Титульный лист

Содержание

Введение....3
1. ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ПРОЕКТИРОВАНИЯ ЛОКАЛЬНЫХ КОМПЬЮТЕРНЫХ СЕТЕЙ....6
1.1. Понятие локальной компьютерной сети....6
1.2. Экономическая сущность задачи....7
1.4. Технологии организации безопасного обмена данными локальной сети и удаленных рабочих мест....9
1.5. Анализ существующих разработок и обоснование выбора технологии проектирования....12
1.6. Обоснование проектных решений по видам обеспечения:....13
1.6.1. по техническому обеспечению....13
1.6.2. по информационному обеспечению....14
1.6.3. по программному обеспечению....15
1.6.4. по технологическому обеспечению....17
Выводы по первой главе....18
2. ПРОЕКТИРОВАНИЕ СЕТИ ПЕРЕДАЧИ ДАННЫХ....19
2.1. Схема планируемой СПД....19
2.3. Пассивное оборудование сети....22
2.4. Активное оборудование сети....23
2.5. Серверное оборудование....28
2.6. Обеспечение безопасного обмена информацией между удаленными АРМ и центральным офисом....29
2.7. Реализация подключения к сети Интернет....31
2.8. Средства улучшения качества электропитания....32
2.9. Документирование и администрирование СКС....34
Выводы по второй главе....37
Заключение....38
Список использованных источников....41

Введение

Назначение локальной сети заключается в объединение разрозненных рабочих станций пользователей и администраторов, осуществляющих информационный обмен по каналам связи с использованием телекоммуникационного оборудования. При этом линии связи определяются совокупностью технических средств и физической среды, обеспечивая передача информации как между рабочими станциями, так и серверным оборудованием.

Ключевой задачей объединения рабочих станций в единую телекоммуникационную систему является предоставление возможности совместного доступа к информационным ресурсам на основе критериев доступа к ним.

Существенной характеристикой любой локальной сети является ее территориально–распределенная структура.

Основная задача объединения удаленных офисов (локальных сетей) в единую коммуникативную систему – это предоставление всех имеющихся сервисов всем сотрудникам компании с быстрым, простым, надежным доступом к ним без необходимости создания отдельной инфраструктуры на каждой из территориально удаленных площадок.

Методологической основой исследования являются анализ нормативно–правовых стандартов обеспечения качества обслуживания, в частности анализ требований стандарта, научные труды отечественных и зарубежных ученых в области организации локально–вычислительных сетей и мероприятий по обеспечению их защищенности.

Актуальность темы исследования определяется комплексом системных мероприятий по обеспечению режима информационной безопасности при организации безопасного обмена данными центрального офиса с сотрудниками, работающими удаленно. Информационная безопасность обладает разнообразными аспектами, среди которых значение имеют все аспекты. Невозможно отказаться от

определенных мероприятий, поскольку разработанная система обеспечения режима информационной безопасности не будет достаточна эффективна.

Новизна темы обуславливается комплексным подходом к разработке системы обеспечения режима информационной безопасности при удаленном доступе сотрудников к ресурсам локальной сети.

Теоретическая значимость темы исследования направлена на минимизацию угроз системе защиты информации, позволяющую если полностью не исключить, то свести к минимуму последствия дестабилизирующих факторов.

Практическая значимость темы исследования заключается в оптимизации выбора аппаратно–технических мер защиты.

Целью выпускной квалификационной работы является организация безопасного обмена данными центрального офиса с сотрудниками, работающими удаленно в компании.

Для достижения поставленной цели необходимо первоначально решить следующие **задачи**:

– провести анализ литературы по теме исследования;

- проанализировать необходимость защиты информации при удаленном доступе к локальным ресурсам;

- оценить перспективные решения в сфере информационной безопасности;

- разработать рекомендации и предложения по проектированию системы удаленного доступа.

Объектом исследования является исследование методов и средств обеспечения информационной безопасности при удаленном доступе сотрудников.

Предметом исследования является проект системы систему удаленного доступа к ресурсам локальной сети компании.

Для защиты информации существуют программные и технические средства. Программные средства – это программы, установленные на серверной части предприятия и каждом компьютере в частности, обеспечивающие защиту информации, её безопасную передачу и хранение. Технические средства – это

инженерно–технические устройства и приспособления, применяемые для фильтрации входящего и исходящего потока информации.

Несмотря на совершенность существующих систем безопасности невозможно достичь сто процентной защиты. Самой уязвимой частью системы защиты являются сотрудники, работающие в компании удаленно. Именно на них приходится восемьдесят процентов всех атак повлекших хищение данных, и лишь двадцать процентов на технические или программные уязвимости.

Данная выпускная квалификационная работа состоит из двух разделов. Первый раздел теоретический, где представлены: анализ предметной области локальных сетей и средств удаленного доступа к ним, программная и техническая архитектура локально–вычислительной сети компании, выявление проблем, сравнение существующих на рынке решений по выбранным функциональным возможностям.

Второй раздел проектный, где рассматривается: схема проектируемой сети безопасного обмена данными центрального офиса с сотрудниками, работающими удаленно в компании, выбор и настройка пассивного и активного оборудования, разработка проекта модернизации технических и программных средств.

1. ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ПРОЕКТИРОВАНИЯ ЛОКАЛЬНЫХ КОМПЬЮТЕРНЫХ СЕТЕЙ

1.1. Понятие локальной компьютерной сети

Локальная компьютерная сеть представляет собой коммуникационную сеть особого рода, в которой информация является продуктом генерирования, переработки, хранения и использования, а узлами сети — вычислительное оборудование. Основным критерием, отличающим компьютерные сети от автономных рабочих станций, является наличие обмена информацией между сетевыми узлами, связанными линиями передачи данных [1, стр. 28].

Локальная компьютерная сеть представляет собой сложный комплекс взаимосвязанных и согласованно функционирующих программных и аппаратных компонентов, основными элементами которого являются [11, стр. 56]:

– рабочие станции и серверное оборудование;

– коммуникационное оборудование;

– системное и прикладное программное обеспечение.

Несмотря на то, что компьютеры занимают центральное место в построении компьютерных сетей, коммуникационные устройства в последнее время играют далеко не последнюю роль. Как по влиянию на характеристики сети, так и по стоимости маршрутизаторы, модульные концентраторы, мосты, коммутаторы, кабельные системы и повторители из вспомогательных компонентов превратились наряду с системным программным обеспечением и компьютерами в базовый элемент создаваемой сети.

Последней составляющей, обеспечивающей информационной составляющую локальной компьютерной сети, является программное обеспечение. Все используемое в сети программное обеспечение можно разделить на системное и прикладное [13, стр. 136].

В общей виде общую структуру локальной компьютерной сети можно представить в виде единой структурированной инфраструктуры, изображенной на рисунке 1.1.

