УВАЖАЕМЫЕ СТУДЕНТЫ!

ВАМ НЕОБХОДИМО ВЫПОЛНИТЬ СЛЕДУЮЩЕЕ:

1. Ознакомиться с теорией и законспектировать, составить и ответить на вопросы.

2. Предоставит отчет, прислать в виде скриншото в течении трех дней .

3. Отправить преподавателю на почту v.vika2014@mail.ru и указать свою Ф.И.О, группу, и название дисциплины тел 072-17-44-9-22

Тема: Цели, функции и задачи защиты информации в сетях: возможные угрозы

Цели защиты информации в сетях эвм

Цели защиты информации в сетях ЭВМ общие для всех информационных систем, а именно: обеспечение целостности (физической и логической) информации, а также предупреждение несанкционированной ее модификации, несанкционированного получения и размножении. **Функции защиты** также носят общий для всех систем характер. **Задачи защиты информации** в сетях ЭВМ определяются теми угрозами, которые потенциально возможны в процессе их функционирования. Для сетей передачи данных реальную опасность представляют следующие угрозы.

1. Прослушивание каналов, т.е. запись и последующий анализ всего проходящего потока сообщений. Прослушивание в большинстве случаев не замечается легальными участниками информационного обмена.

2. Умышленное уничтожение или искажение (фальсификация) проходящих по сети сообщений, а также включение в поток ложных сообщений. Ложные сообщения могут быть восприняты получателем как подлинные.

3. Присвоение злоумышленником своему узлу или ретранслятору чужого идентификатора, что дает возможность получать или отправлять сообщения от чужого имени.

4. Преднамеренный разрыв линии связи, что приводит к полному прекращению доставки всех (или только выбранных злоумышленником) сообщений.

5. Внедрение сетевых вирусов, т.е. передача по сети тела вируса с его последующей активизацией пользователем удаленного или локального узла.

В соответствии с этим специфические задачи защиты в сетях передачи данных состоят в следующем.

1. Аутентификация одноуровневых объектов, заключающаяся в подтверждении подлинности одного или нескольких взаимодействующих объектов при обмене информацией между ними.

2. Контроль доступа, т.е. защита от несанкционированного использования ресурсов сети.

3. Маскировка данных, циркулирующих в сети.

4. Контроль и восстановление целостности всех находящихся в сети данных.

5. Арбитражное обеспечение, т.е. защита от возможных отказов от фактов отправки, приема или содержания отправленных или принятых данных.

Применительно к различным уровням семиуровневого протокола передачи данных в сети задачи могут быть конкретизированы следующим образом.

1. Физический уровень – контроль электромагнитных излучений линий связи и устройств, поддержка коммутационного оборудования в рабочем состоянии. Защита на данном уровне обеспечивается с помощью экранирующих устройств, генераторов помех, средств физической защиты передающей среды.

2. Канальный уровень – увеличение надежности защиты (при необходимости) с помощью шифрования передаваемых по каналу данных. В этом случае шифруются все передаваемые данные, включая служебную информацию.

3. Сетевой уровень – наиболее уязвимый уровень с точки зрения защиты. На нем формируется вся маршрутизирующая информация, отправитель и получатель фигурируют явно, осуществляется управление потоком. Кроме того, протоколами сетевого уровня пакеты обрабатываются на всех маршрутизаторах, шлюзах и других промежуточных узлах. Почти все специфические сетевые нарушения осуществляются с использованием протоколов данного уровня (чтение, модификация, уничтожение, дублирование, переориентация отдельных сообщений или потока в целом, маскировка под другой узел и др.).

Защита от подобных угроз осуществляется протоколами сетевого и транспортного уровней и с помощью средств криптозащиты. На данном уровне может быть реализована, например, выборочная маршрутизация.

4. Транспортный уровень – осуществляет контроль за функциями сетевого уровня на приемном и передающем узлах (на промежуточных узлах протокол транспортного уровня не функционирует). Механизмы транспортного уровня проверяют целостность отдельных пакетов данных, последовательности пакетов, пройденный маршрут, время отправления и доставки, идентификацию и аутентификацию отправителя и получателя и другие функции. Все активные угрозы становятся видимыми на данном уровне.

Гарантом целостности передаваемых данных является криптозащита как самих данных, так и служебной информации. Никто, кроме имеющих секретный ключ получателя и/или отправителя, не может прочитать или изменить информацию таким образом, чтобы изменение осталось незамеченным.

