ДЕПАРТАМЕНТ ОБРАЗОВАНИЯ ГОРОДА МОСКВЫ
ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ПРОФЕССИОНАЛЬНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ГОРОДА МОСКВЫ
«Технологический колледж № 34»

Работа к защите допущена
Заместитель директора по УПР
_____ Н.Ю.Кузнецова
«_____»_____ 2019 г.

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА

Тема: Организация защиты информации от преднамеренных угроз в ЛВС под управлением Windows в ООО «Художественная керамика»

Специальность 10.02.01 Организация и технология защиты информации
код и наименование специальности

Группа Д-04-7ОИ

Студент _____ Лантратов Иван Вячеславович
подпись Фамилия, имя, отчество

Руководитель _____ Егоров Павел Сергеевич
подпись Фамилия, имя, отчество

ВКР представлена «____» _____2019г.

Москва, 2019 г.

ДЕПАРТАМЕНТ ОБРАЗОВАНИЯ ГОРОДА МОСКВЫ
ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ГОРОДА МОСКВЫ
«Технологический колледж № 34»

Утверждено
на заседании ПЦК
протокол № _____
«__» _____201__г.

ИНДИВИДУАЛЬНОЕ ЗАДАНИЕ
на выполнение выпускной квалификационной работы

Студента Лантратов Иван Вячеславович
Фамилия, имя, отчество

по специальности 10.02.01 Организация и технология защиты информации
код и наименование специальности

Тема выпускной квалификационной работы Организация защиты информации от преднамеренных угроз в ЛВС под управлением Windows в ООО «Художественная керамика»

Задание

1. провести анализ текущего состояния локальной сети;
2. описать защитные меры;
3. изучить политику безопасности;
4. разработать модели нарушителя и актуальных угроз;
5. разработать проект локальной сети;
6. осуществить выбор продукта для разработки защищённой сети;
7. разработать проект защищённой локальной сети на базе программного комплекса VipNet.

Дата выдачи задания_____

Срок окончания работы_____

Руководитель ВКР _____ Егоров Павел Сергеевич

Содержание

Введение.....3
1 Анализ текущего состояния локальной сети.....7
1.1 Общие сведения о локальных сетях.....7
1.2 Описание общеизвестных защитных мер.....16
1.3 Изучение политики безопасности.....24
2 Защита информации от преднамеренных угроз в локальной сети посредством VipNet.....26
2.1 Разработка модели нарушителя и актуальных угроз.....26
2.2 Выбор программного продукта для разработки защищённой сети.....33
2.3 Разработка защищённой локальной сети на базе программного комплекса VipNet.....39
2.4 Обоснование экономической эффективности проекта.....47
2.4.1 Расчёт показателей экономической эффективности проекта.....47
Заключение.....49
Список используемой литературы.....53

Введение

Современные автоматизированные системы построены в виде распределенных систем, базирующихся на компьютерных сетях, в ходе эксплуатации которых могут возникать различные нарушения работы их устройств, делающие сеть неработоспособной. Для возвращения локальных вычислительных сетей распределенных автоматизированных систем в режим штатного функционирования обслуживающий сеть персонал должен провести определенные организационно-технические мероприятия. Процесс выявления самих неисправностей и формирования комплекса мероприятий может занять значительное время и существенно повлиять на функционирование системы автоматизации предприятия в целом. Частые отказы или длительные периоды неработоспособного состояния сети могут привести к полной потере работоспособности системы автоматизации предприятия. Для повышения оперативности принятия мер, способных вернуть локальную вычислительную сеть в режим штатного функционирования, необходимо проведение мониторинга сети, который в большей части зависит от человеческого фактора. Профессионального опыта специалиста, эксплуатирующего большие вычислительные сети, зачастую не хватает для оперативной диагностики сети и принятия решения при устранении сбоев в ее работе.

Существуют системы мониторинга, централизованного управления сетью, однако вопросы, связанные с формированием единого комплекса формализованных методик и инструментальных средств автоматизации поддержки процесса обеспечения работоспособности локальной сети, позволяющего по формализованной структуре сети найти нарушения работы ее устройств и предложить обоснованный оперативный вариант их устранения, изучены в недостаточной степени.

Основное число исследований посвящено созданию, описанию работы и диагностике локальных вычислительных сетей. Принципы построения локальных вычислительных систем отражены в работах таких авторов, как Чекмарев Ю.В. Новиков Ю.В., Кондратенко С.В. Самойленко В.В., Таненбаум Э. Теоретические основы технической диагностики рассматриваются в работах Биргера И.А., Гиберта

А.И., Сердакова А.С. Исследованием и описанием параметров, позволяющих описать функционирование и потенциал сети в различных ее состояниях, то есть работоспособном состоянии и состоянии нарушения работы устройств занимаются такие исследователи, как Потапов В.И., Башарин Г.П. Для оперативного реагирования на возникающие нарушения работы устройств сети можно использовать принципы, исследуемые в работах Поспелова Д.А., Клыкова Ю.И. Процесс восстановления сетей после сбоев в работе рассматривается в публикациях Потапова В.И.

Необходимость регулярной передачи региональным филиалам свежей информации о новых ценах и объемах продукции, последних предписаниях и разработанных планах, приводит к тому, что организация встает перед проблемой выбора тех или иных ресурсов компьютерной сети. Разнообразие требований, предъявляемых к сетям пользователями и организациями, работающими с ними, приводит к разнообразию существующих локальных компьютерных сетей.

Актуальность темы. Защита информации в цифровой век - одна из важнейших задач специалистов по безопасности, системных администраторов, и других технических работников, так или иначе обслуживающих информационные системы. Все большее количество сведений, включая конфиденциальные - оказывается в доступных извне сетях и хранилищах, в которые может проникнуть злоумышленник.

Ущерб от взлома и проникновения в информационные системы, составляет, по разным оценкам, сумму от 300 миллиардов до 1 триллиона долларов в год [12]. В России только за 2016 год зафиксировано более 70 миллионов сетевых атак (данные ФСБ, там же). Поэтому, защита информации актуальна.

Несмотря на большое количество работ по теме защиты информации (Руденков Н.А., Нестеров С.А., Бирюков А.А., Эриксон Дж., и др.), полностью безопасное, и, при этом, гибкое и экономически разумное решение стоящих проблем – до сих пор не создано. Это связано, как с разнообразием применяемого оборудования и программного обеспечения, так и с постоянными, стремительными изменениями, происходящими в информационной среде, особенно, сети интернет.

Степень достоверности полученных результатов обеспечивается методологией исследования, базирующейся на различных видах анализа, статистике, экспериментальной проверке данных, применении решений, подтвердивших свою эффективность у авторов по сходной проблематике. Достоверность также подтверждается результатами практических испытаний созданной системы.

Предметом исследования выступают методы обеспечения информационной безопасности в локальных сетях.

Объектом исследования является локальная сеть.

Целью данной работы является разработка защищенной локальной сети, для повышения уровня сетевой безопасности сети, а также увеличение защищенности имеющихся сегментов сети.

Для достижения этих целей необходимо решить следующие задачи:

- провести анализ текущего состояния локальной сети;
- описать защитные меры;
- изучить политику безопасности;
- разработать модели нарушителя и актуальных угроз;
- разработать проект локальной сети;
- осуществить выбор продукта для разработки защищённой сети;
- разработать проект защищённой локальной сети на базе программного комплекса VipNet.

Методологическую базу составляют методы комплексного и системного анализа на основе междисциплинарного исследования актуальных проблем, основных понятий, предмета, структуры информации и безопасности, а также отношений, возникающих, в связи с этим, общенаучные методы познания.

Информационная база исследования послужили труды отечественных ученых таких, как Стрельцов, А.А., Конявский, В.А., Раткин, Л.С. и др., а также справочные материалы, нормативные документы, законодательные акты и Интернет-ресурсы, государственные стандарты по разработке локальных вычислительных сетей (ГОСТ Р 34.10-2012, ГОСТ Р 34.11-2012, ГОСТ Р 50571.21-2000, ГОСТ Р 53245-2008, ГОСТ Р 53246-2008). Международные стандарты, установленные Объединённым

техническим комитетом №1, являющимся подразделением Международной организации по стандартизации в области информационных технологий (ISO/IEC 11801:2010, ISO/IEC 14763-1:1999).

В работе использовались следующие методы исследования.

Теоретические: изучение, систематизация и анализ специальной литературы по исследуемой теме; изучение и обобщение опыта разработки локальных вычислительных сетей; анализ действующих конфигураций корпоративных локальных сетей, обеспечивающих устойчивую и бесперебойную работу; анализ нормативной и правовой документации.

Практические: интервьюирование, осмотр помещения для монтажа локальной сети, разработка модели локальной вычислительной сети.

Теоретическая значимость исследования заключается в том, что рекомендации по проектированию и монтажу локальной вычислительной сети могут быть использованы при организации корпоративной локальной вычислительной сети любой конфигурации, обеспечивающее устойчивую и бесперебойную работу с информацией.

Практическая значимость исследования заключается в том, что в результате проведенной исследовательской работы был создан проект защиты локальной вычислительной сети, проведен ее монтаж и тестирование на работоспособность.

Научная значимость рассматриваемой темы обусловлена важностью ее исследования и изучения, так как проблема информационной безопасности в локальных сетях в нашей стране является сегодня важнейшей задачей для специалистов в области защиты информации.

Работа состоит из введения, заключения, двух глав и списка использованных источников.

1 Анализ текущего состояния локальной сети

1.1 Общие сведения о локальных сетях

Информационно-вычислительная сеть это сеть обмена и распределенной обработки информации, которая образована множеством взаимосвязанных, независимых абонентских систем и средствами телекоммуникаций и связи.

По мнению авторов: «задачей информационно-вычислительной сети является эффективно предоставить различные информационно-вычислительные услуги пользователям сети через организацию доступа к сетевым ресурсам, распределенным в сети. Под сетевыми ресурсами понимается: информация, приложения, программы, различные периферийные устройства, принтеры, модемы, сканеры».

Можно выделить следующие преимущества компьютерных сетей:

- уменьшение затрат за счет коллективного использования разнообразных баз данных и аппаратных средств;
- стандартизация приложений - все пользователи работают на одном и том же программном обеспечении, «говорят на одном языке»;
- оперативность приобретения информации без отрыва от рабочих мест;
- эффективное проектирование и взаимодействие рабочего срока (проведение дискуссий, оперативных заседаний без отрыва от рабочих мест).

Составными элементами всех сетей являются:

- Серверы. «Под сервером в широком смысле понимается любая система, процесс, программа, компьютер, владеющие каким-либо вычислительным ресурсом (памятью, временем, производительностью процессора и т. д.) и передающие ресурсы по запросам в сеть». Один сервер может обслужить запросы сразу нескольких клиентов (поочередно или одновременно);
- Клиенты. «Клиентом называется любая система, процесс, программа, компьютер, пользователь, запрашивающие у сервера сетевой ресурс. Клиент имеет программный модуль сетевой операционной системы, предназначенный для формирования и передачи сообщений-запросов к ресурсам удаленного компьютера от разных приложений с последующим

приемом результатов из сети и передачей их соответствующим приложениям»;

- Среда. Это средства передачи информации;
- Совместно применяемые ресурсы. Информационные, аппаратные, программные;
- Совместно применяемая периферийная аппаратура.

Вычислительные сети классифицируются по различным признакам:

- по типу среды - воздушные, кабельные, беспроводные;
- по скорости - <10 Мбит/с, <100 Мбит/с, < 1000 Мбит/с;
- по архитектуре - одноранговые, клиент - серверные, гибридные;
- по топологии - шина, кольцо, звезда, mesh, смешанная;
- по размеру - LAN (<15 км), MAN (<150 км), WAN (охват Земли).

Локальные вычислительные сети (ЛВС, LAN англ. LAN – Local Area Network) принадлежат к географически ограниченным аппаратно-программным реализациям, в которых несколько компьютерных систем связаны друг с другом с помощью соответствующих средств коммуникации.

Таким образом, сформулировать отличительные признаки локальной сети можно следующим образом. Высокая скорость передачи информации, большая пропускная способность сети. Приемлемая скорость сейчас - не менее 100 Мбит/с. Низкий уровень ошибок передачи. Эффективный, быстродействующий механизм управления обменом по сети. Заранее четко ограниченное количество компьютеров, подключаемых к сети. При таком определении понятно, что глобальные сети отличаются от локальных прежде всего тем, что они рассчитаны на неограниченное число абонентов. Кроме того, они используют не слишком качественные каналы связи и сравнительно низкую скорость передачи. А механизм управления обменом в них не может быть гарантированно быстрым. В глобальных сетях гораздо важнее не качество связи, а сам факт ее существования.