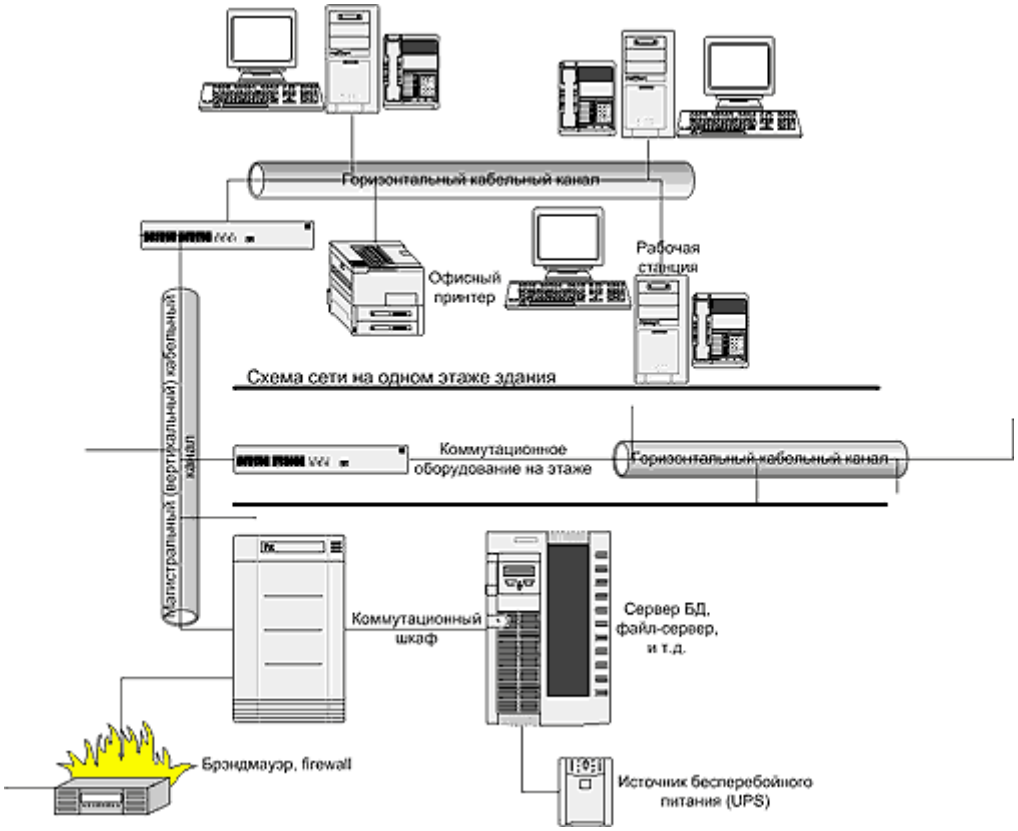

Рисунок 1.1 – Общая структура локальной компьютерной сети

Компьютерная сеть организации не должна представлять собой просто «набор» соединенных воедино рабочих станций, серверов, принтеров и сетевого оборудования.

1.2. Экономическая сущность задачи

Рассмотрим основные причины объединения отдельных рабочих станций в локальную компьютерную сеть [18, стр. 41]:

– организация общего доступа к сетевым ресурсам, расположенным на серверах;

– снижение затрат на программное обеспечение в расчете на одного пользователя.

К локальной сети организации предъявляются требования:

– надежности и отказоустойчивости;

– производительности;

– масштабируемости;

– обеспечения информационной безопасности;

– экономической эффективности.

При проектировании структуры локальной компьютерной сети организации должны быть учтены множество разнообразных аспектов таких как [6, стр. 89]:

– проектирование транспортной подсистемы;

– разработка структуры взаимодействия рабочих станций и серверов;

– обоснование выбора операционной системы рабочих станций и серверов;

– разработка структурированной кабельной системы;

– разработка структуры телефонной сети и необходимость ее интеграции с кабельной системой;

В зависимости от того, какие цели и задачи ставятся при объединении удаленных офисов, зависит и то, какая технологическая платформа будет использована, и, соответственно, какова будет общая стоимость проекта [14, стр. 92].

Если все ресурсы, необходимые удаленным пользователям, находятся в центральном офисе, а удаленные площадки являются лишь потребителями этих ресурсов, заказчику будет достаточно установить у себя в головном офисе терминальный сервер, на котором одновременно будут работать все удаленно подключаемые сотрудники каждый в своем сеансе. При этом не обязательно организовывать постоянно действующий канал VPN. Можно обойтись установлением сеансовых VPN по необходимости, что удешевляет проект.

Если все ресурсы находятся в центральном офисе, а на удаленных площадках достаточно серьезная инфраструктура (свой сервер), то в этом случае необходимо организовывать постоянно действующий канал VPN между площадками, как бы виртуально объединив площадки в общую локальную сеть.

Если все ресурсы находятся в центральном офисе, и ряд сотрудников, работающих удаленно, должны из совершенно произвольных мест регулярно подключаться к офису для обмена информацией с корпоративных ноутбуков или

планшетов, также можно организовать индивидуальные аппаратные или программные VPN каналы к центральному офису.

Выбор конкретного решения, конкретного перечня необходимого оборудования, программного обеспечения, формирование конкретного проекта зависит от ситуации заказчика, где в некоторых случаях VPN канал является необходимой частью инфраструктуры, а в некоторых – дополнительным технологическим элементом, обеспечивающим более высокий уровень защищенности подключения.

1.3. Технические и программные средства организации сети

Оборудование компьютерных сетей классифицируется по исполняемым функциям [5, стр. 82]:

– активное, включает сетевых карты рабочих станций и серверов, маршрутизаторы, концентраторы и т.п.;

– пассивное – кабели, соединительные разъемы, коммутационные панели и т. п.

С физической точки зрения, активное оборудование представляется устройствами, которым для функционирования необходима подача энергии, в то время как пассивному оборудованию подачи энергии не требует.

Также оборудование компьютерных сетей классифицируется на конечные системы или устройства, являющиеся источниками и/или потребителями информации, и промежуточные системы, обеспечивающие прохождение информации по сети.

1.4. Технологии организации безопасного обмена данными локальной сети и удаленных рабочих мест

Объединение удаленных офисов в единое информационное пространство посредством защищенной корпоративной сети передачи данных – один из

важнейших инструментов развития организации, предназначенный для обеспечения эффективного функционирования информационной инфраструктуры предприятия и решения следующих задач [10, стр. 82]:

– доступ к ресурсам через авторизацию (веб–сайт, единые файлы, электронная почта) вне зависимости от места положения пользователей;

– обеспечение обмена заданной информацией с необходимыми скоростями между всеми элементами сети;

– обеспечение обмена заданной информацией с необходимыми внешними сетями;

– безопасное, обеспеченное надежной защитой взаимодействие сотрудников с ресурсами, находящимися в разных офисах;

– оптимизация управления информационными ресурсами;

– практика единых телефонных номеров локальной офисной АТС;

– поддержка работы всех информационно–аналитических процессов предприятия, управление хранением, копированием и восстановлением его информационных активов;

– поддержка соответствующих прав доступа абонентов сети к ее информационным ресурсам, аутентификация пользователей сети и ее элементов;

– оперативность технической поддержки, благодаря наличию удаленного управления серверами, ПК и прочим оборудованием.

Схемы удаленного взаимодействия центрального филиала и территориально–распределенных АРМ приведена на рисунке 1.2.

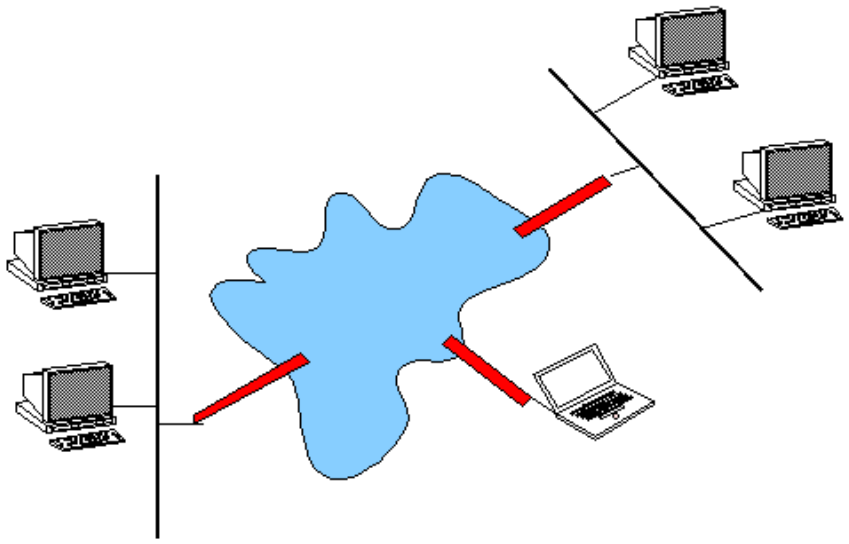

Рисунок 1.2 – Общая схема удаленного доступа

Таким образом, виртуальная частная сеть является некоторой имитацией сети, спроектированной на выделенных каналах. Если публичной сетью предоставляется данный вид сервиса, то в ней одновременно может быть создано несколько виртуальных корпоративных сетей, разделенных общими коммутаторами и физическими каналами связи.

