Основы ИБ

12 февраля 2015 г.

10:07

Литература:

* + Учебное пособие «Основы ИБ», Гвоздевский
  + Шайгин В. С. «Защита компьютерной информации, эффективные методы и средства»
  + Малюк А. А., «Введение в ИБ»
  + Курило А. П., «Основы управления ИБ»
  + Сычев Ю. Н., «Основы ИБ»

6 лаб, РГЗ, зачет.

# Основные понятия и анализ угроз ИБ

Защита информации -- деятельность по предотвращению утечки защищаемой информации несанкционированных и непреднамеренных воздействий на защищаемую информацию.

Объект защиты -- информация либо ее носитель, либо информационный процесс в отношении которых необходимо обеспечивать защиту в соответствии с поставленной целью защиты информации.

Цель защиты информации -- желаемый результат защиты информации в виде предотвращения ущерба собственнику, владельцу, пользователю информации, в результате возможной утечки и/или несанкционированного и непреднамеренного воздействия.

Эффективность защиты информации -- это степень соответствия результатов защиты информации поставленной цели.

Защита информации от утечки -- деятельность по предотвращению неконтролируемого распространения защищаемой информации от ее разглашения, несанкционированного доступа (НСД) к защищаемой информации и получения защищаемой информации злоумышленниками.

Защита информации от разглашения -- это деятельность по предотвращению несанкционированного доведения защищаемой информации до неконтролируемого количества получателей информации.

Защита информации от НСД -- деятельность по предотвращению получения защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником либо владельцем информации прав или правил доступа к защищаемой информации.

Система защиты информации -- это совокупность органов или исполнителей, используемая ими техника защиты информации, а также объекты защиты, организованные и функционирующие по правилам, установленным соответствующими правовыми, организационно-распорядительными и нормативными документами.

Под информационной безопасностью понимают защищенность информации от незаконного ознакомления, преобразования или уничтожения, а также защищенность информационных ресурсов от воздействий, направленных на нарушение их работоспособности.

Современные автоматизированные системы обработки информации представляют собой сложную систему, состоящую из большого числа компонентов различной степени автономности, которые связаны между собой и обмениваются данными. Практически каждый компонент может подвергнуться внешнему воздействию или выйти из строя.

# Классификация компонентов АС

* + Аппаратные средства (компьютеры и их составные части).
  + ПО (приобретенные программы, исходные загрузочные объектные модули, системные программы, утилиты и пр.).
  + Данные (хранимые временно и постоянно на магнитных носителях, печатные журналы, архивы, системные логи).
  + Персонал.

Одной из особенностей обеспечения ИБ является то, что таким абстрактным понятием как информация, объекты, субъекты системы соответствуют физические представления в компьютерной среде.

* + Для представления информации -- используют машинные носители информации.
  + Объектам системы соответствуют пассивные компоненты системы, хранящие, принимающие или передающие информацию. Доступ к объекту означает доступ к хранимой в нем информации.
  + Субъектам системы соответствуют: активные компоненты системы, которые могут стать причиной потока информации от объекта к субъекту, а также изменение состояния системы (пользователи, активные программы, процессы).

ИБ компьютерных систем достигается обеспечением конфиденциальности, целостности, доступности и достоверности обрабатываемых данных, а также доступности и целостности информационных компонентов и ресурсов системы.

Конфиденциальность данных -- это статус, предоставленный данными и определяющий требуемую степень их защиты (учётные записи пользователей, данные о кредитных картах, о разработках, бухгалтерская документация). Конфиденциальная информация должна быть известна только допущенным и прошедшим проверку (авторизованным) субъектам системы. Для остальных субъектов системы эта информация должна быть неизвестной.

Установление градаций важности защищаемой информации называют категорированием.

Целостность информации -- это свойство информации, обеспечивающее сохранение структуры и/или содержания в процессе передачи или хранения. Целостность информации обеспечивается в том случае, если данные в системе не отличаются в семантическом отношении от данных в исходных документах. То есть если не произошло их случайного или преднамеренного искажения или разрушения.