Существуют одноранговые, сети на основе сервера и гибридные архитектуры сетей. В соответствии с рисунком 1 в одноранговой сети все компьютеры равноправны, т.е. нет иерархии в окружении компьютеров и нет выделенного (англ.

dedicated) сервера. Всякий компьютер функционирует и как клиент, и как сервер. Нет отдельного компьютера, ответственного за администрирование всей сети. Все пользователи автономно решают, какие ресурсы локального компьютера делать доступными для сети. Одноранговые сети чаще всего группируют не более 10-15 компьютеров. Отсюда их другое название – рабочая группа, то есть, маленький коллектив пользователей. На каждом компьютере такой сети установлена одноранговая операционная система, например, Microsoft Windows 7, имеющая как клиентский, так и серверный модули .

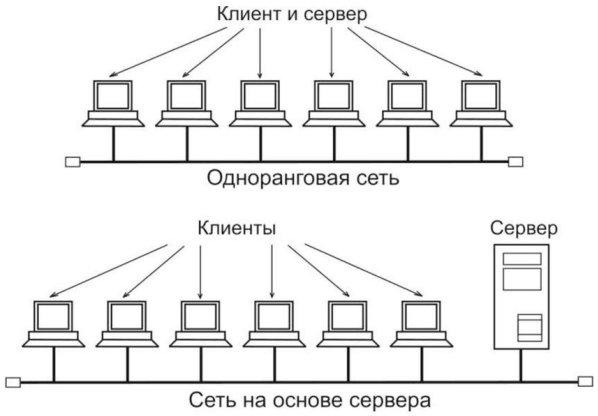

Рисунок 1 - Одноранговая сеть и сеть на основе сервера

Одноранговые сети сравнительно просты. Этим объясняется малая стоимость одноранговых сетей по сравнению со стоимостью сетей на базе сервера. Одноранговая сеть обладает следующими характеристиками:

- количество пользователей не превышает 10-15 пользователей;
- станции размещены компактно;
- защита данных решается каждым пользователем индивидуально (нет необходимости в сетевом администрировании);
- малая стоимость;
- простота построения и эксплуатации.

Однако большее распространение получили клиент–серверные и гибридные сети.

Сети типа клиент-сервер содержат: «серверы – мощные компьютеры, владеющие сетевыми ресурсами, разделяемыми между пользователями и управляющие доступом к ним клиентов; клиенты – менее мощные компьютеры сети, владеющие локальными ресурсами и имеющие доступ к ресурсам серверов».

Выделенный сервер – это «компьютер, который функционирует только как сервер, его сетевая операционная система имеет мощные серверные модули и полное отсутствие или маломощные клиентские модули (см. рис. 2). Они оптимизированы для параллельной, скоростной обработки запросов от сетевых клиентов и имеют защиту файлов и каталогов» .

Файл-серверы (file servers) – «предоставляют доступ к множеству своих файлов, расположенных на дисках». Например: SAMBA (SMB – Server Message Block).

Серверы приложений (application servers) – «обеспечивают вычислительные ресурсы для (удаленного) выполнения определенных классов приложений с других компьютеров». Например: WebSphere (IBM), WebLogic (BEA).

Серверы баз данных (database servers) – «компьютеры и программное обеспечение Например: Microsoft SQL Server, Oracle, обеспечивают доступ к базам данных» .

Web-серверы (Web servers) – «обеспечивают доступ через WWW к Web-страницам, расположенным на этих серверах». Примеры: Apache; Microsoft.NET Web Servers; Java Web Servers .

Proxy-серверы – «обеспечивают эффективное выполнение обращений к Интернету, фильтрацию трафика, защиту от атак».

E-mail-серверы – «обеспечивают отправку, получение и раскладку электронной почты». Могут обеспечивать также криптование почты (email encryption) [11].

Server back-end – «группа (pool) связанных в сети компьютеров (вместо одного сервера), обеспечивающая серверные функции».

Таким образом, архитектура является емким понятием, отражающим взаимосвязь различных структур сети: конфигурации линий, объединяющих ее пункты (топологии), организационной структуры, отображающей устройство сети, функциональной структуры, поясняющей логику работы сети, программной

структуры, характеризующей состав чрезвычайно сложного и многоцелевого программного обеспечения сети; протокольной модели сети, описывающей правила установления связи и обеспечения информационного обмена, физической структуры, позволяющей оценить физические ресурсы сети, типы используемого оборудования.

Термин топология сети характеризует физическое расположение компьютеров, кабелей и прочих компонентов сети. Топология сети обуславливает ее характеристики. В частности, выбор той или иной топологии воздействует:

- на состав и характеристики сетевого оборудования;
- на надежность сети;
- на наименьшее время отклика с сети;
- на производительность сети и ее пропускную способность;
- на возможности масштабирования сети;
- на метод управления сетью.

Для того чтобы вместе использовать сетевые ресурсы, компьютеры должны быть подключены друг к другу через проводящую среду, например, кабельную систему. Любые типы кабелей в сочетании с многообразными сетевыми адаптерами, сетевыми операционными системами и прочими компонентами требуют и многообразного взаимного расположения компьютеров . Всякая топология сети налагает ряд требований, например, она способна диктовать не только тип кабеля, но и средство его прокладки. Топология способна также изменять метод взаимодействия компьютеров в сети. Разным видам топологий соответствуют разные методы взаимодействия, и эти методы оказывают сильное влияние на сеть. Существуют три главных вида топологий: общая шина, звезда, кольцо.

Если компьютеры подключены вдоль одного кабеля (сегмента), топология именуется шиной. Если компьютеры подключены к сегментам кабеля, исходящего из одной точки, например, коммутатора, то топология именуется звездой. Если кабель, к которому подключены компьютеры, замкнут в кольцо, такая топология называется кольцо. Хотя сами по себе базовые топологии просты, в действительности неоднократно встречаются довольно трудные комбинации, объединяющие особенности разных топологий.

Топология Шина

Топологию Шина часто называют «линейной шиной». Такая топология относится к самых несложным и широко используемым топологиям. В соответствии с рисунком 2 в ней применяется один кабель, именуемый магистралью, в противном случае сегментом, вдоль какого подключены все компьютеры и серверы сети. В сети с топологией шина компьютеры адресуют данные одному компьютеру, передавая их по кабелю в виде электрических сигналов. Для представления способа взаимодействия компьютеров по шине опишем следующие понятия: передача сигнала, отражение сигнала, терминатор .

Данные в виде электрических сигналов передаются всем компьютерам сети; однако сообщение получает только тот абонент, чей адрес соответствует адресу получателя, зашифрованному в данных сигналах. В любое время только один компьютер способен вести передачу. Так как данные в сеть передаются только одним компьютером, то производительность сети зависит от численности компьютеров, подключенных к шине. Чем больше компьютеров, желающих вести передачу данных, тем медленнее работает сеть. Данные распространяются по всей сети – от одного конца кабеля к другому. Если не оказывать воздействий на сигнал, то он, достигая конца кабеля, будет отражаться и не позволит прочим компьютерам осуществлять передачу. Поэтому, после того как данные достигнут адресата, электрические сигналы требуется погасить, для этого на концах кабеля размещаются терминаторы, поглощающие эти сигналы. Концы кабеля подключаются к компьютеру через разъем сетевого адаптера или к баррел-коннектору – для повышения длины кабеля. Выход из строя сетевого кабеля совершается при его физическом разрыве или когда на одном или на нескольких концах кабеля отсутствуют терминаторы. При этом сеть «падает».

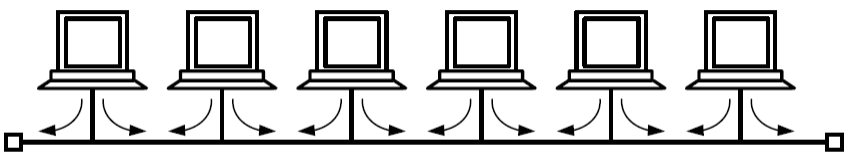

Рисунок 2 - Топология Шина.

Таким образом, топология Шина характеризуется использованием общего канала передачи данных, называемого магистралью, сегментом (trunk, backbone, segment) между оконечными устройствами. Имеет децентрализованное управление. Работает в режиме широковещания – все компьютеры, разделяющие канал связи, принимают всю информацию, передаваемую другими компьютерам. Выход из строя одной рабочей станции не влияет на работу остальных, тогда как разрыв кабеля или отсутствие терминатора ведет к выходу из строя всей сети. Трудно локализовывать отказы из - за большой длины магистрального кабеля и отсутствия точки концентрации. Максимальная длина сегмента сети L равна длине кабеля, ограниченного терминаторами. Для «толстого» коаксиала L=500 м. При соединении 5 сегментов (по правилу 5-4-3) диаметр сети D=5×500=2500м.

Топология Звезда

При топологии Звезда все компьютеры с сегментами кабеля подключаются к центру, именуемому концентратором. В соответствии с рисунком 3 сигналы от передающего компьютера поступают через концентратор ко всем станциям.

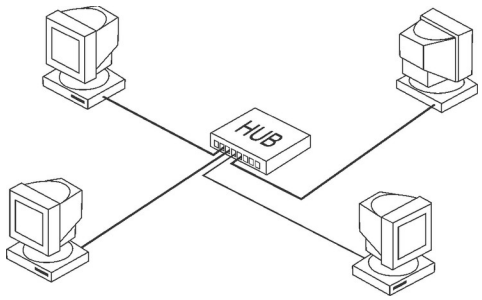

Рисунок 3 - Топология активная Звезда

В сетях с топологией Звезда подключение кабеля и управление сетью централизовано. Но в этом заключается и недостаток: так как все компьютеры подключены к центральной точке, для крупных сетей сильно увеличивается расход кабеля. К тому же, если центральный компонент выйдет из строя, нарушится работа

всей сети. Если выйдет из строя любой компьютер (либо кабель, соединяющий его с центром), то только этот компьютер не будет передавать или получать данные из сети. На остальные компьютеры в сети это не повлияет .

Топология Звезда является самой быстродействующей из всех топологий вычислительных сетей, потому что передача данных производится между рабочими станциями через центральный узел (при его отличной производительности) по отдельным линиям, используемым лишь этими рабочими станциями. Частота запросов передачи информации от одной станции к другой невысокая по сравнению с достигаемой в других топологиях. В соответствии с рисунком 4 центральный узел управления, например, файловый сервер, реализует приемлемый механизм защиты против несанкционированного доступа к информации. Вся вычислительная сеть способна управляться из ее центра. Отказы сети относительно легко локализовать . Диаметр сети составляет D=2×L, где L – длина сегмента. На основе топологии Звезда организуется топология Дерево.

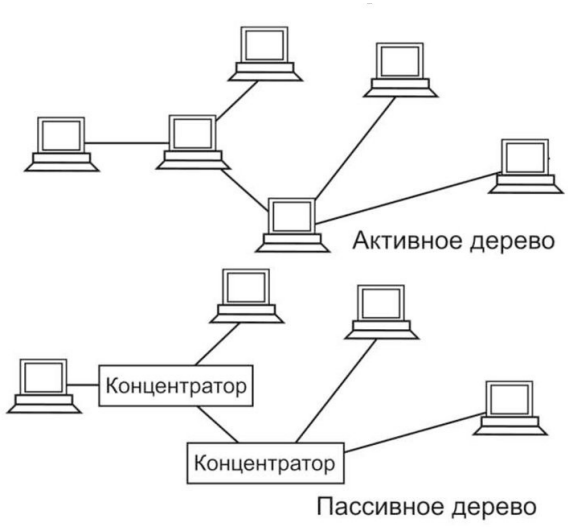

Рисунок 4 - Топология Дерево.

Топология Кольцо

В соответствии с рисунком 5 при топологии кольцо компьютеры подключаются к кабелю, замкнутому в кольцо. Сигналы передаются по кольцу в одном направлении

и проходят через любой компьютер. В отличие от топологии шина, здесь всякий компьютер выступает в роли репитера, усиливая сигналы и передавая их очередному компьютеру. В связи с этим, если выйдет из строя один компьютер, перестает функционировать вся сеть.

Один из алгоритмов передачи данных в кольцевой сети называется «передача маркера». Суть его заключается в том, что маркер последовательно, от 1-ого компьютера к следующему, передается до тех пор, пока его не получит обратно отправитель. Передающий компьютер изменяет маркер, помещает MAC - адрес в кадр и передает его по кольцу. Данные проходят через каждый компьютер, пока не окажутся у того, чей адрес совпадает с адресом получателя, указанного в кадре .