Потоки данных отдельного предприятия образуют виртуальные каналы частной сети.

А вот защищенность от потоков данных других организаций может пониматься по–разному.

Согласно общепринятой терминологии защищенность может пониматься в следующих отношениях [8, стр. 126]:

–параметров пропускной способности сети;

– конфиденциальности обработки данных.

Естественно, каждая организация хотела бы, чтобы виртуальные сети были максимально схожи с внутренними локальными сетями, пропускная способность которых определяется пожеланиями руководства организации. Откуда следуют следующие требования к частной сети:

– пользователям VPN должны быть предоставлены определенные гарантии качества обслуживания виртуальной частной сетью, такие как, уровни задержек кадров и средняя пропускная способность;

– пользователям VPN должны быть доступны инструменты, предназначенные для контроля действительных параметров пропускной способности каналов связи.

1.5. Анализ существующих разработок и обоснование выбора технологии проектирования

Информационная безопасность обеспечивается использованием технических средств [22, стр. 71]:

- построения модели защищенной системы;
- управления доступом к ресурсам системы;
- обеспечения целостности и конфиденциальности;
- обеспечения наблюдаемости;
- защиты от воздействий вирусов и иных воздействий, вызывающих любую несанкционированную модификацию информации;
- защиты информации при передаче информации.

Перечень необходимых мер обеспечения информационной безопасности устанавливается в результате обследования информационной системы, учитывая соотношения затрат на защиту информации к возможному ущербу:

- ответственность сотрудников предприятия за принятие решений, связанных с ее информационными активами, должна быть персонифицирована;
- адекватность ролей сотрудников выполняемым функциям в соответствии с критериями и системой оценки;
- доступность предоставляемых услуг. На предприятии должна обеспечиться доступность предоставляемых клиентам услуг в установленные для этого сроки, установленные соответствующими договорами;
- наблюдаемость и оцениваемость системы обеспечения информационной безопасности. Результат применения должен быть наблюдаем и оценен

сотрудниками, обеспечивающими соблюдение режима информационной безопасности.

1.6. Обоснование проектных решений по видам обеспечения:

1.6.1. по техническому обеспечению

Взаимодействие центрального офиса с сотрудниками, работающими удаленно, должно осуществятся через криптомаршрутизатор.

Маршрутизатор должен быть укомплектован интегрированными средствами аппаратного ускорения шифрования, обеспечивающими функционал систем обнаружения вторжений и межсетевого экранирования [2, стр. 155].

В РД под межсетевым экраном (МЭ) понимается локальное (однокомпонентное) или функционально–распределенное программное (программно–аппаратное) средство (комплекс), реализующее контроль за информацией, поступающей в автоматизированную систему (АС) и/или выходящей из АС.

Указанным документом определены 12 показателей защищенности МЭ, требования к реализации которых задают класс защищенности МЭ.

К каждому классу защищенности МЭ сопоставлено в соответствие требование по защите категории информации ограниченного доступа. Иначе говоря, для того, чтобы АС возможно было аттестовать, объект информатизации должен быть защищен от внешней среды межсетевым экраном не ниже следующего класса:

– 5 класс для АС «1Д», «2Б», «3Б»;

– 4 класс для АС «1Г»;

– 3 класс для АС «1В», а также «2А», «3А» в случае обрабатываемой информации с грифом «секретно»;

– 2 класс для АС «1Б», а также «2А», «3А» в случае обрабатываемой информации с грифом «сов.секретно»;

– 1 класс для АС «1А», а также «2А», «3А» в случае обрабатываемой информации с грифом «особой важности».

Средства анализа защищенности должны обеспечивать возможность выявления уязвимостей, связанных с ошибками в конфигурации программного обеспечения информационной системы, которые могут быть использованы нарушителем для реализации атаки на систему.

1.6.2. по информационному обеспечению

Информационное обеспечение представляет совокупность единой системы классификации и кодирования информации, унифицированных систем документации, схем информационных потоков данных, циркулирующих в организации, а также методологии построения базы данных.

Комплекс технологической документации по организации безопасного обмена данными центрального офиса с сотрудниками, работающими удаленно в компании, включает [19, стр. 34]:

– инструкцию по порядку организации удаленного доступа пользователей в компьютерную сеть;

– инструкцию о порядке действий в нештатных ситуациях;

– инструкцию по порядку резервного копирования и архивирования информации;

– инструкцию по обеспечению работоспособности автоматизированных рабочих мест и серверного оборудования;

– инструкцию по организации антивирусной защиты;

– инструкцию по организации парольной защиты;

– инструкцию по регламентации работы администратора информационной безопасности.

Выполнение работниками организации требований данных инструкций позволяет избежать сбоев в организации безопасного информационного обмена средствами вычислительной техники.

1.6.3. по программному обеспечению

На рабочих станциях удаленных сотрудников должна быть установлена современная операционная система.

Операционная система Windows 10 характеризуется надежностью функционирования и защищенностью от несанкционированного воздействия. Ее проектирование осуществлялось с учетом требований обеспечения информационной безопасности, поэтому она обладает рядом преимуществ по основным ключевым направлениям:

– доверенная загрузка;

– улучшенный процесс идентификации;

– защита пользовательских данных;

– защита от внешних угроз безопасности.

Наибольшую опасность и сложность выявления представляют руткиты и буткиты, стартующие до загрузки операционной системы и работающие в привилегированном режиме, что позволят им получить практически неограниченный доступ к рабочей станции.

Технологии Secure Boot и Trusted Boot, встроенные в Windows 10, контролируют процесс загрузки и разрешают запуск только доверенным приложениям. Дополнительную защиту обеспечивает технология Early Launch Anti–Malware, выполняющая раннюю загрузку антивирусных средств.

Наиболее распространенный способ идентификации, включающий пару «логин–пароль», не обеспечивает требуемый уровень обеспечения информационной безопасности. При этом хакерами были неоднократно успешно реализованы атаки, направленные на взлом или подбор данных сведений. Поэтому в Windows 10 реализован новый метод авторизации, позволяющий использовать более безопасную альтернативу, сформированную на двухфакторной аутентификации.

Применяя технологию Windows Hello, в качестве дополнительной защиты можно использовать PIN–код или биометрические данные пользователя.

На рабочих станциях, оснащенных специальными камерами или сканером отпечатков, можно авторизоваться в системе с помощью отпечатков пальцев или лица.

Одной из наиболее актуальных проблем информационной безопасности является риск утечки конфиденциальной информации вследствие действий внутреннего нарушителя.

Предлагаемые сторонними разработчиками DLP–решения для защиты от данного риск характеризуются сложностью внедрения и сопровождения, а также стоимость лицензирования.

На рабочих станциях под управлением операционной системы Windows 10 Pro стала доступна технология защиты Windows Information Protection. Данное решение для предотвращения утечек информации по инсайдерским каналам позволяет:

– провести разграничение доступа личных и рабочих данных;

– зашифровать рабочие данные;

– надежно контролировать и предотвращать попытки несанкционированной передачи информации в ненадежные источники;

– в случае необходимости централизованно удалять информацию ограниченного распространения.

