Типы угроз в сетях IP-телефонии

Вопрос безопасности связи всегда был одним из важных в сетях телекоммуникаций. В настоящее время в связи с бурным развитием глобальных компьютерных сетей, и в том числе сетей Интернет-телефонии, обеспечение безопасности передачи информации становится еще более актуальным. Разработка мероприятий в области безопасности должна проводиться на основе анализа рисков, определения критически важных ресурсов системы и возможных угроз. Существует несколько основных типов угроз, представляющих наибольшую опасность в сетях IP-телефонии.

1. *Подмена данных о пользователе*

Подмена данных о пользователе означает, что один пользователь сети выдает себя за другого. При этом возникает вероятность несанкционированного доступа к важным функциям системы. Использование механизмов аутентификации и авторизации в сети повышает уверенность в том, что пользователь, с которым устанавливается связь, не является подставным лицом и что ему можно предоставить санкционированный доступ.

2. *Подслушивание*

Во время передачи данных о пользователях (пользовательских идентификаторов и паролей) или частных конфиденциальных данных по незащищенным каналам эти данные можно подслушать и впоследствии злоупотреблять ими. Методы шифровки данных снижают вероятность этой угрозы.

3. *Манипулирование данными*

Данные, которые передаются по каналам связи, в принципе можно изменить. Во многих методах шифрования используется технология защита целостности данных, предотвращающая их несанкционированное изменение.

4. *Отказ от обслуживания (Denial of Service - DoS)*

Отказ от обслуживания (DoS) является разновидностью хакерской атаки, в результате которой важные системы становятся недоступными. Это достигается путем переполнения системы

ненужным трафиком, на обработку которого уходят все ресурсы системной памяти и процессора. Система связи должна иметь средства для распознавания подобных атак и ограничения их воздействия на сеть.

Базовыми элементами в области безопасности являются аутентификация, целостность и активная проверка. Аутентификация призвана предотвратить угрозу обезличивания и несанкционированного доступа к ресурсам и данным. Хотя авторизация не всегда включает в свой состав аутентификацию, но чаще всего одно обязательно подразумевает другое. Целостность обеспечивает защиту от подслушивания и манипулирования данными, поддерживая конфиденциальность и неизменность передаваемой информации. И, наконец, активная проверка означает проверку правильности реализации элементов технологии безопасности и помогает обнаруживать несанкционированное проникновение в сеть и атаки типа DoS [1].

Особенности системы безопасности в IP-телефонии

В системе IP-телефонии должны обеспечиваться два уровня безопасности: системный и вызывной.

Для обеспечения системной безопасности используются следующие функции:

- Предотвращение неавторизованного доступа к сети путем применения разделяемого кодового слова. Кодовое слово одновременно вычисляется по стандартным алгоритмам на инициирующей и оконечной системах, и полученные результаты сравниваются. При установлении соединения каждая система IP-телефонии первоначально идентифицирует другую систему, в случае отрицательного результата связь прерывается и вносится соответствующая запись в журнал.
- Списки доступа, в которые вносятся все известные шлюзы IP-телефонии.
- Запись отказов в доступе.
- Функции безопасности интерфейса доступа, включая: проверку идентификатора и пароля пользователя с ограничением доступа по чтению/записи; проверку прав доступа к специальному WEB-серверу для администрирования.

Функции обеспечения безопасности вызова включают: проверку идентификатора и пароля пользователя (необязательно); статус пользователя; профиль абонента.

При установлении связи шлюза с другим шлюзом своей зоны производится необязательная проверка идентификатора и пароля пользователя. Пользователь в любое время может быть лишен права доступа.

Профили абонентов создаются для каждого пользователя, в них содержится информация о службах/приложениях, доступных данному абоненту. Профиль абонента используется для проверки права доступа абонента к запрошенным службам [1].

Выбор реализации IP-телефонии

Первый, самый простой и выгодный вид использования технологий передачи голоса по IP-сетям - это междугородние и международные звонки. Использовать услуги IP-телефонии можно двумя способами:

1) Купить предоплаченную карточку у одного из провайдеров, звонить на специальный номер дозвона и проходить процесс авторизации при помощи PIN-кода или за счет определения системой вашего номера телефона.

2) Подключиться к серверу провайдера сразу по IP. Для этого необходимо качественное подключение к Интернету и специальное оборудование на стороне клиента.

Первый вариант обладает рядом недостатков:

Неудобство пользования услугой и трудности интеграции с АТС. Нужно постоянно вводить PIN-код (многие телефоны позволяют занести его в память телефона, поэтому это часто не проблема). Когда покупается одна карта на компанию, приходится программировать все

телефоны. В распечатке звонков виден только внешний номер, и нельзя определить, кто, куда и когда звонил. Используется одна из внешних городских линии.

Тарифы для звонков по карточкам обычно выше на 20-30%, чем звонки по IP (как во втором случае). Во многих республиках провайдеров IP-телефонии облагают специальным налогом, а провайдеры его просто переносят на потребителя.

Поэтому далее речь пойдет о втором варианте подключения к IP-телефонии.

Для реализации такого подключения необходимо организовать IP-связь от компании до сервера провайдера. Чаще всего это делается при помощи выделенных линий и специального VoIP оборудования [7].

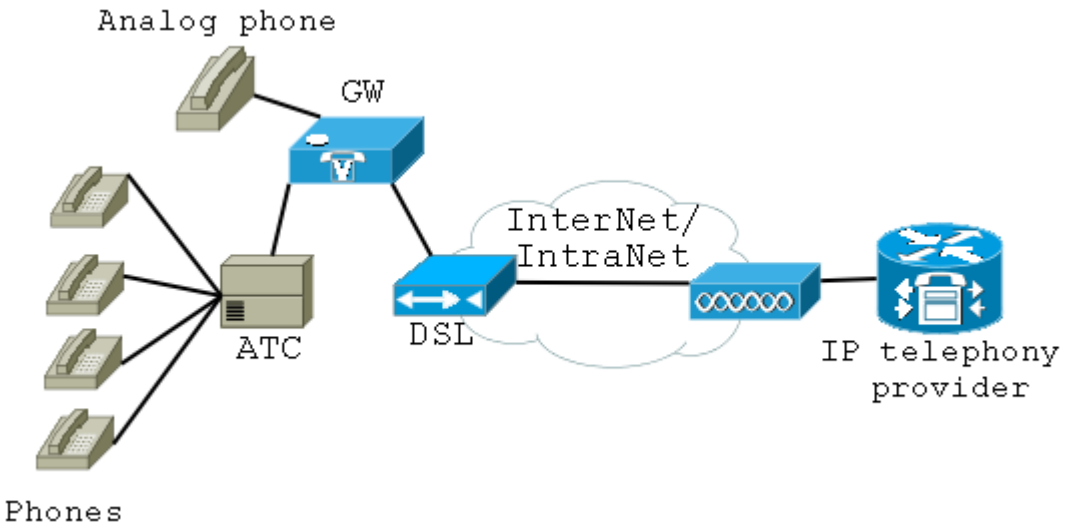


Рис. 6 Схема реализации IP-телефонии при подключении к серверу провайдера

На рисунке 6 представлена схема реализации IP-телефонии при подключении к серверу провайдера, где

GW - VoIP Gateway (голосовой шлюз). Предназначается для преобразования аналоговых голосовых каналов, поступающих с обычных телефонов, подключенных к нему напрямую, либо с телефонов, подключенных к офисной АТС, которая, в свою очередь, подключается к шлюзу.

ATC - обычная офисная телефонная станция.

DSL - выделенный канал связи Internet.

IP Telephony Provider - сервер провайдера IP телефонии, который принимает звонки, поступающий от голосового шлюза по IP, и маршрутизирует их далее.

Преимущества данного решения:

- Более дешевые тарифы (по сравнению с карточками).
- Удобство. АТС настраивается на голосовой шлюз (выход через 9, например), и все телефоны автоматически могут пользоваться IP-телефонией.
- Свободные внешние городские линии.

Подавляющее большинство провайдеров телефонии предлагают своим клиентам именно такую схему подключения. При этом они устанавливают свое оборудование (голосовой шлюз, дают выделенную линию) и подключают компанию к своему сервису телефонии. Минусы такого подключения для корпоративного клиента:

- Ежемесячная абонентская плата за использование оборудования

- Полная зависимость от провайдера телефонии. Компания зависит от провайдера и вынуждена получать услугу телефонии по данным ему ценам и качеству.

Таким образом, решением данных проблем становится только самостоятельный выход на рынок IP-телефонии, установка собственного оборудования и самостоятельный выбор провайдера IP-телефонии.

В условиях данного проекта связь посредством IP-телефонии будет осуществляться внутри офиса НПФ «Микран», тем самым, сотрудники офиса смогут пользоваться услугами IP-телефонии, включая междугороднюю связь.

На рисунке 7 представлена структура подсети НПФ «Микран» до внедрения IP-телефонии.

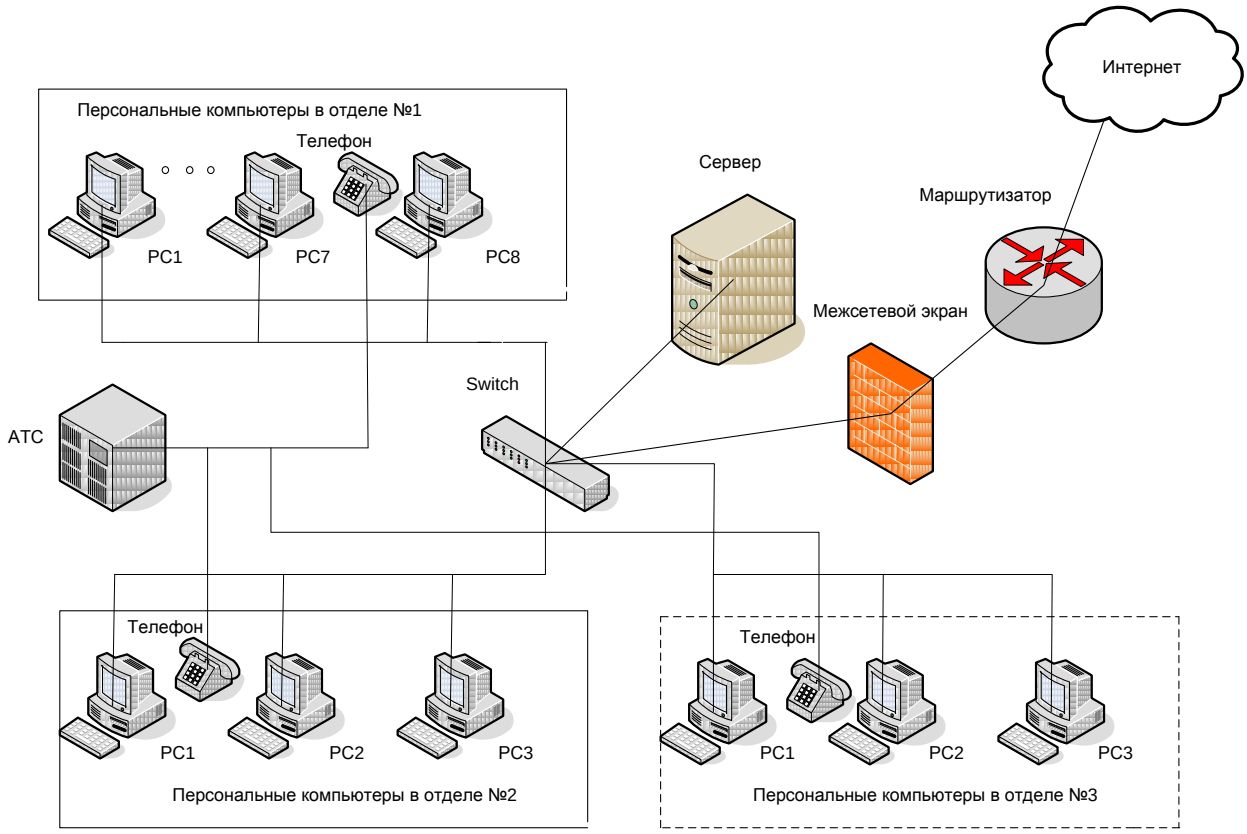


Рис. 7. Структура подсети НПФ «Микран» до внедрения IP-телефонии

Для начала необходимо рассмотреть существующие способы внедрения IP-телефонии в офис предприятия [7].

Первый из них - это VoIP-шлюзы. Их можно приблизительно определить как устройства, которые принимают голосовое сообщение по сети с коммутацией каналов от обычной УАТС, преобразуют его в IP-пакеты и передают по сети ЛВС либо WAN на другой шлюз, где оно воссоздается в формате, понятном для принимающей системы телефонной связи.

Функциональные возможности шлюзов могут быть реализованы через автономные блоки, модули или модульные платы для специализированных устройств, а также через расширяемые маршрутизаторы либо программное обеспечение и платы расширения для серверов под Windows NT.

Шлюзы являются самыми популярными VoIP-продуктами на рынке — их поставляют более 30 производителей, и суть дела здесь состоит в передаче голосовых пакетов по IP-сети.

Но эти пакеты не проходят через Internet, и вы не получите тех возможностей, которые вам обеспечит конвергенция сетей передачи речевой информации и сетей передачи данных. Основной недостаток VoIP-шлюзов это их малофункциональность.

Второй способ – это IP-УАТС (IP-PBX (private branch exchange) - телефонная станция на базе протокола IP). IP-УАТС это великолепное решение, если есть возможность самостоятельно разработать систему. Они представляют собой полноценную систему телефонной связи с различными вариантами построения IP-телефонов, включая многие IP-телефонные приложения, например управление телефонной связью с настольного ПК, многоканальное управление вызовами, автоматическое распределение вызовов.

Обычно IP-УАТС — это PC сервер с телефонным ПО и голосовыми платами. К их недостаткам часто относят низкую масштабируемость и отсутствие тонового набора. Кроме того, PC сервер не может обеспечить такую же надежность, как телефонные сети с коммутацией каналов. Положительная сторона IP-УАТС заключается в способности создать распределенную систему. В результате географически раздельные системы телефонной связи с такими функциональными возможностями, как прямой вызов, перевод телефонного вызова, конференцсвязь и голосовая почта, создают впечатление прямого соединения с местными УАТС.

Для построения сети IP-телефонии в НПФ «Микран» мы будем использовать IP-УАТС, так как в нашем случае нам нужна полноценная система IP-телефонии с большим набором функциональных возможностей.

Выбор протокола системы

Необходимо сформулировать критерии выбора протокола и, следовательно, критерии к выбору устройств.

Выбор протокола будет основан, на сравнении протоколов H.323 и SIP, которое будет проводиться по нескольким критериям.

1. Дополнительные услуги. Набор услуг, поддерживаемых обоими протоколами, примерно одинаков. Дополнительные услуги, предоставляемые протоколом H.323, стандартизированы в серии рекомендаций ITU-T H.450.x. Протоколом SIP правила предоставления дополнительных услуг не определены, что является его серьезным недостатком, так как вызывает проблемы при организации взаимодействия оборудования разных фирм производителя.

Протокол SIP предусматривает возможность организации связи третьей стороной. Эта функция позволяет организовать такие услуги, как набор номера секретарем для менеджера и сопровождение вызова оператором центра обслуживания вызовов. Подобные услуги предусмотрены и протоколом H.323, но реализация их несколько сложнее.

В протоколе SIP есть возможность указывать приоритеты в обслуживании вызовов. В протоколе H.323 такой возможности нет.

2. Персональная мобильность. Протокол SIP имеет хороший набор средств поддержки персональной мобильности пользователей, в число которых входит переадресация вызова к новому местоположению пользователя, одновременный поиск по нескольким направлениям и т.д. Персональная мобильность поддерживается и протоколом H.323, но менее гибко.

3. Расширяемость протокола. Необходимой и важной в условиях эволюционирующего рынка является возможность введения новых версий протоколов и обеспечение совместимости различных версий одного протокола.

Протокол SIP достаточно просто обеспечивает совместимость разных версий. Поля, которые непонятны оборудованию, просто игнорируются. В случае необходимости, в организации IANA (Internet Assigned Numbers Authority) могут быть зарегистрированы новые заголовки. Таким образом, разработчик может внедрять новые услуги.

Новые функциональные возможности вводятся и в протокол H.323, но с некоторыми ограничениями. Архитектура протокола H.323 монолитна и представляет собой интегрированный набор протоколов для одного применения. Протокол состоит из трех основных составляющих, и для создания новой услуги может потребоваться модификация каждой из этих составляющих.

4. Масштабируемость сети. Сервер SIP, по умолчанию не хранит сведений о текущих сеансах связи и поэтому может обработать больше вызовов, чем привратник H.323, который хранит эти сведения.

5. Время установления соединения. Следующей существенной характеристикой протоколов является время, которое требуется, чтобы установить соединение. В запросе INVITE протокола SIP содержится вся необходимая для установления соединения информация, включая описание функциональных возможностей терминала. Таким образом, в протоколе SIP для установления соединения требуется одна транзакция, а в протоколе H.323 необходимо производить обмен сообщениями несколько раз.

6. Сложность протокола. Протокол H.323, несомненно, сложнее протокола SIP. Общий объем спецификаций протокола H.323 составляет примерно 700 страниц. Объем спецификаций протокола SIP составляет 150 страниц.

Протокол SIP использует текстовый формат сообщений, подобно протоколу HTTP. Это облегчает синтаксический анализ и генерацию кода, позволяет реализовать протокол на базе любого языка программирования, облегчает эксплутационное управление, дает возможность ручного ввода некоторых полей, облегчает анализ сообщений. Название заголовков SIP-сообщений ясно указывает на их назначение.

Протокол H.323 использует двоичное представление своих сообщений на базе языка ASN.1, поэтому их непосредственное чтение затруднительно. Для кодирования и декодирования сообщений необходимо использовать компилятор ASN.1. Но, в тоже время, обработка сообщений, представленных в двоичном виде, производится быстрее.

Алгоритмы H.323 не оптимизированы для реальных сетей, они сложны в реализации и требуют больших ресурсов на клиентской стороне. Для нашей системы принятие такого решения является нецелесообразным, так как задачей НПФ «Микран» при внедрении в свою фирму IP-телефонии является получить дополнительные возможности не свойственные обычным телефонным сетями и сократить расходы на междугородные и международные переговоры. Технология H.323 больше подходит для корпоративных сетей и поставщиков услуг IP-телефонии, для которых данные услуги не являются доминирующими и сеть для них, построенная на базе H.323, представляется им хорошо знакомой сетью ISDN, наложенной на IP-сеть.

Из выше изложенного следует, что в рамках данной задачи более подходящим решением является выбор более простого протокола SIP, с его богатым разнообразием услуг.

Выбор программно-аппаратного комплекса

По техническому заданию, необходимо выбрать необходимое оборудование для организации IP-телефонии в НПФ «Микран». Как уже было сказано выше, IP-телефония в нашем случае будет основана на использовании IP PBX, так как это решение позволяет организовать полноценную систему IP-телефонии с большим выбором функциональных возможностей. Ниже рассматриваются предлагаемые продукты IP PBX различных фирм производителей.

Выбор IP PBX поддерживающих протокол SIP

1. Комплекс MCP-IP.ATC

Комплекс MCP-IP.ATC представляет собой мини-АТС, позволяющую организовывать голосовую связь, как через обычные телефонные линии (ТфОП), так и через IP-сети (Ethernet, Internet и т.д.).

Преимущества:

- масштабируемость корпоративной сети,
- архитектура позволяет создавать территориально распределенные телефонные, сети неограниченной емкости с единым номерным планом,
- формирует единый номерной план для любого количества абонентов,
- обеспечивает сервис, доступный каждому абоненту УАТС,
- значительно снижает стоимость междугородных и международных переговоров.