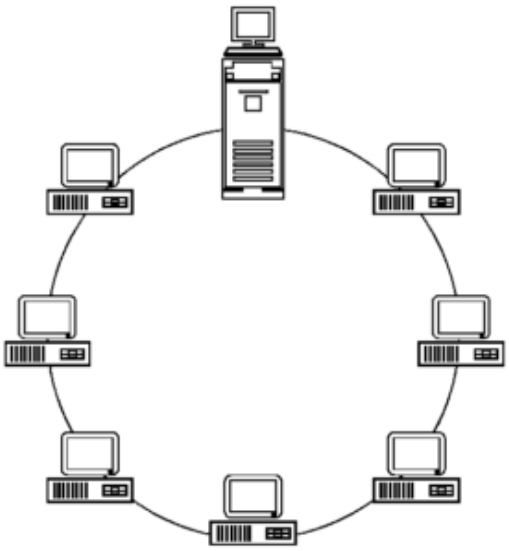

Рисунок 5 - Топология Кольцо.

После этого принимающий компьютер отсылает отправителя данные, подтверждающие факт приема. Получив подтверждение, компьютер - отправитель создает новый маркер и возвращает его в сеть.

Итак, станции в топологии подключаются к общему кольцу, иногда двойному. Выход из строя одной рабочей станции влияет на всю сеть (принимаются меры). Выход из строя кольца ведет к выходу из строя всей сети, поэтому кольца резервируются (Двойное кольцо). Отказы локализовать не очень легко. Диаметр сети

составляет D=N×L сегмента, где N – число станций в кольце. Сравнение описанных выше топологий представлено в таблице ниже (таблица 1).

Таблица 1 - Основные характеристики топологий сетей.

Характеристики	Топологии вычислительных сетей		
	Звезда	Кольцо	Шина
Ценность расширения	Незначительная	Средняя	Средняя
Присоединение абонентов	Пассивное	Активное	Пассивное
Защита ото отказов	Незначительная	Незначительная	Высокая
Размеры системы	Любые	Любые	Ограниченный
Защищенность ото прослушивания	Хорошая	Хорошая	Незначительная
Ценность подключения	Незначительная	Незначительная	Высокая
Действие системы при больших нагрузках	Хорошее	Среднее	Плохое
Потенциальность работы в реальном режиме временить	Очень хорошая	Неплохая	Плохая
Разводка кабеля	Хорошая	Среднее	Хорошая
Обслуживание	Очень хорошее	Среднее	Среднее

Исходя из вышеизложенного можно сделать вывод, что компьютерные сети занимают особое место в нашей повседневной жизни, в нашей производственной деятельности и в других областях. Соединение компьютеров в сети позволяют людям находить необходимую им информацию, используя ресурсы других компьютеров, общаться друг с другом, не выходя за пределы своей комнаты, общаться с людьми, которые находятся на огромных расстояниях.

1.2 Описание общеизвестных защитных мер

Используемая в настоящий момент версия серверной операционной системы - Windows Server 2008 морально устарела, ее поддержка производителем скоро прекратится. Поэтому, необходимо обновление, как минимум, до Windows Server 2012 R2.

В домене Windows для настройки защиты информации применяются, в том числе, политики безопасности. После введения в действие этих политик на центральном сервере, называемом «контроллер домена» - настройки автоматически отражаются на всех участниках домена. В понятие политики безопасности входят:

политики учетных записей, политики паролей, политики блокировки учетных записей, и др.

В системах Windows, учетные записи пользователей делятся на два типа: локальные и доменные. Локальные учетные записи - действуют на одном конкретном компьютере (сервере). Доменные - в рамках всей доменной сети.

Информацию на сервере локальной сети, работающем под управлением операционной системой Windows Server, можно защитить такими способами:

а) создание и настройка политик безопасности домена;

б) ужесточение правил по ограничению доступа учетным записям;

в) отключение компонентов, создающих угрозу;

г) улучшенная антивирусная защита в реальном времени;

д) установка сетевого экрана в режиме повышенной защиты;

е) ужесточение настроек безопасности сервера баз данных SQL;

ж) организация резервного копирования настроек домена и баз данных.

Способ «в» скорее рекомендуется, чем необходим. Остальные – будут применяться в реализации защиты сервера.

Информацию на компьютерах-клиентах локальной сети, работающих под управлением операционной системой Windows, можно защитить такими способами:

а) установка сетевого экрана;

б) жесткая антивирусная защита;

в) физическое отключение неиспользуемых портов ввода-вывода;

г) физическое отключение дисководов, не требующихся в работе;

д) удаление устаревшего программного обеспечения и драйверов.

Наиболее важны способы от «а» до «г».

Маршрутизаторы и коммутаторы – улучшают защиту, и позволяют:

а) ограничить доступ к ресурсам сети на основе IP и MAC-адресов;

б) создать правила фильтрации потоков сетевого трафика;

в) защититься от различных видов сетевых атак (сниффинг, DoS, и др.);

г) распределить пропускную способность физического канала связи.

Здесь наиболее важны способы от «а» до «в» .

Для защиты электронной почты доступны такие методы:

а) использование защищенных протоколов при получении/отправке почты;

б) назначение сложных, уникальных паролей и периодическая их смена;

в) антивирусная проверка почты;

г) задание жестких настроек (фильтров) для входящих писем.

Важны все способы [10; 13], кроме «г», который лишь рекомендуется.

Для настройки возможностей, доступных учетной записи - применяют групповые политики [4; 7]. Группа - это удобный способ создания и управления набором разрешений и/или запретов, сохраненным под уникальным названием.

Для группы можно изменять групповую политику, связанную с ней. Групповая политика построена по принципу разрешений и запретов. Чаще всего, в групповой политике применяются правила:

- на события входа в систему;
- на доступ к объектам (файлам, каталогам, общим ресурсам сети);
- на использование привилегий;
- на системные события.

После создания нужных групп, учетные записи «добавляются» в них, причем, один и тот же пользователь может быть в нескольких группах .

Антивирус снижает вероятность проникновения в систему вредоносного программного обеспечения. Также важно выявление новых угроз - «эвристический анализатор».

Анализатор в режиме реального времени отслеживает работу приложений, и обнаруживая «вирусоподобную» активность - выполняет заданное действие.

В операционной системе Windows хорошо зарекомендовали себя следующие продукты: Bitdefender Internet Security, Kaspersky Internet Security, BullGuard Internet Security, Norton Security Deluxe, Trend Micro Internet Security.

Есть и множество других, менее известных, которые в настоящей работе не рассматриваются. Для выбора антивирусной защиты, учитываем такие факторы:

- наличие других встроенных инструментов, для комплексной защиты;
- совместимость со старыми версиями операционных систем;

- наличие русскоязычной поддержки и официального представительства.

Учитывая это, наиболее подходящим вариантом становится Kaspersky Internet Security. В нем сочетаются наиболее важные качества, а также, в отличие от Bitdefender Internet Security - присутствует защита почтового клиента .

Сетевые экраны, называемые также «брандмауэры» и firewall (англ. «огненная стена»), бывают программные и аппаратные. Отвечают за защиту от сетевых угроз. Сетевой экран уже присутствует в выбранном антивирусном ПО.

Помимо этого, будет применяться ПО ViPNet IDS [29] – система обнаружения вторжений, позволяющая в короткий срок выявлять возникающие и потенциальные сетевые угрозы безопасности. Причины такого выбора:

- российская фирма-разработчик, что облегчает получение технической поддержки, оперативных обновлений, и др.;
- продукт сертифицирован ФСБ за №СФ/СЗИ-0122 и ФТЭК ФСТЭК России за №3804, что важно для его использования в гос. учреждениях;
- разработано для российского сегмента интернет и специфичных угроз.

Принцип работы системы ViPNet IDS изображен на рисунке 6.

Злоумышленник через интернет обходит сетевой экран и передает пакеты данных во внутреннюю сеть. Через коммутатор эти данные транслируются дальше, дублируются в систему ViPNet IDS, которая и выявляет угрозу.

Защита информации в базах данных SQL обеспечивается путем предоставления пользователям БД лишь тех прав доступа, которые им необходимы в работе . В системе управления базами данных (СУБД) содержатся собственные средства управления, в частности, разделение по группам. В правилах безопасности СУБД прописывается, какими правами наделен конкретный пользователь или группа. Чаще всего используются:

- право на извлечение данных (SELECT);
- право на добавление данных (INSERT);
- право на обновление данных (UPDATE).

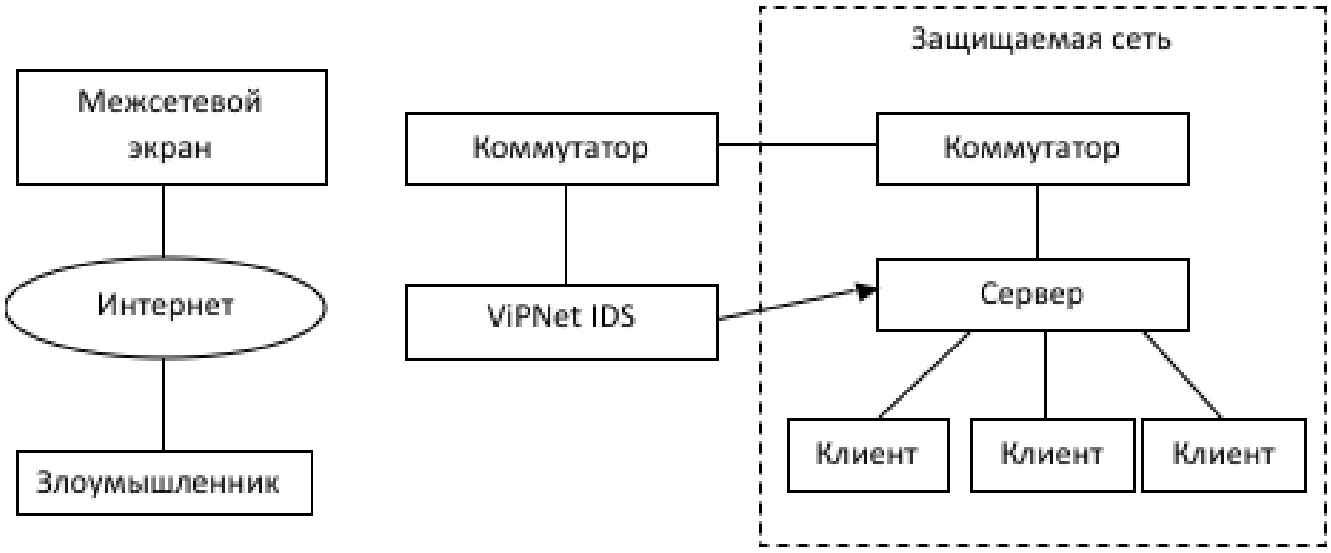

Рисунок 6 - Схема работы IDS

Поэтому, следует выявить уровень привилегий, необходимых каждому виду пользователей БД для его работы.

Создание и применение резервных копий - один из важнейших методов защиты информации. В копировании нуждается такая информация:

- настройки домена Windows, включая политики безопасности;
- база данных SQL (файл базы и файл журнала транзакций);
- системные файлы и каталоги операционной системы;
- каталоги с файлами пользователей;
- содержимое общих сетевых папок.

Для копирования ключевой информации домена и операционной системы удобно пользоваться стандартным инструментом «Система архивации данных Windows Server» [4]. Другие виды информации будут копироваться инструментами командной строки. Копирование должно выполняться по расписанию. Наиболее важные данные сервера - ежедневно, все данные - 1 раз в неделю. Также, полная копия делается после любых изменений в политиках безопасности. Копирование базы данных - несколько отличается, здесь необходимо отключение всех пользователей от базы данных (т. е. завершение сеансов работы с базой) на весь период резервного

копирования. Целесообразно это делать в часы наименьшей нагрузки на информационную систему, между 2 и 4 ч. утра.

Таким образом, все копии будут храниться на отдельных RAID-массивах жестких дисков.

Выбор сетевого экрана для рабочих станций, в целом, аналогичен таковому для сервера локальной сети, с такими отличиями:

- устанавливается «облегченная», клиентская версия IDS - ViPNet IDS HS;
- сетевой экран настраивается более жестко, в частности, запрещается доступ ко всем частям сети, кроме необходимых в работе.

Для рабочих станций необходим более жесткий режим антивирусной защиты, так как, физический доступ к ним имеет гораздо большее количество людей. В частности:

- запрет на запуск программ, не внесенных в список доверенных;
- отключение режимов, где решение по защите принимает пользователь;
- работа антивируса в автоматическом режиме, защита настроек паролем;
- балансировка защиты и потребления ресурсов компьютера .

На многих рабочих станциях есть неиспользуемые порты ввода-вывода, такие, как: порт универсальной последовательной шины (universal serial bus, USB), последовательный порт (COM), параллельный порт (LPT).

Таким образом, хорошей практикой является физическое или программное отключение портов , которые не используются. Особенно опасен порт USB, так как позволяет подключить внешний, зараженный носитель информации. Мы применим надежный физический метод отключения портов. Наиболее распространенный вид дисководов - это CD/DVD-привод, позволяющий считывать информацию с оптических дисков, и записывать ее. В некоторых рабочих процессах учреждения, наличие такого дисковода необходимо. Где необходимости нет - будем отключать устройство.