Также доступны следующие защитные механизмы:

– расширенные функциональные возможности защитника Windows;

– встроенную интеграцию с Windows Defender Advanced Threat Protection – интеллектуальную облачную службу, анализирующую угрозы на основе поведенческого анализа;

– система безопасности Credential Guard на основе виртуализации для защиты систем проверки подлинности;

–набор компонентов Microsoft Device Guard, обеспечивающих контроль целостности аппаратного и программного обеспечения.

Операционная система Windows 10 находится в процессе постоянного и непрерывного развития, предоставляя пользователям наиболее актуальную версию без дополнительной платы.

Поэтому кроме периодических обновлений, повышающих надежность функционирования, добавляются функциональные обновления, улучшающие качество функционирования без дополнительных затрат.

В Windows 10 встроен браузер Microsoft Edge, построенный на качественно ином уровне с поддержкой расширений и высокой скоростью работы.

1.6.4. по технологическому обеспечению

Администрирование является неотъемлемой составной частью ЛВС.

Администрирование включает в себя создание точной системы идентификации и хранения записей всех компонентов, входящих в состав ЛВС, включая трассы, элементы системы заземления и уравнивания потенциалов, кроссы и другие пространства, в которых она была установлена.

Все изменения, вносимые в кабельную систему, должны быть документированы непосредственно после их выполнения.

К функциональным элементам ЛВС, подлежащим администрированию, относятся [20, стр. 81]:

– горизонтальная кабельная подсистема;

– магистральная кабельная подсистема;

– трассы и пространства (помещения).

Администрирование телекоммуникационной инфраструктуры конечного пользователя выполняется с помощью следующих процедур [16, стр. 69]:

– присваивания уникальных идентификаторов компонентам инфраструктуры;

– оформления записей (паспортов) для всех присвоенных идентификаторов;

– определения взаимных ссылок записей с целью получения содержащейся в них информации.

Выводы по первой главе

Главная выгода от использования VPN для центрального офиса с сотрудниками, работающими удаленно – совокупность стоимостной эффективности возможного использования общедоступной сетевой среды для транспортирования частной информации и высокого уровня безопасности. Защищенная виртуальная сеть может предоставить множество уровней безопасности, включая усовершенствование конфиденциальности, целостности и аутентификации. Поскольку VPN использует существующую сетевую инфраструктуру, ее можно реализовать достаточно быстро, так как нет необходимости прокладывать новые (выделенные) линии связи.

Комбинация безопасности, быстрой установки и рентабельности с точки зрения стоимости может сделать VPN превосходным коммерческим коммуникационным решением.

2. ПРОЕКТИРОВАНИЕ СЕТИ ПЕРЕДАЧИ ДАННЫХ

2.1. Схема планируемой СПД

При организации защиты каналов связи, согласно требованиям ФСТЭК/ФСБ, будет использован аппаратно–программный комплекс шифрования «Континент» (рис. 2.1), являющийся централизованным комплексом защиты сетевой инфраструктуры и создания VPN–сетей с использованием алгоритмов ГОСТ. Архитектурно комплекс состоит из нескольких решений:

1. Криптошлюз — основной элемент комплекса, обеспечивающий практически весь необходимый функционал, а именно:

– создание VPN–каналов между узлами с использованием ГОСТ 28 147−89;

– с помощью STUN возможно построение туннеля между устройствами, чей настоящий адрес скрыт за NAT;

– межсетевое экранирование с поддержкой Port Address Translation и Network Address Translation (PAT и NAT, соответственно);

– работа с VLAN;

– статическая и динамическая маршрутизация (поддерживаются в том числе протоколы OSPFv2, RIP и BGPv4, конфигурация задается не через GUI, а в виде текстовых файлов);

– зеркалирование трафика через SPAN–порт для анализа (например, для DLP или IDS);

– приоритизация трафика, он же QoS;

– функции DHCP–сервера или DHCP–релея;

– защита от DoS–атак типа SYN–Flood;

– обеспечение отказоустойчивости в режиме High Availability (Active/Passive).

2. Детектор Атак – система обнаружения вторжений, подключаемая к SPAN–порту и обнаруживающая атаки сигнатурными и эвристическими методами. Детектор атак способен в режиме реального времени информировать администратора или аудитора о выявленных инцидентах либо с помощью специального ПО, либо через электронную почту. Данные об инцидентах можно

просматривать также в виде весьма симпатичных и информативных графических отчётов.

3. Центр Управления Сетью, он же ЦУС – средство централизованного управления и мониторинга перечисленных выше устройств «Континент». Сам по себе может выполнять роль криптошлюза, обеспечивая маршрутизацию, функции NAT и построение L3 VPN. ЦУС – это обязательный компонент системы.

4. СПО «Сервер Доступа» и СКЗИ «Континент–АП», используемые для обеспечения защищенного удаленного доступа отдельных рабочих станций. Сервер доступа – серверный компонент, отвечающий за настройку маршрутизации, добавление или удаление клиентов, а также выпуск сертификатов. Сервер доступа может быть развернут либо на Центре Управления Сетью, либо на криптошлюзе. Континент–АП устанавливается на рабочую станцию сотрудника и обеспечивает VPN–туннель до Сервера Доступа. Поддерживаются операционная система Windows и наиболее популярные дистрибутивы Linux.



Рисунок 2.1 – АПКШ «Континент», платформа IPC–100

Вся экосистема «завязана» на центральное устройство — ЦУС. Первичная инициализация, изменение каких–либо параметров — всё происходит именно через него, так как локальная настройка — скорее, служебная операция с очень ограниченным числом настраиваемых параметров, да и зачастую требующая перезагрузки устройств, что в production environment порой просто недопустимо.

С одной стороны, централизованная настройка — удобный подход: не надо запоминать адреса устройств в сети, поочередно подключаться к каждому, а если ещё и какой–нибудь криптошлюз расположен за NAT’ом, сбор какой–либо диагностической информации с различных устройств также не занимает много времени. Но у всего есть оборотная сторона — у нас появляется точка отказа. Дело в том, что ЦУС может резервироваться только по схеме «холодного устройства». Это означает, что в случае выхода из строя основного ЦУС администраторы должны «вручную» переключить управление на резервное устройство. Только вот рекомендация по приобретению резервного устройства часто игнорируется, либо в нужный момент оно оказывается не настроено должным образом. Кроме того, у некоторых пользователей ЦУС сам по себе выполняет роль криптошлюза. Хотя для более–менее критичной инфраструктуры — это ошибка планирования сети. Не рекомендую так делать.

Что же касается инцидентов выхода из строя прочих устройств АПКШ «Континент», то согласно статистике процент отказов крайне мал. А если отказы и случаются, то случаются они в период тестовой эксплуатации, когда контракт на интеграцию еще в силе и есть возможность оперативно заменить устройство. Но это вовсе не означает, что можно вообще забыть о резервировании и ставить на критичных точках всего одно устройство. Тем более что производитель предоставляет возможность резервирования в режиме High Availability по схеме Active/Passive. Время переключения около 30 секунд.

Непосредственно администрирование осуществляется через СПО «ПУ ЦУС», доступное только для ОС Windows. Логичнее, конечно, в подобных ситуациях осуществлять настройку через web–интерфейс, что и реализовано в большинстве сетевых решений, но такой подход обеспечивает больший уровень безопасности.

Само программное обеспечение управления реализовано весьма удачно. Работать в нем вполне комфортно. Производитель во многих аспектах старался максимально упростить жизнь, например, включение VPN–туннеля между устройствами реализуется в пару кликов мыши, при этом нас может не волновать то, что у устройства нет белого IP–адреса.

2.3. Пассивное оборудование сети

Проект центрального офиса локальной сети компании предусматривает укладку телефонного и сетевого кабеля в кабель–каналы.