Компактный модуль MPC-IP.ATC реализует функции нескольких устройств:

- многоканальный шлюз IP-телефонии,
- факс-аппарат,
- конференц - сервер,
- аппаратура оперативного контроля телефонных переговоров.

Таблица 3. Краткие технические характеристики:

Количество и тип поддерживаемых интерфейсов	FXS, FXO.
Кодеки	G.711, G.723.1, G.729, G.165.
Автоматическое управление кодеками	- Автоматический выбор кодеков при установке IP-соединения между двумя станциями (приоритеты задаются пользователем); - Возможность автоматического выбора кодека G.711 для установки соединений в пределах локальной сети.
Голосовые функции	- Независимая установка усиления принимаемого и передаваемого сигнала; - АРУ с динамическим шумоподавителем; - VOX, VAD для минимизации занимаемой полосы при отсутствии голосовой активности; - Для кодеков G.723.1, G.729 - возможность компенсации потерь пакетов. Станция воспроизводит вместо них "образ" голоса, моделируя его на основании предыдущей информации. Данная функция существенно улучшает субъективное качество разговора по IP-сети в условиях потерь пакетов.
Протоколы	- Собственный (ASP); - SIP; - H.323.
Прием/передача факсимильных сообщений	- Через IP-сеть по протоколу T38; - Через ТФОП по протоколу T30 (режим факсимильного аппарата 3 группы).
Сервис VoIP	- RTP/RTCP; - Динамический джиттер-буфер; - Компенсация потерь пакетов; - Настройка количества аудио-фреймов в пакете; - Возможность дублирования аудиопакетов для компенсации потерь в сети;

	- Передача через IP служебных сигналов АТС (цифры тонального и импульсного набора, сигналы "HOOK FLASH") для реализации ДВО УПАТС.
Безопасность (функции мониторинга - перехвата трафика)	Возможность постановки на контроль (прослушивание) любых абонентов станции. При любом звонке, принимаемом или инициируемом контролируемым абонентом, станция установит соединение с контролирующим номером (местным или удаленным через ТфОП, IP-сеть) и будет передавать на этот номер всю служебную и голосовую информацию из контролируемого соединения.
Контроль вызовов (все функции доступны как при локальных звонках, так и для соединении через IP-сеть)	- Постановка вызова на удержание; - Прием второго вызова с уведомлением абонента; - Ведение двух разговоров одновременно; - Перевод вызовов; - Переадресация вызовов; - Режим прямого вызова.
Сервис УПАТС (все функции доступны как при локальных звонках, так и для соединении через IP-сеть)	- Групповой вызов; - Перехват вызова; - Многоканальный звонок; - Конференц-сервер; - "Тональный" донабор (DISA); - Возможности "ручного" и "автоматического" приема передачи факсимильных сообщений.
Взаимодействие с компьютером	Возможность установления соединения по IP-сети с приложениями CTI. Приложения могут выступать как инициаторы соединения, и принимать звонки от станции.
Питание	Любой нестабилизированный источник питания с выходным напряжением 9-18 В и соответствующей мощностью (зависит от количества и типа каналов). Входит в комплект поставки.

2. **Серия IP АТС Tainet - IPBX 230 и IPBX 2500**

Данное решение TAINET объединяет традиционную телефонию (PSTN) и IP- телефонию. Теперь организация может использовать VoIP для междугородных и международных звонков. Это существенно сокращает расходы на такие звонки. TAINET обеспечивает также решением интеграции нескольких территориально распределенных АТС в единую АТС, что упрощает процесс связи между АТС и позволяет поддерживать также традиционные телефонные функции. Используя существующую сетевую архитектуру, это программное обеспечение позволяет передавать голос, данные и видео информацию по более низким тарифам, одновременно получая доступ к интеграции данных, виртуальной телефонии, речевой почте, видео конференциям, факс сервисам и т.п.

Особенности:

- Поддержка до 30/200 внешних регистраций и эквивалентных email счетов;
- Поддержка10/50конкурирующихзвонков;
- Совместимость с функциями, которые поддерживают традиционные АТС;

- 3 типа конференций;
- Поддержка различных типов оконечного оборудования - IP телефоны, программные; телефоны, WiFi телефоны, аналоговые телефоны
- Запись CDR и звонков;
- Web конфигурация и управление.

Технические характеристики

SIP функции

- Статическая/динамическая регистрация;
- Внешняя прокси регистрация;
- Конфигурируемый PBX Caller ID;
- Профайл пользователей;
- NAT traversal для клиентов;
- Outbound proxy с или без WAN;
- SIP proxy сервер;
- QoS механизм для VoIP и данных.

Функции АТС

- Удержание звонка, конференция;
- Переадресация вызовов;
- Переадресация безусловная, для отсутствующих, занятых ; (Unconditional, unavailable, busy call forward);
- Количество переадресаций или отказов на номер (Per-calling-number forward and rejection);
- Конференции (Multi-room meet-me conference);
- Привилегии звонков групп (Call privilege grouping);
- Inter-PBX SIP trunking;
- Intra-PBX stackable trunking через Ethernet;
- Эхоподавление In-band/RFC 2833/SIP-INFO DTMF трансляция;
- FXO определение тона разрыва связи (disconnection tone detection).

Голосовая почта

- Код пользователя (User PIN);
- Поддержка нескольких языков;
- Структурированный архив;
- Уведомление о приходе почты и присоединений (унифицированный обмен; сообщениями);
- Переадресация.

Управление

• Web конфигуратор;
• Системный лог событий;
• Call Detail Record (CDR);
• Состояние выходных линий (Extension status display);
• TFTP сервер;
• Network Time Protocol синхронизация времени;
• Обновление Firmware через Web интерфейс.

Модели:

1. IPBX 2500
- до 200 регистраций и voice mail счетов;
- до 50 конкурентных звонков с RTP;

- Поддержка 8 аналоговых PSTN линий;
- 2.5" HDD для хранения.
2. IPBX 2300
- до 30 регистраций и voice mail счетов;
- до 10 конкурентных звонков с RTP;
- Поддержка 4 аналоговых PSTN линий;
- Flash диск для хранения.

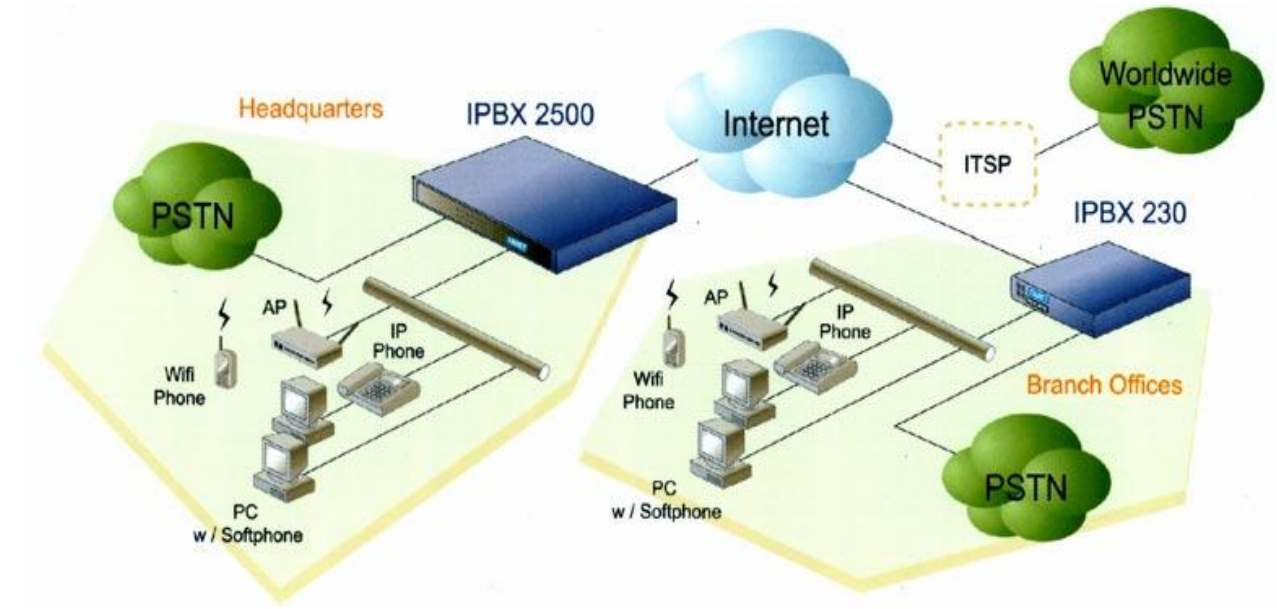


Рис. 8. Пример применения IPBX 2500 и IPBX 230

3. Snom VoIP Box

Рис. 9. IP PBX Snom VoIP Box

Минимальный по размерам (9x8x5 см), snom VoIP box является полноценным IP PBX решением, элементарно подключаемым к локальной сети Вашего офиса. snom VoIP Box не имеет в составе себя каких либо движущихся частей (как Жесткий Диск-HDD или вентилятор), что делает его надежным и легким в обслуживании.

Технические характеристики:

- Plug-and-play IP PBX;
- SIP Proxy, Registrar и Location Server в соответствии RFC3261;
- Перевод звонков;
- MOH - музыка на hold;
- Многосторонняя конференция;
- Голосовая почта;

- Автоответчик;
- Интерактивный голосовой автоответчик (IVR);
- Automatic Call Distribution (ACD);
- Управление через Web интерфейс;
- Call Hunting;
- Dialog Agent;
- Speed dial;
- цена – 56388.8 рублей;.

4. Решение от компаний Mitel и Pingtel

Компания Mitel, специализирующаяся на выпуске традиционных PBX с коммутацией каналов и фирма Pingtel, занимающаяся продажей IP-телефонов с поддержкой SIP, представили интегрированное телефонное оборудование для узлов, включающих в себя от 10 до 500 рабочих мест.

Устройство Pingtel SIPxchange IP PBX базируется на протоколе SIP, поддерживаемом продуктами 3Com и частично оборудованием Cisco. Дебют компании на арене пакетной передачи голоса ознаменовался выпуском модели SIPxchange, которая обеспечивает контроль вызовов, возможность обмена голосовой почтой, голосовые ответы в интерактивном режиме и организацию управления на основе браузера. Кроме того, устройство поддерживает приложения с использованием технологий XML, Java и voiceXML.

Стек протокола SIP, реализованный в модуле SIPxchange, позволяет осуществлять обмен информацией с телефонами SIP Pingtel Expressa или с другими телефонами на базе SIP, которые выпускаются корпорациями Cisco и Siemens. Клиенты Windows XP, использующие приложение Windows Messenger, которое также базируется на SIP, имеют возможность подключаться к серверу SIPxchange. Поставки модуля SIPxchange начались осенью по цене около $600 за рабочее место.

5. Asterisk

Многие производители наладили выпуск оборудования, но это оборудование достаточно дорогое и многие компании не хотят переходить на новые технологии из-за боязни больших расходов. Но есть более демократичное решение. Этим решением является Asterisk.

Asterisk – это гибкая платформа для построения решений по передаче и обработке голоса, на которой можно построить решения разного уровня для совершенно разных задач. Asterisk программный продукт, работающий под управлением Linux и поддерживающий популярные протоколы IP-телефонии SIP и H323. Как Linux является ядром операционной системы, так Asterisk – ядро системы передачи голосовых данных. И, что также очень важно, Asterisk имеет легко расширяемую архитектуру, позволяющую реализовать любую функциональность современных цифровых АТС, а также многие возможности, недоступные для них.

Его можно использовать как для подключения обычных клиентов, так и для передачи голосового трафика между несколькими серверами Asterisk. Для сопряжения с «традиционной телефонией» имеются аналоговые PCI карты (FXO, FXS) и цифровые PCI карты (E1, T1). С помощью Asterisk вы сможете реализовать проект любого масштаба – от простого домашнего сервера голосовой почты до телефонного сервера предприятия с функциями IVR (Interactive Voice Response – система голосовых меню).

Asterisk позволяет организовать соединение с большинством используемого сейчас оборудования и программного обеспечения для передачи голоса. Ситуация, когда имеется несколько офисов, между которыми нужно организовать связь, возникает очень часто, особенно у крупных организаций. Также при особо тесных партнерствах между организациями, телефонный трафик между ними становится столь большим, что появляется смысл в установлении связи между их АТС.

Самой эффективной схемой объединения офисов является так называемая “полносвязка”, когда Asterisk в каждом из офисов соединён с каждым из остальных офисов. Таким образом, выход из строя любой из офисных АТС никак не повлияет на связь в других офисах. [5]
Мало того, некоторые пользовательские устройства можно настроить так, что при выходе из строя местной АТС они будут подключены к какой-либо из других АТС. Таким образом, даже при аварии телефонная связь будет замечательно работать.
Использование Asterisk в настоящее время это:

- экономия на лицензиях к программному обеспечению (Asterisk – это свободный продукт);
- отсутствие зависимости от поставщика – в настоящий момент количество компаний, предоставляющих услуги по созданию и поддержке решений на базе Asterisk быстро растёт, и если поставщик начнёт “заламывать” цены на свои услуги, то его можно быстро и безболезненно сменить на другого;
- экономия на разговорах между офисами – объединение офисов с помощью IP-телефонии может значительно сократить расходы на связь, особенно при наличии офисов в разных городах;
- улучшение качества работы офисной связи – автоответчики, автоматические секретари, голосовые меню, и многие другие возможности реализуются на основе Asterisk быстро и недорого.

Результатом использования Asterisk, будет являться полноценная IP АТС или IP-PBX (private branch exchange) - телефонная станция на базе протокола IP. Как и любая мини АТС, коммутирует телефонные каналы внутренних абонентов во внешнюю телефонную сеть (как правило, внешних каналов несколько меньше, чем, в общем случае, внутренних). В качестве интерфейса подключения к IP PBX внутренних абонентов используется Ethernet интерфейс сервера, в составе которого мы будем реализовывать решение. Соответственно, транспортом для абонентских телефонных каналов, служит Ethernet среда, по определению, не гарантирующая качества канала (и это является основным камнем преткновения технологии). Поэтому первое, на что стоит обратить внимание при реализации решения, это меры по предотвращению коллизий в Ethernet сегменте. Часто для пакетной телефонии выделяется отдельный Ethernet сегмент в рамках СКС предприятия, что определенным образом гарантирует качество абонентских каналов. Программное обеспечение (ПО) Asterisk позволяет гибко управлять коммутацией при возникновении перегрузок, задействуя все внешние каналы безотносительно того, каким способом они подключены к IP АТС. [5]

Преимущества использования Asterisk IP-PBX:

- *Нулевая стоимость приобретения.* Asterisk – это открытый продукт, поэтому использование и приобретение системы не сопряжено с лицензионными выплатами.
- *Большой набор функциональных возможностей.* Голосовая почта, конференцсвязь, электронное голосовое меню - все это изначально находится в системе. Вы можете в любой момент настроить и запустить нужный вам модуль без необходимости покупать доп. программное обеспечение или платы расширения, как было бы в случае с "классическими" системами.
- *Полная свобода выбора провайдера IP телефонии.* Компания самостоятельно выбирает, к какому провайдеру подключиться. Более того, изучив цены и протестировав качество нескольких провайдеров, можно подключиться сразу ко всем, выбрав, какое направление кому отправлять.
- *Масштабируемость.* В зависимости от объема переговоров, выбирается первоначальная конфигурация оборудования. Например, для обеспечения 4-х одновременных разговоров по IP, необходимо аналоговая PCI карта с 4-мя FXS интерфейсами (для подключения к АТС по аналоговым соединениям). Для

обеспечения 30 одновременных разговоров, необходимо сменить/добавить цифровую PCI карту с E1 интерфейсом. Для обеспечения 120 одновременных разговоров, необходимо PCI карта с 4-мя E1 интерфейсами. Модернизация системы делается просто сменой карты в сервере.

- *Глобальность.* Где бы не находись работники компании, они могут пользоваться собственной телефонией с любого места, подключенного к Интернет (отели, Интернет кафе, Wi-Fi споты).

Целесообразнее будет выбрать проект Asterisk - потому что это бесплатное, широко распространенное (а значит, по его внедрениям проще найти информацию), и что не менее важно, opensource решение, реализующее большинство необходимых мелкому и среднему офису функций. Использование Asterisk экономит значительные деньги на самой телефонной системе без ущерба функциональности.

Для реализации поставленных задач на базе Asterisk IP-PBX будут нужны следующие компоненты:

- Сервер (в нашем случае, сервер представляет собой персональный компьютер с процессором Pentium D820 2.8 2G RAM.);
- Операционная система ОС Linux (является открытым продуктом);
- ПО Asterisk IP-PBX;
- PCI-плата, для связи IP-телефонии с ТфОП.

Минус Астериска в том, что телефонный интерфейс программный. Поэтому оборудование дешевое. Поэтому же для использования в больших проектах делают связки Астериска с SIP-серверами. Так как Астериск достаточно медленен. Его предназначение мини-АТС.

9.2 Выбор оборудования для сопряжения Asterisk с АТС

Наиболее часто используемым оборудованием в IP-телефонии являются шлюзы. Задачей шлюза является сопряжение "обычных" телефонных сетей с IP. И если с одной стороны этого шлюза всегда будет IP, то количество интерфейсов с другой стороны запросто может поставить в тупик неподготовленного человека. [5] Рассмотрим наиболее известные "телефонные" интерфейсы:

- FXO (Foreign eXchange Office) - аналоговый интерфейс телефонных станций. К голосовым шлюзам с таким интерфейсом могут подключаться обычные телефонные аппараты, факсы и другие абонентские устройства. Фактически, интерфейс FXS это то, что приходит к нам по телефонному кабелю от городской или мини-АТС. В задачу устройств, реализующих этот интерфейс, входят: генерация сигнала готовности АТС (гудок в линии), сигналов вызова абонента и
  т. д.
- FXS (Foreign eXchange Subscriber) - аналоговый интерфейс абонентских устройств телефонных станций. Устройства с таким интерфейсом подключаются к интерфейсу FXS. Так те же самые факсовые аппараты, телефоны, модемы реализуют интерфейс FXO. Существует такое простое правило - если есть провод, соединяющий два аналоговых устройства телефонии, то с одной стороны этого провода должен быть FXS (АТС), а с другой - FXO (телефон). Таким образом, шлюзы с интерфейсом FXO подключаются вместо телефона. С их помощью можно организовать связь с ТФОП или предоставить доступ к IP-телефонии, используя "внутренние" (более дешевые) линии мини-АТС.
- E1 - цифровой интерфейс, используемый для создания высокоскоростных магистралей. В цифровом потоке E1 имеется 32 канала (2 из них служебные) по 64 кБит. Таким образом, используя один поток E1, возможно организовать до 30 одновременных телефонных разговоров. В IP-телефонии такие интерфейсы обычно используются для организации связи с ТФОП или для организации связи между АТС.

С Asterisk можно не только использовать обычные шлюзы H323, SIP с портами FXO, FXS, E1, но и специализированные модули выпускаемые специально для Asterisk. Фактически они представляют собой PCI-платы с соответствующими разъемами, необходимой электроникой, а также драйверами, позволяющими PCI-платам работать с Asterisk.

Компания Digium, чьей торговой маркой является Asterisk, предлагает пользователям широкий набор интерфейсных плат, оптимизированных для работы с Asterisk. Спектр выпускаемых ею плат достаточно велик - от однопортовых FXS и FXO адаптеров, до модулей с четырьмя интерфейсами E1/T1.