Ограничения по доступу к ресурсам сети задаются в настройках маршрутизаторов и коммутаторов в виде правил deny / permit (англ. «запретить /

разрешить») в конфигурации устройства . Правила могут включать разные ограничения доступа, в частности, нам потребуются:

- запрет на прямое терминальное подключение от клиента к серверу;
- запреты на доступ к интернет с клиентов, где такой доступ не нужен;
- запрет на прямое подключение к локальной сети из внешнего мира;
- разрешения на терминальный доступ для избранных клиентов сети.

Как и в случае с ограничением доступа к ресурсам сети, фильтрация сетевого трафика построена на принципе разрешений и запретов.

В каждом таком фильтре указываются :

- сетевой интерфейс, куда информация поступает (WAN, VPN, и др.);
- использованный протокол передачи данных (TCP, UDP или ICMP);
- тип фильтра - по IP или по MAC-адресу;
- использованный для соединения сетевой порт;
- политика фильтра - «разрешающая», либо «запрещающая».

Для защиты информации будет применяться система обнаружения вторжений ViPNet IDS, направленная на выявление угроз путем анализа сетевого трафика, выявления аномалий в потоках данных, ведения журналов событий безопасности и уведомления администраторов о возникающих угрозах .

Для защиты маршрутизаторов от сетевых атак, следует:

- установить свежие обновления прошивки;
- отключить удаленный доступ, там, где это возможно;
- сменить стандартный, «заводской» пароль на новый;
- отключить UPnP .

Кроме этого, есть настройки, влияющие на защиту. Важно отключение Wi-Fi Protected Setup (WPS), которая создает серьезную уязвимость . Также, рекомендуется включение защит против DoS/DDoS (Denial of Service – отказ в обслуживании), SYN Flood и других атак, направленных на перегрузку каналов и/или оборудования связи. Эти функции есть у оборудования Cisco. Защищенный обмен данными в сети осуществляется при помощи ViPNet Client , с такими функциями:

- фильтрация трафика (сетевой экран);

- контроль сетевой активности приложений и компонентов операционной системы;
- шифрование по ГОСТ 28147-89 на ключах длиной 256 бит.

Таким образом, благодаря этому, а также возможности интеграции с программным обеспечением других разработчиков, обеспечивается повышенная защита информационной системы.

Разумеется, такие меры не дают абсолютной гарантии защиты , однако, снижают вероятность успешной реализации угроз.

Обязательные требования к надежному паролю :

- пароль должен содержать не менее 8 символов;
- пароль должен содержать заглавные и строчные буквы, цифры, пробелы и специальные символы (такие, как: !?*$&#@%+-=).

Пароль не должен содержать:

- личную информацию (имя, фамилию, дату рождения);
- очевидные и простые слова, фразы, устойчивые выражения и наборы символов, которые легко подобрать (например: password, qwerty, 1234567).

Рекомендуется назначать пользователям уникальные (не повторяющиеся) пароли, и менять пароль каждые 2-3 месяца, по утвержденному расписанию. Антивирусная проверка почты осуществляется при получении на почтовом сервере (у стороннего провайдера), а также модулем из состава Kaspersky Internet Security - уже на стороне клиента, в момент приема поступивших сообщений.

Таким образом, мы изучили более подробно предложенные ранее методы защиты информации, выбрали условия их применения и необходимое для этого программное обеспечение, и можем переходить к дальнейшей реализации, которая будет описана в следующем разделе.

1.3 Изучение политики безопасности

Политика информационной безопасности определяет цели и задачи системы обеспечения информационной безопасности и устанавливает совокупность правил, требований и руководящих принципов в области информационной безопасности,

которыми руководствуется организация в своей деятельности. Политика разрабатывается в соответствии с законодательством Российской Федерации и нормами права в части обеспечения информационной безопасности.

Основными целями политики информационной безопасности являются защита информации и обеспечение эффективной работы всего информационно-вычислительного комплекса при осуществлении деятельности.

Политика информационной безопасности направлена на защиту информационных активов от угроз, исходящих от противоправных действий злоумышленников, уменьшение рисков и снижение потенциального вреда от аварий, непреднамеренных ошибочных действий персонала, технических сбоев, неправильных технологических и организационных решений в процессах обработки, передачи и хранения информации и обеспечение нормального функционирования технологических процессов.

Риск аварий и технических сбоев определяется состоянием технического парка, надежностью систем энергоснабжения и телекоммуникаций, квалификацией персонала и его способностью к адекватным действиям в нештатной ситуации.

Стратегия обеспечения информационной безопасности заключается в использовании заранее разработанных мер противодействия возможным атакам, а также программно-технических и организационных решений, позволяющих свести к минимуму возможные потери от технических аварий и ошибочных действий персонала.

Задачами настоящей политики являются:

- описание системы управления информационной безопасностью;
- определение политик информационной безопасности, а именно:
- политика реализации антивирусной защиты;
- политика учетных записей;
- политика предоставления доступа к информационному ресурсу;
- политика защиты автоматизированного рабочего места;
- политика использования паролей;
- политика конфиденциальности;

- определение порядка сопровождения информационной системы и локальной сети.

Таким образом, политика информационной безопасности и в соответствии с ней построенная система управления информационной безопасностью будет являться наиболее правильным и эффективным способом добиться минимизации рисков нарушения информационной безопасности для локальной сети. Необходимо учитывать, что с течением времени меняется характер угроз, поэтому следует своевременно, используя данные мониторинга и аудита, обновлять модели угроз и нарушителя.

2 Защита информации от преднамеренных угроз в локальной сети посредством VipNet

2.1 Разработка модели нарушителя и актуальных угроз

Ставиться задача разработки модели угроз и модели нарушителя информационной безопасности, основываясь на специфике деятельности данной организации и обеспечивая соответствие государственным стандартам и нормам в области информационной безопасности. Модель угроз информации содержит перечень угроз информации при ее обработке в информационной системе и локальной сети, в частности. В Модели угроз дается описание: информационной системы как объекта защиты, с учетом ее назначения и условий функционирования, состава и категории обрабатываемой защищаемой информации, актуальных источников угроз безопасности информации, потенциального нарушителя безопасности информации.

Угрозы безопасности информации локальной сети, могут дополняться и уточняться по мере выявления новых угроз, появления средств и способов реализации угроз безопасности, изменения требований законодательства в области защиты информации. Модель угроз возможно пересмотреть в будущем по решению руководства или рекомендации уполномоченных органов государственной власти на основе проводимых мероприятий по контролю выполнения требований по обеспечению информационной безопасности.Модель угроз разработана в соответствии с «Методикой ФСТЭК «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных» от 15.02.2008г, Методика определения актуальных угроз безопасности ПДН утв. ФСТЭК РФ 14.02.2008г, Федеральный закон РФ «Об электронной подписи» от 06.04.2011 г. №63-ФЗ, Федеральный закон РФ «О персональных данных» от 27.07.2006 г. №152-ФЗ, Федеральный закон РФ «Об информации, информационных технологиях и защите информации» от 27.07.2006 г. №149-ФЗ. Состав технических средств и программного обеспечения представлен в таблице 2.

Таблица 2 - Состав технических средств и программного обеспечения

№	Наименование
1	Технические средства
1.1	ПЭВМ (системный блок, монитор, клавиатура, мышь)
2	Программное обеспечение:
2.1	Операционная система со всеми компонентами, необходимыми для работы
2.2	Антивирусное СЗИ «Kaspersky Endpoint Security»
2.3	СЗИ от НСД «Secret Net 7»
2.4	Пакет программ управления VipNet IDS
Дополнительные компоненты	
1	VipNet IDS, выполняющий роль межсетевого экрана (МЭ)
2	Сетевой коммутатор
3	Источник бесперебойного питания
4	Многофункциональное устройство (МФУ), выполняющее роль принтера
5	Съемные носители информации для хранения ключевой информации
6	Съемные носители информации для передачи данных
7	Съемные носители информации для резервного копирования
8	Линии передачи информации между компонентами локальной сети в границах контролируемой зоны
9	Линии передачи информации между компонентами локальной сети, выходящие за границы контролируемой зоны
10	Линии электропитания и заземления
11	Линии охранной и пожарной сигнализации

На основе анализа условий создания и использования ЗИ определена информация, соответствующая процессам создания и использования ЗИ (далее - сопутствующая информация), которая также может быть объектом угроз.

1. Ключевая, аутентифицирующая и парольная информация:

- ключи защиты канала связи;
- ключи Администраторов/Операторов АРМ для подключения к компонентам серверов;
- ключи к СЗИ от НСД для доступа к информационным ресурсам;
- пароли доступа к ключевым носителям (личным идентификаторам) и ключевым контейнерам Администраторов, Операторов АРМ, администратора безопасности.

2. Криптографически опасная информация (КОИ);

- конфигурационная информация:
- конфигурационные файлы ПО;

- таблицы адресной маршрутизации;
- конфигурация СЗИ.

3. Информация в электронных журналах регистрации:

- информация в журналах событий компонентов ОС;
- информация в журналах средств ФС;
- информация в журналах СЗИ;
- информация в журналах СУБД.

4. Побочные электромагнитные сигналы, которые появляются при эксплуатации технических средств в которых содержится защищаемая информация полностью или частично;

5. Резервные копии файлов с информацией, подлежащей защите, которые создаются при обработке таких файлов;

6. Удаленная информация на различных магнитных носителях информации.

Перечни возможных объектов угроз:

Объектами угроз являются:

- защищаемая информация (таблица 3);
- сопутствующая информация (таблица 4);
- программное обеспечение (таблица 5);
- технические средства (таблица 6).

Таблица 3 - Защищаемая информация

№	Защищаемая информация	Форма фиксации	Обозначение
1	Ключи ЭП владельцев сертификатов ключей проверки ЭП	Области оперативной памяти ТС - в процессе генерации ключей ЭП	ЗИ1
		Файлы на съемном ключевом носителе	ЗИ2
2	Ключ ЭПФС	Области оперативной памяти ТС	ЗИ3
		Файлы на съемном ключевом носителе	ЗИ4
3	Персональная и корпоративная информация пользователей ИС, не подлежащая рассылке	Записи БД на жестких дисках ТС	ЗИ5
		Записи БД на съемных носителях резервного копирования	ЗИ6
		Данные в сетевых пакетах	ЗИ7
		Изображение на экране монитора	ЗИ8

Продолжение Таблица 3

4	Сертификаты ключей проверки ЭП пользователя и их статус	Файлы и записи БД на жестких дисках ТС	ЗИ9
		Записи БД на съемных носителях резервного копирования	ЗИ10
		Данные в сетевых пакетах	ЗИ11
		Бумажные документы	ЗИ12
		Изображение на экране монитора	ЗИ13
5	Запросы на получение, аннулирование (отзыв), приостановление и возобновление действия сертификатов пользователя	Файлы и записи БД на жестких дисках ТС	ЗИ14
		Записи БД на съемных носителях резервного копирования	ЗИ15
		Данные в сетевых пакетах	ЗИ16
		Файл на съемном носителе информации	ЗИ17

Таблица 4 – Сопутствующая информация

№	Защищаемая информация	Форма фиксации	Обозначение
1	Ключевая, аутентифицирующая и парольная информация	Записи БД (реестр ОС) на жестких дисках ТС Файл на съемном ключевом носителе	СИ1 СИ2
2	Криптографически опасная информация	Области оперативной памяти ТС	СИ3
3	Конфигурационная и управляющая информация	Файлы на жестких дисках (или иных энергонезависимых модулях памяти) ТС Изображение на экране монитора	СИ4 СИ5
4	Управляющая информация	Данные в сетевых пакетах	СИ6
5	Информация в электронных журналах регистрации	Файлы и записи БД на жестких дисках (или иных энергонезависимых модулях памяти) ТС. Данные в сетевых пакетах Изображение на экране монитора	СИ7 СИ8 СИ9
6	Побочные электромагнитные сигналы, которые появляются при эксплуатации технических средств в которых содержится защищаемая информация полностью или частично	Электромагнитное излучение, Токи в сетях связи и электропитания	СИ10
7	Резервные копии файлов с информацией, подлежащей защите, которые создаются при обработке таких файлов	Файлы на жестких дисках ТС	СИ11
8	Удаленная информация на различных магнитных носителях информации	Остаточная информация на жестких дисках ТС Остаточная информация на съемных носителях информации	СИ12 СИ13