Система прокладки кабелей на основе кабель–каналов обеспечивает [12, стр. 69]:

– возможность изменения конфигурации системы в любое время;

– разделение, защиту и отвод кабелей электроустановки (разделение силовых и слаботочных сетей даже в углах);

– широкий выбор профилей, отделочных и монтажных аксессуаров (заглушки, накладки на стык крышки, профиля, внутренние, внешние и плоские углы, отводы).

Перегородки, крышки и накладки на защелках позволяют выравнивать профили, что упрощает их монтаж.

Продукция отвечает требованиям к надежности, безопасности и основным техническим характеристикам стандарта EN 50085–2–1 (IP 40, IK 07).

Профиль в виде моноблочных кабель–каналов поставляется в комплекте с крышкой и имеет стандартную длину профиля в 2 метра.

Варианты крепления к стене:

– клеевое (капсюль с неопреновым клеем для пистолета);

– дюбель для быстрого крепления;

– монтажный адаптер Spit (для быстрого крепления профилей);

– винты и гвозди.

Для резки профиля используется пила по металлу и шаблон для резки.

Внутренние и внешние регулируемые углы предназначены для соединения двух кабель–каналов одинакового сечения под внутренним углом и позволяют:

– не разрезать кабель–канал под острым углом;

– обеспечить заявленную степень защиты;

– улучшение внешнего вида, скрывая место разреза без излишнего утолщения кабельной трассы.

При этом суппорты под электроустановочное оборудование следует устанавливать на расстоянии не менее 10 сантиметров от краев угла.

Углы защелкиваются на корпусе кабель–канала.

Допускается установка на кабель–каналы с разделительными /несущими перегородками или без них.

Предназначены для установки под углом 80–100 градусов.

Внутренние углы включают в себя два элемента для верхней и нижней частей кабель–канала между которыми устанавливается гибкая крышка.

Розетка автоматизированного рабочего места (АРМ) представлена на рисунке 2.2.



Рисунок 2.2 – Розетки для подключения рабочей станции и телефона

Качественный монтаж горизонтальной подсистемы локальной сети позволит в дальнейшем избежать проблема с масштабируемостью и управляемостью.

2.4. Активное оборудование сети

На любом предприятии, в процессе функционирования которого обрабатывается конфиденциальная информация, вместе с ней возникает необходимость ее защиты. Постоянно идет создание более совершенных каналов передачи данных, способов защиты данных каналов и программное совершенствование системы передачи данных.

В зависимости от каналов передачи данных, в которых циркулирует информация, применяются различные методы ее защиты и требуются концептуально разные подходы к защите.

Для предприятий, отличительной особенностью которых является постоянный рост и увеличение штата сотрудников, а также имеющих удаленные офисы, наиболее оптимальным станет использование виртуальных частных сетей. Виртуальные частные сети представляют собой защищенное соединение, которое создается внутри незащищенной сети с использованием открытых каналов связи путем создания зашифрованного канала. Проще говоря, такое соединение можно представить как туннель, проложенный через интернет [15 ,стр. 95].

Виртуальные сети получили большое распространение за счет экономичности и высокой безопасности, особенно при использовании распределенных вычислительных сетей. В технологии VPN для защиты компьютерных сетей используются технологии, включающие в себя элементы межсетевого экранирования и механизмы криптографической защиты сетевого трафика [21 , стр. 69].

VPN с помощью специальных программ объединяет отдельные компьютеры и локальные сети для защиты передаваемой информации. При соединении с сервером, находящимся в сети общего доступа VPN, технология образует канал защищаемый информацию с помощью алгоритмов шифрования. Таким образом, внутри незащищенной сети образуется защищенный туннель для передачи данных. Проще говоря, VPN позволяет виртуально подключить одну сеть к другой таким образом, как будто они соединены проводами, при этом весь исходящий и входящий трафик шифруется, что делает эту технологию безопасной.

Для разработки алгоритма организации безопасного подключения распределенной корпоративной сети к интернету необходимо представить типичную структуру организации сети предприятия. За основу взято предприятие малого или среднего бизнеса, имеющее центральный офис и несколько удаленных, и для которого требуется осуществлять обмен конфиденциальной информации между офисами. Вследствие ограниченности бюджета содержание выделенных

провайдером каналов не представляется возможным, поэтому обмен информацией обеспечивается по открытым каналам интернета [7, стр. 126].

Требуется разработать архитектуру, включающую следующие компоненты: структуру главного и удаленных офисов, имеющих возможность осуществлять информационный обмен между собой, организацию безопасной сетевой инфраструктуры, характерной для сетей любого масштаба и обеспечивающей защиту от основных угроз информационной безопасности; гибкие возможности сетевых настроек.

Сравнительный анализ протоколов организации VPN сетей [4, стр. 42] представлен в таблице 2.1.

Таблица 2.1 – Сравнительный анализ протоколов организации VPN сетей

Протокол	Преимущества	Недостатки
PPTP	- распространенность; - простота настройки; - быстрота; - поддержка множества протоколов	- небезопасен (уязвимый протокол аутентификации MS-CHAP v.2 все еще используется); - слабая устойчивость к атакам.
L2TP-IPsec	- очень безопасен; - простота настройки; -доступен в современных операционных системах; - создание туннелей в различных сетях	- работает медленнее, чем OpenVPN; - может потребоваться дополнительная настройка роутера; - недостаточная эффективность; - применение протоколов Internet Key Exchange (IKE) с заранее согласованными ключами требует статических IP-адресов
IPsec	- очень безопасен (поддерживают множество криптографических алгоритмов, например, AES, Blowfish, 3DES, CAST-128, Camelia и другие); - поддерживает три вида установления соединения: Gateway-to-Gateway; Gateway-to-Host; Host-to-Host.	– невозможность динамической маршрутизации; Внедрить ее в данных условиях невозможно – все IGP требуют прямого L2-линка между соседями, чего не обеспечивает IPSec. Поэтому в данной реализации трафик отправляется в туннель на основе ACL и карты шифрования, а не таблицы маршрутизации. – существуют проблема с мультикастом, связанная с заданием конкретных подсетей в ACL; – не работает с NAT из-за особенностей ESP-пакета.

Продолжение таблицы 2.1

OpenVPN (SSL)	- гибко настраивается; - очень безопасен (поддерживают множество криптографических алгоритмов, например, AES, Blowfish, 3DES, CAST-128, Camelia и другие); - может работать сквозь файрволлы; -высокая переносимость между платформами; - клиентские хосты могут иметь статические и динамические IP-адреса; - поддержка режимов маршрутизации (routed) и моста (bridged)	- необходимо программное обеспечение стороннего разработчика; - не очень неудобен в настройке; - ограниченная поддержка портативными устройствами.
GRE	- позволяет эффективно организовать туннель с низкими накладными расходами; - работает по принципу симметричного туннеля точка-точка, а не сервер-мультиклиент; - GRE может пропускать как данные второго уровня, так и данные третьего уровня, совмещая таким образом функциональность PPTP и L2TP	- протокол не осуществляет шифрования; - проблема бита DF; - GRE является протоколом сетевого уровня и не использует порты, то работа протокола GRE через межсетевой экран может быть затруднена; - при туннелировании IP через IP возникает зацикливание маршрутизации

Алгоритм создания VPN соединения представлен на рисунке 2.3.

Рисунок 2.3 – Алгоритм создания VPN соединения

Для организации локальной сети внутри сегмента корпоративной сети передачи данных используем криптомарутизаторы «Континент–К, а передачи данных между удаленными сотрудниками и ресурсами локальной сети СПО «Континент–АП».

2.5. Серверное оборудование

Наиболее уязвимым звеном сети является серверное оборудование, именно поэтому выбор сервера является важным условием надежного функционирования.