Рассматривать цифровые модули мы не будем, так как они наиболее интересны средним и большим предприятиям (1 плата 4E1 - 120 цифровых каналов) и стоят они значительно дороже аналоговых модулей.

Соглашение обозначения для связок TDM следующие: TDM X Y B, где "TDM" обозначает, что используется карта - TDM, "X" обозначает, что число модулей FXS, "Y" обозначает число модулей FXO, и "B" указывает, что то это изделие - связка. Под TDM связкой подразумевается карта Wildcard TDM400 с установленными FXS и FXO
(опционально) модулями. [10]

Стандартные конфигурации

- TDM10B - 1-порт FXS
- TDM40B - 4-порта FXS
- TDM01B - 1-порт FXO
- TDM04B - 4-порта FXO
- TDM11B - 1-порт FXS и 1-порт FXO
- TDM22B - 2-порта FXS и 2-порта FXO
- TDM31B - 3-порта FXS и 1-порта FXO

Также компанией Digium выпускается плата, относящаяся к нестандартным конфигурациям Wildcard TDM400P.

Wildcard TDM400P

Wildcard TDM400 - это PCI 2.2 совместимая карта половинной длины, которая поддерживает от одного до четырех телефонных интерфейсов, позволяющих соединить аналоговые телефоны, или аналоговые телефонные линии с ПК. Используя программное обеспечение Asterisk PBX и стандартные аппаратные средства ПК можно создать SOHO (Small Office Home Office) – телефонную систему, отвечающую всем требованиям современных деловых телефонных систем. Также в Wildcard TDM400 установлен модуль подавления эха.

TDM400P достаточно дорогие устройства для построения банка каналов, но их применение позволяет снизить общие затраты на построение системы. При использовании FXO и FXS модулей вместе с TDM400 можно создать решение с поддержкой разного количества телефонных портов. Например, такое решение: три порта FXO и один порт FXS.

Модуль FXO позволяет карте TDM400P активизировать порт для подключения аналоговой телефонной линии (POTS). Модуль FXS позволяет карте TDM400P активизировать порт для подключения аналогового телефона.

Модули FXO и FXS позволяет использовать все возможности работы с телефонной сетью, которыми обладает любой стандартный аналоговый телефон.

Поскольку система имеет модульную архитектуру, пользователь может активизировать дополнительные порты на используемой карте в любое время, установив дополнительные FXS или FXO модули.

Для того чтобы в последствии масштабировать данное решение, необходимо просто добавлять новые карты TDM400 с установленными модулями.

Рис. 10. Wildcard TDM400P

Другой вариант сопряжения Asterisk с офисной АТС это использование "внешних" голосовых шлюзов. Наиболее известными производителями таких устройств (совместимых с Asterisk) являются - Cisco, Mediatrix, Quintum, AddPac, VegaStream и D-Link. Этот вариант используется когда нет возможности использования оборудования Digium. Например, в ввиду физических ограничений иногда бывает несколько затруднительно установить PCI-платы в стандартные стоечные серверы (1U, 2U). Кроме того, рынок оборудования IP-телефонии в России все еще находится в состоянии, близком к зачаточному, и найти в продаже платы Digium по разумным ценам может быть несколько проблематичным.

Выбор IP-телефонов

Телефоны для IP-телефонии бывают трех видов: программные IP-телефоны, аппаратные IP-телефоны и IP-телефоны подключающиеся к USB порту. Существует огромное множество различных IP-телефонов, от самых многофункциональных до самых простых, предлагаемые различными компаниями. При выборе телефонной системы заказчик в основном оценивают удобство пользования, внешний вид и цену. Изучив характеристики IPтелефонов от разных фирм производителей, был сделан вывод, что нет смысла описывать характеристики IP-телефонов от каждого производителя, так как они очень похожи. Для сравнения было выбрано два вида телефонов от компаний Cisco и KingTel. Опишем их характеристики.

Выбор аппаратного телефона

1. Cisco Color IP Phone 7970G

Рис. 11. Cisco Color IP Phone 7970G

Модель IP-телефона Cisco 7970G представляет собой усовершенствованное устройство, предназначенное для обеспечения доступа с высокой разрешающей способностью к корпоративным приложениям для крупных, средних и малых предприятий. Отличительной особенностью новой модели Cisco 7970G является наличие цветного графического дисплея, что позволяет использовать телефон как средство для настольного доступ к расширенным

графическим изображениям с большей детализацией данных на тех рабочих местах, где нет персонального компьютера.

Кроме того, новая модель телефона поддерживает широкий набор функций, и прежде всего приложениям XML, работающие в среде корпоративной сети. Аппарат оснащен также системой подсветки и функцией «Touch-Screen», обеспечивающей простоту и наглядность применения функциональных возможностей телефона. Все это, а также функция быстрого доступа, делают IP-телефон Cisco 7970G не только средством для обеспечения телефонных переговоров, но и устройством, повышающим производительность и качество обслуживания клиентов. Сочетание графического цветного изображения и доступности XML-приложений с IP технологией превращают телефон Cisco 7970G в мультимедийный деловой инструмент, обеспечивающий быстрое, легкое и интуитивно понятное взаимодействие.

Cisco IP Phone 7970G дает пользователю возможность одновременного переключения между восемью телефонными линиями (или комбинации из линий и номеров прямого набора), имеет высококачественную систему громкой связи, встроенный разъем для телефонной гарнитуры, и поддерживает технологию Inline Power (питание телефона от коммутатора ЛВС по линии Ethernet).

Дополнительные функции

Модель Cisco IP Phone 7970G оснащен встроенным двухпортовым коммутатором Fast Ethernet 10/100TX, обеспечивающим подключение к ЛВС не только телефона, но и персонального компьютера. Коммутатор поддерживает протокол IEEE 802.1Q, который позволяет размещать телефон и компьютер в разных VLAN в составе ЛВС, что в свою очередь обеспечивает повышенную безопасность голосовой подсистемы, а также разделение голосового трафика от трафика данных. Благодаря выделенному порту для подключения гарнитуры нет необходимости в дополнительном усилителе, что значительно упрощает использование.

Установки и спецификация

Телефон Cisco 7970G IP Phone поддерживает следующие пользовательские установки:

– Сетевые настройки
– Состояние вызова
– Контрастность дисплея
– Тип звонка

Сетевые функции

Телефон Cisco 7970G IP Phone обеспечивает следующие сетевые функции:

– Поддержка CDP (Cisco Discovery Protocol)
– Автоматическая конфигурация IEEE 802.1Q
– Поддержка кодеков G.711a, G.711u, G.729ab, iLBC
– Встроенный коммутатор Ethernet
– Подключение к ЛВС портом 10/100BaseTX с разъемом RJ-45
– Обновление системного ПО через сервер TFTP
– Автоматическая настройка сетевых параметров по протоколу DHCP
– Функции VAD (Voice Activity Detection), подавление пауз, генерация шума
– Поддержка Cisco CallManager 3.3(3) или более новая, протокол SCCP (Skinny Client Control Protocol).

2. VoIPVoice VP3302

IP-телефон производства VoIPVoice

Рис. 12. IP-телефон VoIPVoice VP3302

IP-телефон VP3302- представляет собой устройство для подключения к сетям (VoIP) IP-телефонии в качестве абонентского терминала.

IP-телефон обладает широким набором функциональных возможностей, как телефонных, так и сетевых, что позволяет предоставлять качественный и функциональный сервис, реализовывать простое и быстрое внедрение на VoIP сетях, в том числе предварительную настройку под конкретного оператора.

IP-телефон VP3302 обеспечивает высокое качество передачи голоса на различных каналах передачи данных, поддерживает основные алгоритмы голосовой компрессии и обработки голоса.

Основные характеристики:

- Протоколы - H.323/SIP/MGCP/IAX2;
- 2 порта 10/100Mb Ethernet;
- Обработка голоса:
  - VAD (Voice Activity Detection) ;
  - CNG (Comfort Noise Generation);
  - Эхокомпенсация G.165/168 16ms.
- Сетевые возможности:
  - Поддержка кодеков G.729ab, iLBC
  - DHCP клиент;
  - Статический IP адрес;
  - Обновление системного ПО через сервер TFTP;
  - PPPoe.
- RTP (Real -Time Transport Protocol);
- Поддержка DDNS (Dynamic Domain Name Service) ;
- Поддержка стандартов ITU-T/DTMF;
- LCD дисплей: 2x16 знаков;
- Высокое качество звука через спикерфон;
- Записная книга на 1000 номеров;
- По 180 номеров для входящих / набранных / пропущенных вызовов;
- Индикатор голосовой почты;
- Разъем 2.5мм для гарнитуры (опционально);
- Настройка уровня громкости звонка.

Сравнивая эти телефоны можно сделать выводы, что по техническим характеристикам они оба удовлетворяют требованиям данной системы.

Cisco - лидирующий производитель всего сетевого оборудования, работают очень стабильно, как правило, не имеют каких-либо отклонений (расширений) от стандартов. Благодаря своему имени, обладают очень большой стоимостью. Обычно минусом IP-телефонов от Cisco является очень трудоемкая настройка. Но в сетях такого масштаба, как в нашем случае, их использование не является необходимым.

Компания VoIPVoice занимает менее лидирующую позицию в отличие от Cisco, но при этом оборудование, производимое для IP-телефонии, также является стабильным и качественным. Это удобные телефоны, с очень хорошим качеством звука. Кроме этого они могут загружать конфигурационные файлы с FTP сервера. Кроме этого они стоят дешевле аналогичных телефонов от Cisco.

Замечено, что чем дешевле аппараты, тем проще их конфигурировать. Там меньше возможных настроек и соответственно меньше шагов для конфигурации. Как правило, меньше возможностей сделать ошибки.

Также можно было бы рассмотреть телефон от компания Sipura, которая предлагает более дешевый продукт. Такой телефон стоит раза в полтора меньше VoIPVoice, легок в настройке через WEB интерфейс, ничего сложного в настройке нет даже для начинающих. Но качество звука у такого телефона значительно хуже. Все перечисленные телефоны отлично работают с Астериском.

Таким образом, был выбран IP-телефон компании VoIPVoice VP3302.

USB IP-телефон был выбран по тому же принципу и той же фирмы производителя.

USB телефон для IP-телефонии

3. VoIPVoice CyberPhone K

USB-телефон CyberPhone K - от компании VoIPVoice позволяет удобно и привычно совершать и принимать звонки через Интернет с помощью персонального компьютера и специального программного обеспечения SoftPhone, обеспечивая наилучшее качество голосового соединения.

Элегантный дизайн продукта гармонично вписывается в деловую обстановку, аппарат удобен в обращении и отвечает самым высоким требованиям корпоративного пользователя. Телефонный аппарат, имея дополнительное утяжеление, устойчиво и надежно располагается на столе и не «прыгает» вслед за поднятой трубкой.

Цифровая наборная клавиатура, кроме стандартных клавиш (0-9,*,#), расширена клавишами регулировки уровня звука, отключения микрофона во время разговора и многофункциональными клавишами. Набор телефонного номера может производиться с цифровой клавиатуры самого телефона. Аппарат не требует дополнительного питания.

Разработанный компанией-производителем алгоритм кодирования речи ASTI и эхо-компенсации DSP позволяет максимально приблизить качество разговора к традиционной телефонии. Аппарат адаптирован к среде Windows, протестирован с различными программными продуктами (SoftyPhone): Skype, Net2Phone, MSN Messenger, InfinityPhone и другими.

Возможности и особенности

1. Звуковой сигнал для всех поступающих вызовов, выбор типа звукового сигнала с помощью клавиатуры телефона.
2. Возможность подключения наушников.
3. Функция АОН для Skype и SIPNET (sip) звонков, поддержка разных языков.
4. Выбор Skype или SIPNET (sip) абонентов и набор телефонного номера с помощью клавиатуры.
5. Предотвращение эха, подавление шума, дуплексная связь.
6. Драйвер и встроенная звуковая плата.

7. Не требуется внешнее питание.

Системные требования

1. Windows 2000 или XP, MAC.
2. 400 МГц процессор и свободный USB1.1 или USB2.0 порт.
3. Оперативная память 128 Мб и свободное пространство на жестком диске 15 Мб.
4. Любое широкополосное подключение к интернету или модемное соединение со скоростью не ниже 33.6 Kbps.

4. Программный телефон

Наиболее известные из программных телефонов: X-Ten X-Lite, sjPhone, FireFly, MS Messenger. Возможности этих программ лучше всего сравнивать, представив их в виде таблицы 9.2. [5]

Таблица 4. Сравнение возможностей программных клиентов SIP

Возможность	X-ten xlite	Sjphone	FireFly	MS Messenger
Поддержка протокола SIP	+	+	+	+
Работа с Asterisk	+	+	+	+
Поддерживаемые ОС	Windows	Windows, Linux	Windows	Windows
Поддерживаемые кодеки	G711, GSM, Speex	G711, GSM, iLBC	G711, G729, GSM, iLBC, Speex	G711
Поддержка функций Caller-ID, Call Transfer, Call Hold	+	+	+	–
Интерфейс пользователя	4	5	3	3
Возможность учета времени разговора	+	+	+	–
Доступность	бесплатно	бесплатно	бесплатно	бесплатно

В зависимости от решаемой задачи можно использовать различные программные клиенты. Если сервер будет преимущественно использоваться для внутренних звонков, то имеет смысл обратить внимание на программы с более функциональным интерфейсом (X-lite, sjPhone). В случае большого количества междугородних звонков (либо работы в условиях ограниченной пропускной способности или ненадежного канала) лучше использовать программы, поддерживающие кодек G729.

В нашем случае сервер будет использоваться преимущественно для внутренних звонков, поэтому выбор должен стоять между программными телефонами X-lite и sjPhone. Чтобы сделать выбор между этими телефонами, необходимо посмотреть на их характеристики. Программный телефон sjPhone поддерживает кодек iLBC, который будет использоваться для кодирования речи в нашей системе (об этом речь пойдет далее), а программный телефон X-lite его не поддерживает, поэтому в нашей системе в качестве программного телефона будет являться sjPhone.

Таким образом, структура сети на основе Asterisk IP PBX показана на рисунке 13.

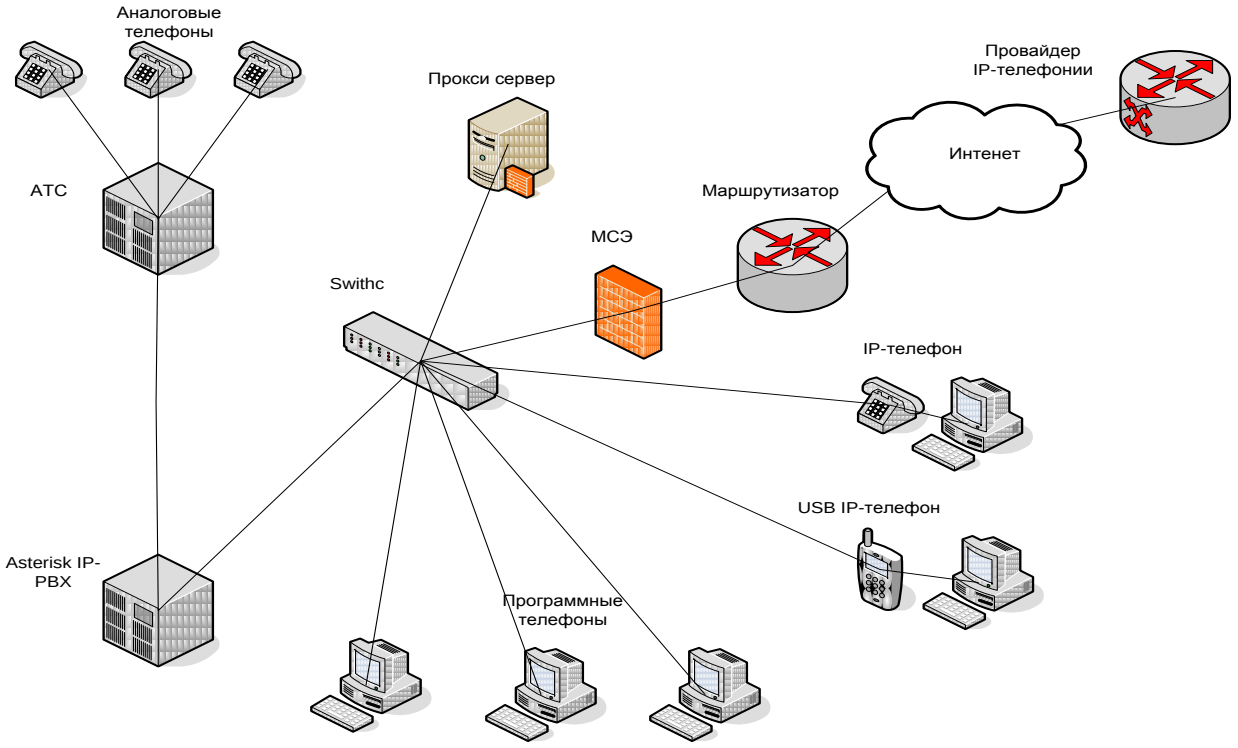


Рис. 13. Структура сети IP-телефонии на основе Asterisk IP PBX

10 Формирование критерия оптимальности для проектируемой сети

Для проектирования сети IP-телефонии, необходимо задаться некими качественными требованиями к системе, иначе говоря, - сформулировать критерий оптимальности системы. Это позволит нам на основе заданных критериев качества, определить технологию, наилучшим образом подходящую для проектирования.

Итак, сформулируем и поясним основные требования, предъявляемые к сети IP-телефонии.

1. Обеспечение качества IP-телефонии

Обеспечение необходимого качества связи (Quality of Service, QoS) является существенной проблемой в VoIP. Основные факторы, влияющие на качество:

- Потери пакетов. Если сеть загружена, то маршрутизаторы или другие сетевые устройства могут отбрасывать некоторые пакеты.
- Задержка при прохождении пакетов от одного клиента к другому.
- Колебания задержки (jitter). Время прохождения маршрута от пакета к пакету может изменяться. Чтобы погасить эти колебания, на клиентском терминале используется специальный буфер (jitter buffer). Если колебания времени доставки очень большие, то буфер перестанет справляться со своей задачей.

Задержка создает неудобство при ведении диалога, приводит к перекрытию разговоров и возникновению эхо. Эхо возникает в случае, когда отраженный речевой сигнал вместе с

сигналом от удаленного конца возвращается опять в ухо говорящего. Эхо становится трудной проблемой, когда задержка в петле передачи больше, чем 50 мс.

2. Безопасность и защищенность сети IP-телефонии

Вопрос безопасности связи всегда был одним из важных в сетях телекоммуникаций. В настоящее время в связи с бурным развитием глобальных компьютерных сетей, и в том числе сетей Интернет-телефонии, обеспечение безопасности передачи информации становится еще более актуальным. Разработка мероприятий в области безопасности должна проводиться на основе анализа рисков, определения критически важных ресурсов системы и возможных угроз.

Ключевой задачей, безусловно, является обеспечение требуемого уровня безопасности информации, циркулирующей в сети. Вопросы информационной и технической безопасности в сети IP-телефонии становятся основополагающими при проектировании такой системы. Но при этом, если сеть IP-телефонии не будет никак защищена, она все равно будет полностью функционировать, если будет обеспечено качество хорошего уровня. Чего не скажешь в обратном случае.

На этом основании можно сделать следующее заключение: для построения сети IP-телефонии критерием оптимальности является время задержки при передаче речевого сигнала.