Анализ трафика предотвращается передачей сообщений, не содержащих информацию, которые, однако, выглядят как реальные сообщения. Регулируя интенсивность этих сообщений в зависимости от объема передаваемой информации, можно постоянно добиваться равномерного трафика. Однако все эти меры не могут предотвратить угрозу уничтожения, переориентации или задержки сообщения. Единственной защитой от таких нарушений может быть параллельная доставка дубликатов сообщения по другим путям.

5. Протоколы верхних уровней обеспечивают контроль взаимодействия принятой или переданной информации с локальной системой. Протоколы сеансового и представительного уровня функций защиты не выполняют. В функции защиты протокола прикладного уровня входит управление доступом к определенным наборам данных, идентификация и аутентификация определенных пользователей, а также другие функции, определяемые конкретным протоколом. Более сложными эти функции являются в случае реализации полномочной политики безопасности в сети.

Особенности защиты информации в вычислительных сетях обусловлены тем, что сети, обладающие несомненными (по сравнению с локальными ЭВМ) преимуществами обработки информации, усложняют организацию защиты, причем основные проблемы при этом состоят в следующем.

1) Разделение совместно используемых ресурсов. В силу совместного использования большого количества ресурсов различными пользователями сети, возможно находящимися на большом расстоянии друг от друга, сильно повышается риск НСД – в сети его можно осуществить проще и незаметнее.

2) Расширение зоны контроля. Администратор или оператор отдельной системы или подсети должен контролировать деятельность пользователей, находящихся вне пределов его досягаемости, возможно в другой стране. При этом он должен поддерживать рабочий контакт со своими коллегами в других организациях.

3) Комбинация различных программно-аппаратных средств. Соединение нескольких подсистем, пусть даже однородных по характеристикам, в сеть увеличивает уязвимость всей системы в целом. Подсистема обычно настроена на выполнение своих специфических требований безопасности, которые могут оказаться несовместимы с требованиями на других подсистемах. В случае соединения разнородных систем риск повышается.

4) Неизвестный периметр. Легкая расширяемость сетей ведет к тому, что определить границы сети подчас бывает сложно; один и тот же узел может быть доступен для пользователей различных сетей.

Более того, для многих из них не всегда можно точно определить сколько пользователей имеют доступ к определенному узлу и кто они.

5) Множество точек атаки. В сетях один и тот же набор данных или сообщение могут передаваться через несколько промежуточных узлов, каждый из которых является потенциальным источником угрозы. Естественно, это не может способствовать повышению защищенности сети. Кроме того, ко многим современным сетям можно получить доступ с помощью коммутируемых линий связи и модема, что во много раз увеличивает количество возможных точек атаки. Такой способ прост, легко осуществим и трудно контролируем; по этому он считается одним из наиболее опасных. В списке уязвимых мест сети также фигурируют линии связи и различные виды коммуникационного оборудования: усилители сигнала, ретрансляторы, модемы и т.д.

6) Сложность управления и контроля доступа к системе. Многие атаки на сеть могут осуществляться без получения физического доступа к определенному узлу – с помощью сети из удаленных точек. В этом случае идентификация нарушителя может оказаться очень сложной, если не невозможной. Кроме того, время атаки может оказаться слишком мало для принятия адекватных мер.

Понятие сервисов безопасности

Для решения перечисленных задач в вычислительных сетях создаются специальные механизмы защиты (или сервисы безопасности). Их перечень и содержание для общего случая могут быть представлены следующим образом.

Идентификация / аутентификация. Современные средства идентификации / аутентификации должны удовлетворять двум условиям:

- быть устойчивыми к сетевым угрозам (пассивному и активному прослушиванию сети);
- поддерживать концепцию единого входа в сеть.

Первое требование можно выполнить, используя криптографические методы. (Еще раз подчеркнем тот очевидный факт, что современная криптография есть нечто гораздо большее, чем шифрование; соответственно, разные ветви этой дисциплины нуждаются в дифференцированном подходе с нормативной точки зрения). В настоящее время общепринятыми являются подходы, основанные на системе Kerberos или службе каталогов с сертификатами в стандарте X.509.

Единый вход в сеть – это, в первую очередь, требование удобства для пользователей. Если в корпоративной сети много информационных сервисов, допускающих независимое обращение, то многократная идентификация/аутентификация становится слишком обременительной. К сожалению, пока нельзя сказать, что единый вход в сеть стал нормой, доминирующие решения пока не сформировались.

