Содержание:

Введение

Актуальность. В наш век компьютерных технологий ни одна фирма не обходится без использования компьютеров. А если компьютеров несколько, то они, как правило, объединяются в локальную вычислительную сеть. Компьютерная сеть - это система объединенных между собой компьютеров, а также, возможно, других устройств, которые называются узлами (рабочими станциями) сети.

Инфраструктура сети - это набор физических и логических компонентов, которые обеспечивают связь, безопасность, маршрутизацию, управление, доступ и другие обязательные свойства сети.

Сети дают огромные преимущества, недостижимые при использовании ЭВМ по отдельности.

Среди них:

- Разделение ресурсов процессора. При разделении ресурсов процессора возможно использование вычислительных мощностей для одновременной обработки данных всеми станциями, входящими в сеть.

- Разделение данных. Разделение данных предоставляет управлять базами данных с любых рабочих мест, нуждающихся в информации и другие.

Таким образом, сетевая инфраструктура нашла широкое применение в системах автоматизированного проектирования и технологической подготовки производства, системах управления производством и технологическими комплексами, в конторских системах, бортовых системах управления и т.д.

Сетевая инфраструктура является эффективным способом построения сложных систем управления различными производственными подразделениями.

Цель темы исследования – рассмотреть защиту сетевой инфраструктуру на предприятии. Данной целью обусловлены следующие задачи:

– Дать определение сетевой инфраструктуры;

– Изучить методы защиты сетевой инфраструктуры;

– Рассмотреть современные задачи защиты сетевой инфраструктуры предприятия;

– Исследовать безопасность сетевой инфраструктуры предприятия и рекомендации по ее повышению.

1. Общая характеристика сетевой инфраструктуры

1.1 Определение сетевой инфраструктуры

Сетевая инфраструктура представляет собой совокупность различного оборудования, а также программного обеспечения, которая формирует особую среду для эффективного процесса обмена данными, а также для работы бизнес-приложений.

В настоящее время будущее каждой компании напрямую связано с возможностью её оперативного реагирования на тенденции развития рынка. Именно поэтому современная компания обязана функционировать как хорошо отлаженный механизм. Она должна быть управляемой.

Степень такой управляемости организации зависит от того, как хорошо в ней поставлен сбор, обработка и хранение информации, необходимой для принятия решения.

Если информационная система (ИС) организована должным образом, то компания в состоянии решать поставленные задачи.

В основе такой ИС лежит сетевая инфраструктура. Когда в организации установлено более одного персонального компьютера (ПК), которые не объединены в одну общую локальную сеть, это приводит к возникновению многочисленных проблем[1].

Все они связаны со следующим:

1. с поиском, восстановлением и передачей информации;
2. отсутствием возможности пользоваться данными дома либо во время командировок;

3. совместной работой над различной документацией;
4. подключением к сети интернет при помощи периферийного оборудования.

Это и многое другое существенно уменьшает эффективность работы любой организации. Но правильная организация и эксплуатация объектов сетевой инфраструктуры легко решает данные проблемы. Именно поэтому любой руководитель компании обязан обращать на это своё внимание.

Сетевая инфраструктура предприятия представляет собой комплекс следующих устройств:

1. Локальная сеть. Сюда входит и программное обеспечение аппаратных средств, которые объединены в одну общую платформу.
2. Активное оборудование. К нему относятся коммутаторы, маршрутизаторы и конверторы интерфейсов.
3. Пассивные устройства. Это различные монтажные шкафы, кабели, коммутационные панели, кабельные каналы, розетки информационного типа.
4. Периферийное оборудование и компьютеры. Рабочие станции, копиры, серверы, сканеры и принтеры.

Самое основное место в СИ занимает локальная вычислительная сеть (ЛВС). С её помощью осуществляется объединение вычислительных и локальных ресурсов с возможностью организации раздельного доступа к ним. Благодаря локальной сети осуществляется связь всех компьютерных установок. Она может быть как проводной или беспроводной, так и комбинированной. Такая сеть может располагаться в одном помещении на различных этажах, в разных помещениях, а также на большом расстоянии друг от друга. Для связи всех её пользователей используются специальные устройства – коммутаторы (свитчи) и маршрутизаторы.