Таблица 5 – Программное обеспечение

№	Программное обеспечение	Обозначение
1	Операционная система ТС, включая все ее компоненты, необходимые для работы	П01
2	Средство ИС, включая все его компоненты, установленные на разных ТС ИС	П02
3	СКЗИ, выполняющее функции СКЗИ и средства ЭП	П03
4	СУБД	П04
5	Антивирусное СЗИ	П05
6	Пакет программ управления МЭ	П06
7	Программа управления шаблонами контроля целостности	П07
8	СЗИ от НСД	П08
9	Операционная система и иные программные компоненты МЭ	П09

Таблица 6 - Технические средства

№	Технические средства	Обозначение
1	Сервер ФС	ТС1
2	Сервер ВС	ТС2
3	АРМ	ТС3
4	Межсетевой экран	ТС4
5	Терминал управления ФС и ВС	ТС5
6	Источник бесперебойного питания	ТС6
7	Сетевой коммутатор	ТС7
8	Сетевые кабели между компонентами ИС	ТС8
9	Сетевые кабели, соединяющие компоненты ИС с КИС	ТС9
10	Принтер	ТС10
11	Съемные носители информации для резервного копирования	ТС11
12	Съемные носители информации для хранения ключевой информации	ТС12
13	Съемные носители информации для передачи данных	ТС13
14	Линии электропитания и заземления	ТС14
15	Линии охранной и пожарной сигнализации	ТС15

Защищаемую информацию можно сгруппировать по объектам доступа на программном и аппаратном уровнях (таблица 7):

Таблица 7 - Объекты доступа

Защищаемая информация	Объект доступа	Объект доступа на аппаратном уровне
ЗИ1, ЗИ3, СИ3	Области ОЗУ	Модули оперативной памяти
ЗИ5, ЗИ9, ЗИ14, ЗИ18, СИ1, СИ4, СИ7, СИ11	Базы данных и отдельные файлы	Жесткие диски
СИ12		Жесткие диски
ЗИ2, ЗИ4, СИ2	Файлы	Съемные защищенные носители информации
ЗИ6, ЗИ10, ЗИ15	Базы данных	Съемные носители информации для целей резервирования информации
ЗИ17, ЗИ20, СИ13	Файлы	Съемные носители информации для целей переноса информации
ЗИ7, ЗИ11, ЗИ16, ЗИ19,	Сетевые пакеты	Сетевые кабели

Продолжение таблица 7

СИ6, СИ8		
ЗИ8, ЗИ11, СИ5, СИ9	-	Монитор
С10	-	ТС, сетевые кабели
ЗИ12	-	Принтер

Основными характеристиками безопасности являются конфиденциальность, целостность и доступность. Характеристики безопасности защищаемой информации локальной сети (таблица 8) .

Таблица 8 - Характеристика безопасности ЗИ

№	Объект угроз	Характеристика безопасности		
		Конфиденциальность	Целостность	Доступность
1	ЗИ1	+	+	-
2	ЗИ2	+	+	-
3	ЗИ3	+	+	-
4	ЗИ4	+	+	+
5	ЗИ5	+	+	+
6	ЗИ6	+	+	+
7	ЗИ7	+	+	+
8	ЗИ8	+	-	+
9	ЗИ9	-	+	+
10	ЗИ10	-	+	+
11	ЗИ11	-	+	+
12	ЗИ12	-	-	+
13	ЗИ13	-	-	+
14	ЗИ14	-	+	+
15	ЗИ15	-	+	+
16	ЗИ16	-	+	+
17	ЗИ17	-	+	+
18	ЗИ18	-	+	+
19	ЗИ19	-	+	+
20	ЗИ20	-	+	+
21	СИ1	+	+	+
22	СИ2	+	+	+
23	СИ3	+	-	-
24	СИ4	-	+	+
25	СИ5	-	-	+
26	СИ6	-	+	+
27	СИ7	-	+	+
28	СИ8	-	+	+
29	СИ9	-	-	+
30	СИ10	+	-	-
31	СИ11	+	-	-
32	СИ12	+	-	-
33	СИ13	+	-	-

Характеристики безопасности программного обеспечения локальной сети (таблица 9)

Таблица 9 - Характеристика безопасности программного обеспечения

№	Объект угроз	Характеристики безопасности		
		Конфиденциальность	Целостность	Доступность
1	П01	-	+	+
2	П02	-	+	+
3	П03	-	+	+
4	П04	-	+	+
5	П03	-	+	+
6	П06	-	+	+
7	П07	-	+	+
8	П08	-	+	+
9	П09	-	+	+

Характеристики безопасности технических средств локальной сети (таблица 10).

Таблица 10 - Характеристика безопасности ТС

№	Объект угроз	Характеристики безопасности		
		Конфиденциальность	Целостность	Доступность
1	ТС1	-	+	+
2	ТС2	-	+	+
3	ТС3	-	+	+
4	ТС4	-	+	+
5	ТС5	-	+	+
6	ТС6	-	+	+
7	ТС7	-	+	+
8	ТС8	-	+	+
9	ТС9	-	+	+
10	ТС10	-	+	+
11	ТС11	-	+	+
12	ТС12	-	+	+
13	ТС13	-	+	+
14	ТС14	-	+	+
15	ТС15	-	+	+
16	ТС16	-	+	+

Нарушение характеристик безопасности ТС может привести к нарушениям характеристик безопасности ПО, ЗИ и СИ, обрабатываемой на данном ТС или с его

помощью. Нарушение характеристик безопасности ПО может привести к нарушению доступности ЗИ и СИ, обрабатываемой при помощи данного ПО. Соотношение ТС, ПО, ЗИ и СИ представлено в таблице 11. Данные таблицы созданы и упорядочены опираясь на базовую модель угроз ФСТЭК.

Таблица 11 - Соотношение ТС, ПО, ЗИ и СИ

Техническое средство	Функционирующее ПО	Обрабатываемая, хранящаяся, передаваемая информация	
		Защищаемая информация	Сопутствующая информация
ТС1	П01, П02, П03, П05, П07, П08	ЗИ9, ЗИ12, ЗИ18	СИ1, СИ4, СИ7, СИ10
ТС2	П01, П02, П03, П04, ПО3, П07, П08	ЗИ5, ЗИ9, ЗИ12, ЗИ18	СИ1, СИ4, СИ7, СИ10, СИ11, СИ12
ТС3	П01, П02, П03, П03, П06, П07, П08	ЗИ1, ЗИ3, ЗИ8, ЗИ9, ЗИ13, ЗИ12	СИ3, СИ4, СИ7, СИ10
ТС4	-	-	СИ4, СИ7
ТС5	П09	-	СИ4, СИ7, СИ10
ТС6	-	-	СИ5, СИ9, СИ10
ТС8	-	ЗИ7, ЗИ11, ЗИ16, ЗИ19	СИ6, СИ8, СИ10
ТС9	-	ЗИ7, ЗИ11, ЗИ16, ЗИ19	СИ6, СИ8, СИ10
ТС10	-	ЗИ11,ЗИ16, ЗИ19	-
ТС11	-	ЗИ11	-
ТС12	-	ЗИ6, ЗИ10, ЗИ15	-
ТС13	-	ЗИ2, ЗИ4	СИ2, СИ11
ТС14	-	ЗИ17, ЗИ20	-

Таким образом, угроза безопасности объекта в нашем случае это возможное нарушение характеристики безопасности объекта.

2.2 Выбор программного продукта для разработки защищённой сети

После сбора всей необходимой информации, необходимо определить при помощи каких программных или программно-аппаратных средств будет осуществляться защищенное взаимодействие между офисами, а также внутри каждой из них. Целью данной главы является разработка структуры сети и способ взаимодействия определенных сегментов сети.

Для решения поставленной задачи проводился сравнительный анализ компаний и их предлагаемых ими продуктов. Для этого было отобрано две компании,

предоставляющие средства наиболее подходящие для решения поставленной задачи, это компании ИнфоТеКС и Код безопасности.

Компания ИнфоТеКС предлагает программные и программно-аппаратные комплексы – VipNet, они позволяют создавать защищенные виртуальные сети двух конфигураций:

- сеть VipNet для организации электронного документооборота (без реализации технологии VPN);
- сеть VipNet, в которой реализована технология VPN.

Сеть без реализации VPN для решения нашей задачи не подходит, поэтому была рассмотрена конфигурация, которая позволяет реализовать VPN. Такая конфигурация позволяет:

- осуществить интеграцию в существующую структуру сети;
- фильтровать защищенный и открытый трафик;
- осуществлять централизованное управление политиками безопасности;
- организовать иерархическую систему сетей;
- вести слежение за состоянием сети.

На рисунке 7 представлена типовая схема сети, построенной на базе программного обеспечения VipNet.

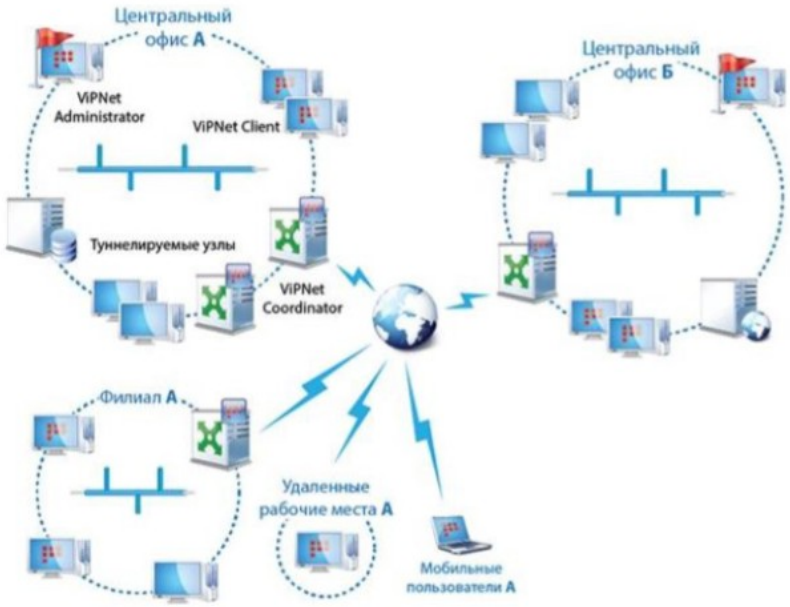

Рисунок 7 - Схема сети на базе программного комплекса VipNet

Программный комплекс VipNet CUSTOM состоит из набора различных компонентов, которые могут использоваться для обеспечения надежной доверительной среды, при передаче данных по незащищенным каналам связи. На рисунке 8 представлены компоненты, которые могут быть использованы в разработке защищенной локальной сети.

Оборудование и программные средства компании имеют все необходимые сертификаты ФСБ и ФСТЭК. Межсетевые экраны или «координаторы», а также клиентская часть имеют 3 и 4 классы защищенности, также соответствуют требованиям ФСБ России к шифровальным (криптографическим) средствам класса КС1, КС2 и КС3 (в зависимости от варианта исполнения). Компания Код Безопасности представляет различные решения для защиты персональных рабочих мест, защиты серверов, организации VPN каналов между серверами, а также между сервером и удаленным пользователем. Для достижения цели данного проекта наиболее подходящими средствами из всей линейки продуктов является Secret Net Studio работающим в паре с АПКШ «Континент» 3.7.

Данная система предназначается для обеспечения безопасности информационных систем, функционирующих под управлением операционных систем семейства Windows. Система предоставляет следующие возможности:

- защита от НСД к ИР компьютеров;
- контроль устройств, подключаемых к компьютеру;
- обнаружение вторжений в локальную сети;
- антивирусную защиту;
- межсетевое экранирование трафика;
- авторизация сетевых соединений;
- создание отказоустойчивой VPN-сети между территориально распределенными сетями;
- централизованное развертывание, управление и мониторинг;

- создание защищенного соединения с удаленными пользователями;
- разделение сети на сегменты с различным уровнем доступа.