Затруднение диалога и перекрытие разговоров становятся серьезным вопросом качества, когда задержка в одном направлении передачи превышает 250мс.

Таким образом, критерием оптимальности является время задержки не превышающее 250с.

Обеспечение качества системы

Выбор кодека для кодирования речевой информации

Одним из важных факторов эффективного использования пропускной способности IP-канала, является выбор оптимального алгоритма кодирования/декодирования речевой информации – кодека.

За все время существования данного направления было разработано большое количество кодеков, используемых для передачи аудио- и видеоинформации в системах IP-телефонии. Наиболее популярными (по количеству пользователей и поддержки в конечных устройствах) в настоящее время являются:

- G711 - стандартизованный ITU-T кодек, используемый в устройствах ISDN. Требуемая пропускная способность - 64 кбит/сек. Существуют две разновидности кодека a-law и u-law, отличающиеся алгоритмами кодирования. Кодек поддерживается практически всеми устройствами IP-телефонии.
- G729 - стандартизованный ITU-T кодек, предназначенный для передачи речи с "хорошим качеством" при использовании небольшой пропускной способности (8 кбит/сек). Существуют две популярные (и несовместимые между собой) версии данного стандарта: Annex A (более "простая" схема кодирования) и Annex B (с использованием алгоритмов сжатия пауз). По субъективным оценкам, данный кодек обладает качеством лучшим, чем у G.723, но худшим, чем G711. Содержит детектор голосовой активности VAD (Voice Activity Detector) и генератор комфортного шума. Поддерживается практически всеми производителями оборудования. При коммерческом использовании требуется лицензия.
- G723.1 - кодек, стандартизованный ITU-T. Отличительной особенностью является возможность работы при очень низком потоке (5.3, 6.3 кбит/сек). По субъективными оценкам, обладает самым плохим качеством (среди рассматриваемых кодеков) речи. Поддерживается значительной частью устройств IP-телефонии. При коммерческом использовании требуется лицензия.
- GSM (RPE-LTP) - голосовой кодек, разработанный для использования в системах сотовой связи стандарта GSM. При кодировании кадра используется информация

предыдущего кадра, кодирование осуществляется блоками по 20 мс со скоростью 13 кбит/с. Поддерживается производителями оборудования, в основном в шлюзах между сотовыми и VoIP-сетями.

- iLBC (Internet low bitrate codec) - открытый (не требуются лицензионные отчисления) голосовой кодек. Предназначен для кодирования с потоком 13.33 кбит/сек (при размере кадра 30 мс) и 15.20 кбит/сек (при размере кадра 20 мс). Содержит VAD и генератор комфортного шума. По субъективным оценкам экспертов, качество речи данного кодека превышает G.729a. Кроме того, кодек более устойчив (по сравнению с g729) к потере кадров, что позволяет эффективно использовать его при организации сеансов связи через сеть Интернет. Поддерживается ограниченным числом производителей оборудования [1].

Сравнительные характеристики кодеков приводятся в таблице:

Таблица 5. Основные параметры кодеков IP-телефонии

Кодек	Поток	Размер пакета (мс)	Алгоритмическая задержка (мс)	Оценка MOS	Суммарный поток
G.711	64 кбит/с	0.125	0	4.4	81.2
G.729	8 кбит/с	20	15	4.07	31.2
G.723.1a	6.3 кбит/с	30	37.5	3.87	21.9
G.723.1g	5.3 кбит/с	30	37.5	3.69	20.8
GSM	13 кбит/с	20	20	3.5	35.4
iLBC	13.33 кбит/с	30	30	4	28
iLBC	15.2 кбит/с	20	30	4	29
G.726	16/24/32 кбит/с	0,125	1	2 - 4.6	-

При передаче через Ethernet пакет "обрастает" различными заголовками (MAC, IP, RTP). В колонке «Суммарный поток» приводится суммарная пропускная способность (без сжатия заголовков RTP, удаления пауз и потерь при передаче). В таблице 11.1 приводятся данные для одного голосового канала, в то время как при сеансе их обычно 2 (прямой и обратный).

Таким образом, по показателю качества кодеки можно расположить следующим образом (в порядке ухудшения качества): G711, iLBC, G729, gsm, G723. По используемой пропускной способности (в порядке увеличения:) G723, iLBC, G729, GSM, G711.

По-умолчанию Asterisk идёт с поддержкой кодеков:

- G.711 a-law/u-law — несжатый поток;
- G.726;
- iLBC;
- GSM;
- G.729 (доступен при приобретении коммерческой лицензии);
- G.723.1 (также доступен при приобретении коммерческой лицензии)

Из вышеперечисленных кодеков, поддерживаемых Asterisk было отдано предпочтение iLBCa, так как размер пакета составляет 30мс и при этом суммарная пропускная способность составляет 28 кбит/с. Этот выбор объясняется следующим:

- Использование G.711 в системах IP-телефонии обосновано лишь в тех случаях, когда требуется обеспечить максимальное качество кодирования речевой информации при небольшом числе одновременных разговоров.
- Кодек G.729 обеспечивает очень хорошее качество кодирования речевой информации при достаточно высокой компрессии. Единственным недостатком является то, что требуется коммерческое приобретение лицензии и его собирать только с использованием библиотеки Intel IPP.
- Кодек G.723.1 по субъективными оценкам, обладает самым плохим качеством (среди рассматриваемых кодеков) речи, и также как и у кодека G.729 при коммерческом использовании требуется лицензия.
- Кодек GSM поддерживается производителями оборудования, в основном в шлюзах между сотовыми и VoIP-сетями. Также качество кодирования речевой информации по оценкам MOS хуже, чем у iLBC.
- Процесс преобразования не вносит существенной задержки у кодека G.729. Но при этом размер пакета составляет 0.125 мс. При передаче через Ethernet пакет "обрастет" различными заголовками, что приведет к увеличению суммарной пропускной способности. Поэтому кодек G.726 предназначен для использования в системах видеоконференций.
- Кодек iLBC является открытым (не требующим лицензионного отчисления). Содержит VAD и генератор комфортного шума. По субъективным оценкам экспертов, качество речи данного кодека превышает G.729a. Кроме того, кодек более устойчив (по сравнению с g729) к потере кадров, что позволяет эффективно использовать его при организации сеансов связи через сеть Интернет.

На основании всех вышеизложенных факторов можно сделать следующее заключение: для кодирования речевой информации наилучшим вариантом будет использовать кодек iLBCa.

Процедуры обработки речи в IP-телефонии

Для обеспечения качественной передачи речевых сигналов в IP-телефонии необходима их следующая обработка [1].

1. Устранение всех нежелательных компонентов из входного аудиосигнала. После оцифровки речи необходимо удалить эхо из динамика в микрофон, комнатное эхо и непрерывный фоновый шум (например, шум от вентиляторов), а также отфильтровать шумы переменного тока на низких частотах звукового спектра.

Эффективное эхоподавление и уменьшение шумов абсолютно необходимо в любой конфигурации с «открытым микрофоном» и с громкоговорителем на базе персонального компьютера (ПК) для традиционной и IP-телефонии. Эти функции все в большей мере реализуются аудиокомпонентами ПК, так что сама система IP-телефонии может их и не иметь. Шлюзам IP-телефонии требуется выполнять меньший объем предварительной обработки, нежели конечным решениям, потому что УАТС и телефонная сеть обеспечивают фильтрацию и уменьшение шумов.

2. Подавление пауз в речи, распознавание остаточного фонового шума (внешних шумов) и кодирование для восстановление на дальнем конце, то же самое для опознаваемых сигналов. Паузы лучше всего полностью подавлять на ближнем конце. Для сохранения окружающих звуков необходимо смоделировать фоновые шумы, чтобы система на дальнем конце могла восстановить их для слушателя. Сигналы многочастотного набора номера DTMF и другие сигналы можно заменить на короткие коды для восстановления на дальнем конце (или для непосредственной обработки). Возможные проблемы: из-за того, что функция подавления пауз активизируется, когда громкость речи становится ниже определенного порога, некоторые системы обрезают начала и концы слов (в периоды нарастания и снижения энергии речи).

Как было сказано выше, кодек iLBC содержит VAD и генератор комфортного шума.

Технология VAD используется совместно с большим числом речевых кодеков. Проиллюстрируем кратко механизм VAD на простейшем примере. Входной аналоговый сигнал поступает на вход устройства сравнения, в котором измеряется его амплитуда и сравнивается с заданным пороговым значением. При превышении амплитудой входного сигнала заданного порога, сигнал поступает на вход кодека и кодируется по определённому алгоритму (интервал $T_2 - T_3$). Если амплитуда входного сигнала ниже порогового значения (например в интервал $T_1 - T_2$), то в момент времени T_1 передаётся только служебная информация (длиной в несколько бит) о начале паузы, а в момент T_2 о её окончании. На приёмной стороне, во время паузы, для улучшения субъективного восприятия кодированной речи может передаваться комфортный шум.

3. Сжатие голосовых данных. Сжать оцифрованный голос можно разными способами.

Сжатие голосовых данных также осуществляется кодеком iLBCa до 13.3 кбит/с.

4. «Нарезание» сжатых голосовых данных на короткие сегменты равной длины, их нумерация по порядку, добавление заголовков пакетов и передача. Хотя стек протоколов TCP/IP поддерживает пакеты переменной длины, их использование затрудняет достижение устойчивой и предсказуемой межсетевой маршрутизации в голосовых приложениях. Маршрутизаторы быстро обрабатывают небольшие пакеты и рассматривают обычно все передаваемые по одному и тому же IP-адресу пакеты одного размера одинаковым образом. В результате пакеты проходят по одному маршруту, поэтому их не надо переупорядочивать.

5. Прием и переупорядочивание пакетов в адаптивном «буфере ресинхронизации» для обеспечения интеллектуальной обработки потерь или задержек пакетов. Главной целью здесь является преодоление влияния переменной задержки между пакетами. Решение этой проблемы состоит в буферизации достаточного числа поступающих пакетов (при отложенном их воспроизведении) с тем,- чтобы воспроизведение было непрерывным, даже если время между поступлением пакетов сильно разнится.

Задержка создает неудобство при ведении диалога, приводит к перекрытию разговоров и возникновению эхо. Эхо возникает в случае, когда отраженный речевой сигнал вместе с сигналом от удаленного конца возвращается опять в ухо говорящего. Эхо становится трудной проблемой, когда задержка в петле передачи больше, чем 50 мс.

Для борьбы с эхом в выбранном IP-телефоне VoIPVoice VP3302 предусмотрена эхокомпенсация.

Иногда возникающее эхо можно подавить с помощью настройки параметров громкости (команда voice -volume). За счет уменьшения уровня передаваемого сигнала на одном шлюзе или IP-телефоне и увеличения уровня принимаемого сигнала на другом шлюзе/IP-телефоне можно вполне успешно бороться с эффектом эхо. При этом не происходит изменения громкости звука, воспринимаемого абонентом. Кроме того, в шлюзах также предусмотрена функция адаптивного эхоподавления (команда voice -echo).

11.2 Обеспечение качества IP-телефонии на базе протоколов RTP и RTCP

Протокол RTP (RFC 1889) предназначен для доставки чувствительной к задержкам информации с использованием сетевых служб одноадресной или групповой рассылки. Он не имеет собственных механизмов, гарантирующих своевременную доставку пакетов или другие параметры качества услуг — это осуществляют нижележащие протоколы. Он даже не обеспечивает все те функции, которые обычно предоставляют транспортные протоколы, в частности, функции по исправлению ошибок или управлению потоком. Обычно RTP работает поверх UDP и использует его службы, но может функционировать и поверх других транспортных протоколов.

Служба RTP предусматривает указание типа полезной нагрузки и последовательного номера пакета в потоке, а также применение временных меток. Отправитель помечает каждый RTF-пакет временной меткой, а получатель извлекает ее и вычисляет суммарную задержку.

Разница в задержке пакетов позволяет определить джиттер и смягчить его влияние - все пакеты будут выдаваться приложению с одинаковой задержкой.
Таким образом, главная особенность RTP — это вычисление средней задержки некоторого набора принятых пакетов и выдача их пользовательскому приложению с постоянной задержкой, равной этому среднему значению. Однако следует иметь ввиду, что временная метка RTP соответствует моменту кодирования первого дискретного сигнала пакета. Поэтому, если RTF-пакет, например, с видеоинформацией, разбивается на несколько пакетов нижележащего уровня, то временная метка уже не будет соответствовать истинному времени их передачи, поскольку они перед передачей могут быть организованы в очередь.
Возможности RTF можно расширить, объединив его с еще одним протоколом IETF, а именно с протоколом управления передачей в реальном времени (Real-time Transport Control Protocol, RTCP). С помощью RTCP контролируется доставка RTF-пакетов и обеспечивается обратная связь с передающей стороной и другими участниками сеанса. RTCP периодически рассылает свои управляющие пакеты, используя тот же механизм распределения, какой применяется и для RTF-пакетов с пользовательской информацией.
Основной функцией RTCP является организация обратной связи с приложением для отчета в качестве получаемой информации. RTCP передает сведения (как от приемника, так и от отправителя) о числе переданных и потерянных пакетов, значении джиттера, задержке и т.д. Эта информация может быть использована отправителем для изменения параметров передачи, например, для уменьшения коэффициента сжатия информации с целью улучшения качества ее передачи. RTCP также предусматривает идентификацию пользователей-участников сеанса.
При всех своих достоинствах протокол RTP далеко не совершенен. Например, протокол никак не способен повлиять на задержку в сети, но он помогает сократить дрожание звука при воспроизведении при наличии задержек. Кроме того, хотя пакеты UDP получают порядковые номера, при этом принимающая станция может установить факт потери пакетов, RTP не предпринимает никаких мер для восстановления потерянных пакетов. [3]

11.3 Оценка максимально возможных одновременных разговоров

Необходимо оценить максимальное количество одновременных возможных соединений. Тип ЛВС в НПФ «Микран» представляет собой: проводная, Fast Ethernet 100 Мбит, по спецификации физического уровня – 100Base-TX. Таким образом, максимальная пропускная способность сети составляет 100Мбит/с. В действительности же сеть максимально загружена примерно на 10%, поскольку основная загрузка ЛВС НПФ «Микран» предусмотрена организационными мерами в выходные дни и определенные часы. Поэтому здесь надо смотреть на то, какую нагрузку сможет выдержать сервер.
Однопроцессорный сервер, где будет установлено ПО Asterisk, Pentium D820 2.8 2G RAM способен выдерживать 120 одновременных звонков по FXO/FXS/E1 и 240 звонков по IP. [6]
Таким образом, приблизительно можно сказать о суммарной задержке, в рамках данной сети, в одну сторону передачи голосового трафика.

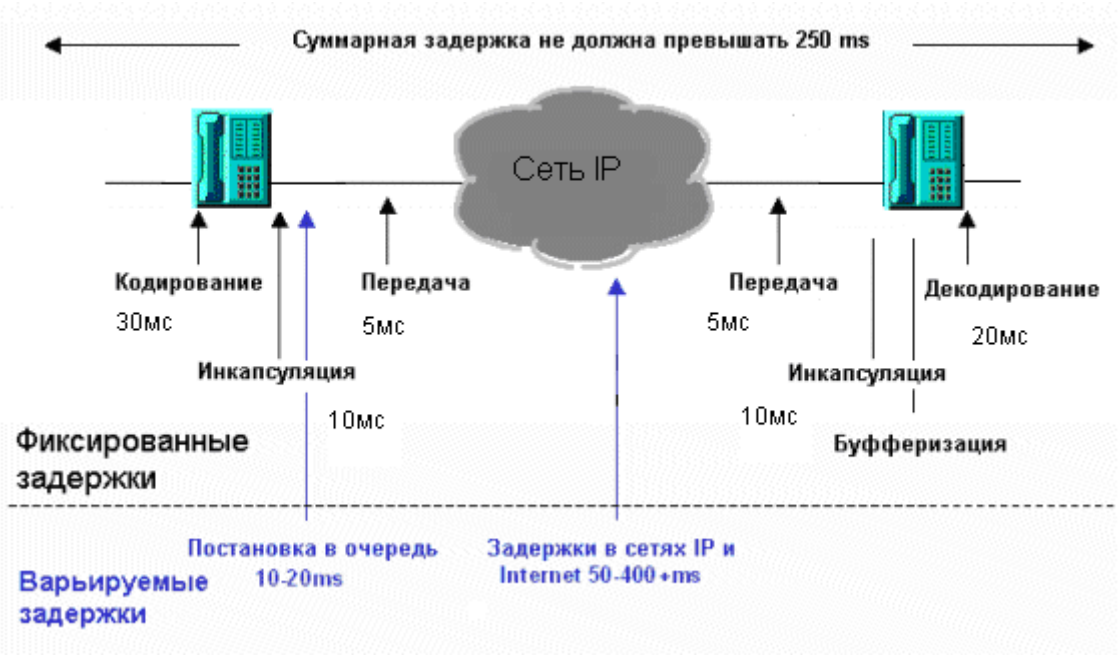


Рис. 14. Составляющие задержки в сети IP-телефонии

Так как сеть в рабочие дни не является загруженной графической информацией, а трафик составляет в основном лишь текстовая информация, то такая сеть имеет довольно таки высокую пропускную способность, а значит, задержка в IP-сети должна быть небольшой. И можно предположить, что суммарная задержка не будет превышать 250мс.

Обеспечение безопасности и защиты сети

Имеющиеся решения по защите VoIP на основе протокола SIP

Сегодня на рынке предлагается три типа решений по безопасности для VoIP: пограничные контроллеры сессий, обычные межсетевые экраны и межсетевые экраны SIP-приложений (или межсетевые экраны SIP).

Пограничные контроллеры сессий (SBC)

Изначально услуги VoIP предоставлялись просто как дополнение к существующей телефонной сети общего пользования (PSTN). SBC являются зримым примером такого подхода. Концептуально контроллеры – это устройства, предназначенные для поддержки исключительно сервиса VoIP, поэтому по-настоящему построенная IP-сеть на базе таких контроллеров была бы крайне сложной и дорогостоящей. Контроллеры не предназначены для обработки трафика данных или выполнения других сетевых функций. Это означает, что их необходимо дополнять межсетевыми экранами и другими сетевыми устройствами, что крайне затрудняет обеспечение качества обслуживания (QoS) в такой сети. Поскольку контроллеры терминируют трафик SIP и RTP, их необходимо постоянно модернизировать для поддержки новых версий и опциональных возможностей протоколов SIP и RTP, а также появляющихся на рынке новых моделей IP-телефонов и видеофонов. При наличии в корпоративной сети нескольких контроллеров SBC, постоянное их одновременное обновление и синхронизация с IP PBX становится крайне недешевым занятием.

Стоимость контроллеров обычно достаточно велика, и большинство предприятий малого или среднего бизнеса просто не могут позволить себе их приобретение.

Межсетевые экраны для сетей передачи данных

В отличие от контроллеров SBC обычные МСЭ являются достаточно недорогими и широко применяемыми устройствами, имеющими целый ряд функций, необходимых для управления сетью. С другой стороны, МСЭ – это устройство, изначально предназначенное для

обеспечения безопасности данных, что в свою очередь делает проблематичным построение по-настоящему конвергентных сетей.

Концептуально обычные МСЭ защищают сеть по статически предустановленным правилам, согласно которым разрешается или блокируется прохождение определенного трафика. Использование же протокола SIP требует динамического изменения правил. В результате для поддержки услуг VoIP, основанных на использовании протокола SIP, МСЭ необходимо постоянно держать открытыми для целого ряда портов и адресов IP. Такой подход по определению противоречит требованиям безопасности, и для ее обеспечения приходится разносить сети передачи данных и сеть VoIP. К тому же это не защищает IP PBX и IP-телефоны от атак DoS и других видов атак. Использование обычных МСЭ не позволяет решить проблему NAT и крайне затрудняет решение задач QoS.