Все возможности локальной сети могут использоваться одновременно, независимо от того, где находятся рабочие места. С её помощью открывается моментальный доступ к нужной информации, возможность обмениваться данными и мультимедийными носителями, а также подсоединяться к существующей на предприятии сети интернет. Именно поэтому внедрение сетевой инфраструктуры очень важно для любой компании.

Таким образом, сетевая инфраструктура – это совокупность различного оборудования, а также программного обеспечения, которая формирует особую среду для эффективного процесса обмена данными, а также для работы бизнес-приложений. Надёжность и производительность локальной сети, независимо от

того, будет она кабельной или беспроводной, зависит ещё и от того, какие в ней применяются технологии, активное оборудование и сетевое программное обеспечение. Если вы хотите правильно и эффективно спроектировать такую сеть, то обязательно производить анализ информационных потоков вашей организации, при этом учитывая перспективу развития самой инфраструктуры.

1.2 Методы защиты сетевой инфраструктуры

Наиболее важным шагом в планировании эффективной безопасности сети является разработка стратегии безопасности.

Существуют следующие основные методы защиты:

- физические;

- организационные;

- программно- аппаратные[2].

Физические методы защиты состоят в физическом преграждении доступа посторонних лиц в помещения ВС на пути к данным и процессу их обработки.

Организационная защита реализуется совокупностью организационно - технических мероприятий, направленных на обеспечение защиты информации, разработкой и принятием законодательных актов по вопросам защиты информации.

Программно аппаратные средства защиты реализуются следующими методами:

- программно-аппаратные шифраторы сетевого трафика, защищенные сетевые криптопротоколы;

- методика Firewall;

- программные средства обнаружения атак;

- защищенные сетевые ОС.

Существуют три основных типа межсетевых экранов – брандмауэров: пакетный фильтр, шлюз на сеансовом уровне и шлюз на прикладном уровне[3].

Шлюзы приложений предоставляют наибольшую безопасность, так как с одной стороны брандмауэра и с другой никогда на самом деле не общаются друг с другом.

В отличие от использования пакетных фильтров или шлюзов канального уровня, оба компьютера воспринимают такой брандмауэр как конечную точку сетевого потока данных[4].

Таким образом, межсетевые экраны являются необходимыми, но не достаточными средствами обеспечения информационной безопасности.

Одной из разновидностей несанкционированных программ являются компьютерные вирусы, количество которых постоянно растет, уже есть даже новая инженерная дисциплина - компьютерная вирусология.

Возможность шифрования вирусами корпоративных сетей становится серьезной проблемой.

Опасность действия вирусов определяется возможностью частичной или полной потери ценной информации, а также потерей времени и средств, направленных на восстановление нормального функционирования ИС.

Основным принципом работы сетевого вируса является возможность самостоятельно передать свой код на удаленный сервер или рабочую станцию и возможностью запустить на выполнение свой код на удаленном компьютере[5].

Таким образом, методы безопасности сетевой инфраструктуры - это логические и структурированные способы обеспечения безопасности. Существуют следующие основные методы защиты: физические; организационные; программно-аппаратные.

2. Защита сетевой инфраструктуры и обеспечение ее безопасности на предприятии

2.1 Современные задачи защиты сетевой инфраструктуры предприятия

На сегодняшнем этапе развития сетевой инфраструктуры предприятий вопрос защиты информации стоит очень остро, даже можно сказать болезненно. И это понятно и объяснимо.

С одной стороны, для развития и конкурентоспособности необходимо использовать новейшие разработки в области IT.

С другой стороны, это приводит к серьезному усложнению информационной инфраструктуры и применяемых сервисов.

Такое усложнение и расширение неизбежно приводит к росту угроз информационной безопасности.

Очевидно, что на данный момент технологии развиваются значительно опережая возможности систем безопасности. Вернее, даже не так. Различных решений в области обеспечения защиты информации - предостаточно. Но сами эти решения становятся так же колоссально сложны, что вполне объяснимо.

