**Информационная безопасность.**

Компьютерная сеть - является самой распространенной на сегодня способ общения и обмена информацией. Всемирная сеть хранит гигабайты персональной информации о своих пользователях. А ПК и сервера в локальной сети - внутреннюю информацию компании. Все данные нуждаются в защите от постороннего вмешательства.

**Что такое информационная безопасность**

Уровень защиты сетевых операционных систем позволяет сохранять данные, а также противостоять угрозам и атакам, несанкционированному доступу в сеть. Тем не менее говорить об исключительной, универсальной системе средств защиты информации не приходится. Возникают ситуации, когда она дает сбой, и устройства оказываются уязвимыми для проникновения.

Информационная безопасность (ИБ) заключается в обеспечении ряда факторов-

1. защищенности сведений от неавторизованного создания, частичной или полной потери;
2. гарантии доступа для авторизованных пользователей;
3. конфиденциальности;

В отдельных областях (банковской, финансовой, государственном управлении, правоохранительной и оборонной) требуется создание дополнительной, более надежной, системы обеспечения безопасности информации.

**Защита информации в информационных сетях**

Создаваемые масштабные компьютерные линии - корпоративные, локальные, телекоммуникационные - ставят задачу взаимодействия большого количества компьютеров, серверов, сетей и подсетей. Создается проблема определения наиболее эффективного метода защиты информации.

Системная топология, основанная на расположении межкомпьютерных связей, остается главным компонентом всех локальных и корпоративных сетей. Безопасность данных в компьютерных сетях достигается путем обработки критической информации. Этим термином обозначаются факторы, способствующие эффективному управлению основными структурными элементами сети и максимально полному выполнению стратегических задач любого уровня секретности (для личного, служебного пользования, коммерческая тайна либо интеллектуальная собственность юридического или физического лица).

Уязвимость большинства информационных сетей связана с кабельной системой. Есть подтверждение, что именно она становится причиной сбоев и нарушений функционирования. Это необходимо учитывать уже на этапах проектирования сетевых связей.

Широкое распространение получили структурированные системы кабелей. Принцип их устройства - наличие однотипных проводов для передачи всех видов информации (цифровой, видео, телефонной, сигналов систем охраны). Структурированность заключается в возможности разделить систему кабелей на ряд уровней по их назначению и наличию различных компонентов: внешней, администрирующей, аппаратной, горизонтальной, магистральной подсистем.

Внешняя подсистема из меди и оптоволокна включает устройства электрической защиты, заземления и устанавливает связи коммуникационной и обрабатывающей аппаратуры в помещении. Входят устройства контактов внешних и внутренних кабельных систем. Аппаратные нужны для размещения оборудования, они обеспечивают работу подсистемы администратора.

**Основные проблемы в процессе защиты материалов**

Решая вопрос защиты информации в корпоративных сетях, необходимо обратить внимание на возможные перебои и нарушения в процессе доступа, способные уничтожить или исказить сведения. Возможные проблемы, связанные с нарушением безопасности в компьютерных сетях, можно разделить на несколько типов:

1**.**Нарушения работы системного оборудования: разрыв кабелей, перебои в электропитании, сбой в дисковой системе, нарушения функционирования серверов, сетевых карт, рабочих станций, системы архивации.

2. Уничтожение данных вследствие некорректной работы программного обеспечения (ПО): ошибки системы, заражение компьютерными вирусами.

3. Следствие несанкционированного доступа: пиратское копирование, работа посторонних с секретными материалами, устранение или фальсификация данных.

4. Ошибки технического штата и пользователей сетевого ресурса: случайное искажение или уничтожение информации, некорректное пользование программными продуктами.

5. Неграмотное сохранение архивов.

В каждом из перечисленных случаев требуется устранить нарушения и усилить систему безопасности компьютерной сети.

**Какими средствами можно защитить информацию**

Как показывает практика, неавторизованные пользователи либо программные продукты вирусного типа могут получить доступ даже к защищенным сетевым ресурсам. Для этого они должны иметь определенный опыт в сфере сетевого или системного программирования и желание подключиться к определенным файлам.