Достоверность информации -- это свойство информации, выражающееся в строгой принадлежности субъекту, который является ее источником, либо тому субъекту от которого эта информация была принята.

Юридическая значимость означает, что документ, являющийся носителем информации обладает юридической силой.

Доступность данных -- это свойство обеспечения доступа того или иного субъекта к разрешённым ему данным.

Оперативность доступа к информации -- это способность информации или некоторого информационного ресурса быть доступными для конечного пользователя в соответствии с его оперативными потребностям.

Доступ к информации -- получение субъектом возможности ознакомления с информацией в том числе при помощи технических средств.

Собственник информации -- это субъект в полном объеме реализующий полномочия владения, пользования, распоряжения информацией в соответствии с законодательными актами.

Владелец информации -- это субъект, осуществляющий владение и пользование информацией и реализующий полномочия распоряжения в пределах прав установленных законом и/или собственником информации.

Пользователь -- это субъект, пользующийся информацией, полученной от ее собственников, владельца или посредника в соответствии с установленными правами и правилами доступа к информации, либо с их нарушением.

Право доступа к информации -- это совокупность правил доступа, установленных правовыми документами или собственником либо владельцем информации.

Правила доступа к информации -- это совокупность правил, регламентирующих порядок и условия доступа субъекта к информации и ее носителям.

Санкционированный доступ к информации -- это доступ, не нарушающий установленные правила разграничения.

НСД -- это нарушение установленных правил разграничения доступа.

Лицо или процесс, осуществляющие НСД являются нарушителями правил разграничения доступа.

Доступность информации подразумевает доступность компонентов или ресурсов компьютерной системы для законных субъектов.

Целостность ресурса или компонента системы -- это свойство ресурса или компонента быть неизменным в семантическом смысле при функционировании системы в условиях случайных или преднамеренных искажений, а также разрушающих воздействий.

Идентификатор -- это некоторая информация (число, строка, символы), идентифицирующая объект.

Идентификация субъекта -- это процедура распознавания субъекта по его идентификатору.

Аутентификация субъекта -- это процедура проверки подлинности проверки субъекта с данным идентификатором.

Авторизация субъекта -- это процедура предоставления законному субъекту успешно прошедшему идентификацию и аутентификацию соответствующих полномочий и доступных ресурсов системы (сети).

Первая лабораторная:

Поставить 12-ый сервер из дримспарка на виртуальную машину. Essential, Foundation, Standard, Datacent. Сравнить редакции и виртуальные машины в отчете. Если не встанет 12, поставить 8 (или 8.2).

Установить службу каталогов на сервер -- Active directory (понятия: домен, лес, объект, объект-юнит). Открыть на хабре любую статью AD.

К службам относятся дополнительные сервисы от Майкрософта и других.

Посмотреть, что такое Powershell. Посмотреть на группы команд. Попробовать создать пользователя с какими-то параметрами.

В отчете указать, какие загружались модули и какие использовались команды. Указать результаты, полученные в консоли.

В работе пункты по контрольным вопросам.

Вторая лаба:

Вместо NTBackup есть VBAdmin. Чем отличаются разные типы резервных копирований. Попробовать сделать резервную копию какого-нибудь архива. ShadowCopy.

05.03.2015

Причинами случайных воздействий при эксплуатации автоматизированных систем могут быть:

* + Аварийные ситуации из-за стихийных бедствий и отключения электропитания;
  + Отказы и сбои аппаратуры;
  + Ошибки в программном обеспечении;
  + Ошибки в работе обслуживающего персонала и пользователей;
  + Помехи в линиях связи из-за воздействия внешней среды.

Преднамеренные угрозы связаны с целенаправленным действием нарушителя. Модель потенциального нарушителя можно представить следующим образом:

* + Квалификация нарушителя может быть на уровне разработчика данной системы;
  + Нарушителем может быть, как постороннее лицо, так и законный пользователь системы;
  + Нарушителю известна информация о принципах работы системы;
  + Нарушитель выберет наиболее слабое звено в защите.