Обе эти проблемы в значительной степени ограничивают топологию сети, а их решение может потребовать дополнительной инфраструктуры (оборудование, линии и т.д.).

Шлюзы прикладного уровня (ALG) или межсетевые экраны SIP

В упрощенном виде ALG представляет собой обычный МСЭ с возможностью терминировать трафик SIP. Так же, как и в случае с SBC, терминация протокола SIP в ALG крайне затрудняет или делает вообще невозможным применение кодирования для повышения безопасности протоколов SIP и/или RTP. А по аналогии с обычным МСЭ шлюз ALG не способен решить проблему NAT, когда несколько филиалов используют один и тот же частный адрес IP. Эта проблема связана с особенностями протокола SIP и ограничивает топологию сети. Как и SBC, ALG требует постоянного обновления для синхронизации с IP PBX, поддержки новых опций протокола SIP, а также при использовании новых моделей IP-телефонов и видеофонов, что представляет собой большую головную боль. Как правило, шлюз ALG обходится дешевле контроллера SBC, но значительно дороже обычного МСЭ.

В Ranch Networks было разработано уникальное решение, способное справиться со всеми перечисленными проблемами. Можно сказать, что инженеры этой компании создали новый класс устройств для обеспечения нужд корпоративной сети [4].

Ranch Networks

Компания Ranch Networks представила устройства модельного ряда RN, которые стали первыми в мире аппаратами, способными обеспечить безопасность и контроль полосы пропускания для приложений VoIP. Предлагаемые Ranch Networks устройства для IP-телефонии обеспечивают безопасность, управление и масштабирование трафика VoIP на уровне, неизмеримо превосходящем возможности существующих ныне межсетевых экранов. Устройства RN разделяют голосовой трафик, видеотрафик и трафик данных по множественным зонам безопасности, не требуя при этом реконфигурации IP-адресов [4].

Разработанная Ranch Networks технология предназначена для работы с IP PBX и способна поддерживать корпоративные и провайдерские сети любых масштабов. Там, где другим системам требуются громоздкие устройства, работающие по листам доступа, к тому же разнящиеся от протокола к протоколу и от шлюза к шлюзу, устройства Ranch Networks управляются самим IP PBX и обеспечивают динамический, независимый от протокола доступ к сети для конкретного звонка. Такой уникальный подход одновременно и упрощает организацию сетевой безопасности, и укрепляет ее, позволяя проходить зашифрованным потокам.

Начав свою деятельность в этом направлении с интеграции с IP PBX на открытых кодах Asterisk, компания Ranch Networks предлагает модели RN300, RN500 и RN700 в задачу которых входит организация для каждого звонка динамического, независимого от протокола доступа к сети. Эти устройства обеспечат беспрецедентный уровень безопасности для VoIP, управление полосой пропускания, поддержку VPN, возможности по учету и коммутации

трафика для небольших и среднего размера организаций, провайдеров услуг и операторов связи.

Главное назначение Ranch - повышение уровня сетевой безопасности и управляемости сетью. Это решение отличается умеренной стоимостью и обладает целым рядом преимуществ, важнейшими из которых являются следующие:

- многозонные межсетевые экраны RN по умолчанию закрыты, и весь трафик RTP (UDP) блокируется;
- Когда IP PBX и IP-телефоны расположены за устройствами RN, они хорошо защищены от атак DoS и вирусов;
- между IP PBX и IP-телефонами возможна организация любых типов NAT;
- трафики SIP и RTP могут быть закодированными и, таким образом, они защищены от перехвата;
- осуществляется динамическое выделение полосы пропускания для каждого конкретного звонка на основе конкретного кодека;
- количество звонков, обрабатываемых IP PBX в секунду, при использовании RN значительно увеличивается даже при использовании видеофонов.

Уникальная многофункциональность устройств RN предоставляет корпоративным пользователям возможность организовать надежную и недорогую систему IP-телефонии на базе IP PBX Asterisk с характеристиками, отвечающими самым высоким требованиям.

Одно из наиболее важных достоинств устройств Ranch Networks состоит в том, что оно многофункционально и поэтому экономически выгодно. Особенно это важно при построении/реконфигурации локальной сети, когда необходимо инвестировать большие суммы на различное оборудование. Для уже существующих сетей, устройства Ranch позволяют экономить на поддержке оборудования в рабочем состоянии и его управлением, поскольку поддерживать надо только одно устройство вместо нескольких.

Кроме того, многофункциональность значительно увеличивает надёжность сети т.к. вместо множества блоков питания, вентиляторов, кабелей и т.п., рассредоточенных по нескольким устройствам, Ranch концентрирует все в себе. Безусловно, вероятность отказа одного устройства гораздо ниже вероятности отказа большого количества отдельных устройств. В дополнение к вышесказанному, все устройства Ranch Networks были разработаны с учётом высоких требований стандартов NEBS, а так же Telco.

Защита VoIP соединения с помощью Ranch Networks

Обычно VoIP телефоны расположены за межсетевым экраном. Но в реальности традиционный межсетевой экран не обеспечивает никакой защиты.

Чтобы установить VoIP соединение, некоторые порты на межсетевом экране приходится держать "открытыми". Первая проблема состоит в том, что эти порты должны быть постоянно "открытыми", вторая в том, что неизвестно на какой порт и с какого IP придет запрос на входящее VoIP соединение.

В Ranch Networks был разработан код NetSec, который был интегрирован в коды IP PBX Asterisk. Этот код использует протокол MIDCOM (MiddleBox Communication) для связи между IP PBX Asterisk и устройствами RN. Протокол MIDCOM базируется на стандарте IETF (RFC 3303) и позволяет приложениям давать команды сетевым устройствам на динамическое изменение политик и правил в режиме реального времени. Команды могут передаваться как в закодированной, так и в обычной формах [4].

В устройствах Ranch Networks для защиты от атак на незащищенные порты UDP используется протокол MIDCOM и так называемый “динамический” firewall. Это позволяет держать постоянно открытым только один UDP порт 5060, что очень важно для защиты локальной сети. Порты для RTP будут открыты, только по команде с Asterisk и будут немедленно закрыты после того, как звонок завершится.

Поскольку никогда не известно, откуда и куда будет произведён звонок, то если не использовать RN придется открыть доступ в локальную сеть (где находится Asterisk) со всего земного шара на все возможные UDP порты.

Становится очевидно, что даже с традиционным межсетевым экраном IP телефоны (и сеть, где расположенные IP телефоны) не защищены.

Устройство безопасности Ranch Networks будет работать в одной связке с IP АТС, чтобы обеспечить доступ к ресурсам IP АТС (установить SIP соединение) только тогда, когда это действительно необходимо. Для этого в устройствах Ranch Networks используется протокол MIDCOM, обеспечивающий безопасную передачу сообщений SIP между устройством RN (Ranch Networks) и IP АТС.

Рисунок 11.1 показывает взаимодействие между Asterisk (SIP IP АТС) и устройством RN.

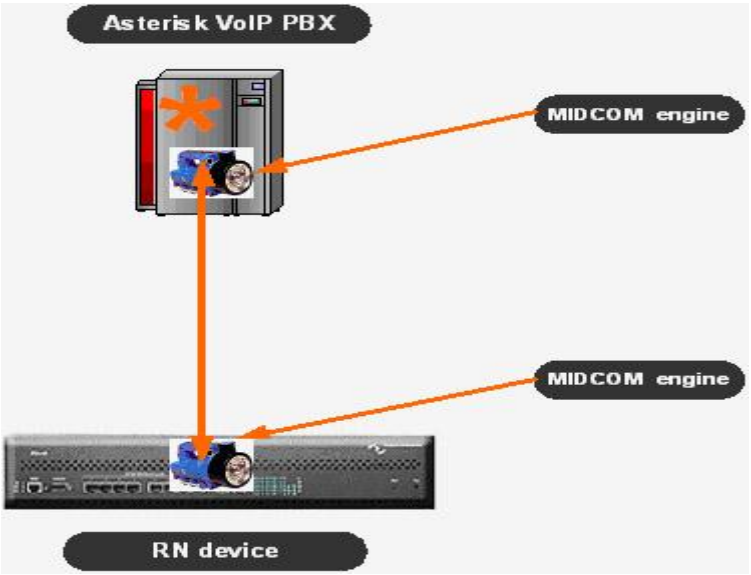


Рис. 15. Взаимодействие между Asterisk (SIP IP АТС) и устройством RN

Объединенные Asterisk и RN позволяют осуществлять технологию безопасности “по требованию” (security-on-demand) для VoIP соединений. В этом случае Asterisk сообщает RN устройству, какие правила необходимо добавить в межсетевой экран для данного VoIP соединения. Такие правила будут создаваться для каждого VoIP соединения, прошедшего через устройство RN. Это означает, что каждый запрос на установление VoIP соединения будет обработан динамически - правила межсетевого экрана (которые разрешают прохождение голосового трафика), будут созданы, когда это необходимо и удалены сразу после окончания разговора.

Таким образом, объединение Asterisk и любого из RN устройств это лучший способ обеспечить безопасность VoIP переговоров.

На момент установления соединения Asterisk располагает всей необходимой информацией о телефонах и их IP-адресах, типе кодека и т.д. Встроенный в Asterisk компанией Ranch Networks код NetSec трансформирует эту информацию в четыре вида правил и направляет их устройствам RN, используя протокол MIDCOM [4]. Эти четыре вида правил включают:

Правила безопасности – эти правила определяют, какие «дырки» (исходящий IP, исходящий порт, входящий IP, входящий порт) должно устройство RN открыть именно для этого разговора. Таким образом, в межсетевом экране RN открыты только конкретные небольшие участки, затребованные станцией Asterisk, а весь остальной трафик блокируется.

Правила NAT – эти правила определяют для устройств RN, каким образом реализовать функции NAT и PAT для этого конкретного звонка. Таким образом, как IP-телефоны во внутренней сети филиала, так и Asterisk могут иметь любые частные или публичные IP-адреса. Кроме того, это позволяет иметь несколько филиалов с одним и тем же частным IP-адресом для IP-телефонов.
Правила выделения полосы пропускания – эти правила определяют устройствам RN, какие полоса и QoS должны быть назначены для данного звонка. Эта информация базируется на выбранном типе кодека и позволяет устройствам RN предотвращать атаки DoS. Например, если в ходе установления соединения Asterisk определил кодек G711 (64 Кбит/сек), а со стороны одного из телефонов пойдет RTP-поток большего объема (скажем, 1 Мбит/сек), устройство RN ограничит входящий поток на уровне 64 Кбит/сек, защищая таким образом другой телефон и его сеть от переполнения. Устройства RN гарантируют данному звонку полосу в 64 Кбит/с независимо от всплесков данных в сети. Для каждого нового соединения будут назначаться свои правила выделения полосы, и устройства RN будут использовать имеющийся в распоряжении запас производительности в соответствии с индивидуальным контрактом на звонок, что является конфигурируемым параметром в устройствах RN. Если очередное соединение превышает лимит контрактов для VoIP, RN по протоколу MIDCOM пошлет соответствующее уведомление на Asterisk, и вызывающий абонент не сможет дозвониться.
Правила соединения абонентов – эти правила определяют устройствам RN каким образом соединить абонентов. Во многих случаях, включая наш пример, устройства RN могут соединить абонентов «напрямую». Устройства RN обеспечивают прямое соединение абонентов на аппаратном, а не на программном уровне, как это имеет место в случае, когда соединение идет через Asterisk. Такое прямое соединение помогает уменьшить задержки и искажения потока RTP, что выражается в повышении качества голосовой и видеосвязи. Следует отметить, что код NetSec направит команду устройству RN на «прямое» соединение только тогда, когда оба телефона используют один и тот же тип кодека. В противном случае голосовой поток пойдет через IP PBX Asterisk.

После установления соединения и начала обмена RTP-потоками устройства RN просто дожидаются от Asterisk команды «Отменить правила», которую IP PBX посылает им по протоколу MIDCOM по окончании телефонного разговора. Получив такую команду, устройства RN закрывают «дырки» в межсетевых экранах и обновляют лимит контрактов VoIP. Проще говоря, устройства RN «отменяют» действие всех четырех примененных ранее правил.

Концепция Зон Безопасности

Оборудование Ranch Networks может быть добавлено «поверх» сети и предоставлять множество функций по защите и повышению производительности. Существующая сеть может быть разбита на логические сегменты с использованием виртуальных локальных сетей (VLAN). VLAN "приходят" в устройство RN, где они группируются в виртуальные зоны безопасности (Secure Virtual Zones), каждая из которых представляет собой «Зону Доверия» (“Area of Trust”) в пределах сети. Так, например, локальная сеть может быть «разбита» в соответствии с различными параметрами, такими как структура организации, «гостевые» и «не-гостевые» Зоны, зоны речевого трафика и трафика данных [4].

Зоны безопасности с точки зрения инженеров-разработчиков Ranch Networks – это независимые сегменты сети, состоящие из одного или нескольких устройств (размер неограничен), трафику между которыми внутри сегмента можно доверять. Разбиение на сегменты осуществляется исходя из бизнес-логики конкретной компании. Зоной может быть к примеру:

- Провайдер Интернета №1, №2,..;

- Демилитаризованная зона;
- Сервера типа A, B,..;
- Бухгалтерия, Отдел продаж, Финансовый отдел, Дирекция,..;
- Гостевая, переговорная, конференц-зал,..;
- Wi-Fi зона;
- Зона с IDS (Система обнаружения атак);
- Телефонная станция IP;
- Телефоны IP;

и т.д.

Для связи каждой созданной зоны с каждой зоной устанавливается отдельный межсетевой экран. По умолчанию все экраны закрыты. К примеру: если необходимо чтобы гости из переговорной смогли выходить в Интернет со своих мобильных ПК, то достаточно добавить правило в МСЭ для соответствующей зоны – открыть 80-ый порт для прохождения в зону Интернет с заданной минимальной и максимальной шириной канала. Таким образом, гость будет видеть только гипертекстовые страницы в сети Интернет и ничего более.

При конфигурировании устройств Ranch Networks необходимо различать понятия физической и виртуальной зоны. *Физическая зона* – это порт на устройстве RN. Понятие *Виртуальная зона* намного шире. Она может быть реализована на одном порту и включать в себя:

- диапазон IP адресов, например 192.168.1.10 - 192.168.1.128, 192.168.6.24 - 192.168.6.30;
- несколько VLAN;
- несколько конкретных IP адресов, например 172.20.45.10, 172.20.45.11, 172.20.45.12;
- несколько MAC-адресов, например: 00-0B-DB-DE-B1-DC, 00-0B-DB-DE-A4-C2.

Виртуальная зона также может состоять из любых комбинаций портов RN и перечисленных выше компонентов.

Зона безопасности RN – это физическая или виртуальная зона, для которой действуют некоторые правила МСЭ. Для всех пользователей, находящихся в одной зоне безопасности, будут действовать единые правила МСЭ, если иное не оговорено для конкретного IP / MAC в этой зоне.

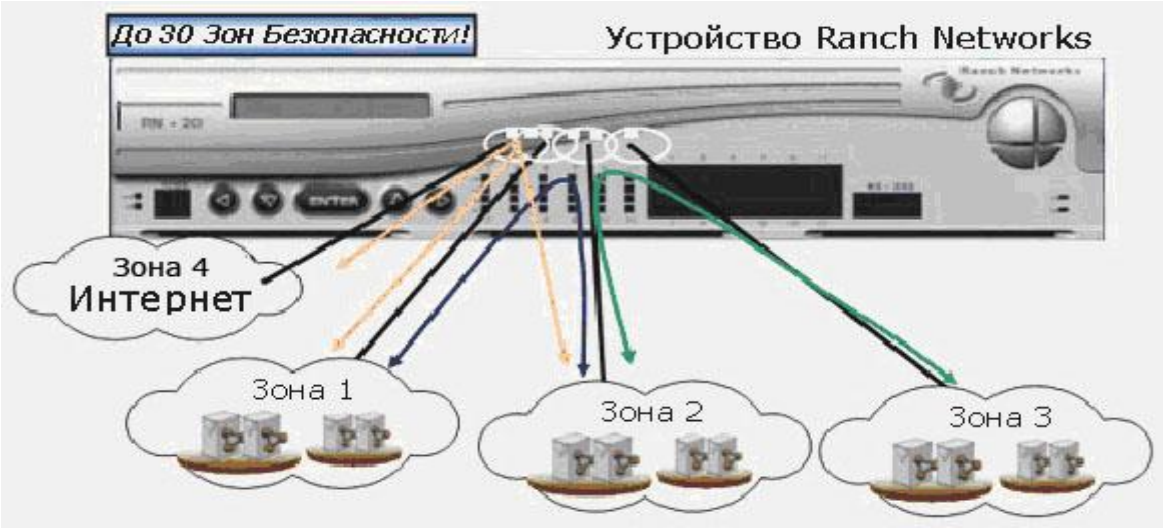


Рис. 16. Примет разбиения сети на 4 зоны безопасности

Как показано на рисунке 16 , RN физически сегментирует корпоративную сеть организации на несколько зон безопасности, тем самым, обеспечивая защищенность данных,

передающихся от зоны к зоне внутри организации и из Интернета. Это становится возможным за счет жесткого контроля и фильтрации трафика, передающегося между зонами безопасности, с помощью межсетевых экранов.

Принцип работы МСЭ Ranch Networks

Межсетевые экраны (МСЭ) можно условно разделить на несколько классов, согласно уровням модели взаимодействия открытых систем (Open Systems Interconnection, OSI):

- МСЭ сетевого и транспортного уровня (packet-swit-ched firewall);
- МСЭ сеансового уровня (circuit-level gateway);
- МСЭ прикладного уровня (application-level gate-way);
- МСЭ экспертного уровня (Statefull Packet Inspections), работающие практически на всех уровнях OSI.

МСЭ *сетевого* взаимодействия обеспечивают фильтрацию пакетов и наиболее просты в реализации. По заданным администратором спискам контроля доступа ACL (Access Control List) проводится анализ адресов отправителя и получателя пакетов и номера протокола, но при этом не анализируются информация, содержащаяся в пакетах. Эти решения позволяют ограничивать трафик и разбивать сеть на области с различным уровнем доверия.

МСЭ *сеансового уровня* работают на сетевом, транспортном и сеансовом уровнях взаимодействия. Такие устройства могут формировать динамические правила прохождения пакетов информации, согласно которым при установлении сессии, разрешенной списком контроля доступа, МСЭ создает таблицу прохождения пакетов (session state table) за пределы периметра сети. После этого МСЭ обеспечит прохождение внешних пакетов на тот же порт и на тот же адрес, с которого была инициирована сессия. Как и в предыдущем случае, полезная информация в пакетах не анализируется. Такие устройства позволяют предотвратить атаки типа DoS (Denial of Service - отказ в обслуживании), не позволяя открыть сессий больше, чем устройство сможет обработать, и запретить сессии, инициируемые из внешней сети.

МСЭ *прикладного уровня* работают на верхнем (прикладном) уровне OSI и позволяют производить анализ передаваемой информации. Различают два подкласса:

- «прозрачные» МСЭ (transparent);
- МСЭ-посредники (proxy).