Для полной конфиденциальности разработаны дополнительные средства защиты информации:

1. Аппаратные (антивирусные программы, брандмауэры, сетевые экраны и фильтры, устройства шифрования протоколов).
2. Административные (ограничение доступа в помещения, разработка планов действий при ЧС и стратегии безопасности компании).
3. Программные (сетевой мониторинг, архивация данных, криптография, идентификация и аутентификация пользователя, управление доступом, протокол и аудит).

Любые из этих способов способны ограничить доступ вредоносных программ и файлов или полностью отказать в нем. Задача системных администраторов ИБ - выбрать наиболее актуальные. Для надежности барьера часто используют комбинацию нескольких видов защитных средств.

**Архивирование и дублирование информации**

Сохранить информацию в сети способна грамотная и надежная система архивации данных. Если сеть невелика, то система архивации устанавливается в свободный слот сервера. Большие корпоративные сети лучше оснастить отдельным архивирующим сервером.

Такое устройство архивирует данные в автоматическом режиме и с заданной периодичностью представляет отчет. При этом управлять процессом резервного копирования можно, используя консоль (ПО для ввода команд и вывода системных сообщений). Другое название консоли - командная строка системного администратора.

Возможно использование установки на архивирование сведений в связи с отсутствием на жестком диске какого-то количества свободного места или по причине сбоя «зеркального» диска сервера. Эта функция может быть подключена также в автоматическом режиме.
Распространение компьютерных вирусов в информационных сетях происходит с большой скоростью. Тысячи уже известных вредоносных программ регулярно пополняются сотнями новых. Самые доступные средства борьбы с ними - антивирусные программные обеспечения (ПО).

Подобные программные пакеты способны перекрыть доступ к информации и решить проблему с зараженными файлами. Оптимальным для сохранения системных сведений будет использование комбинации программного и аппаратного барьера. Чаще всего это специализированные платы для борьбы с вирусами.

**Защита данных от несанкционированного доступа**

Вопрос защиты информации в компьютерной системе от неразрешенного входа связан с широким охватом информационного пространства глобальными телекоммуникационными сетями. Простейшие ошибки самих пользователей наносят более ощутимый вред, чем сбой в системе или поломка оборудования. Для предотвращения подобных ситуаций необходимо разграничить пользовательские полномочия.

С этой целью используются встроенные программы операционных систем сети. Каналов утечки данных и возможностей несанкционированного входа десятки. Наиболее распространенные:

1. информация, оставшаяся после разрешенного запроса;
2. имитация запроса системы;
3. взлом системы защиты информации и копирование нужных файлов;
4. представление зарегистрированным пользователем;
5. программные ловушки;
6. несовершенства операционной системы;
7. неутвержденное подсоединение к сетевой аппаратуре;
8. взлом системы безопасности;
9. введение вирусов.

В целях полноценной защиты информации рекомендуется использовать ряд организационных и технических методов.

Организационные мероприятия заключаются, прежде всего, в ограничении доступности зданий и офисов, где проводится работа с информацией. Взаимодействовать с ней имеют право только аттестованные и проверенные специалисты. Все носители информации, журналы регистрации и учета необходимо хранить в закрытых сейфах. Необходимо исключить возможность просмотра материалов посторонними через мониторы или принтеры. При передаче секретных сведений по каналам связи лучше использовать криптографическое кодирование. А также необходимо следить за тем, чтобы все отработанные устройства и носители, которые содержат ценные данные, были вовремя уничтожены.

К организационно-техническим средствам защиты можно отнести устройство независимого блока питания для системы обработки ценных файлов, оснащение входных дверей кодовыми замками и использование ЖК или плазменных дисплеев с высокочастотным излучением электромагнитных импульсов. Отправляя оргтехнику в ремонт, необходимо стереть все имеющиеся данные. Помещения, в которых происходит работа с секретными материалами, необходимо оборудовать стальными экранами.

Технические защитные средства включают в себя установку системы охраны операционных залов и организацию работы контрольно-пропускных пунктов. Необходимо обеспечить контроль за возможностью проникновения в память ЭВМ, и блокировку сведений, а также использованием ключей.