Серверное оборудование комплектуется надежными функциональными подсистемами, включающими:

– оперативную память с коррекцией ошибок, обеспечивающую повышенную устойчивость к сбоям;

– резервирование критически важных узлов (блоков питания, процессоров, жестких дисков, охлаждающих подсистем), позволяющих минимизировать периоды неработоспособности серверного оборудования;

– дополнительные каналы для контроля большего количества параметров сервера: датчики температуры контролируют температурные режимы всех процессоров, модулей памяти, температуру в отсеках с установленными жёсткими дисками.

Центральным звеном проектируемой локальной компьютерной сети является сервер, обеспечивающий надежное хранение необходимой информации в сочетании с возможность быстрого доступа к ней. Сервер установлен в коммутационном шкафу, что повысит надежность и управляемой проектируемой локальной компьютерной сети.

Сервер HP ProLiant DL380 (рис. 2.4) является продолжением традиций инженерного и технологического совершенства решений компании Hewlett–Packard. Сервер предоставляет уникальное сочетание повышенной гибкости и высокой производительности, высокой управляемости и длительным временем безотказной службы, высокой плотности размещения в 2U корпусе и 2–сокетной архитектуры с процессорами Intel Xeon.



Рисунок 2.4 – Сервер HP ProLiant DL380 G8

В сервере HP высочайший уровень производительности и экономии электроэнергии обусловлены использованием новейших процессоров Intel Xeon с поддержкой встроенного контроллера памяти и технологий Intel QuickPath, Turbo Boost, Intelligent Power и Trusted Execution Technology.

Сервер HP ProLiant DL380 поддерживает до 192Gb оперативной памяти, что значительно увеличивает эффективность работы ресурсоемких приложений. Установлены 16 жестких дисков HP SAS обеспечивающие высокую пропускную способность, быстрый доступ к данным и высокую производительность.

2.6. Обеспечение безопасного обмена информацией между удаленными АРМ и центральным офисом

СКЗИ Континент–АП предназначено для безопасной передачи данных через общедоступные (незащищенные) сети. Защита данных обеспечивается криптографическими методами, вследствие чего через общедоступную сеть данные передаются в зашифрованном виде. На удаленной рабочей станции устанавливается абонентский пункт, который для передачи данных соединяется со специализированным сервером доступа, проверяющим полномочия на доступ и разрешающим доступ к ресурсам локальной сети организации.

При установке Континент–АП на компьютере автоматически создается соединение с одноименным названием «Континент АП». Для правильной работы Абонентского пункта необходимо произвести настройку указанного соединения. Настройка соединения выполняется под учетной записью пользователя с правами администратора рабочей станции.

Для настройки соединения необходимо нажать правую кнопку мыши на пиктограмме программы управления Абонентским пунктом (значок в виде щита с буквой «К» в правом нижнем углу экрана) и в появившемся контекстном меню выбрать пункт «Настройка соединения →Континент АП» (рис. 2.5).

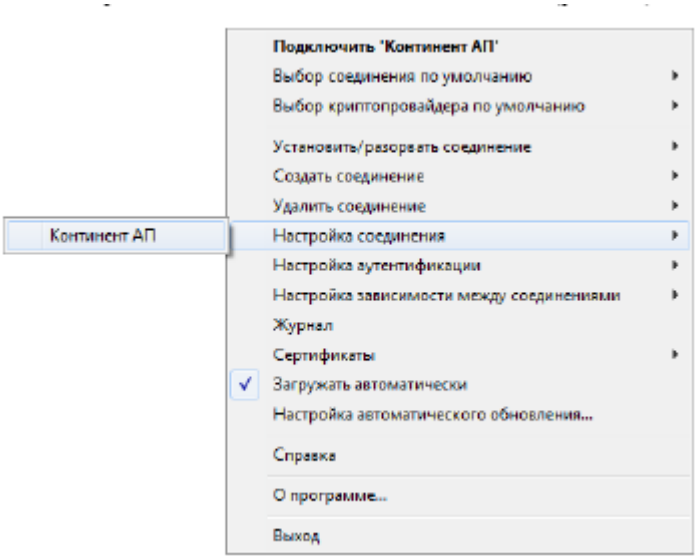

Рисунок 2.5 – Настройка соединения СКЗИ «Континент–АП»

Откроется окно свойств соединения «Континент АП». В этом окне в поле «Адрес СД:» вводится IP–адрес сервера доступа организации (рис. 2.6).

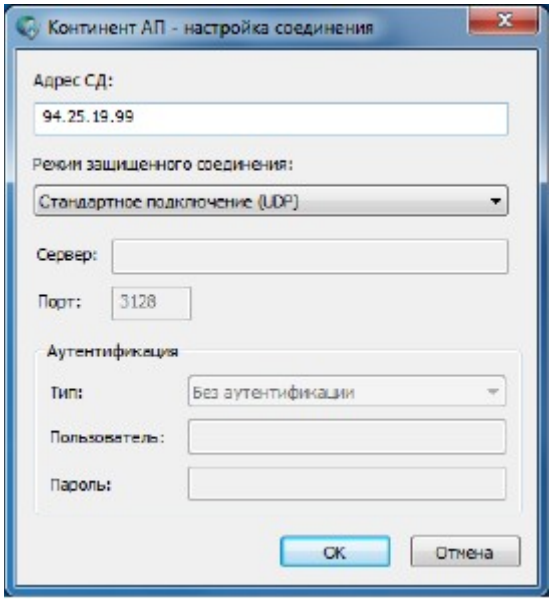

Рисунок 2.6 – Настройка сервера доступа в СКЗИ «Континент–АП»

Для авторизации на сервере доступа сотруднику необходимо иметь закрытый ключ аутентификации и сертификат открытого ключа.

Для генерации нового ключевого носителя необходимо правой кнопкой мыши на пиктограмме программы управления выбрать пункт «Сертификаты → Создать запрос на пользовательский сертификат…».

2.7. Реализация подключения к сети Интернет

Системы измерения и контроля трафика пакетов информации (далее СИКТ) предназначены для определения характеристик трафика пакетов информации в точках подключения к сети оператора связи: количества передаваемой информации, длительности и скорости передачи информации.

СИКТ является функциональной системой измерений и контроля трафика пакетов информации, входящей в состав технических систем с измерительными функциями «Системы контроля, мониторинга и управления трафиком КМУТ» (далее – КМУТ). СИКТ не имеет выделенных блоков, плат или самостоятельных программ, а использует возможности и функции аппаратуры и программного обеспечения КМУТ.

Принцип действия СИКТ основан на измерении и регистрации характеристик трафика пакетов информации в оператора связи. КМУТ состоит из зондов периферийных узлов, сервера и зонда центрального узла. Зонды подключаются к сети оператора связи в заданных точках подключения через оборудование оператора связи – коммутаторы и каналообразующую аппаратуру «последняя миля».

Информация об измеряемых характеристиках канала связи оператора через сеть связи общего пользования передаётся для сбора и дальнейшей обработки в сервер центрального узла КМУТ. Измерению подлежат характеристики каналов связи, образованных между периферийными зондами КМУТ, зондом и сервером центрального узла КМУТ.

Нормируемыми и регистрируемыми характеристиками являются диапазон и пределы допускаемой погрешности измерений:

– количества передаваемой информации;

– длительности передачи информации;

– скорости передачи информации.

Конструктивно КМУТ выполнен в виде зондов, размещаемых в периферийных узлах сети оператора связи и центрального узла оператора связи, в котором размещены сервер и зонд.

Для увеличения надежности измерения и контроля характеристик каналов каждый зонд содержит две идентичных части, которые подключаются к основным и резервным каналам оператора, а также к основным и резервным каналам сети связи общего пользования.

ООО «ЭнергоСтройЛизинг» является разработчиком, правообладателем и производителем систем повышения надежности и эффективности использования ресурсов телекоммуникационной инфраструктуры.