Первые называются «прозрачными» из-за прозрачности прохождения информации и отсутствия необходимости в специальной настройке клиентских и серверных приложений. Вторые устанавливают отдельные сессии с клиентом и сервером и являются транзитной точкой на пути прохождения пакетов по маршруту «клиент-сервер». Каждый вариант имеет свои преимущества - используя «прозрачные» МСЭ можно добиться высокой производительности, а при использовании «посредников» - повышенной защищенности.

МСЭ *экспертного уровня* с полной пакетной проверкой (Statefull Packet Inspections) производят анализ пакетов практически на всех уровнях OSI - начиная с сетевого и заканчивая прикладным. Именно этот класс устройств наиболее перспективен и активно развивается. Такие МСЭ проверяют корректность работы приложений по протоколам прикладного уровня, могут блокировать отдельные команды протоколов, контролировать корректность их работы, последовательность команд и формат структуры пакетов.

Подавляющее большинство выпускаемых в настоящее время устройств могут производить полную пакетную проверку. Однако в недорогих устройствах такой анализ выполняется, как правило, лишь для протокола HTTP.

Существует еще один тип анализа - *углубленная проверка пакетов* (Deep Packet Inspection). Такой тип анализа применяется в устройствах предотвращения и обнаружения атак и МСЭ высокого класса защиты. В отличие от полной пакетной проверки здесь анализируется не только заголовок и проверяется корректность работы протокола, но и

«просматривается» содержимое пакета. Такой анализ может обнаруживать скрытые атаки и потенциально опасное содержимое, например, вирусы и троянские программы.

Отметим еще один нюанс, который касается поддержки VPN межсетевыми экранами. Эта функция давно стала стандартной и продиктована не только удобством (не нужно покупать отдельное устройство), но и жесткой необходимостью. Дело в том, что если для шифрования и дешифрования трафика, проходящего через VPN-туннель, используется отдельное устройство, находящееся внутри сети, то МСЭ не сможет выполнить анализ зашифрованного трафика и, соответственно, не сможет ограничивать доступ к сети. Кроме того, если мы вынесем это устройство за пределы сети, оно может быть подвержено атакам извне. Поэтому современные МСЭ имеют модуль VPN, позволяющий вначале расшифровывать трафик, а затем производить его фильтрацию.

Полнофункциональный МСЭ RN

Мультизонные МСЭ - это полнофункциональные МСЭ с запоминанием состояния, работа которых основана на запатентованной Ranch Networks технологии однопроходного сканирования пакетов «Single Packet Path». Все устройства RN используют операционную систему реального времени VxWorks, поверх которой работает операционная система RanchOS. Устройства используют не функционал МСЭ VxWorks, а собственный запатентованный метод полнофункциональных мультизонных МСЭ, которые всецело сочетаются со стандартами IETF. Устройства Ranch Networks обеспечивают функции безопасности на многих уровнях модели OSI:

Физический уровень

Когда сконфигурирована физическая зона безопасности на МСЭ RN, тогда обеспечивается безопасность на физическом уровне.

Канальный уровень

Устройства RN обеспечивают безопасность по MAC-адресам + IEEE802.3x

3-7 уровни

МСЭ RN обеспечивают защиту на этих уровнях при помощи пакетного фильтра и полнофункционального инспектирования.

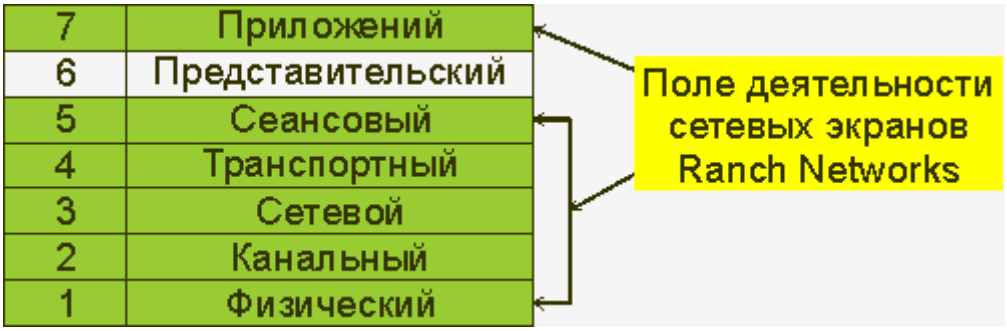


Рис. 17. Обеспечение функций безопасности на уровнях модели OSI

Полнофункциональное инспектирование

Когда хост на сети открывает любую сессию (TCP, ICPM и т.д.), устройство RN ее терминирует (прерывает) и открывает новую сессию к заданному IP-адресу назначения. Динамически или «полнофункционально» МСЭ будет сохранять состояние этой сессии в оба конца и будет поддерживать таблицу активных TCP, ICMP сессий и псевдо-активных UDP сессий. МСЭ RN записывает IP-адреса источника и назначения, номера портов и последовательность номеров пакетов для всех TCP-сессий или UDP-потоков, которые

удовлетворяют установленным политикам безопасности (правилам). Если пакет не принадлежит ни одной из открытых сессий, то он поступает на проверку соответствия правилам МСЭ RN. Пакеты, не сочетающиеся с правилами МСЭ - уничтожаются.
Полнофункциональное инспектирование более надежно, чем пакетная фильтрация, потому как последняя пропускает все пакеты, относящиеся к разрешенным сессиям. Например, вместо того чтобы позволить любому хосту или программе посылать любой тип TCP-трафика на 80-ый порт, полнофункциональное инспектирование проверит принадлежность пакета к какой-либо существующей сессии. Потом, более того, МСЭ может аутентифицировать пользователя, когда сессия будет установлена, может так же определить – действительно ли поток несет HTTP трафик и может запрещать требуемые типы трафика на 7-ом уровне (к примеру фильтровать URL по черному списку сайтов).

Обработка пакетов

Когда приходит пакет, RN начинает его просматривать на сетевом уровне. RanchOS выполняет проверку корректности пакета. Например, если MAC-адрес весь по нулям, то пакет уничтожается сразу, т.е. система не будет тратить ресурсов впустую. Если пакет нормальный, то RanchOS просматривает таблицу соединений, что бы узнать – является ли пакет частью существующей TCP-сессии. (Хотя UDP – это протокол без установления соединения, но RN все равно создает псевдо-сессию для отображения каждого UDP-потока).
Если сессия уже создана, RanchOS проверяет порядковый номер пакета, код сегмента для удостоверения в том, что пакет действительно принадлежит этой очереди. Например, неправильный порядковый номер пакета может служить признаком перехваченной сессии.
Если сессия не создана, то пакет должен быть классифицирован – т.е. как мы должны найти правило (политику безопасности), которое определит, что нужно делать с пакетом. Это то в чем другие МСЭ проигрывают, требуя системных администраторов выбирать между безопасностью и производительностью [4].

Выбор модели Ranch Networks - RN300, RN310 и RN500

RN300, RN310 – это экономичные, но вместе с тем мощные сетевые продукты для решения вопросов информационной безопасности, рассчитанный на маленькие и средние организации. RN300 предлагает множество функций сосредоточенных в едином устройстве, призванных удовлетворить потребности самого искушенного специалиста по информационной безопасности, при чем по самой низкой цене [4].

RN500 – это прогрессивный программно-аппаратный продукт, комбинирующий в себе многочисленные функции, которые обычно реализуются в отдельных устройствах. Благодаря реализованной в RN500 технологии однопроходного сканирования пакетов стала возможной интеграция множества сервисов в единой конструкции – 30 зон безопасности; управление полосой пропускания; балансировка нагрузки; мониторинг состояния серверов в режиме реального времени; автоматическое определение сети; аккаунтинг; коммутация на 2-4 уровнях – с полной управляемостью, и все это по единой низкой цене. Встроенный полнофункциональный firewall эффективно разобьет существующую локальную сеть на множество индивидуально-защищенных зон – каждая с собственной политикой безопасности в обоих направлениях между всеми зонами. Также включены дополнительные уровни безопасности: аутентификация пользователей, виртуальные зоны, «безопасность по требованию». Зона может быть посвящена департаменту корпорации или другому целевому сегменту сети.

Описание оборудования RN300

Рис. 18. Оборудования RN300

Качество

Все устройства RN работают на базе операционной системы реального времени VxWorks немецкой фирмы WIND RIVER. Поверх нее работает собственная операционная система RanchNetworks, написанная специалистами компании Ranch Networks.

В качестве центрального процессора был выбран PowerPC - микропроцессорная RISC-архитектура, созданная в 1991 году альянсом компаний Apple-IBM-Motorola, известном как AIM.

Безопасность

В RN300 встроено 20 полнофункциональных межсетевых экранов (МСЭ), обеспечивающих многоуровневую фильтрацию пакетов, приоритезацию трафика критически-важных приложений реального времени (например, голосовой и видеосвязи), выделение полосы пропускания для данного трафика.

RN300 позволяет сегментировать сеть на 5 зон безопасности.

Возможно построение динамического МСЭ, где им управляет IDS Snort. В этом случае мы получаем IPS, т.к. IDS Snort может динамически добавлять и удалять правила в МСЭ RN.

Поддержка протоколов и SNMPv3 и MIDCOM гарантирует безопасность управления, благодаря аутентификации и шифрованию управляющего трафика.

Использование Asterisk для VoIP

Это запатентованная и единственная в мире технология динамического открытия и закрытия портов для RTP трафика. Здесь телефонная станция Asterisk управляет МСЭ RN, используя протокол MIDCOM / SNMP.

Управление

Управление RN300 осуществляется через WEB-интерфейс и с помощью протоколов SNMP/MIDCOM. Протоколы SNMP/MIDCOM могут динамически добавлять правила в МСЭ, ограничивать полосу пропускания. Все основные настройки осуществляются через WEB-интерфейс, по протоколу Secure Sockets Layer (SSL/HTTPS), препятствуя попыткам злоумышленников получить доступ к коммутатору по IP-сетям. WEB-интерфейс одинаков у всех устройств и логически понятен.

Аутентификация

Поддержка механизма аутентификации IEEE802.1X Network Login обеспечивает защиту при подключении пользователей к сети. В устройства RN встроен собственный RADIUS сервер. Средства предотвращения вторжений защищают сеть и отклоняют все пакеты от неавторизованных пользователей.

Приоритезация и управление пропускной способностью

Наличие неограниченного числа очередей на каждую сессию и способность динамически выделять ширину полосы пропускания позволяет устройствам RN эффективно использовать

сетевые ресурсы и обеспечивать QoS «важного для бизнеса» и «чувствительного ко времени задержки» трафика, в том числе голосового трафика (VoIP).

Пример решения с RN300

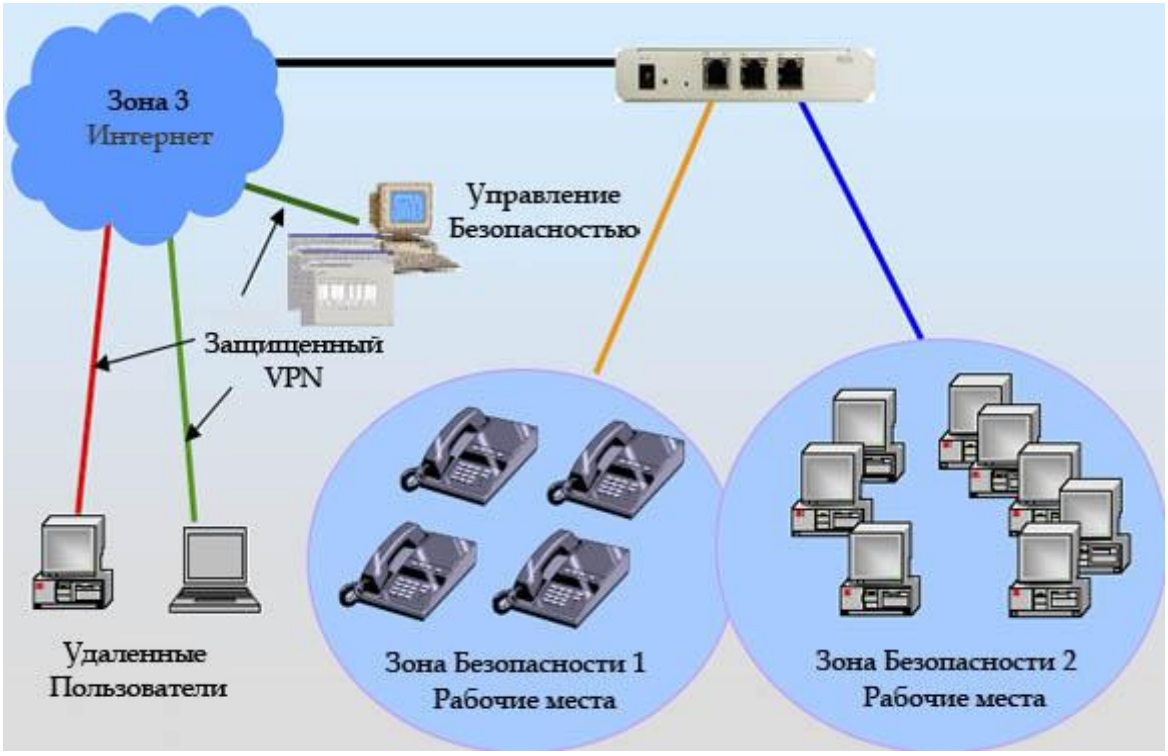


Рис. 19. Пример решения с RN300

Техническая характеристика RN300

Производительность

- Кол-во одновременных сессий: 24000;
- Пропускная способность МСЭ: 100 Мбит/с.

Дополнительные возможности

- Поддержка 20 полнофункциональных МСЭ;
- Управление полосой пропускания для пользователей / приложений;
- Мониторинг состояния серверов (ICMP ping);
- Поддержка VPN IPSEC (DES, 3DES, AES, RC4, RC5); 32 туннелей VPN;
- Построение динамического МСЭ (системы IPS) на базе IDS Snorth;
- Поддержка VoIP (SIP) с использованием Asterisk (динамический МСЭ).

Порты

- 3 RJ45 порта 100 Мбит/с.

Управление

- WEB интерфейс;
- Управление по протоколу SNMP v1, 2, 3;
- Управление по протоколу MIDCOM.

Описание оборудования RN310

Рис. 20. Оборудование RN310

Безопасность

В RN310 встроено 132 полнофункциональных межсетевых экранов (МСЭ), обеспечивающих многоуровневую фильтрацию пакетов, приоритезацию трафика критически-важных приложений реального времени (например, голосовой и видеосвязи), выделение полосы пропускания для данного трафика.

RN310 позволяет сегментировать сеть на 12 Зон Безопасности.

Все остальные функции RN310 идентичны функциям RN300.

Пример решения с RN310

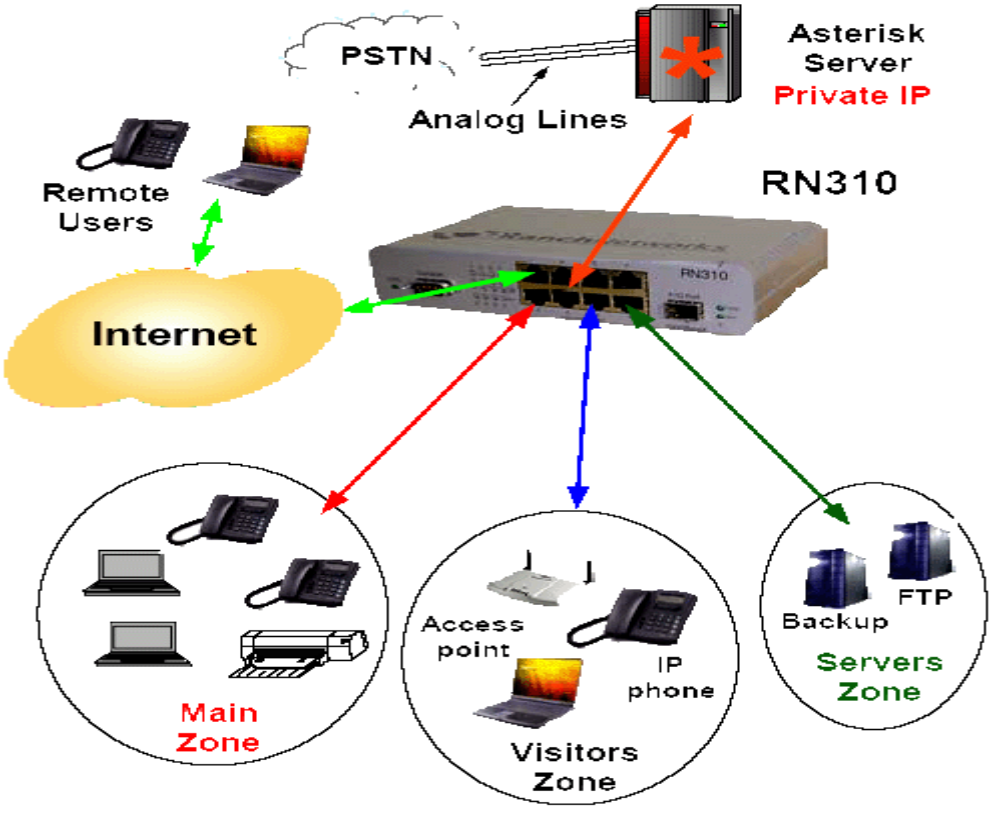


Рис. 21. Пример решения с RN310

Техническая характеристика RN310

Производительность

- Количество одновременных сессий: 50000;
- Пропускная способность МСЭ: 100 Мбит/с.

Дополнительные возможности

- Поддержка 132 полнофункциональных МСЭ;
- Управление полосой пропускания для пользователей / приложений;
- Мониторинг состояния серверов (ICMP ping);
- Поддержка VPN IPSEC (DES, 3DES, AES, RC4, RC5); 32 туннелей VPN
- Построение динамического МСЭ (системы IPS) на базе IDS Snorth;
- Поддержка VoIP (SIP) с использованием Asterisk;
- Функция дублирования IP PBX Asterisk (1+1 High Availability).

Порты

8 RJ45 портов 100 Мбит/с;
1 порт GBIC 10/100/1000 Мбит/с;
1 порт RS232;
1 порт USB.

Описание оборудования RN500

Рис. 22. Оборудование RN500

Качество:

Устройства RN500 и RN700 построены по конвейерной архитектуре. На каждом порту стоит свой процессор, затем четыре порта объединяют и ставят еще один процессор, получившиеся три процессора объединяет центральный процессор (в случае RN500 с 12 портами).

Безопасность

В RN500 встроено 870 полнофункциональных межсетевых экранов (МСЭ), обеспечивающих многоуровневую фильтрацию пакетов, приоритезацию трафика критически-важных приложений реального времени (например, голосовой и видеосвязи), выделение полосы пропускания для данного трафика.

RN500 позволяет сегментировать сеть на 30 зон безопасности.

Использование Asterisk для VoIP

Отказоустойчивость

Два устройства RN500 могут быть объединены, для построения более надежной системы (MTBF 200'000 часов) с “горячей заменой” (redundancy). Второе устройство находится в спящем режиме. При выходе из строя одного устройства все сессии переключаются на второе устройство.

Дополнительно для RN500 можно докупить внешний аварийный блок питания, который при выходе из строя основного (на 220В) будет подавать на шину устройства уже стабилизированное напряжение 48В.

Простота эксплуатации

RN500 автоматически определяет и настраивает соответствующий режим для соединений с использованием кабелей с прямой или перекрестной разводкой пар (auto MDI/MDIX), позволяя избежать необходимости поиска кабеля нужного типа.

Аутентификация

Устройство RN500 имеет возможность аутентификации на основе MAC-адресов, что обеспечивает контроль доступа на границе сети.