Архитектура программного оборудования заключается в жестком контроле безопасности при вхождении в систему, регистрации в специальных книгах, контроле действий пользователей. Требуется установка системы реагирования (в т.ч. числе звуковой) на проникновение в корпоративную сеть.

Для надежности систему безопасности и защиты данных нужно регулярно тестировать, проверять готовность и работу всех ее элементов. Большое значение имеет и фиксация всех манипуляций, имеющих хоть какое-то отношение к системной защите.

Значительно повысить степень секретности можно с помощью смарт-карт. Для этого сервер нужно оборудовать устройством для их чтения. Входящий в систему пользователь вставляет в него карту и вводит индивидуальный код доступа. Весь этот процесс фиксирует и контролирует служба охраны.

**Механизмы достижения гарантированной безопасности**

Разработаны и с успехом применяются различные методы защиты сведений. Самые актуальные и доступные из них:

1**.**Использование криптографии - это применение шифра, позволяющего изменять содержимое файла, делая его нечитаемым. Узнать содержание возможно только с помощью специальных ключей или паролей.

Для создания шифровки используются два взаимосвязанных понятия: ключ и алгоритм. Первое задает способ кодировки, второе помогает интерпретировать послание. Это просто и доступно без больших финансовых вложений. Один алгоритм можно использовать с несколькими ключами для разных получателей, при утрате секретности, ключи можно сразу сменить, не нарушая алгоритма. Безопасность в таком случае связана только с ключами. Для достижения большего эффекта кодовые ключи можно делать длинными и сложными.

2.Применение электронно-цифровой подписи (ЭЦП). Она подтверждает личность отправителя, создается при помощи его личного ключа. Дополнительная степень сохранности ЭЦП - это уникальный номер владельца.

3. Аутентификация пользователей, это основной способ защиты данных в сети. Для получения доступа к ресурсу пользователь должен подтвердить это право. Соответствующий сервер принимает запрос на использование ресурса и пересылает его серверу, отвечающему за аутентификацию. Только после получения положительного результата пользователю открывается доступ.

Одна из версий подтверждения личности – это использование пароля. Это может быть любое секретное слово, которое вводится в начале работы с системой. В особых случаях сервер может запросить новый пароль на выходе. Причем они могут быть разными.

Брешь возможна, если секретным словом завладеет кто-то другой. Для предотвращения подобного пароли лучше делать разовыми. Даже перехваченное кодовое слово будет бесполезным при следующем сеансе. Генерировать пароли можно при помощи программ или специальных устройств, вставляемых в слот компьютера.

4. Защита информации внутри корпоративной сети. Сетевые системы корпораций, как правило, подключены к всемирной сети. Это создает дополнительные возможности, но и делает систему безопасности уязвимой. Для защиты материалов во внутренней сети нужны брандмауэры (межсетевые экраны), способные разделить трафик на несколько потоков и обозначить условия обмена данными из одного потока в другой. Брандмауэр анализирует проходящий трафик и, проверяя каждый пакет данных, решает – пропускать его или нет. Для этого формируется алгоритм работы программы, где прописаны правила и порядок прохождения данных.

Брандмауэры реализуются аппаратными способами (как специализированный физический элемент) либо в виде отдельной программы, установленной на компьютере. Для обеспечения безопасного функционирования межсетевого экрана в систему, отвечающую за его функционал, регулярно вносятся корректировки. Возможности входа для рядовых пользователей в эту программу нет, он доступен только для системных администраторов.

Брандмауэр (защитный экран) между глобальным интернетом и локальной компьютерной сетью организации. Он выполняет функцию проверки и фильтрации данных, поступающих из интернета) состоит из нескольких компонентов, в том числе фильтров либо экранирующих устройств для блокирования части трафика. Можно выделить два вида подобных программных элементов:

1. Пакетные - фильтрующие информационные блоки с помощью маршрутизаторов.
2. Прикладные - блокирующие доступ к отдельным сетевым ресурсам;

В итоге весь трафик, исходящий из внешней системы во внутреннюю и обратно, проходит через систему брандмауэра. Только данные, которые соответствуют стратегии обеспечения безопасности, достигнут адресата.