Необходимо обеспечить защиту от вторжений из вне, защиту сетевых служб и прикладных сервисов, защиту от перехвата информации при передаче по общедоступным сетям, защиту от вирусов, контролировать информационные потоки в реальном времени. И это только малая часть мероприятий в плане обеспечения информационной безопасности предприятия[6].

Естественно бизнес применяет несколько решений, одни для защиты от внешних атак, другие для контроля доступа к информации, третьи для обеспечения конфиденциальности, четвертые для защиты от DDOS атак. Да еще необходимо развернуть систему сбора событий безопасности, систему формирования отчетности.

При этом каждый день появляются все новые виды угроз, бизнес расширяется, устанавливает новые связи с партнерами, открывает новые филиалы, привлекает к работе удаленных сотрудников, задействует облачные сервисы, что требует постоянного обновления и мониторинга систем защиты.

Проблема здесь не в отсутствии решений по защите информации, а в их сложности, большом количестве компонентов и самое главное в отсутствии специалистов, способных корректно настроить системы безопасности и поддерживать их в актуальном состоянии.

При реализации систем защиты невозможен подход – включил, заработало и забыл. Здесь нужно постоянное изучение предмета, мониторинг состояния системы и непрерывная настройка с учетом всех, появляющихся изменений.

Очень серьезные решения в области сетевой безопасности предлагает компания Check Point Software Technologies, которая является признанным лидером в сфере разработки продуктов для защиты корпоративных сетей. Компания предлагает

программно-аппаратные комплексы безопасности в виде интернет шлюзов. При этом такие решения не стоит рассматривать, как элементарный фаервол[7].

Продукты стоит рассматривать, как мощное масштабируемое решение, собираемое из так называемых программных блэйдов.

Таким образом, в зависимости от потребностей организации в данный момент можно задействовать те или иные компоненты защиты и при этом еще и выбрать уровень производительности системы.

Интересной особенностью является то, что в целом вся система управляется централизованно с единой консоли управления, что позволяет, серьезно масштабировать систему и упростить ее конфигурирование и обслуживание.

Комплекс так же обладает гибко настраиваемой центральной системой сбора событий безопасности и построения отчетов.

Это далеко не полный перечень возможностей продуктов компании. С учетом сложности предлагаемых решений, компания Check Point разработала свою систему обучения и сертификации специалистов.

Обучение специалистов разбито на несколько этапов, от начальной инсталляции и конфигурирования и до тонкой оптимизации и диагностики неисправностей.

На каждом этапе слушатели получают теоретический материал, учебные пособия и подготовленную лабораторную среду для отработки рекомендованных практических заданий.

Таким образом, главными задачами любой системы информационной безопасности являются: обеспечение доступности данных для авторизированных пользователей — возможности оперативного получения информационных услуг; гарантия целостности информации — ее актуальности и защищенности от несанкционированного изменения или уничтожения; обеспечение конфиденциальности сведений.

2.2 Безопасность сетевой инфраструктуры предприятия и рекомендации по ее повышению

В наше время, когда информационные технологии уже крепко связаны с бизнес-процессами большинства компаний, а способы и методы сетевых атак постоянно совершенствуются и развиваются, все еще бытует мнение что установка обычного сетевого экрана на границе сети достаточно для защиты внутренних корпоративных ресурсов. Это, к сожалению, не совсем так, а, вернее, совсем не так.

Как пример малой эффективности обычного межсетевого экрана, пользователь системы может самостоятельно нажать на ссылочку, полученную от хорошо знакомого друга в социальной сети либо по почте, скачать и запустить вирус, который, используя известный эксплоит не обновлённой операционной системы или программы, получит права администратора и будет выполнять злонамеренную задачу изнутри корпоративной сети[8].

При этом копии вируса будут активно рассылаться по контакт листу пораженной системы.

В Интернете доступны онлайн системы для тестирования подозрительных файлов разными антивирусными программами, но ими в первую очередь пользуются те же злоумышленники для написания новых «незаметных» вирусов.

В связи с этим в наше время существует такое огромное количество бот-нет сетей, достаточно просто купить номера ворованных кредитных карточек и все больше взлом компьютеров стает обычным методом зарабатывания денег.

Поэтому задача обеспечения безопасности требует комплексного подхода на всех уровнях сетевой инфраструктуры и компьютерных ресурсов.