Дополнительные удобства создает применение биометрических методов аутентификации, основанных на анализе отпечатков (точнее, результатов сканирования) пальцев. В отличие от специальных карт, которые нужно хранить, пальцы “всегда под рукой” (правда, под рукой должен быть и сканер). Подчеркнем, что и здесь защита от нарушения целостности и перехвата с последующим воспроизведением осуществляется методами криптографии.

Разграничение доступа. Разграничение доступа является самой исследованной областью информационной безопасности.

В настоящее время следует признать устаревшим (или, по крайней мере, не полностью соответствующим действительности) положение о том, что разграничение доступа направлено исключительно на защиту от злоумышленных пользователей. Современные информационные системы характеризуются чрезвычайной сложностью и их внутренние ошибки представляют не меньшую опасность.

Динамичность современной программной среды в сочетании со сложностью отдельных компонентов существенно сужает область применимости самой употребительной – *дискреционной модели* управления доступом (называемой также моделью с произвольным управлением). При определении допустимости доступа важно не только (и не столько) то, кто обратился к объекту, но и то, какова семантика действия. Без привлечения семантики нельзя выявить троянские программы, противостоять которым произвольное управление доступом не в состоянии.

В последнее время появляются новые модели управления доступом, например модель *“есочницы”* в Java-технологии.

Активно развиваемое *ролевое управление* доступом решает не столько проблемы безопасности, сколько улучшает управляемость систем (что, конечно, очень важно). Суть его в том, что между пользователями и их привилегиями помещаются промежуточные сущности – роли. Для каждого пользователя одновременно могут быть активными несколько ролей, каждая из которых дает ему определенные права.

Сложность информационной системы характеризуется, прежде всего, числом имеющихся в ней связей. Поскольку ролей много меньше, чем пользователей и привилегий, их (ролей) использование способствует понижению сложности и, следовательно, улучшению управляемости. Кроме того, на основании ролевой модели можно реализовать такие важные принципы, как разделение обязанностей (невозможность в одиночку скомпрометировать критически важный процесс). Между ролями могут быть определены статические или динамические отношения несовместимости

(невозможности одному субъекту по очереди или одновременно активизировать обе роли), что и обеспечивает требуемую защиту.

Для некоторых употребительных сервисов таких, как Web, ролевое управление доступом может быть реализовано относительно просто (в Web-случае – на основе cgi-процедур).

Протоколирование/аудит. Протоколирование и аудит традиционно являлись рубежом обороны, обеспечивающим анализ последствий нарушения информационной безопасности и выявление злоумышленников. Такой аудит можно назвать пассивным.

Довольно очевидным обобщением пассивного аудита для сетевой среды является совместный анализ регистрационных журналов отдельных компонентов на предмет выявления противоречий, что важно в случаях, когда злоумышленнику удалось отключить протоколирование или модифицировать журналы.

В современный арсенал защитных средств несколько лет назад вошел активный аудит, направленный на выявление подозрительных действий в реальном масштабе времени. Активный аудит включает два вида действий:

- выявление нетипичного поведения (пользователей, программ или аппаратуры);
- выявление начала злоумышленной активности.

Нетипичное поведение выявляется статистическими методами, путем сопоставления с предварительно полученными образцами. Начало злоумышленной активности обнаруживается по совпадению с сигнатурами известных атак. За обнаружением следует заранее запрограммированная реакция (как минимум – информирование системного администратора, как максимум – контратака на систему предполагаемого злоумышленника).

Важным элементом современной трактовки протоколирования/аудита является протокол автоматизированного обмена информацией о нарушениях безопасности между корпоративными системами, подключенными к одной внешней сети. В наше время системы не могут считаться изолированными,

они не должны жить по закону “каждый за себя”; угрозам следует противостоять сообща.

Экранирование. Экранирование как сервис безопасности выполняет следующие функции:

- разграничение межсетевого доступа путем фильтрации передаваемых данных;
- преобразование передаваемых данных.

Современные межсетевые экраны фильтруют данные на основе заранее заданной базы правил, что позволяет, по сравнению с традиционными операционными системами, реализовать гораздо более гибкую политику безопасности. При комплексной фильтрации, охватывающей сетевой, транспортный и прикладной уровни, в правилах могут фигурировать сетевые адреса, количество переданных данных, операции прикладного уровня, параметры окружения (например, время) и т.п.

Преобразование передаваемых данных может затрагивать как служебные поля пакетов, так и прикладные данные. В первом случае обычно имеется в виду трансляция адресов, помогающая скрыть топологию защищаемой системы. Это уникальное свойство сервиса экранирования, позволяющее скрывать существование некоторых объектов доступа. Преобразование данных может состоять, например, в их шифровании.