Пример решения с RN500

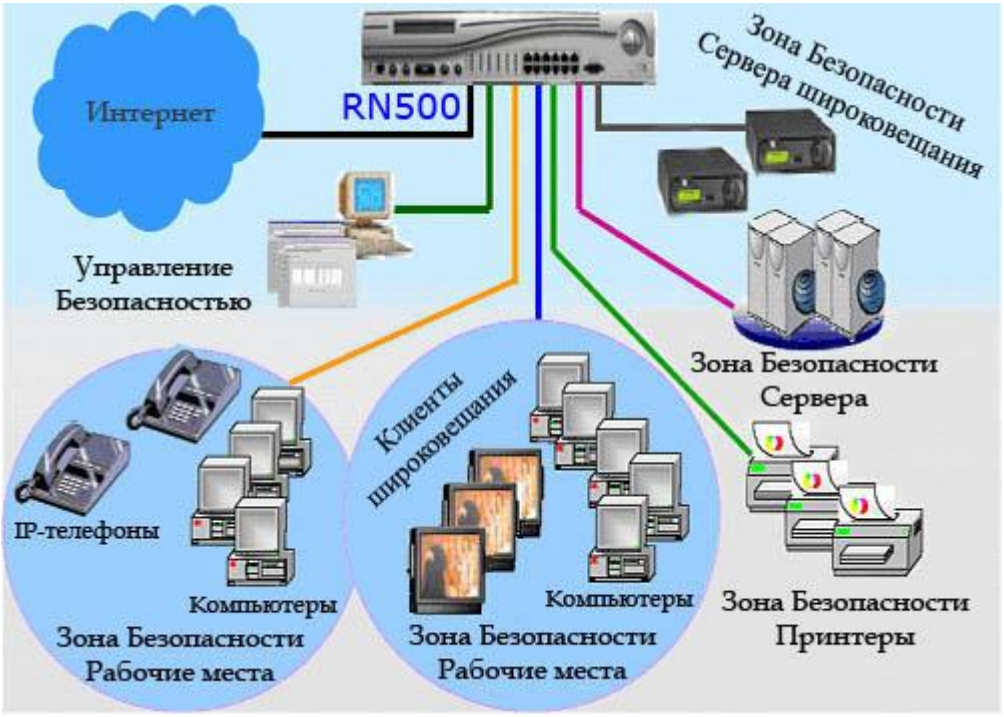


Рис. 23. Пример решения с RN500

Техническая характеристика RN500

Производительность

- Кол-во одновременных сессий: 256000;
- Пропускная способность МСЭ: 500 Мбит/с.

Дополнительные возможности

- Поддержка 870 полнофункциональных МСЭ;
- Балансировка нагрузки в каждой зоне безопасности (алгоритмы Round Robin, Weighted Round Robin, Least connections);
- Управление полосой пропускания для пользователей / приложений;
- Мониторинг состояния серверов (ICMP ping);
- Поддержка VPN IPSEC (DES, 3DES, AES, RC4, RC5); 128 туннелей VPN;
- Построение динамического МСЭ (системы IPS) на базе IDS Snorth;
- Поддержка VoIP (SIP) с использованием Asterisk;

- Функция дублирования IP PBX Asterisk (1+1 High Availability);
- Поддержка масштабирования Asterisk ("Matrix" Scalability);
- Поддержка режима “горячей замены” (redundancy);
- Резервирование электропитания с помощью аварийного блока питания.

Порты

- 12+1 RJ45 порта 100 Мбит/с.

Также компания Ranch Networks предлагает устройство RN700, которое представляет собой прогрессивный программно-аппаратный продукт, комбинирующий в себе многочисленные функции, которые обычно реализуются в отдельных устройствах. RN700 позволяет сегментировать сеть на 30 зон безопасности, также в RN700 встроено 870 полнофункциональных межсетевых экранов (МСЭ), обеспечивающих многоуровневую фильтрацию пакетов, приоритезацию трафика критически-важных приложений реального времени (например, голосовой и видеосвязи), выделение полосы пропускания для данного трафика.

Эти устройства предназначены для больших корпоративных предприятий, поэтому в рамках данного проекта нет смысла их рассматривать.

Необходимо выбрать модель Ranch Networks для ее реализации в нашем проекте. НПФ «Микран» представляет собой не большое предприятие, штат сотрудников которого составляет не более 200 человек. Также выше было сказано, что однопроцессорный сервер, где будет установлено ПО Asterisk, Pentium D820 2.8 2G RAM способен выдерживать 120 одновременных звонков по FXO/FXS/E1 и 240 звонков по IP. Тип ЛВС в которую внедряется IP-телефония в НПФ «Микран»: проводная, Fast Ethernet 100 Мбит, по спецификации физического уровня – 100Base-TX.

Теперь рассмотрим технические характеристики RN300, RN310 и RN500.

Таблица 5. Технические характеристики RN300, RN310 и RN500

Модель RN	Кол-во одновременных сессий	Пропускная способность МСЭ, Мбит/с	Максимальное количество зон безопасности	Количество МСЭ, поддерживаемых RN
RN300	24000	100	5	20
RN310	50000	100	12	132
RN500	256000	500	30	870

Из таблицы 5 мы видим, что в нашем случае будет излишним использовать модель RN500, так как она также как и RN700 рассчитана на предприятия более крупного масштаба.

Таким образом, необходимо сделать выбор между RN300 и RN310. Количество зон безопасности является основным критерием при выборе RN (конечно количество одновременных сессий у RN310 больше, чем у RN300, но это не является показателем для нашей сети, так как сервер Asterisk способен поддерживать всего около 240 одновременных разговоров), так как все функции RN310 идентичны функциям RN300. Так как НПФ «Микран» постоянно «растет», как в плане количества сотрудников так и внедрению новых технологий, то наилучшим образом будет выбрать устройство RN310, так как оно имеет большее количество зон безопасности.

Реализация RN300 в сети IP-телефонии

Ранее была показана структура сети IP-телефонии на основе Asrerisk IP PBX. При этом эта сеть является абсолютно не защищенной, так как сам по себе Asterisk не предусматривает какую-либо защиту. В Ranch Networks был разработан код NetSec, который был интегрирован в коды IP PBX Asterisk. Этот код использует протокол MIDCOM (MiddleBox Communication)

для связи между IP PBX Asterisk и устройствами RN. Таким образом, для защиты сети был выбран продукт Ranch Networks RN310, который позволяет организовать до 12 зон безопасности и поддерживает 132 полнофункциональных межсетевых экранов.

Итак, что же представляет собой МСЭ RN310 для нашей сети? МСЭ RN310 – это устройство экспертного уровня, которое может выполнять фильтрацию на всех уровнях модели OSI, имеет до 132 независимых полнофункциональных МСЭ с запоминанием состояния, поддерживает списки доступа ACL и VPN-шифрование, скрывает IP-адреса внутренней сети (NAT) и порты приложений (PAT), обеспечивает обнаружение распространенных атак.

В качестве примера, первоначально разобьем ЛВС на три виртуальные зоны безопасности: зона 1 – представляет собой виртуальную локальную сеть, являющуюся частью всей сети ЛВС, зона 2 – является также VLAN и включает в себя удаленное крыло, и зоной 3 – будет являться Интернет. Впоследствии при установке RN310 в зависимости от структуры предприятия и его политики безопасности заказчик сам разобьет сеть на то количество зон, которое этому предприятию необходимо, а также определит специфику этих зон: физической или виртуальной она будет. Разбиение на зоны осуществляется исходя из бизнес-логики конкретной компании.

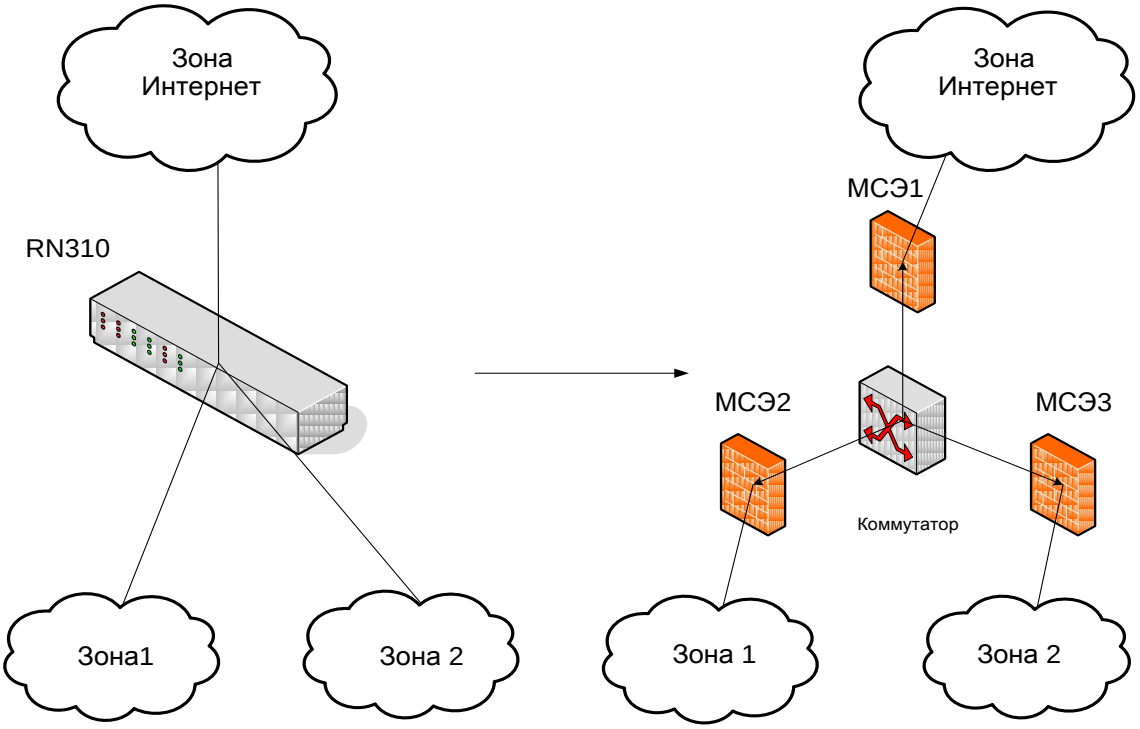


Рис. 24. Логическое изображение продукта RN310 для сетевой топологии с 3-мя зонами безопасности

На этом рисунке зона 1 и 2 во внутренней сети олицетворяют LAN, зона Интернета во внешней сети – WAN. Как видно каждый пакет следует из любой зоны в любую зону, проходя через полнофункциональный firewall с запоминанием состояния. Это означает, что каждая сессия TCP/UDP или ICMP будут терминироваться и затем передаваться как новая сессия TCP/UDP или ICMP в другую зону. Это произойдет даже между зонами 1 и 2, которые относятся к внутренней сети. Такая функциональность полнофункциональных МСЭ дает пользователям следующие преимущества:

Безопасность

Если вирус или хакер будут атаковать зону 1, к примеру, используя SYN, FIN, ICMP/UDP затопление, «Ping of Death», или другие хорошо известные типы атак, все зоны будут защищены, потому что эти атаки будут отражены межсетевым экраном МСЭ1. Другими словами, весь входящий трафик из зоны 1 в устройство RN310 будет проверен точно так же, как если бы это был трафик из зоны Интернет. Следует отметить, что атака на зону 1 никак не повлияет на трафик между зоной 2 и Интернет зоной. Таким образом, устройство RN310 с зонами безопасности будет защищать от атак, зловредных кодов и вирусов даже маленькие части корпоративной сети клиента.

Пассивные вирусы или шпионское программное обеспечение обычно прослушивают сеть, собирая информацию о хостах, серверах и трафике на сети, затем посылают во внешнюю сеть всю собранную информацию. Поскольку все сессии между зонами обрабатываются полнофункциональными МСЭ в устройстве RN310, пассивные вирусы или шпионские программы будут не в состоянии отсылать информацию о всей сети – только об инфицированной зоне. Для примера, если такая шпионская программа работает на хосте в зоне 1, то он не сможет послать информацию о хостах и других активных членах зоны 2. Если в зоне 2 имеется секретная информация, то она не станет известна хакерам. Так как зона безопасности может быть сколь угодно малой, вплоть до одного хоста или сервера, то устройство RN310 может полностью защитить внутри сетевых пользователей и ресурсы от такого рода угроз.

*NAT (*Network Address Translation*)*

Используя концепцию зон безопасности RN310 может реализовать множественные преобразования сетевых адресов (NAT) с полнофункциональными МСЭ между ними. В данном случае активизировано 3 full NAT – из зоны 1 в Интернет, из зоны 2 в Интернет и из зоны 1 в зону 2. Предположим, что в организации есть «плохой сотрудник», который хочет атаковать внутренние сервера. Если использован full NAT между зоной 1 и зоной 2, то «плохой сотрудник» из зоны 1 не узнает реальных IP адресов серверов. Таким образом, как бы не пытался «плохой сотрудник» из зоны 1 получить доступ серверам, он получит IP адрес в зоне 1 и не реальный IP адрес сервера в зоне 2. Даже если «плохой сотрудник» имеет физический доступ к серверам, он не сможет идентифицировать искомый сервер, особенно, если число серверов в зоне 2 велико.

Описанная выше функциональность full NAT возможна, только благодаря продукту RN300 с зонами безопасности и полнофункциональными МСЭ между ними.

Регистрация

Поскольку продукт RN310 имеет зоны безопасности с полнофункциональными МСЭ между ними, все устройства RN310 проверяют TCP/UDP/ICMP соединения. Фактически это позволяет регистрировать события безопасности, такие как SYN, FIN, ICMP/UDP затопление, «Ping of Death» или другие известные типы атак из внутренних или внешних Зон.

Управление Полосой Пропускания

Реализован точный и «мелкозернистый» контроль над полосой пропускания (основанный не только на QoS), используя полнофункциональные МСЭ между зонами безопасности.

Полнофункциональный МСЭ на каждую зону функционирует, как независимый источник исходящего или входящего трафика из/в любую другую зону. Можно быть уверенными, что используемые в устройстве RN310 контракты для управления полосой пропускания, будут функционировать корректно.

Например, полнофункциональный межсетевой экран МСЭ1 зоны 1 посылает только разрешенные сессии полнофункциональному межсетевому экрану МСЭ2 зоны 2. Тогда, количество трафика, отправленного из зоны 1 в зону 2 будет контролироваться определённым «исходящим контрактом» межсетевого экрана МСЭ1. Количество исходящего трафика будет всегда правильным, поскольку состоит только из проверенного трафика (который не

содержит вирусов). В тоже время, объем трафика, который принимает МСЭ2 от МСЭ1 и МСЭ3 (зона Интернет) контролируется «входящими контрактами» МСЭ2, и, так как оба потока тщательно проверены, то «исходящие контракты» зоны 2 тоже верны.
Объединив Asterisk и RN310 мы осуществляем технологию безопасности “по требованию” (security-on-demand) для VoIP соединений. В этом случае Asterisk сообщает RN300, какие правила необходимо добавить в межсетевой экран для данного VoIP соединения. Такие правила будут создаваться для каждого VoIP соединения, прошедшего через устройство RN310. Это означает, что каждый запрос на установление VoIP соединения будет обработан динамически - правила межсетевого экрана (которые разрешают прохождение голосового трафика), будут созданы, когда это необходимо и удалены сразу после окончания разговора.
Таким образом, объединение Asterisk и RN310 это лучший способ обеспечить безопасность VoIP переговоров.
Следующий рисунок 25 представляет сценарий установления соединения.

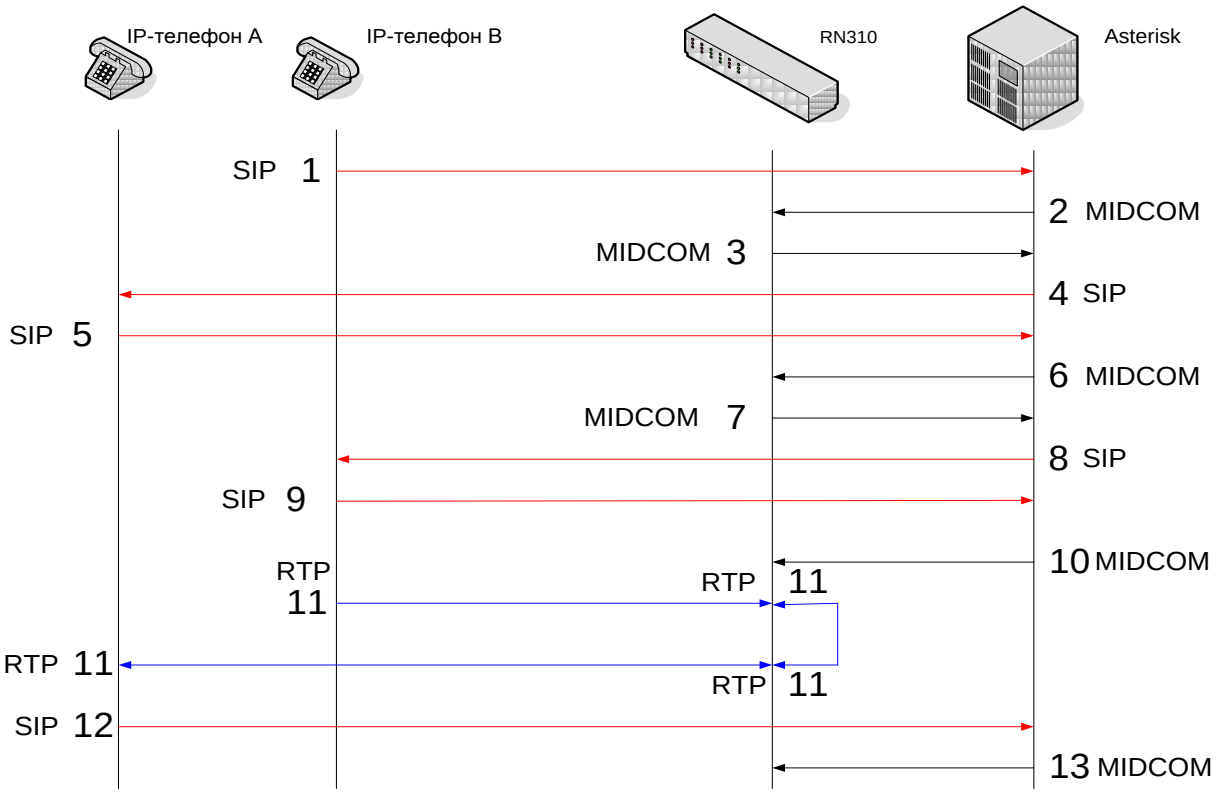


Рис. 25. Сценарий установления соединения

1. Абонент B посылает сообщение INVITE серверу Asterisk.
2. Asterisk посылает запрос RN300 на установление правил для абонента B.
3. RN310 создает правила установления соединения для абонента B.
4. Далее Asterisk посылает сообщение INVITE абоненту A для установления соединения с абонентом B.
5. Если вызываемый пользователь ответил на звонок, то на запрос INVITE высылается ответ OK.
6. Asterisk посылает запрос RN300 на установление правил для абонента A.
7. RN310 создает правила установления соединения для абонента A.
8. Asterisk посылает сообщение INVITE абоненту B для установления соединения с абонентом A.

9. Вызывающий пользователь отправляет сообщение ACK, сообщающее Asterisk о том, что он получил ответ на свой запрос INVITE, им задаются окончательные параметры соединения. На этом этапе все готово к установлению соединения по протоколу RTP (Real-time Transport Protocol).
10. RN310 создает RTP мост внутри себя для передачи RTP трафика между абонентами A и B.
11. Устанавливается RTP-соединение с заранее согласованными параметрами.
12. Для завершения соединения, завершающим пользователем (кладет трубку) высылается запрос BYE, на которое высылается ответ OK.
13. Asterisk посылает запрос на удаление правил для данного соединения.