Общие подходы и технологии для построения безопасной сети

Процесс построения безопасной сетевой инфраструктуры начинается с планирования.

На этом этапе перечисляются сервисы, которые будут использоваться в сети, связанные с ними риски, определяются необходимые шаги и механизмы для снижения этих рисков.

На основании данных, полученных на этапе планирования, разрабатывается соответствующий дизайн сетевой инфраструктуры и создается набор политик безопасности. После этого идет этап непосредственного внедрения.

Поскольку безопасность это не конечный результат, а процесс, внедрением и первоначальной настройкой какой-либо системы защиты ничего не заканчивается.

Решения безопасности требуют постоянного «внимания»: отслеживания событий безопасности, их анализа и оптимизации соответствующих политик.

От написания эффективных политик безопасности и их строгого соблюдения очень зависит работа всего комплекса защиты. Правильные политики должны быть зафиксированы документально, не иметь большого количества исключений.

На все оборудование должны регулярно устанавливаться обновления. Также большую угрозу для безопасности составляют простые пользовательские пароли, ошибки в конфигурации устройств, использование настроек по умолчанию, незащищенных протоколов и технологий.

Для обеспечения полной безопасности всей IT инфраструктуры необходимо внедрять механизмы защиты на всех уровнях сети от границы до коммутаторов доступа.

На уровне доступа крайне рекомендуется:

1. использовать управляемые коммутаторы с поддержкой функционала защиты протоколов ARP, DHCP, STP;
2. авторизовать пользователей при подключении с помощью технологии 802.1x;
3. подключать сотрудников в разные VLAN в зависимости от их функциональных обязанностей и задавать правила взаимодействия и доступа к разным ресурсам на уровне распределения.

При подключении к сети WAN и Интернет важно помимо межсетевого экрана иметь возможность сканировать трафик на уровне приложений, проверять наличие угроз с помощью IPS систем.

Пограничное оборудование должно быть стойким к DoS и DDoS атакам.

Крайне рекомендуется для выхода пользователей в Интернет использовать прокси сервера с дополнительной проверкой на вирусы, нежелательное, вредоносное и шпионские ПО[9].

На прокси дополнительно можно организовать веб и контент фильтрацию.

Также важно наличие решения для проверки почты на предмет спама и вирусов.

Все корпоративные ресурсы, к которым нужно обеспечить доступ извне в целях безопасности должны быть вынесены в отдельную демилитаризированную зону DMZ.

Для удаленного доступа использовать технологию VPN с шифрованием передаваемых данных.

Для управления всем сетевым оборудованием должны использоваться защищенные протоколы SSH, HTTPS, SNMPv3. Для возможности анализа логов время на устройствах должно быть синхронизировано. Для понимания, какой трафик ходит в сети, насколько загружено оборудование, какие события на нем происходят, использовать протоколы Syslog, RMON, sFlow, NetFlow.

Очень важно вести учет, кто, когда и какие изменения вносит в конфигурацию оборудования.

Наличие в оборудовании достаточного количества проводных и беспроводных интерфейсов, поддержка удаленного доступа к корпоративным ресурсам, интеграция с различными службами каталогов делает эти устройства идеальным решениям для небольшого офиса. Для подключения проводных пользователей в решение рекомендуем добавить управляемый коммутатор второго уровня с настроенной защитой от атак из локальной сети.

Для средних офисов рекомендуется модульная организация сети, где каждое устройство отвечает за определенный круг задач. На таких предприятиях локальную сеть необходимо строить с обязательным разделением уровней ядра и доступа пользователей.

При большом количестве серверов отдельно выносить коммутаторы агрегации дата центра. Рекомендуется разграничить функции пограничного маршрутизатора и межсетевого экрана, разделив их на два разных устройства.

Резервирование модуля подключения к Интернет можно достичь путем дублирования всего оборудования и настройки на них соответствующих протоколов отказоустойчивости[10].

При наличии в компании филиалов, надомных и мобильных сотрудником, подключения к корпоративным ресурсам необходимо обеспечить по технологии VPN.