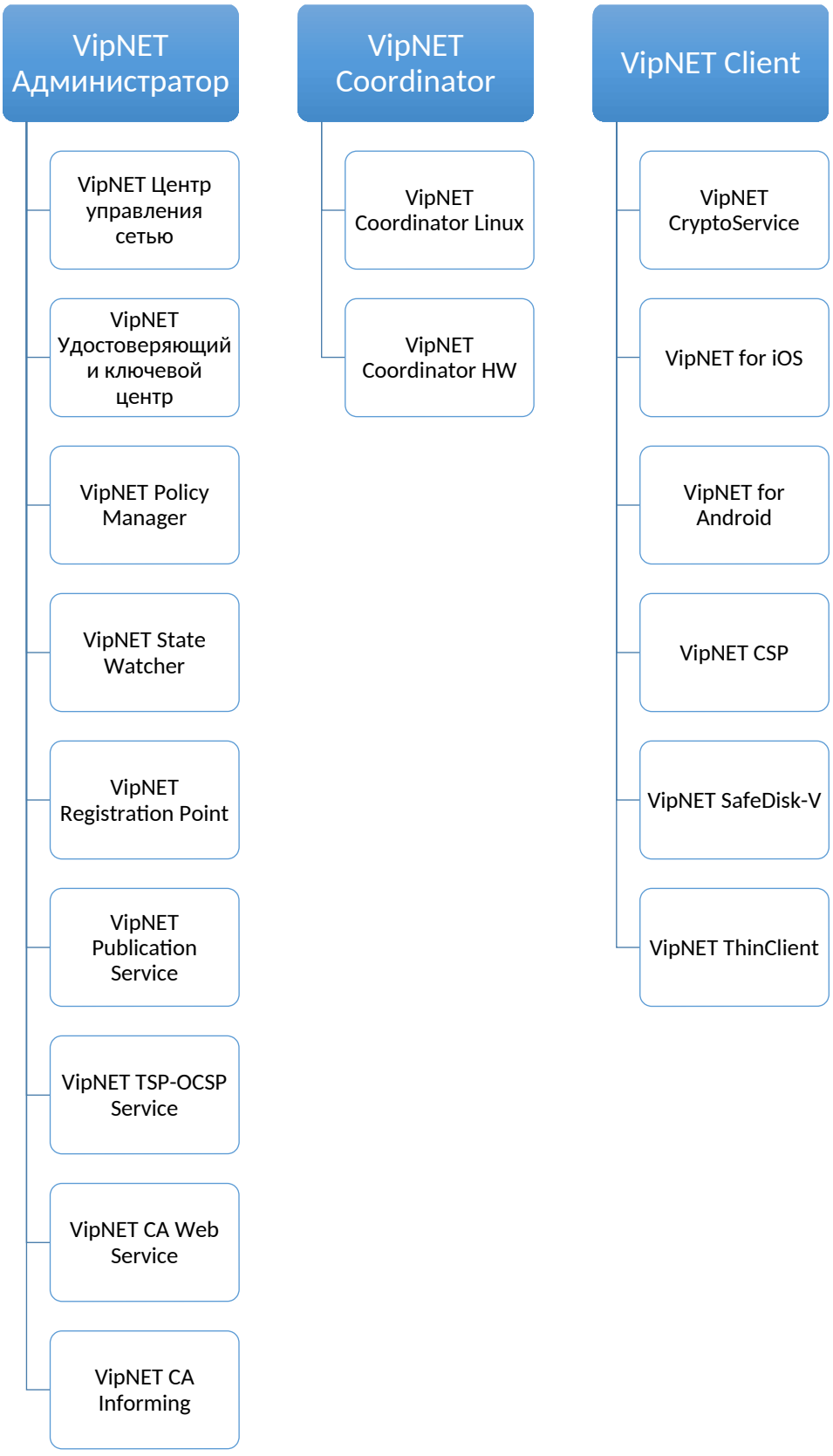

Рисунок 8 - Компоненты, входящие в программный комплекс VipNet

На рисунке 9 представлена типовая схема сети, построенная на базе Secret Net Studio работающим в паре с АПКШ «Континент» 3.7.

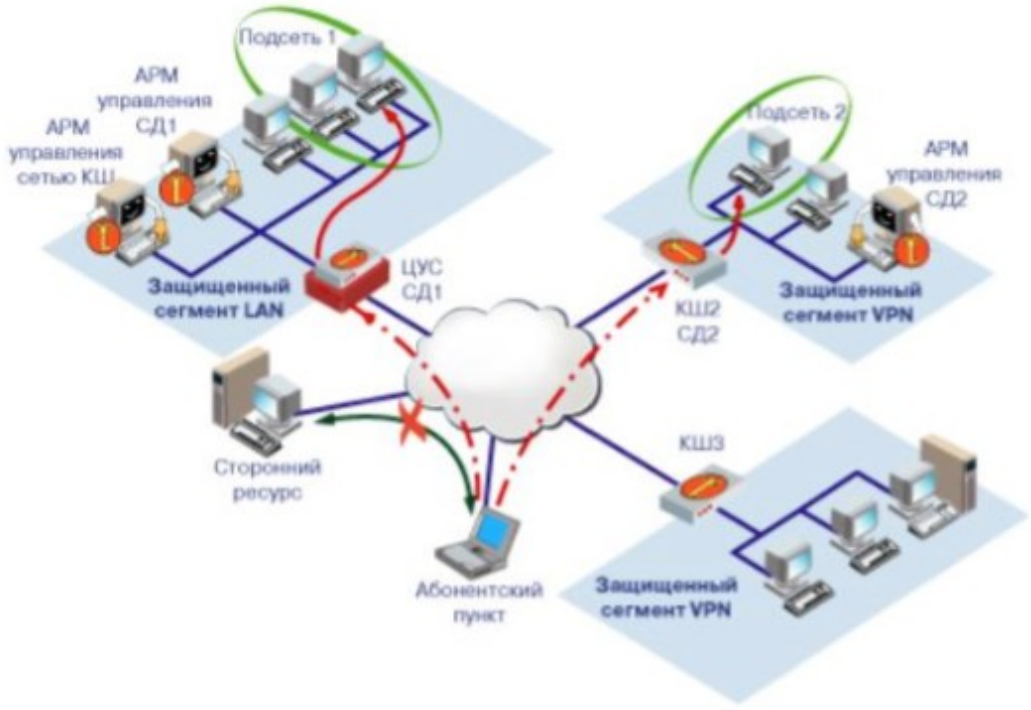

Рисунок 9 - Схема сети на базе АПКШ «Континент» 3.7

Оборудование и программные средства компании имеют все необходимые сертификаты ФСБ и ФСТЭК. Secret Net Studio имеет 3 класс защищенности МЭ, может применяться в АС до класса 1Г включительно, ИСПДн до У31 включительно.

АПКШ «Континент» имеет 4 класс защищенности устройств типа межсетевые экраны и соответствуют требованиям ФСБ России к шифровальным (криптографическим) средствам класса КС1, КС2 и КС3 (в зависимости от варианта исполнения).

Сравнительная таблица приведена ниже. Так как по условию необходимо создать защищенную локальную сеть для большой сети клиник, сравниваться будут 2 продукта это комплекс VipNet CUSTOM и АПКШ «Континент» 3.7.

Таблица 12 - Сравнение VipNet и АПКШ «Континент»

Критерий	VipNet CUSTOM	АПКТТТ «Континнт» 3.7
Сертификация СКЗИ	КС1 КС2 КС3	КС1 КС2 КС3
Сертификация МЭ	ФСБ 4-й ФСТЭК 3-й	ФСБ 4-й ФСТЭК 3-й
ИСПДн	К1	К1
Объединение двух и более сетей	ВОЗМОЖНО	Нет возможности
Возможность работы с пересекающейся IP адресацией	есть	нет
Возможные архитектуры	«клиент» - «клиент» «клиент» - «сервер» «сервер» - «сервер»	«клиент» - «сервер» «сервер» - «сервер»
Возможность работы с удаленными пользователями	есть	есть
Стоимость	7 790,00	6 600,00

Таким образом, на основании проведенного анализа, для создания защищенной сети более удачным является комплекс VipNet CUSTOM, так как он позволяет создавать защищенной канал до самого рабочего места, в то время как другой продукт имеет такую возможность только для удаленного пользователя.

2.3 Разработка защищённой локальной сети на базе программного комплекса VipNet

Локальная сеть подразумевает наличие обмена информацией между серверами и рабочими местами, помимо этого, существует вероятность необходимости связи между отдельными рабочими местами разных филиалов. Технология VipNet позволяет осуществлять такие соединения, благодаря использованию пиринговых соединений, которые обеспечивают автоматическое оповещение связанных узлов о параметрах доступа друг к другу. Это позволяет реализовать не только классические для IPSec схемы «сервер-сервер» и «клиент-сервер», но также схему «клиент-клиент» - в автоматическом режиме и с возможностью объединения компьютеров независимо от точки их подключения к сети, принадлежности определенной VPN-сети, без централизованной раздачи IP- адресов.

Для развертывания сети ViPNet достаточно установить на рабочие станции программное обеспечение ViPNet. Для организации защищенного соединения используется схема с автоматически распределенными на этапе установки программного обеспечения симметричными ключами шифрования, а также автоматизированной процедурой синхронизации. Каждый пакет, который отправляется в сеть, автоматически шифруется с использованием уникального производного ключа, без каких-либо процедур установления соединения. Это позволяет организовывать защищенную передачу данных по ненадежным каналам, по каналам, которые характеризуются большими потерями трафика, а также обеспечивать бесперебойную работу локальной сети.

Технология ViPNet без потери качества соединения обеспечивает постоянство свойств защищенного соединения, которые существенно влияют на безопасность. А именно, постоянное шифрование всего IP-пакета вместе с исходными IP-адресами и протоколами, постоянное обеспечение защиты от навязывания ложных пакетов, исключение возможности шифрования только части трафика в направлении заданного защищенного узла. Протокол, используемый в рамках технологии ViPNet, обеспечивает защищенную передачу данных по любым каналам связи, через любые устройства NAT/PAT - даже в том случае, когда интернет-провайдер препятствует установлению соединения путем запрета авторизующих соединений IPSec.

Рассмотрим несколько вариантов построения сети. Как говорилось выше, чаще всего структура сети VipNet совпадает с реально существующей структурой.

Такая структура является удобной для небольших организаций, однако, в нашем случае имеется достаточно большой штат сотрудников, а также 3 филиала, между которыми так же необходимо организовать взаимодействие. Такое построение приведет к загрузке каналов центрального «координатора» служебной информацией, и «координатор» будут занят её обработкой.

Использование программного обеспечения VipNet позволяет организовывать взаимодействие между различными сетями, для этого технология ViPNet предоставляет возможности по каскадированию защищенных соединений, без промежуточного расшифровывания информации. Это позволяет организовать

пиринговые соединения между подсетями и узлами, которые расположены в пределах других защищенных сетей. Поэтому существует возможность развертывание нескольких сетей VipNet с организацией межсетевого взаимодействия. Это становится возможным, так как ViPNet CUSTOM имеет развитую систему виртуальных адресов, что позволяет устанавливать необходимые защищенные каналы связи между произвольным числом защищенных сетей, построенных с использованием ViPNet CUSTOM. Также система виртуальных адресов скрывает реальную структуру сети, что является неотъемлемым плюсом, для построения защищенной сети. Распределение сетей будет делаться по территориальному расположению.

В соответствии с рисунком 10 первой сетью будет являться большая сеть главного офиса, в которой существуют различные сегменты, и требуется использование каскадной схемы установки координаторов.

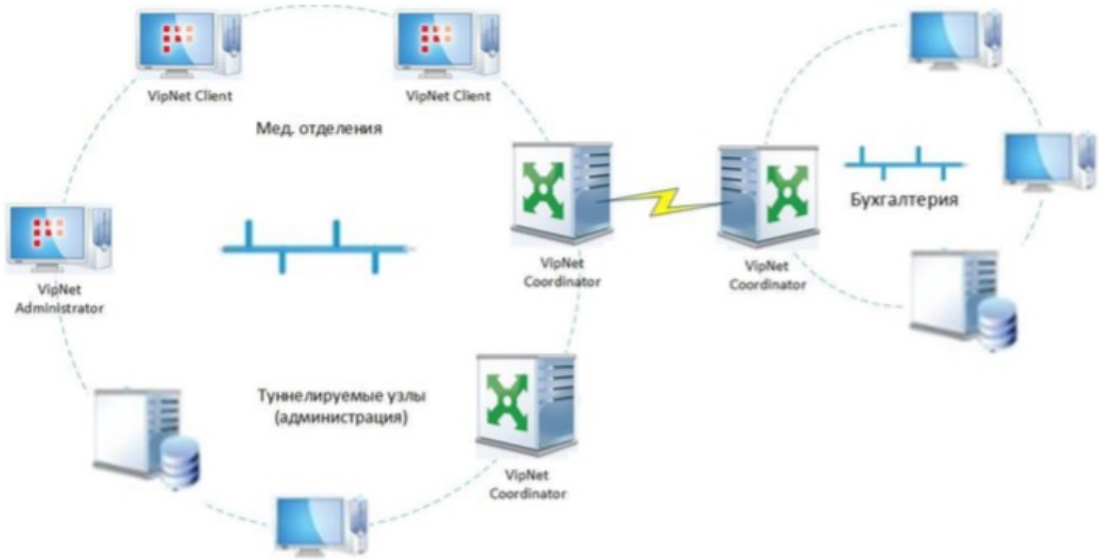

Рисунок 10 - Первая сеть VipNet

В соответствии с рисунком 11 второй сетью будут являться удаленные офисы, расположенные в соседнем здании.