Как показано на рисунке, устройство RN310, работая в паре с Asterisk IP ATC, создает и удаляет правила в межсетевом экране. Также, RN устройство создает RTP мост внутри себя, что разгружает IP ATC и дает возможность Asterisk обрабатывать большее количество звонков в единицу времени.

Как уже было сказано выше, RN310 поддерживает механизм аутентификации IEEE802.1X. Network Login обеспечивает защиту при подключении пользователей к сети. В устройства RN встроен собственный RADIUS сервер. Средства предотвращения вторжений защищают сеть и отклоняют все пакеты от неавторизованных пользователей.

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 умный коммутатор) будет открыт и пользователь получит доступ к ресурсам сети.

IEEE 802.11x определяет три основных компонента в сетевом окружении:

Сапликант (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. Его роль выполняет Asterisk IP PBX.

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.

RADIUS - сервер

RADIUS-протокол предназначен для работы в связке с сервером аутентификации, в качестве которого обычно выступает RADIUS-сервер

Для того, чтобы пользователи проектируемой сети имели разграниченный доступ (в зависимости от логина и пароля), а также для того, чтобы избежать атак извне, необходимо иметь отдельный сервер авторизации (AAA-сервер).

В качестве такого сервера, в нашей сети будет выступать RADIUS сервер.

На данный момент существует большое множество RADIUS серверов, реализованных как программно, так и аппаратно. Большинство из них – это коммерческие продукты [1].

Ниже приведен рисунок 26, на котором показан механизм авторизации.

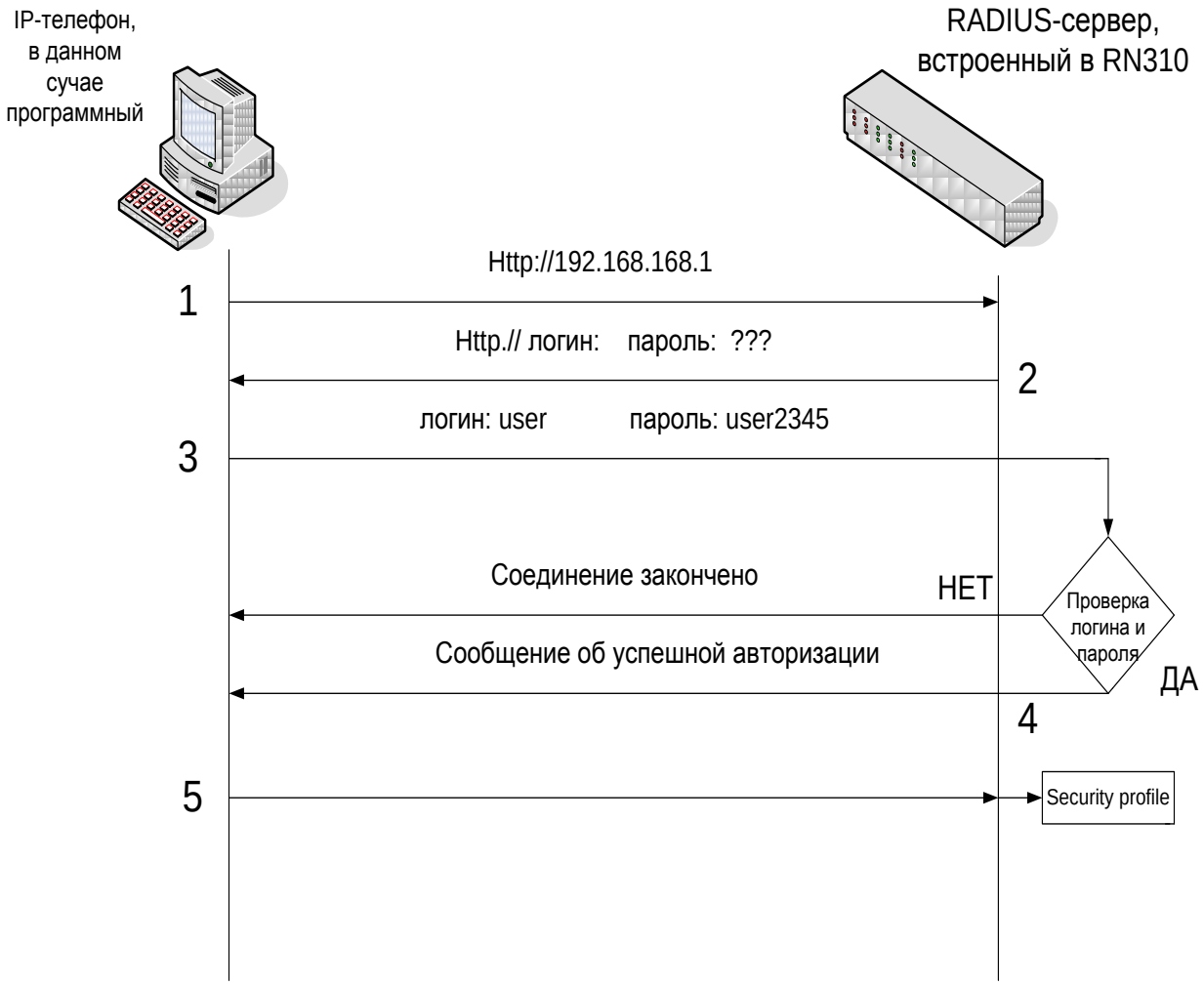


Рис. 26. Механизм авторизации в RN310

1. Пользователь обращается к RADIUS-серверу за авторизацией: WWW браузер направляется на RN310 IP interface для данной зоны. Если IP, к примеру, равно 192.168.168.1 то URL строка будет такая: http:// 192.168.168.1.

2. RADIUS–сервер отвечает пользователю страницей на которой предлагается ввести имя и пароль для авторизации.

3. Пользователь вводит требуемую информацию, и она отсылается на RADIUS-сервер.

4. На основании полученной информации RADIUS-сервер проверяет имя и пароль. Если есть несоответствие полученной и хранимой информации, то запрос на авторизацию аннулируется, и пользователь получает (в окне браузера) сообщение об отказе. В этом случае пользователь не сможет выйти за пределы своей зоны. В положительном случае RADIUS-сервер авторизует пользователя, и пользователь получает (в окне браузера) сообщение об успешной авторизации. В этом случае пользователь получает права доступа к сети в соответствии с правилами безопасности, которые были сконфигурированы для него.

5. Направление сетевого потока от авторизированного пользователя (который направлен в другие зоны безопасности) будет регулироваться согласно правилам безопасности установленным для этого пользователя в security profile.

В результате, используя гонцепцию «Зон Безопасности», мы имеем следующее:
1. Сеть IP-телефонии разбита на 3 зоны безопасности с собственными независимыми профилями безопасности для каждой зоны.

Как было сказано выше, устройство RN310 поддерживает до 5 таких зон, разделенных между собой полнофункциональными МСЭ. Правила МСЭ могут быть установлены на 2-ом, 3-ем,4-ом и 7-ом уровнях модели OSI. Доступны все возможности NAT. В несанкционированной попытке доступа к зоне или IP – адресу будет отказано так же, как и в такой попытке из зоны или IP–адреса.

При установке RN300 в НПФ «Микран» заказчик сам определит количество зон которое ему необходимо и их структуру в зависимости от бизнес-логики этой компании.
2. Защита от DoS, SYN – атак, ICMP затоплений обеспечивается между каждой парой защищенных зон.
3. Аутентификация для входа или выхода из зоны безопасности. Это означает, что ни один пакет не пройдет через устройство RT310, до тех пор, пока пользователь в первый раз не введет логин и пароль. Однажды аутентифицированный, он получит доступ только к той области корпоративной сети, к которой он имеет авторизацию.
4. RN310 автоматически или вручную, благодаря зонам безопасности, может изолировать внезапно возникшие проблемные места.
5.Ограничение полосы пропускания будет настроена для каждой зоны.
6. Качество обслуживания (QoS) (имеется в виду управление полосой пропускания)
1. Гарантированная, минимальная, максимальная и групповая полоса пропускания может быть выделена на основании зоны отправителя/получателя, IP – адреса (группы), MAC – адреса, номера порта (группы). Таким образом, возможна приоритезация трафика по пользователю или по приложению внутри входящего/исходящего потока.
2. Полоса пропускания может быть выделена как статически (конкретное значение), так и динамически (разделяемую полосу использовать по требованию, нечто близкое к Frame Relay).

Устройство RN310 имеет полнофункциональные МСЭ с запоминанием состояния на каждую зону безопасности для проверки TCP/UDP/ICMP соединений. Каждому соединению (потоку) МСЭ назначает выделенную полосу пропускания, и затем создаются очереди для каждого потока. Количество поддерживаемых соединений в RN310 равно 50000, а в нашем случае максимальное количество соединений поддерживаемых сервером всего 240. Это значит, что логически и физически 240 очередей могут быть созданы в памяти устройства RN310.

Провайдер IP-телефонии - SIPNET

Как уже говорилось выше (п.2) IP-телефония позволяет существенно сократить расходы на междугородные и международные переговоры. Чтобы использовать эту возможность, необходимо подключиться к провайдеру IP-телефонии.
Можно выделить два наиболее популярных варианта подключения к провайдерам междугородной и международной телефонии:

- Через ТФОП (Телефонная сеть Общего Пользования) - при подключении пользователь набирает "городской" номер сервера IP-телефонии провайдера, проходит аутентификацию (по pin-коду) и набирает нужный ему номер. Чтобы пользоваться IP-телефонией по этой схеме, достаточно иметь обычный городской номер.
- Через программные (в том числе и бесплатные) и аппаратные IP-телефоны.

Российских провайдеров IP-телефонии довольно много. Один из популярных провайдеров IP-телефонии, поддерживающих протокол SIP является SIPNET [8].

SIPNET — является российским провайдером IP-телефонии.
SIPNET — это сеть Интернет-телефонии нового поколения, в которой реализованы последние достижения в области инфокоммуникаций, обеспечивающие эффективный обмен голосовой и мультимедийной информацией.
Пользователи сети могут неограниченно и бесплатно общаться через Интернет со всеми участниками сети SIPNET, бесплатно говорить по Интернету из любого города мира с абонентами городских сетей Москвы и Санкт-Петербурга, а так же с абонентами сотовых сетей Москвы, имеющих прямые номера.
С абонентами обычных городских сетей любой страны пользователи сети SIPNET могут общаться из любого города, где есть Интернет, причем по очень низким тарифам и с максимально возможным качеством, соответствующим варианту подключения к Интернету.
Среди главных преимуществ SIPNET — альтернативная нумерация, при которой каждый пользователь становится владельцем персонального сетевого номера — SIP ID, являющегося единым идентификатором пользователя в любой точке мира. В отличие от обычного телефонного номера этот номер не зависит от городских телефонных сетей, междугородных и международных линий связи и будет работать в любом месте, где есть Интернет.
В сети SIPNET реализована система интернет-пейджинга. За каждым пользователем автоматически закрепляется E-mail адрес, который также является его персональным идентификатором и по которому можно отправить мгновенные текстовые и голосовые сообщения или организовать сеанс голосовой связи.
Все пользователи SIPNET получают возможность:

- Персонально настроить стоимость и качество по любому направлению (настройка маршрутизации);
- Заказать соединение двух абонентов в любых точках мира;
- Переадресовать входящие звонки с SIP ID на любое абонентское устройство;
- Анализировать статистику совершенных соединений и управлять всеми сервисами SIPNET в Личном кабинете в режиме on-line.

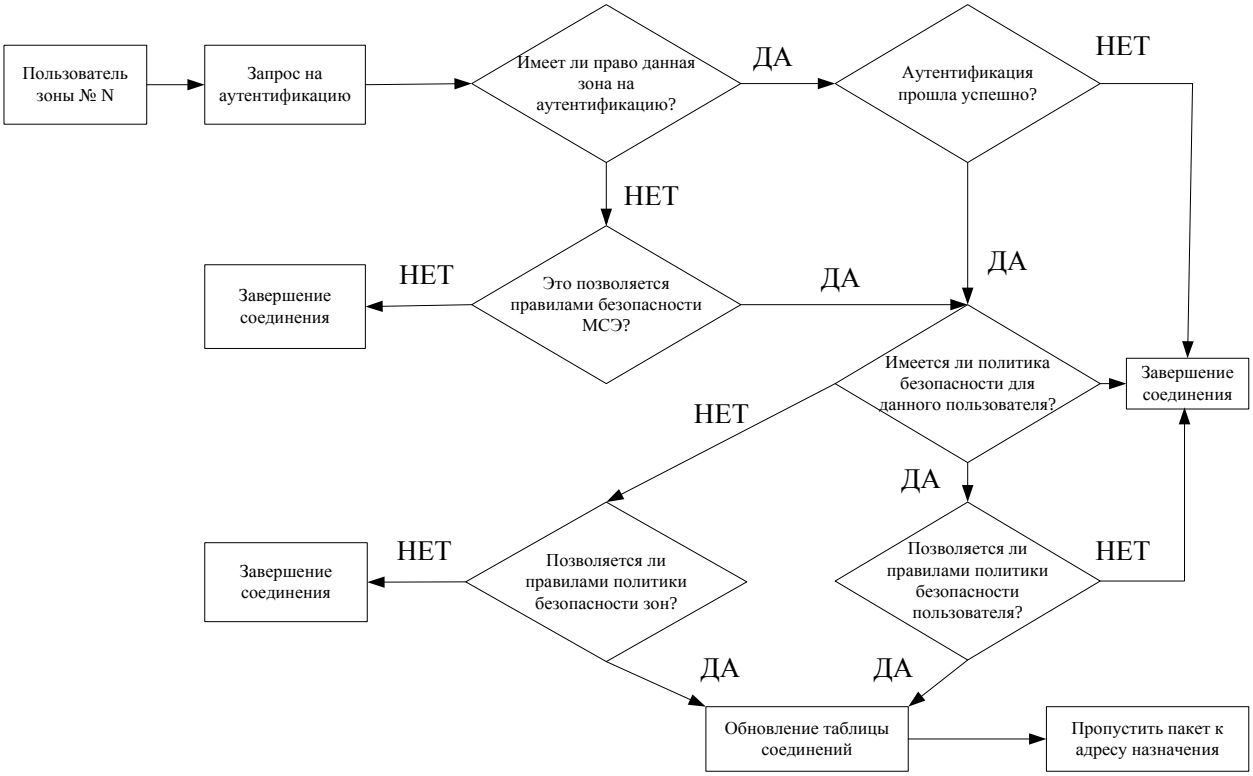
Для подключения к сети SIPNET можно использовать любое сертифицированное SIP-оборудование или компьютер с программным SIP-телефоном.
Интернет-телефония SIPNET обеспечивает высокое качество передачи голоса и конфиденциальность соединений, а также возможность осуществлять настройки соединений по цене, качеству и другим параметрам.
Пополнить счет можно через мобильный кошелек Билайн, Яндекс.Деньги, WebMoney. Наличные можно внести в платежных терминалах ОСМП, Кредит-пилот, Dixis и в отделениях Сбербанка (нужно предварительно распечатать квитанцию). Перевести платеж с банковской карты (Visa, Eurocard/MasterCard) можно при помощи системы КиберПлат.
Подключение и оплата услуг
Подключение к SIPNET — бесплатное. Более того, после подключения на вашем счёту уже будет находиться 1 у.е.
Самый простой путь подключится к SIPNET купить гарнитуру, бесплатно установить на свой компьютер один из программных телефонов и пройти регистрацию в SIPNET. Подключение к SIPNET компьютера с программным телефоном минимизирует начальные расходы — сегодня это самый популярный способ подключения.
По соотношению «цена/качество/возможности» Интернет-телефония не имеет себе равных, существенно уменьшая расходы на связь.
Только Интернет-телефония обеспечивает бесплатные соединения между пользователями, независимо от того, где они находятся.
Бесплатно говорить с пользователями SIPNET могут жители около 60-ти городов России, СНГ, США.

Участники SIPNET имеют возможность не только пользоваться услугами голосовой связи, но и обмениваться мгновенными текстовыми и голосовыми сообщениями, передавать любые файлы, устраивать аудио- и видеоконференции.

Структурная схема лабораторного макета

«Защищенной телекоммуникационной сети связи на основе технологии IP-телефонии»

Блок-схема алгоритма защиты сети IP-телефонии



Анализ перспективы развития сети

Имеется перспектива развития сети IP-телефонии, так как в скором будущем НПФ «Микран» открывает еще один офис, который будет территориально удален от основного офиса, для которого была спроектирована данная система.

Asterisk позволяет организовать соединение, когда имеется несколько офисов, между которыми нужно организовать связь. Самой эффективной схемой объединения офисов является так называемая “полносвязка”, когда Asterisk в каждом из офисов соединён с каждым из остальных офисов. Таким образом, выход из строя любой из офисных АТС никак не повлияет на связь в других офисах.

Сеть IP-телефонии в новом офисе будет идентична сети спроектированной для данного офиса. Она также будет основана на ПО Asterisk и иметь такую же структуру сети как показано на рисунке 9.7.

Обеспечение сетевой безопасности в территориально распределенных офисах, которые используют VoIP дело весьма сложное. Как правило, такая задача решается комплексно, с применением различных сетевых устройств и программного обеспечения. Однако очень часто компании не могут предоставлять услуги VoIP, Video конференций и т.д. удаленным филиалам и/или пользователям, так как не в состоянии обеспечить внутреннюю безопасность сети и необходимое качество передачи голоса или видео. Именно в решении таких задач и помогают устройства Ranch Networks в интеграции с IP PBX на открытых кодах Asterisk.

Для обеспечения безопасности и повышения качества голосовой связи офис №2 подключен к Интернету через другое устройство Ranch Networks, скорее всего это будет RN300. Так же, как и устройство, установленное в центральном офисе, RN300 обеспечит безопасность, NAT/PAT, VPN, DHCP, QoS, управление полосой пропускания и т.д.

Все удалённые филиалы могут иметь одинаковые частные IP-адреса, при этом устройства RN полностью решают проблему VoIP NAT traversal без применения VPN-туннелей или

использования выделенных линий. Очень важно отметить, что оба офиса имеют внутренние конвергентные сети, которые используются для одновременной передачи данных и голоса, так как устройства RN защищают эти сети и обеспечивают гарантированную полосу пропускания для голосового трафика.
Но если все-таки необходимо шифрование и дешифрование трафика, проходящего через VPN-туннель, то современные МСЭ имеют модуль VPN, позволяющий вначале расшифровывать трафик, а затем производить его фильтрацию.

4.Рекомендованная литература

1. Росляков А.В., Самсонов М.Ю., Шибаева И.В IP-телефония. - М.:, 2003.-250с
2. Жданов А. Г., Смирнов Д. А., Шипилов М. М. Передача речи по сетям с коммутацией пакетов (IP-телефония). – М.:, 2001. – 145с
3. Гольдштейн Б. С., Пинчук А. В., Суховицкий А. Л. IP-телефония. – М.: «Радио и связь», 2001. – 334с
4. Платов М.В. Asterisk и Linux: миссия IP-телефония. - Журнал "Системный администратор", N6, 2005 г. - 12-19 с
5. Платов М.В., Что важно знать об IP-телефонии. - Журнал "Системный администратор", N5, 2005 г. - 20-25 с
6. http://www.ietf.org/html.charters/midcom-charter.html
7. http://www.voipgateway.us