В частности, для автоматизированных систем можно выделить следующие преднамеренные угрозы:

* + НСД лиц не принадлежащих к числу служащих и ознакомление с хранимой конфиденциальной информацией;
  + Ознакомление служащих с информацией, к которой они не должны иметь доступ;
  + Несанкционированное копирование программы данных;
  + Кража магнитных носителей, а также распечатанных документов;
  + Умышленное уничтожение информации;
  + Несанкционированная модификация финансовых документов, отчётностей и баз данных;
  + Фальсификация сообщений, передаваемых по каналам связи;
  + Отказ от факта получения информации;
  + Разрушение информации, вызванное вирусными воздействиями.

НСД наиболее распространённый и многообразный вид компьютерных нарушений, суть которого состоит в получении пользователем (нарушителем) доступа к объекту в нарушение правил разграничения доступа, установленных в соответствии с принятой в организации политикой безопасности.

НСД используют любую ошибку в системе защиты и возможен при нерациональном выборе, а также их некорректной установки и настройки.

НСД может быть осуществлён как штатными средствами автоматизированный системы, так и специально созданными аппаратными и программными средствами.

Основные каналы НСД:

* + Штатные каналы доступа к информации;
  + Технологические пульты управления;
  + Линии связи между аппаратными средствами автоматизированных систем;
  + Побочные линии связи, электромагнитное излучение и т. п.

Перехват паролей — это НСД в виде специально разработанной программы, имитирующей работу системы авторизации конечного пользователя.

Маскарад — это выполнение каких-либо действий одним пользователем от имени другого пользователя, обладающего соответствующими полномочиями. Примерами реализации маскарада являются:

* + Вход в систему под именем и паролем другого пользователя;
  + Передача сообщений в сети от имени другого пользователя.

Незаконное использование привилегий приводит к возможности выполнения нарушителем определённых действий либо при наличии ошибок в системе защиты, либо из-за халатности администратора при управлении системой и назначении привилегий.

Угроза нарушения конфиденциальности направлена на разглашение конфиденциальной или секретной информации.

Угроза нарушения целостности информации, хранящейся в компьютерной системе или передаваемой по каналу связи, которые направлены на её изменение или искажение, приводящее к нарушению её качества или полному уничтожению.

Угроза нарушения работоспособности (отказ в обслуживании) направлена на создание таких ситуаций, когда определённые преднамеренные действия либо снижают работоспособность автоматизированных систем, либо блокируют доступ к некоторым её ресурсам.

Угроза, связанная с реализацией отказа в доступе.

Для современных IT-подсистем системы защиты информации являются неотъемлемой частью автоматизированных систем. Зачастую преодоление защиты также представляет собой угрозу.. Бла-бла.

При рассмотрении вопросов защиты автоматизированных систем целесообразно использовать четырёхуровневую градацию доступа к хранимой, обрабатываемой и защищаемой АС информацией:

* + Уровень носителя информации
  + Уровень средств взаимодействия с носителями
  + Уровень представление информации
  + Уровень содержания информации

К основным направлениям реализации злоумышленником информационных угроз относятся:

* + Непосредственное обращение к объектам доступа
  + Создание программных и технических средств, выполняющих обращение к объектам доступа в обход средств защиты
  + Модификация средств защиты, позволяющая реализовать угрозы ИБ
  + Внедрение в технические средства АС программных или технических механизмов, нарушающих предполагаемую структуру и функции АС

12.03.15

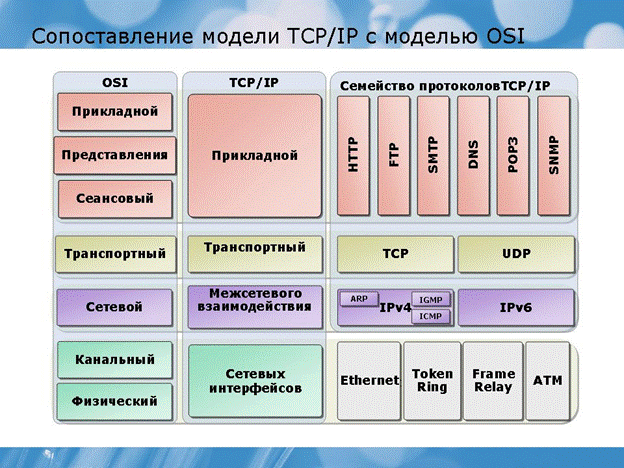
Модель OSI определяет различные уровни взаимодействия систем и указывает, какие функции должен выполнять каждый уровень.