Также одним из важных составляющих решения безопасности есть программное обеспечение для мониторинга сети, наличие которого существенно облегчит работу сетевых администраторов и позволит вовремя реагировать на угрозы, обеспечивая этим непрерывность работы всех сетевых сервисов.

Сетевая безопасность в большой распределенной сети предприятия.

Сеть большого распределенного предприятия по принципу реализации подобна к среднему и отличается большим распределением функций между устройствами, высшим требованием к отказоустойчивости, наличием выделенной WAN сети для передачи данных между филиалами. Модуль подключения к WAN в целях безопасности реализуется отдельно от модуля подключения к Интернету.

Для построения такой сети используется оборудование тех же производителей, которые были перечислены для среднего предприятия.

Таким образом, во многих организациях управление обновлениями представляет собой большую проблему. Отслеживание обновлений для снижения уровня уязвимости систем, а также тестирование этих обновлений перед установкой на функционирующие системы занимает очень много времени, но эти задачи очень важны для любой организации.

Заключение

На сегодняшний день компьютеризация на рабочих местах не является чем-то необычным. Наличие компьютеров в офисе с большим потоком информации и объем работы с документами замедляет работу сотрудников, создает неудобства.

Успех практически любого предприятия, организации связан или зависит от наличия и настройки информационных систем, которые сейчас часто называют корпоративными сетями.

Съемные носители данных больше не нужны для обмена данными, нет необходимости печатать на бумажных документах, которые необходимо предоставить нескольким пользователям.

Сетевой принтер, модем, сканер можно установить в сети, а сетевой сервер используется в качестве сервера приложений.

Кроме того, такие сети являются закрытыми сетями, доступ к ним разрешен только определенному числу пользователей, что вызывает защиту информации.

Все эти функции не могут быть реализованы с использованием только операционных систем и прикладных программ. Поэтому большинство современных предприятий используют ЛВС.

Сеть передачи данных, открытые широкие возможности для бизнеса. Трудно представить современную организацию, которая не использует ее системы, электронную почту, телефонию для организации своей деятельности.

Локальные и глобальные сети часто являются основой, без которой невозможно работать с внутренними и внешними услугами, деятельностью отдельных сотрудников, отделов или даже всей компании в целом.

Поэтому обеспечение бесперебойной работы сети является одной из важнейших задач этого сервиса.

Использование систем мониторинга сетевой инфраструктуры значительно улучшит доступность сети, предотвратит возникновение аварий и сократит время, необходимое для восстановления после сбоев.

Выбор конкретной реализации зависит от конфигурации сети, которая будет использовать систему мониторинга, функциональные требования системы, возможности развертывания и возможности поддержки.

Список использованной литературы

1. Айвенс К. Внедрение, управление и поддержка сетевой инфраструктуры MS Windows Server 2003 / К. Айвенс. — М. : Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. — 914 с.

2. Алексеев В.А. Маршрутизация и защита сетевого трафика в сетях TCP/IP: методические указания к проведению лабораторных работ по курсу «Сетевые технологии» / В.А. Алексеев. — Липецк: Липецкий государственный технический университет, ЭБС АСВ, 2013. — 35 с.
3. Андрончик А.Н. Сетевая защита на базе технологий фирмы Cisco Systems. Практический курс: учебное пособие / А.Н. Андрончик [и др.]. — Екатеринбург: Уральский федеральный университет, 2014. — 180 с.
4. Астахова А.В. Информационные системы в экономике и защита информации на предприятиях — участниках ВЭД: учебное пособие / А.В. Астахова. — СПб. : Троицкий мост, 2014. — 216 с.
5. Башлы П.Н. Информационная безопасность и защита информации: учебное пособие / П.Н. Башлы, А.В. Бабаш, Е.К. Баранова. — М. : Евразийский открытый институт, 2012. — 311 с.
6. Бурняшов Б.А. Меры защиты информации на уровне пользователя информационно-технологическими средствами: методические указания к самостоятельной работе студентов / Б.А. Бурняшов. — Саратов: Вузовское образование, 2014. — 55 с.
7. Жидко Е.А. Логико-вероятностно-информационный подход к моделированию информационной безопасности объектов защиты: монография / Е.А. Жидко. — Воронеж: Воронежский государственный архитектурно-строительный университет, ЭБС АСВ, 2016. — 121 с.
8. Иванов А.Л. Информационная безопасность и защита информации: учебно-методический комплекс / А.Л. Иванов. — Алматы: Нур-Принт, 2012. — 98 с.
9. Ложников П.С. Обеспечение безопасности сетевой инфраструктуры на основеоперационных систем Microsoft: практикум / П.С. Ложников, Е.М. Михайлов. — Москва, Саратов: Интернет-Университет Информационных Технологий (ИНТУИТ), Вузовское образование, 2017. — 264 с.
10. Мифтахова Л.Х. Программно-аппаратные средства защиты информации: учебное пособие для студентов вузов по направлению подготовки «Информационная безопасность» / Л.Х. Мифтахова [и др.]. — СПб. : Интермедия, 2018. — 408 с.
11. Новиков Д.А. Сетевые структуры и организационные системы: монография / Д.А. Новиков. — М. : ИПУ РАН, 2013. — 102 с.
12. Пакин А.И. Информационная безопасность информационных систем управления предприятием: учебное пособие по части курса / А.И. Пакин. — М. : Московская государственная академия водного транспорта, 2014. — 41 с.