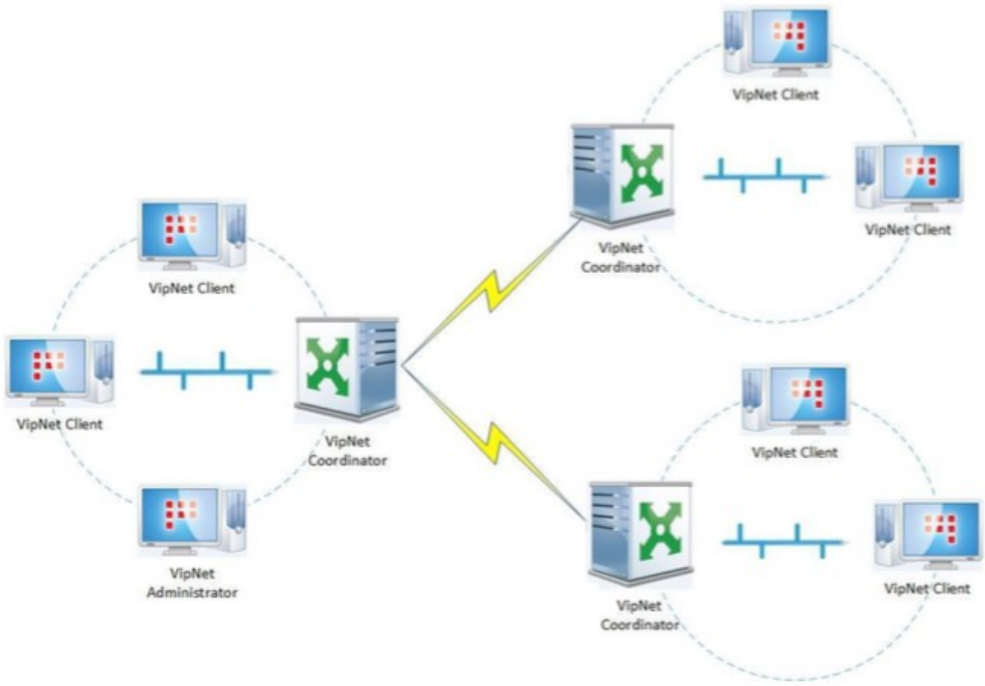

Рисунок 11 - Вторая сеть VipNet

В соответствии с рисунком 12 третьей - филиалы, расположенные в другом городе.

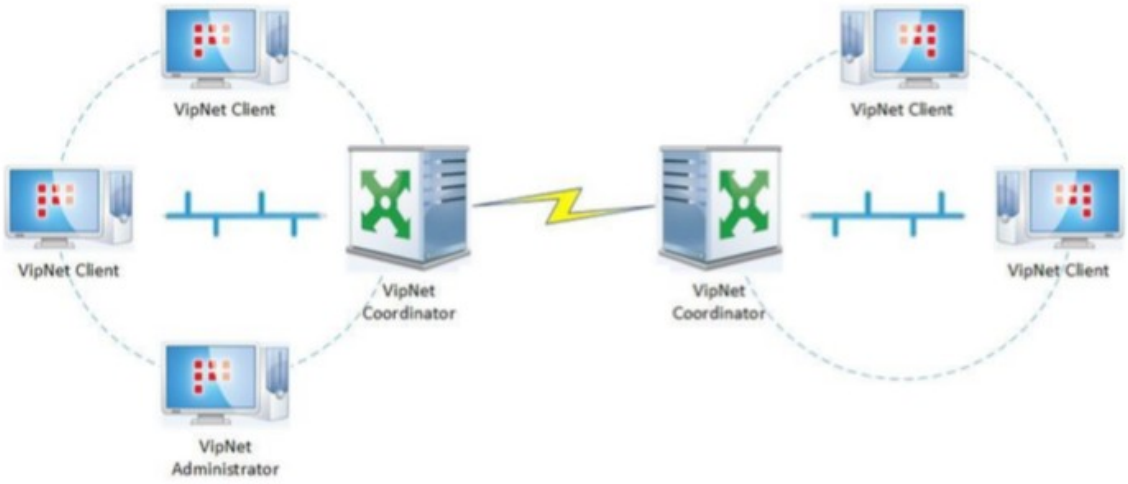

Рисунок 12 - Третья сеть VipNet

В качестве «координаторов» возможно использование специального программного обеспечения ViPNet Coordinator 4, предназначенного для установки на компьютерные устройства, функционирующие под управлением операционной системы Microsoft Windows и Linux. Кроме программного обеспечения, компания предлагает различные программно-аппаратные комплексы (ПАК).

ПАК ViPNet Coordinator HW1000 версии 3 является универсальным шлюзом безопасности и предоставляет возможность создать в любой телекоммуникационной инфраструктуре, включая сеть связи общего пользования, распределенную виртуальную сеть (VPN), защищенную от сетевых атак и несанкционированного доступа к информации. ПАК ViPNet Coordinator HW1000 легко инсталлируется в существующую инфраструктуру и соответствует самым жестким требованиям по функциональности, удобству эксплуатации, надежности и отказоустойчивости.

ПАК ViPNet Coordinator KB2 100 это программно-аппаратный шлюз безопасности, удовлетворяющий требованиям к СКЗИ по классу KB2. Отсутствие лицензионных ограничений на количество одновременно установленных соединений через шлюз безопасности ViPNet Координатор- KB2.

Все координаторы в качестве центра генерации ключей шифрования используют ПО ViPNet Administrator. Coordinator KB2 100 имеет возможность генерировать ключи из ключевого блокнота ДСДР. На рисунке 13 приведена структура с организацией межсетевого взаимодействия, все три сети являются доверенными.

Таким образом, каждый ПАК, а так же программное обеспечение ViPNet Coordinator соответствует требованиям ФСБ России к устройствам типа межсетевые экраны 4 класса защищенности. Сертифицирован по требованиям к СКЗИ уровня КС1, КС2, КС3.

Прикладную структуру можно представить, как второй слой, который накладывается поверх сетевой структуры. Объектами в прикладной структуре являются коллективы пользователей, которой регистрируются на рабочих станциях и серверах, включенных в защищенную сеть на сетевом уровне.

Коллектив это совокупность пользователей одного сетевого узла, имеющих одинаковые ключи для шифрования конфиденциальной информации.

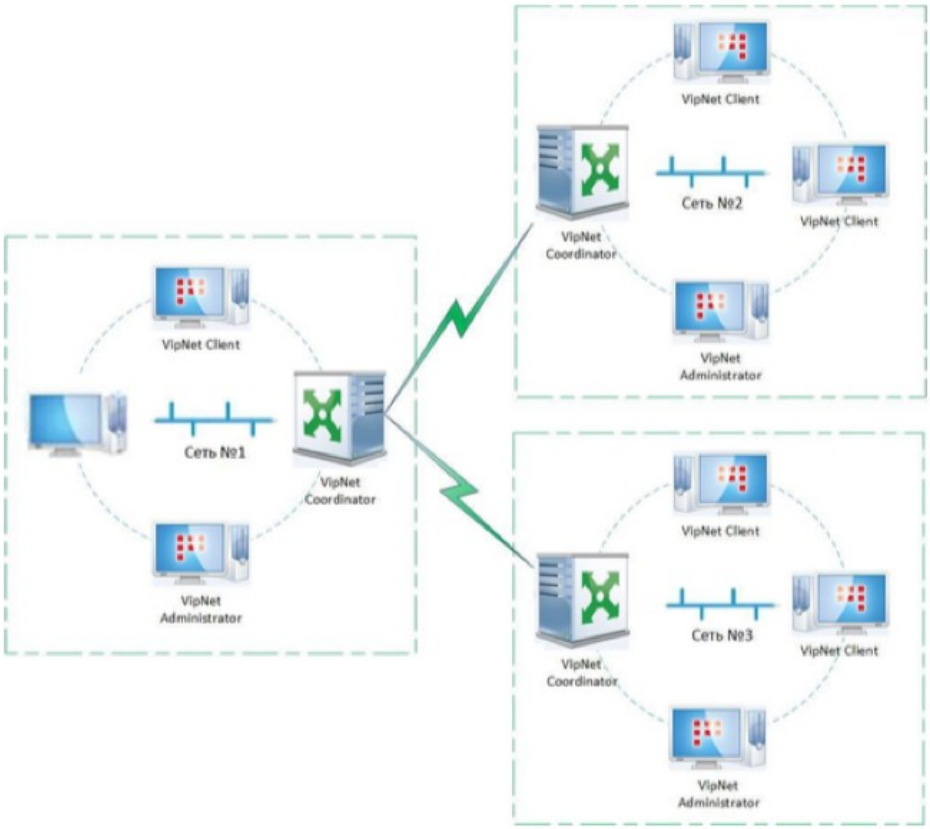

Рисунок 13 - Структура сети с организацией межсетевого взаимодействия.

Тип коллектива - это сущность, которая позволяет идентифицировать коллектив среди множества других коллективов и позволяет зарегистрировать его на определенном сетевом узле.

Между типами коллективов создаются так называемые «связи», это означает, что коллективы будут видеть друг друга в адресных справочниках своих АП и имеют возможность связи между собой, при помощи шифрованной связи на уникальных парных ключах. Также, связь между коллективами означает, что в ключах узлов, на которых зарегистрированы коллективы, ещё будут присутствовать ключи транспортного уровня, для связи между абонентскими пунктами, которые включены в коллективы. Эта система также является гибкой.

Также имеется возможность включения одного пользователя в несколько коллективов, но среди них должен быть всегда выделен один - главный. Например, если врач является многопрофильным и работает в разных кабинетах. В этом случае, ключи отправляются только на один АП, на главный, а на другие абонентские пункты ключ пользователя необходимо перенести самостоятельно.

На границе сети главного офиса рекомендуется установка ПАК ViPNet Coordinator HW1000 версии 3, это позволит не загружать имеющиеся сервера и распределить нагрузку, а так же трафик, так как планируется организация выхода в открытый Интернет. Для защиты сегментов, которым не требуется ОИ, возможно установка программное обеспечение ViPNet Coordinator 4, функционирующие под управлением операционной системы Microsoft Windows и Linux, на обычный компьютер, который будет выступать в роли сервера. Затем устанавливается межведомственное взаимодействие с ПАК ViPNet Coordinator HW1000. В филиалах устанавливается ПО ViPNet Coordinator 4 и устанавливается межсетевое или же межведомственное взаимодействие, в зависимости от участка сети и требуемых связей.

Защита рабочих мест, а так же трафика идущего от них обеспечивается установкой программного комплекса VipNet Client, который надежно защищает от внешних и внутренних сетевых атак за счет фильтрации трафика. Кроме того, ViPNet Client обеспечивает защищенную работу с корпоративными данными через зашифрованный канал, в том числе для удаленных пользователей.

Для авторизации пользователей в системе рекомендуется использование USB-ключей или смарт-карт. VipNet поддерживает различные типы устройств: eToken Aladdin, SmartCard RIK, Shipka, ruToken, ruTokenECP, Аккорд-5MX. Выбор в пользу использования USB-ключей, так как они удобны в использовании и имеют меньший раз по сравнению со смарт-картами. Для выбора ключевых носителей, которые будут использоваться в учреждении, представлены продукты Rutoken и eToken (являются единственными сертифицированными USB-токенами). Среди представленных USB-токенов, выбор с пользу Rutoken S, так как данный продукт имеет низкую цену по сравнению с ruTokenECP, что является решающим фактором при почти одинаковом

спектре функций. В сравнение не попал eToken, в связи с тем, что компания Аладдин сняла его с производства, сертификат ФСТЭК действителен у него до 2016 года, а срок жизненного цикла истекает в 2020 году. Ниже описаны некоторые преимущества использование технологии ViPNet.

По сравнению с обычными VPN-решениями ViPNet предоставляет целый ряд дополнительных возможностей по защищенному обмену информацией: встроенные службы мгновенного обмена сообщениями (чат и конференция) и файлами, а также собственная защищенная почтовая служба с элементами автоматизации обмена письмами, файлами и поддержкой механизмов ЭЦП. Дополнительные сетевые возможности комплекса ViPNet, такие как контроль сетевой активности приложений, строгий контроль доступа в Интернет, механизмы аварийной перезагрузки и защиты от вторжений на этапе загрузки операционной системы позволяют организовать защиту от большинства сетевых атак и минимизировать затраты на систему безопасности в целом.

Так как ViPNet CUSTOM может поставляться в виде программного комплекса, его установка и настройка не потребует приобретения специализированного оборудования и может быть произведена уже на существующей ИС. В большинстве случаев также не требуется реконфигурация сетевого оборудования.