Обслуживание локальной сети – это необходимое условие для работы информационной системы учреждения. Ведь именно от этого оборудования в большей степени зависит сохранность конфиденциальной информации и защита данных от несанкционированного доступа [9, стр. 113]. Техническое обслуживание локальной сети включает в себя широкий список разных мероприятий, начиная от монтажа и настройки, заканчивая вводом в эксплуатацию и последующим сопровождением. Для достижения максимально возможного эффекта на каждом этапе, проводится тщательный анализ всех требований со стороны предприятия. Благодаря этому гарантируется, что обслуживание локальной сети будет учитывать особенности бизнеса и позволит существенно увеличить скорость обработки производственных задач.

2.8. Средства улучшения качества электропитания

Для работы электронного оборудования требуется качественное и бесперебойное электропитание. По оценкам специалистов, причиной более половины сбоев компьютерных систем является некачественное электроснабжение.

В России требования к качеству электроэнергии регулируются двумя стандартами. ГОСТ 23875–88 дает определения показателям качества электроэнергии, а ГОСТ 13109–97 устанавливает значения этих показателей.

Электронное оборудование, питающееся от сети переменного тока, подвергается различным негативным воздействиям со стороны этой питающей сети. Стандартным требованием к питающей сети является напряжение питания 220 В с допустимыми отклонениями от –15% до +10% от номинала (187–242 В) при частоте 50±1 Гц. Среди различных сбоев в электрической сети встречаются кратковременное и длительное отклонение напряжения от номинала, высоковольтные импульсы, электромагнитные и радиочастотные помехи, отклонение частоты и т.д.

Существуют следующие типы источников бесперебойного питания:

– standby;

Является самым простым и недорогим типом ИБП, не стабилизирующим выходное напряжение.

– smart или линейно–интерактивные;

Данное название закрепилось со времен легендарной серии линейно–интерактивных ИБП Smart–UPS от компании APC by Schneider Electric. Являясь одним из наиболее известных брендов–производителей ИБП для рабочих станций и серверного оборудования, APC был внедрен комплекс уникальных инженерных решений, позволяющих не только предотвратить потерю ценной информации, но и управлять группами розеток ИБП, перенаправляя электроэнергию на приоритетные устройства, а также программировать сценарии на случай отключения питающей сети.

– double conversion;

Данный тип ИБП обеспечивает максимальный уровень защиты, полностью преобразуя входящее напряжение переменного тока в постоянное и выполняя обратное преобразование. Обеспечивает максимальный уровень защиты от всевозможных проблем в питающей сети, отличаясь высокой стоимостью.

На рабочих станциях установлены ИБП APC 900VA Back–UPS Pro (рис. 2.7). Помимо требуемой для решения типовых задач мощности, данный ИБП характеризуется возможностью защиты телефонных линий и телекоммуникационного оборудования.



Рисунок 2.7 – ИБП APC 900VA Back–UPS Pro

На серверном оборудование установлены ИБП APC SMX3000HVNC серии Smart–UPS X – интеллектуальное эффективное решение для защиты сетевых устройств от любых нарушений питающей сети от начального уровня до систем, масштабируемых по времени работы на аккумуляторах. Устройство идеально подходит для серверов, кассовых терминалов, маршрутизаторов, коммутаторов, концентраторов и других сетевых устройств. Модель обладает возможностью наращивать время автономной работы за счет подключения к ней дополнительных внешних аккумуляторных батарей, что позволяет защитить запитанное через данное устройство оборудование в течение многочасовых отключений электроэнергии. APC SMX3000HVNC может размещаться как в стойке 19", так и на полу (на специальных шасси, входящих в комплект поставки), в стойке занимает высоту 4U. В ИБП встроена сетевая карта удаленного управления и контроля AP9631.

2.9. Документирование и администрирование СКС

В современных зданиях требуется применять эффективные коммуникационные инфраструктуры способные поддерживать работоспособность разнообразных сервисных систем, основанных на электронном информационном

обмене. Данную инфраструктуру следует рассматривать как конгломерат телекоммуникационного оборудования, кабельных линий, элементов системы заземления, которые обеспечивают начальную систему поддержки распределения информационных потоков в здании. Администрирование сетевой инфраструктуры начинается с документирования (маркировки, составления записей, отчетов и нарядов на выполнения работ, изготовления чертежей) кабелей, телекоммуникационного оборудования, кроссировочных и коммутационных панелей, телекоммуникационных шкафов.

Эксплуатационная документация по локальной сети может быть представлена совокупностью следующих документов [17, стр. 89].

1. Документы, описывающие структуру локальной сети:

1.1. Поэтажный план здания с указанием:

– помещений с установленными компьютерами и средствами вычислительной и оргтехники;

– помещения серверной;

– элементов компьютерных сетей (провода и др.);

– сетей 220 В (щиты, проводка, розетки, линии заземления).

1.2. Для каждого кабинета с компьютерами, серверной – отдельные схемы с указанием размещения в них:

– рабочих станций, серверов и активного сетевого оборудования;

– пассивного оборудования;

– линий электропитания.

1.3. Описание среды передачи данных:

– кабельной поэтажной подсистемы;

– схемы прокладки оптоволоконного обрудования.

1.4. Описания подключения компьютеров к сетевому оборудованию и связь сетевого оборудования между собой (подключение с точностью до порта сетевого оборудования).

1.5. Описание адресного пространства локальной вычислительной сети: какие IP–адреса какими компьютерами используются при фиксированной адресации или

какой диапазон IP–адресов выделен для DHCP для организации, для выхода в Интернет.

2. Документы по учету технических средств локальной сети:

– рабочих станций и серверного оборудования;

– сетевого оборудования;

– средств вычислительной и оргтехники.

3. Документы учета программного обеспечения, установленного на серверах и рабочих станциях

– операционных систем и офисного программного обеспечения;

– специализированного программного обеспечения;

– средств криптографической защиты информации;

– систем управления базами данных.

4. Документы, подтверждающие лицензионную чистоту программного обеспечения:

– лицензии;

– документация по подсистеме программного обеспечения;

– голограммы.

5. Документы по организации доступа к глобальной сети Интернет:

– приказ на предоставление доступа с указанием ответственного лица;

– схема подключения локальной к глобальной геоинформационной сети с указанием параметров сетевых подключений;

– документы по организации контентной фильтрации;

– документы по контролю посещаемых ресурсов.

6. Должностные инструкции для системного администратора и администратора информационной безопасности.

7. Документы по обеспечению безопасной работы в локальной сети [3, стр. 82]:

– документы по организации парольной защиты;

– документы по организации антивирусной защиты;

– план резервного копирования и восстановления информации;

– документы по организации защиты персональных данных в локальной сети;

– документы по организации режима информационной безопасности при работе в сетях общего пользования;

– документация по технике безопасности.

Выводы по второй главе

В зависимости от того, какие цели и задачи ставятся при объединении удаленных офисов, зависит и то, какая технологическая платформа будет использована, и, соответственно, какова будет общая стоимость проекта.

Если все ресурсы находятся в центральном офисе, и ряд сотрудников, работающих удаленно, должны из совершенно произвольных мест регулярно подключаться к офису для обмена информацией с корпоративных ноутбуков или планшетов, также можно организовать индивидуальные аппаратные или программные VPN каналы к центральному офису.

Взаимодействие центрального офиса с сотрудниками, работающими удаленно, должно осуществятся через криптомаршрутизатор.

Заключение

Представить работу современной успешной организации без наличия общей информационной среды сегодня практически невозможно. Воспользоваться всеми достоинствами и выгодами новейших технологических разработок поможет совершенствование локально-вычислительной сети. Подобный шаг позволяет значительно повысить эффективность работы всего учреждения.