В процессе фильтрации (точнее, параллельно с ней) может выполняться дополнительный контроль (например, антивирусный). Возможны и дополнительные преобразования, наиболее актуальным из которых является исправление заголовков или иной служебной информации, ставшей некорректной после наступления 2000 года.

Применение межсетевого экранирования поставщиками Интернет-услуг в соответствии с рекомендациями разработчиков позволило бы существенно снизить шансы злоумышленников и облегчить их прослеживание. Данная мера еще раз показывает, как важно рассматривать каждую информационную

систему как часть глобальной инфраструктуры и принимать на себя долю ответственности за общую информационную безопасность.

Туннелирование. Его суть состоит в том, чтобы “упаковать” передаваемую порцию данных, вместе со служебными полями, в новый “конверт”. Данный сервис может применяться для нескольких целей:

- осуществление перехода между сетями с разными протоколами (например, IPv4 и IPv6);
- обеспечение конфиденциальности и целостности всей передаваемой порции, включая служебные поля.

Туннелирование может применяться как на сетевом, так и прикладном уровнях. Например, стандартизовано туннелирование для IP и двойное конвертирование для почты X.400.

Комбинация туннелирования и шифрования (с необходимой криптографической инфраструктурой) на выделенных шлюзах позволяет реализовать такое важное в современных условиях защитное средство, как виртуальные частные сети. Такие сети, наложенные обычно поверх Интернета, существенно дешевле и гораздо безопаснее, чем действительно собственные сети организации, построенные на выделенных каналах. Коммуникации на всем их протяжении физически защитить невозможно, поэтому лучше изначально исходить из предположения об уязвимости и соответственно обеспечивать защиту. Современные протоколы, направленные на поддержку классов обслуживания, помогут гарантировать для виртуальных частных сетей заданную пропускную способность, величину задержек и т.п., ликвидируя тем самым единственное на сегодняшний день реальное преимущество собственных сетей.

Шифрование. Шифрование – важнейшее средство обеспечения конфиденциальности и одновременно самое конфликтное место информационной безопасности. У компьютерной криптографии две стороны – собственно криптографическая и интерфейсная, позволяющая сопрягаться с другими частями информационной системы. Важно, чтобы были обеспечены

достаточное функциональное богатство интерфейсов и их стандартизация. Криптографией, в особенности шифрованием, должны, разумеется, заниматься профессионалы. От них требуется разработка защищенных инвариантных компонентов, которые можно было бы свободно (по крайней мере, с технической точки зрения) встраивать в существующие и перспективные конфигурации.

У современного шифрования есть и внутренние проблемы как технические, так и нормативные. Из технических наиболее острой является проблема производительности. Программная реализация на универсальных процессорах не является адекватным средством (здесь можно провести аналогию с компрессией видеоизображений). Еще одна техническая задача – разработка широкого спектра продуктов, предназначенных для использования во всех видах компьютерного и сетевого оборудования, – от персональных коммуникаторов до мощных шлюзов.

Контроль целостности. В современных системах контроль целостности должен распространяться не только на отдельные порции данных, аппаратные или программные компоненты. Он обязан охватывать распределенные конфигурации, защищать от несанкционированной модификации потоки данных.

В настоящее время существует достаточно решений для контроля целостности и с системной, и с сетевой направленностью (обычно контроль выполняется прозрачным для приложений образом как часть общей протокольной активности). Стандартизован программный интерфейс к этому сервису.

Контроль защищенности. Контроль защищенности по сути представляет собой попытку “взлома” информационной системы, осуществляемого силами самой организации или уполномоченными лицами. Идея данного сервиса в том, чтобы обнаружить слабости в защите раньше злоумышленников. В первую очередь, имеются в виду не архитектурные (их ликвидировать сложно), а “оперативные” бреши, появившиеся в результате

ошибок администрирования или из-за невнимания к обновлению версий программного обеспечения.

Средства контроля защищенности позволяют накапливать и многократно использовать знания об известных атаках. Очевидна их схожесть с антивирусными средствами; формально последние можно считать их подмножеством. Очевиден и реактивный, запаздывающий характер подобного контроля (он не защищает от новых атак). Следует помнить, что оборона должна быть эшелонированной, так что в качестве одного из рубежей контроль защищенности вполне адекватен. Подавляющее большинство атак носит рутинный характер; они возможны только потому, что известные уязвимости годами остаются неустраненными.