13. Прохорова О.В. Информационная безопасность и защита информации: учебник / О.В. Прохорова. — Самара: Самарский государственный архитектурно-строительный университет, ЭБС АСВ, 2014. — 113 с.
14. Рогозин В.Ю. Основы информационной безопасности: учебник для студентов вузов, обучающихся по направлению подготовки «Правовое обеспечение национальной безопасности» / В.Ю. Рогозин [и др.]. — М. : ЮНИТИ-ДАНА, 2017. — 287 с.
15. Шаньгин В.Ф. Информационная безопасность и защита информации / В.Ф. Шаньгин. — Саратов: Профобразование, 2017. — 702 с.

1. Айвенс К. Внедрение, управление и поддержка сетевой инфраструктуры MS Windows Server 2003 / К. Айвенс. — М. : Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. — С. 273. ↑

2. Бурняшов Б.А. Меры защиты информации на уровне пользователя информационно-технологическими средствами: методические указания к самостоятельной работе студентов / Б.А. Бурняшов. — Саратов: Вузовское образование, 2014. — С. 22. ↑

3. Башлы П.Н. Информационная безопасность и защита информации: учебное пособие / П.Н. Башлы, А.В. Бабаш, Е.К. Баранова. — М. : Евразийский открытый институт, 2012. — С. 172. ↑

4. Ложников П.С. Обеспечение безопасности сетевой инфраструктуры на основеоперационных систем Microsoft: практикум / П.С. Ложников, Е.М. Михайлов. — Москва, Саратов: Интернет-Университет Информационных Технологий (ИНТУИТ), Вузовское образование, 2017. — С. 163. ↑

5. Иванов А.Л. Информационная безопасность и защита информации: учебно-методический комплекс / А.Л. Иванов. — Алматы: Нур-Принт, 2012. — С. 52. ↑

6. Пакин А.И. Информационная безопасность информационных систем управления предприятием: учебное пособие по части курса / А.И. Пакин. — М. : Московская государственная академия водного транспорта, 2014. — С. 32. ↑

7. Астахова А.В. Информационные системы в экономике и защита информации на предприятиях — участниках ВЭД: учебное пособие / А.В. Астахова. — СПб. : Троицкий мост, 2014. — С. 118. ↑

8. Прохорова О.В. Информационная безопасность и защита информации: учебник / О.В. Прохорова. — Самара: Самарский государственный архитектурно-строительный университет, ЭБС АСВ, 2014. — С. 76. ↑

9. Рогозин В.Ю. Основы информационной безопасности: учебник для студентов вузов, обучающихся по направлению подготовки «Правовое обеспечение национальной безопасности» / В.Ю. Рогозин [и др.]. — М. : ЮНИТИ-ДАНА, 2017. — С. 183. ↑

10. Шаньгин В.Ф. Информационная безопасность и защита информации / В.Ф. Шаньгин. — Саратов: Профобразование, 2017. — С. 271. ↑