Эффективность работы локальной сети определяется исходя из параметров, которые были выбраны при её формировании. Структура ЛВС основывается на финансовых возможностях, имеющихся в нынешнее время технологиях, стандартах и предъявляемых требованиях. В каждом отдельном случае выбирается индивидуальная топология самой сети, ее кабельная структура, соединительные устройства, способы передачи информации, сетевая ОС, методы взаимодействия.

Проектирование локальной сети организации позволило:

- обеспечить существенную экономию затрат при относительно высоких начальных вложениях за счёт низких эксплуатационных расходов при длительном сроке эксплуатации;
- повысить эффективность работы предприятия за счет совместного использования данных и сетевых устройств, применения современных систем контроля управления трафиком.

Система информационной безопасности – это функционирующая как единое целое совокупность мероприятий и средств, устремленная на ликвидацию внутренних и внешних угроз жизненно важным интересам субъекта безопасности, создание, поддержание и развитие состояния защищенности его информационной среды.

Рассмотрен перечень аппаратно–программных средств обеспечения безопасности информации и проведено экономическое обоснование применимости данных средств.

Термин «информационная безопасность» может трактоваться, с одной стороны, как состояние защищенности человека, общества и государства в

информационной сфере, а с другой – как результат деятельности по обеспечению информационной безопасности.

Выделяются следующие направления защиты информации:

– правовая защита информации;

– техническая защита информации;

– криптографическая защита информации;

– физическая защита информации.

Рассмотренные программно-технические меры защиты информации от актуальных угроз подразумевают изменение вектора защиты данных и использование инструментов, которые помогают обнаружить неизвестные угрозы и странное «поведение» данных.

Внедрение данных программно-технических мер защиты позволит повысить общий уровень защищенности системы защиты локальной предприятия.

Основываясь на практическом опыте, организация системы безопасности предприятия должна осуществляться в соответствие со следующими принципами:

– непрерывность;

– комплексность;

– своевременность;

– законность;

– активность;

– универсальность;

– экономическая целесообразность;

– надежность;

– профессионализм;

– взаимодействие и координация;

– определенность целей.

При организации безопасного обмена данными центрального офиса с сотрудниками, работающими удаленно, выявлены преимущества использования для данной цели технологии VPN и межсетевого экранирования компании «Код Безопасности».

АПКШ «Континент» – эффективный и гибкий инструмент для выстраивания защищенных каналов обмена данными с территориально распределенными подразделениями предприятия, удаленно работающими сотрудниками и партнёрами. Решение позволяет выстраивать виртуальные частные сети (VPN) любой архитектуры и обеспечивает безопасность информации, транслируемой между составляющими VPN (локальными сетями, их сегментами, отдельными рабочими ПК). Применение системы уникальных ключей для шифрования каждого пакета данных в АПКШ «Континент» IPC-100 гарантирует невозможность расшифровки информации сторонними лицами в случае её перехвата. Защиту от несанкционированного доступа обеспечивает фильтрация трафика. Решение полностью соответствует требованиям ГОСТ 28147-89.

Небольшие размеры никак не сказываются на качестве и эффективности шифровки данных. По этим показателям АПКШ «Континент» IPC-100 ничуть не уступает тяжеловесным аналогам. Всё дело в применяемой системе уникальных ключей, которая обеспечивает стопроцентную конфиденциальность транслируемой информации. Даже в случае перехвата данных из сети риск их дешифровки будет полностью исключен.

Еще одно немаловажное преимущество АПКШ «Континент» IPC-100 заключается в его энергоэффективности. Значительно сокращена потребляемая мощность криптошлюза. Усовершенствованные сетевые интерфейсы позволяют непосредственно, без задействования медиаконвертеров, осуществлять криптографическую обработку данных, транслируемых по оптическим каналам связи.

Таким образом, цель работы – организация безопасного обмена данными центрального офиса с сотрудниками, работающими удаленно в компании – достигнута, поставленные задачи решены.

Список использованных источников

1. Алиев Т.И., Соснин В.В., Шинкарук Д.Н. Компьютерные сети и телекоммуникации: задания и тесты: Учебно-методическое пособие. – СПб.: ИТМО, 2018. – 112 с.
2. Бауткин М.С. Организация удаленного доступа на базе технологии VPN // Актуальные вопросы эксплуатации систем охраны и защищенных телекоммуникационных систем. – 2018. – № 3.– С.155–157.
3. Бондаренко Н.А., Буханцов А.Д., Лихолоб П.Г. О корпоративной политике информационной безопасности предприятия // Актуальные вопросы обеспечения информационной безопасности. – 2015. – № 3.– С.82–92.
4. Калистратов А.П. Анализ протоколов, используемых при организации удаленного доступа. // Молодежный научно-технический вестник. – 2016. – № 9.– С.42.
5. Куроуз Дж., Росс К. Компьютерные сети. Настольная книга системного администратора – М.: Эксмо, 2016.– 912 с.
6. Куроуз Дж, Росс К. Компьютерные сети. Нисходящий подход – М.: Эксмо, 2016.– 912 с.
7. Ленкин А.В., Колесников А.А., Лучанинов Д.В. Система организации удаленного доступа к базам данных. // Постулат. – 2017. – № 1.– С.28.
8. Лимончелли Т., Хоган К., Чейлап С. Практика системного и сетевого администрирования. Том 1 – М.: Вильямс, 2018.– 1104 с.
9. Минаев В.А., Журавлев В.С. Моделирование системы защиты информационно–телекоммуникационных объектов от угроз непосредственного и удаленного доступа. // Вестник Российского нового университета. Серия: Сложные системы: модели, анализ и управление. 2013. № 4. С. 113-115. – 2013. – № 4.– С.113–115.
10. Наполова В.И., Кожевников С.В. Защита компьютерных сетей на основе технологии VIRTUAL PRIVATE NETWORK. // Экономика и качество систем связи. – 2018. – № 2.– С.82–85.

11. Новиков Ю.В., Кондратенко С.В. Основы локальных сетей. Учебное пособие – М.: Интуит, 2014.– 360 с.

12. Остроух А.В. Выполнение работ по монтажу, наладке, эксплуатации и обслуживанию локальных компьютерных сетей. Учебник – М.: «Академия», 2018.– 160 с.

13. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы. Учебник – СПб.: Питер, 2016.– 992 с.

14. Романенкова О.Н. Новые формы организации коммерческой деятельности в современных условиях удаленного доступа. // Экономика. Бизнес. Банки. – 2013. – № 4.– С.92–99.

15. Русаков В.А. Средства поддержки сетевого доступа к удаленным ресурсам. // Современные тенденции развития науки и технологий. – 2016. – № 4.– С.95–98.

16. Сабанов А.Г. Аутентификация в распределенных информационных системах. // Защита информации. Инсайд. – 2013. – № 4.– С.69–73.

17. Семенов А.Б., Стрижаков С.К. Структурированные кабельные системы – М.: ДМК Пресс, 2017.– 640 с.

18. Сергеев А.Н. Основы локальных компьютерных сетей. Учебное пособие – СПб.: Лань, 2016.– 184 с.

19. Савельева Т.С., Байрушин Ф.Т. Решения по обеспечению информационной безопасности при использовании удаленного доступа. // Инновационное развитие. – 2017. – № 4.– С.34–36.

20. Таненбаум Э., Уэзеролл Д. Компьютерные сети. 5–е изд. – СПб.: Питер, 2017.– 960 с.

21. Ярмак Д.А. Удаленный доступ к корпоративной сети с помощью VPN. // Наука, техника и образование. – 2017. – № 4.– С.69–72.

22. Ярочкин В.И. Информационная безопасность. Учебное пособие – М.: Международные отношения, 2013. – 544 с.