Существуют как коммерческие, так и свободно распространяемые продукты для контроля защищенности. Впрочем, в данном случае важно не просто один раз получить и установить их, но и постоянно обновлять базу данных уязвимостей. Это может оказаться не проще, чем следить за информацией о новых атаках и рекомендуемых способах противодействия.

Обнаружение отказов и оперативное восстановление. Обнаружение отказов и оперативное восстановление относятся к числу сервисов, обеспечивающих высокую доступность (готовность). Его работа опирается на элементы архитектурной безопасности, а именно на существование избыточности в аппаратно-программной конфигурации.

В настоящее время спектр программных и аппаратных средств данного класса можно считать сформировавшимся. На программном уровне соответствующие функции берет на себя программное обеспечение промежуточного слоя. Среди аппаратно-программных продуктов стандартом стали кластерные конфигурации. Восстановление производится действительно оперативно (десятки секунд, в крайнем случае, минуты), прозрачным для приложений образом.

Обнаружение отказов и оперативное восстановление может играть по отношению к другим средствам безопасности роль инфраструктурного

сервиса, обеспечивая высокую готовность последних. Это особенно важно для межсетевых экранов, средств поддержки виртуальных частных сетей, серверов аутентификации, нормальное функционирование которых критически важно для корпоративной информационной системы в целом. Такие комбинированные продукты получают все более широкое распространение.

Управление. Управление относится к числу инфраструктурных сервисов, обеспечивающих нормальную работу функционально полезных компонентов и средств безопасности. Сложность современных систем такова, что без правильно организованного управления они постепенно (а иногда и довольно быстро) деградируют как в плане эффективности, так и в плане защищенности.

Особенно важной функцией управления является контроль согласованности конфигураций различных компонентов (имеется в виду семантическая согласованность, относящаяся, например, к наборам правил нескольких межсетевых экранов). Процесс администрирования идет постоянно; требуется, однако, чтобы при этом не нарушалась политика безопасности.

Место сервисов безопасности в архитектуре информационных систем. Выше был перечислен десяток сервисов безопасности. Как объединить их для создания эшелонированной обороны, каково их место в общей архитектуре информационных систем?

На внешнем рубеже располагаются средства выявления злоумышленной активности и контроля защищенности. Далее идут межсетевые экраны, защищающие внешние подключения. Они вместе со средствами поддержки виртуальных частных сетей (обычно объединяемых с межсетевыми экранами) образуют периметр безопасности, отделяющий корпоративную систему от внешнего мира.

Сервис активного аудита должен присутствовать во всех критически важных компонентах и, в частности, в защитных. Это позволит быстро

обнаружить атаку, даже если по каким-либо причинам она окажется успешной.

Управление доступом также должно присутствовать на всех сервисах, функционально полезных и инфраструктурных. Доступу должна предшествовать идентификация и аутентификация субъектов.

Криптографические средства целесообразно выносить на специальные шлюзы, где им может быть обеспечено квалифицированное администрирование. Масштабы пользовательской криптографии следует минимизировать.

Наконец, последний рубеж образуют средства пассивного аудита, помогающие оценить последствия нарушения безопасности, найти виновного, выяснить, почему успех атаки стал возможным.

Расположение средств обеспечения высокой доступности определяется критичностью соответствующих сервисов или их компонентов. Для обеспечения доступности (непрерывности функционирования) могут применяться следующие защитные меры:

- внесение в конфигурацию той или иной формы избыточности (резервное оборудование, запасные каналы связи и т.п.). Это элемент архитектурной безопасности, рассматриваемой в следующем разделе;
- наличие средств обнаружения отказов. Если требуется постоянная высокая готовность, необходим специализированный сервис. В остальных случаях достаточно протоколирования/аудита в квазиреальном времени;
- наличие средств реконфигурирования для восстановления, изоляции и/или замены компонентов, отказавших или подвергшихся атаке на доступность. Это или специализированная функция, или одна из функций управления;
- рассредоточенность сетевого управления, отсутствие единой точки отказа. Это, как и следующий пункт, – элементы архитектурной безопасности;

- выделение подсетей и изоляция групп пользователей друг от друга. Данная мера ограничивает зону поражения при возможных нарушениях информационной безопасности.

Каждый компонент, вообще говоря, не обязан поддерживать все перечисленные выше сервисы безопасности. Важно, чтобы он обладал программными и/или протокольными интерфейсами для получения недостающих сервисов от других компонентов и чтобы не существовало возможности обхода основных и дополнительных защитных средств.