В состав пакетов «Координатор» и «Клиент» входят дополнительные модули, обеспечивающие защищенный обмен транспортными конвертами (файлами, сообщениями, электронной почтой) между клиентами защищенной сети. Основной транспортный модуль называется MFTP и предназначен для обеспечения надежной и безопасной передачи транспортных конвертов между узлами сети ViPNet посредством протоколов TCP (канал передачи MFTP) и SMTP/POP3. При связи по каналу MFTP устанавливается TCP-соединение с узлом-получателем конвертов, проводится взаимная аутентификация узлов и осуществляется прием/передача конвертов друг для друга. Базовыми компонентами ViPNet CUSTOM является программное обеспечение ViPNet Administrator , ViPNet Coordinator (в разных вариантах исполнения) и ViPNet Client. Эти компоненты являются основой для

развертывания виртуальной частной сети и инфраструктуры открытых ключей. С целью расширения возможностей базовых компонент могут использоваться дополнительные компоненты ViPNet CUSTOM: ViPNet Registration Point, и ViPNet CryptoService.

В проекте развертывается три сети с межсетевым взаимодействием, по исходным данным видно, что ИТ-отдел находится только в главном офисе, поэтому целесообразно использовать иерархическую структуру сетей VipNet, чтобы централизованно управлять распределением лицензий в подчиненных сетях из главного Центра управления сетью.

Таким образом выбран продукт, при помощи которого будет осуществляться разработка защищенной сети, осуществлена разработка защищенной сети, с учетом деятельности и расположения, разработан способ применения защищенной сети, на уже имеющиеся информационные ресурсы.

2.4 Обоснование экономической эффективности проекта

2.4.1 Расчёт показателей экономической эффективности проекта

Таблица 12 – Затраты на закупку ПО и комплектующих

Наименование оборудования и материалов	Количество, шт	Стоимость, руб	Сумма, руб
VipNet	1	203000	203000
Итого:			203000

Таким образом, величина затрат на реализацию проекта составляет 203000 рублей. Установкой системы занимается IT-отдел. Затраты на заработную плату основную и дополнительную с отчислениями в социальные фонды рассчитываются по формулам ниже.

Данные для расчета основной заработной платы специалистов занесены в таблицу 13

Таблица 13 – Расчет основной заработной платы специалистов

Должность	Кол-во чел.	Должностной оклад, руб.	Дневная ставка, руб	Количество рабочих дней	Фонд заработной платы, руб.
Системный администратор	1	8000	381	366	139446
Итого: 139446					

Общая сумма внедрения проекта: 139446 +203000= 342446 руб.

Общая стоимость компании составляет 10000000 руб. Риск утери данных может нанести ущерб с фактором воздействия 50%. Вероятность происшествия - раз в 5 лет, т.е. 0,5.

Расчет цены потерь (Q) производится по формуле 1.

Q = K * C, (1)

K - Общая стоимость компании

C - фактор воздействия риска

Q = 10000000 * 0,5 = 5000000 рублей.

Величина риска (R) в данной ситуации зависит от двух факторов и считается по формуле 2.

R = P * Q (2)

P - Вероятность наступления риска

R = 0,5 * 5000000= 2500000 рублей, т.е. существует риск потери такой суммы ежегодно.

Вывод: разработка проекта экономически целесообразна для организации. Разработанная система защиты информации от преднамеренных угроз в ЛВС оправдает себя через полгода.

Заключение

Информация, несомненно, один из наиболее ценных ресурсов предприятия, она необходима на стадии принятия решения, при реализации задач хозяйственной деятельности и управления, именно с помощью использования и анализа нужной информации менеджер готовит соответствующие отчеты, предложения, для конечной выработки и принятия управленческих решений.

Очевидно, что перед началом работы с информацией необходимо ее структурировать и подготовить к использованию, потому что на начальном этапе предприятие взаимодействует чаще всего с необработанной информацией. Проблему перевода информации в состояние полезности, решает действующая на предприятии это информационная система.

Наличие большого количества циркулирующих информационных потоков значительно увеличивает вероятность возникновения информационных рисков на предприятии, связанных с нарушением конфиденциальности пользования и целостности информации.

Любой вид деятельности человека можно представить как процесс, в результате которого появляется продукт, материальный или интеллектуальный, имеющий определенную ценность, то есть стоимость.

Информация является одной из разновидностей таких ценностей, стоимость ее может оказаться настолько высокой, что ее потеря или утечка, даже частичная, способна поставить под вопрос само существование компании. Поэтому защита информации с каждым днем приобретает все большее значение, практически во всех более или менее крупных организациях существуют свои подразделения, выполняющие задачу по обеспечению информационной безопасности компании.

В различных сферах деятельности человек пользуется различными определениями понятия информации, в сфере информационной безопасности в России на сегодняшний день используется определение данное в Законе РФ «Об информации, информатизации и защите информации».

Одним из наиболее характерных и популярных средств обеспечения информации в настоящее время являются программно-аппаратные комплексы.

В данной работе был проведен подробный анализ предметной области, показаны причины возникновения задачи проектирования защищенного сегмента сети. Также была показана общая характеристика локальных сетей и проведено ее изучение.

Описан процесс деятельности с точки зрения защищенного информационного обмена. Показана структура и состав защищаемой системы и структуры локальной сети. Показаны процессы реализующие прикладные задачи. Обоснована актуальность разработки.

Проведена разработка подсистемы сетевой защиты сегмента сети предприятия, для чего проведена разработка защищенной структуры сегмента сети предприятия на базе технологии VipNet, показана структура защищенной локальной вычислительной сети на базе программы VipNet, структура межведомственного взаимодействия на базе программы VipNet.

Показано решение для защиты сегмента сети предприятия на базе выбранного комплекса ViPNet. Разработан способ применения технологии VipNet для защищаемого сегмента. Предложен состав комплекса ViPNet CUSTOM. Показано применение предложенного состава комплекса АПК VipNet. Показано применение защищенной структуры для сегмента сети.

Приведены общие настройки системы, схема применения компонент VipNet, подсистема защиты VoIP, применение удостоверяющего и ключевого центра для защищаемого сегмента сети.

В данной работе были даны рекомендации по защите локальной сети:

- требуется защита информационного обмена при прохождении через открытый Интернет;
- требуется, чтобы защищенный туннель был прозрачен для пользователей, которые работают с ресурсами удаленных локальных сетей;
- требуется, чтобы пользователи локальной сети не имели доступа к ресурсам открытого Интернета, за исключением ресурсов других локальных сетей,

определенных администратором, с которыми организуется защищенное взаимодействие и, возможно, ресурсов мобильных пользователей;

- требуется исключить необходимость установки ПО ViPNet [Координатор] на шлюзы локальной сети.

Для обеспечения защиты данной локальной сети, достаточно установить программное обеспечение ViPNet [Координатор]

В результате получем, что он:

- туннелирует открытый информационный обмен между компьютерами удаленных локальных сетей в защищенное соединение от ViPNet [Координатора] данной локальной сети до ViPNet [Координатора] удаленной локальной сети;
- туннелирует открытый информационный обмен между компьютерами своей локальной сети в защищенное соединение от ViPNet [Координатора] данной ЛВС до защищенного мобильного пользователя с программным обеспечением ViPNet [Клиент];
- разграничивает доступ удаленных туннелируемых компьютеров и защищенных мобильных пользователей к ресурсам «своей» локальной сети (компьютеры удаленной локальной сети и защищенные мобильные пользователи смогут получить доступ не к каждому компьютеру данной локальной сети);
- разграничивает доступ «своих» туннелируемых компьютеров к ресурсам удаленной локальной сети и защищенных мобильных пользователей (не каждый компьютер данной локальной сети сможет получить доступ к компьютерам удаленной локальной сети и защищенным мобильным пользователям);
- является сервером IP-адресов, то есть является справочным бюро, которое сообщает защищенным мобильным пользователям о текущем состоянии других объектов VPN (включены или выключены) и их IP-адресах;
- является сервером для рассылки обновлений (программного обеспечения, справочная и ключевая информация);

- является сервером-маршрутизатором для рассылки почтовых сообщений (если используется программа «Деловая Почта») и файлов, посылаемых по «файловому обмену» между объектами VPN;
- является Межсетевым Экраном, который запрещает несанкционированный доступ в локальной сети из Интернета.

Так же, мы рассмотрели основные угрозы на данную не защищенную автоматизированную систему и программное обеспечение ViPNet, что позволило нам построить защиту этой автоматизированной системы.

Проделав этот анализ можно сказать, что предъявленные требования по защите автоматизированной системы были выполнены, и организована защита канала между несколькими локальными сетями через Internet, а так же организованы туннели на однокарточных Координаторах.

Список используемой литературы

1. Байков, В. Интернет: поиск информации и продвижение сайтов / В. Байков. - М.: БХВ-Петербург, 2017. - 907 с.
2. Бройдо, В. Л. Вычислительные системы, сети и телекоммуникации / В.Л. Бройдо, О.П. Ильина. - М.: Книга по Требованию, 2019. - 560 с.
3. Викторович, С.А. Система формирования кадрового потенциала для высокотехнологичных отраслей промышленности / С.А. Викторович. - М.: Нобель Пресс, 2018. - 696 с.
4. Глушаков, С.В. Компьютеры, программы, сети / С.В. Глушаков. - М.: АСТ, 2018. - 351 с.
5. Гольдштейн, А.Б. Технология и протоколы MPLS / А.Б. Гольдштейн, Б.С. Гольдштейн. - М.: БХВ-Петербург, 2019. - 304 с.
6. Даниленков, А. О. Локальная сеть своими руками / А.О. Даниленков, Ю.В. Васильев. - М.: Триумф, 2015. - 320 с.
7. Жуков, Юрий Основы веб-хакинга. Нападение и защита / Юрий Жуков. - М.: Книга по Требованию, 2017. - 208 с.
8. Журнал сетевых решений LAN, сентябрь 2013. - М.: Открытые Системы, 2019. - 840 с.
9. Злобин, В. К. Нейросети и нейрокомпьютеры: моногр. / В.К. Злобин, В.Н. Ручкин. - Москва: ИЛ, 2017. - 256 с.
10. Ирвин, Д. Передача данных в сетях: инженерный подход / Д. Ирвин. - М.: БХВ-Петербург, 2018. - 451 с.
11. Ирвин, Д. Передача данных в сетях: инженерный подход / Д. Ирвин. - М.: БХВ-Петербург, 2017. - 723 с.
12. Иртегов, Д.В. Введение в сетевые технологии / Д.В. Иртегов. - М.: БХВ-Петербург, 2018. - 947 с.
13. Кенин, Александр Практическое руководство системного администратора / Александр Кенин. - М.: БХВ-Петербург, 2018. - 282 с.

14. Ковалева, Наталья Эффективность внедрения облачных сервисов при автоматизации бизнеса / Наталья Ковалева. - М.: LAP Lambert Academic Publishing, 2017. - 116 с.
15. Колисниченко, Д. Беспроводная сеть дома и в офисе / Д. Колисниченко. - М.: БХВ-Петербург, 2016. - 480 с.
16. Колисниченко, Д. Беспроводная сеть дома и в офисе / Д. Колисниченко. - М.: БХВ-Петербург, 2017. - 480 с.
17. Малыгин, Иван Широкополосные системы связи / Иван Малыгин. - М.: LAP Lambert Academic Publishing, 2017. - 200 с.
18. Назаров, А. Н. Модели и методы расчета структурно-сетевых параметров сетей АТМ / А.Н. Назаров. - М.: Горячая линия - Телеком, 2017. - 256 с.
19. Назаров, А.Н. Модели и методы расчета структурно-сетевых параметров сетей АТМ / А.Н. Назаров. - М.: Горячая линия - Телеком, 2019. - 718 с.
20. Нгуен, Хынг Организация удостоверяющих центров на основе мультиагента: моногр. / Хынг Нгуен , Алексей Кизим und Валерий Камаев. - М.: LAP Lambert Academic Publishing, 2019. - 164 с.
21. Немет, Эви Unix. Руководство системного администратора / Эви Немет и др. - М.: Питер, БХВ-Петербург, 2017. - 928 с.
22. Поляк-Брагинский, А. В. Локальные сети. Модернизация и поиск неисправностей / А.В. Поляк-Брагинский. - М.: БХВ-Петербург, 2017. - 754 с.
23. Поляк-Брагинский, Александр Сеть под Microsoft Windows / Александр Поляк-Брагинский. - М.: БХВ-Петербург, 2019. - 336 с.
24. Росляков, А.В. Виртуальные частные сети. Основы построения и применения / А.В. Росляков. - М.: Эко-Трендз, 2017. - 242 с.
25. Самарский, Павел Анатольевич Основы структурированных кабельных систем / Самарский Павел Анатольевич. - М.: ДМК Пресс, 2016. - 506 с.
26. Старовойтов, Алексей Сеть на Linux. Проектирование, прокладка, эксплуатация / Алексей Старовойтов. - М.: БХВ-Петербург, 2016. - 865 с.