В Модели OSI средства взаимодействия делятся на 7 уровней:

* + Прикладной
  + Представительный
  + Сеансовый
  + Транспортный
  + Сетевой
  + Канальный
  + Физический

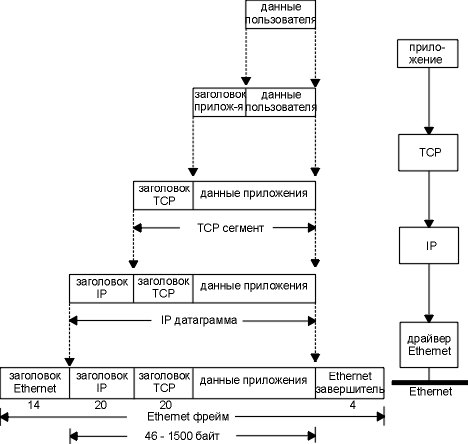
Обмен данными через каналы связи происходят путем перемещения данных с верхнего уровня на нижний, затем транспортировкой по линиям связи, и, наконец, обратным воспроизведением данных путем перемещения с нижнего уровня на верхний. Для обеспечения необходимой совместимости на каждом из уровней, действую специальные стандартные протоколы, которые представляют собой формализованные правила, определяющие последовательность и формат сообщений, которыми обмениваются сетевые компоненты, лежащие на одном уровне, но в разных узлах сети.

Стек протоколов TCP/IP является промышленном стандартом стека коммуникационных протоколов, разработанным для глобальных сетей. Коммуникационные протоколы могут быть реализованы как программно, так и аппаратно. Протоколы нижних уровней часто реализуются комбинацией программных и аппаратных средств, а протоколы верхних уровней — только программными средствами. Модули, реализующие протоколы соседних уровней и находящиеся в одном узле сети, должны взаимодействовать друг с другом в соответствии с четко определенными правилами, называемыми межуровневым интерфейсом. Межуровневый интерфейс определяет набор сервисов, предоставляемых данным уровнем соседнему уровню.



Протокол управления передачей (tcp) решает задачу обеспечения информационной связи между двумя конечными узлами с установлением соединения.

Протокол дата-грамм пользователя (udp) обеспечивает передачу прикладных пакетов дата-граммным способом, то есть каждый блок передаваемой информации обрабатывается и распространяется от узла к узлу как независимая единица информации(дата-грамма). Необходимость в протоколе udp обусловлена тем, что udp может различать приложения и доставлять информацию от приложения к приложению.



19.03.2015

Проблема безопасности IT-сетей

Распределённые системы подвержены прежде всего удалённым атакам, поскольку компоненты распределённых систем обычно используют открытые каналы связи. Нарушитель может проводить не только пассивное подслушивание, но и активное воздействие на передаваемый трафик.

Основной задачей злоумышленника может являться перехват служебной информации и использование её в целях НСД.

Наиболее распространённые атаки:

* + Подслушивание (сниффинг). Сниффер пакетов представляет собой прикладную программу, позволяющую перехватывать все сетевые пакеты, передаваемые через определённый домен. Основными задачами сниффинга являются анализ состояния локальной или глобальной среды передачи данных и возможности осуществить несанкционированный доступ к ресурсам таких сетей.
  + Угроза изменения данных. Направлена на перехват пакета информации и внедрения в него каких-то «левых» данных. Злоумышленник может изменить данные в пакете, ничего не зная ни об отправителе, ни об получателе. Целью такой угрозы является либо получение служебной информации от целевой системы, либо нарушение информационного обмена.
  + Подмена доверенного субъекта (айпи-спуффинг). Айпи-спуффинг имеет место, когда злоумышленник, находящийся внутри локальной сети организации или за её пределами выдаёт себя за законного пользователя, используя айпи-адрес, находящийся в пределах диапазона санкционированных адресов, или авторизованный внешним адресом, которому разрешается доступ к определённым сетевым ресурсам.
  + Угроза посредничества (man-in-the-middle). Эта атака подразумевает активное подслушивание, перехват и управление передаваемыми данными невидимым промежуточным узлом. Обычно атака реализуется на низких сетевых уровнях, когда компьютеры не всегда могут определить с кем именно они обмениваются данными. Такие атаки проводятся с целью кражи информации, перехвата текущей сессии и получение доступа к частным сетевым ресурсам. В частности, для проведения атак типа DoS, а также искажение и ввода несанкционированной информации в сетевые сессии.
  + Перехват сеанса. По окончании начальной процедура аутентификации, соединение, установленное законным пользователем (почтовым сервером) переключается злоумышленником на новый хост. А исходному серверу выдаётся команда разорвать соединение.
  + Отказ в обслуживании. Атака DoS направлена на превышение допустимых пределов функционирования сети операционной системы или приложения. В ходе атак используются обычные интернет-протоколы, TCP, ICMP. Различают распределённый вид атаки DoS, проводящийся одновременно через множество устройств (DDoS).
  + Парольные атаки. Основная их цель завладение паролем и логином законного пользователя. Злоумышленники могут проводить парольные атаки, используя такие методы, как подмена айпи-адреса, подслушивание и простой перебор.
  + Угадывание ключа.
  + Атаки на уровне приложения. Могут проводиться несколькими способами:
    1. Использование известных слабостей серверного ПО (FTP, HTTP, SQL-серверов)
    2. Использование недокументированных функций ОС
  + Сетевая разведка. Сбор информации о сети с помощью общедоступных данных и приложений (разведка проводится в форме запросов к DNS, эхо-тестирования и сканирования портов).
  + Злоупотребление доверием — не является атакой в полном смысле этого слова. Представляет собой злонамеренное использование отношений доверия, существующих в сети. Отношения доверия должны ограничиваться определенными протоколами и проходить аутентификацию не только по айпи адресам, но и по другим параметрам. Системы, расположенные с внешней стороны межсетевого экрана, никогда не должны пользоваться абсолютным доверием со стороны систем, защищенных межсетевым экраном.
  + Компьютерные вирусы, сетевые черви, троянские программы.

Вирусы представляют собой вредоносные программы, внедряющиеся в программы или процессы, для выполнения определенных нежелательных функций на рабочей станции конечного пользователя. Вирус обычно разрабатывается таким образом, чтобы как можно дольше оставаться не обнаруженным. Проявляется в полной мере в конкретный момент времени.

Сетевой червь — программа-вирус, которая распространяется по локальным и глобальным сетям. Используя механизмы поддержки сети для определения узла, который может быть поражен.

Троянская программа — программа, которая имеет вид полезного приложения, а на деле выполняет вид вредоносного программного обеспечения.

Для защиты от указанных вредоносных программ необходимо:

* + исключение несанкционированного доступа к исполняемым файлам
  + тестирование приобретаемых программных средств
  + осуществление контроля целостности исполняемых файлов и системных областей
  + создание замкнутой среды исполнения программа

Сетевые атаки с помощью червей, троянских программ и пр вирусов на айпи-сети возможны в результате:

* + при использовании общедоступных каналов передачи данных
  + уязвимости в процедурах идентификации, реализованных в стеке tcp/ip
  + отсутствие в базовой версии стека протоколов tcp/ip механизмов, обеспечивающих конфиденциальность и целостность передаваемых сообщений
  + аутентификация отправителя по его айпи адресу без дальнейшей проверки подлинности принимаемых пакетов
  + при отсутствии контроля за маршрутом прохождения сообщений в сети интернет

Угрозы уязвимости проводных корпоративных сетей

Информация, обрабатываемая в корпоративных сетях, является особенно уязвимой, чему способствуют следующие факторы:

* + увеличение объемов обрабатываемой передаваемой и хранимой в компьютерах информации
  + сосредоточение в БД информации различного уровня важности и конфиденциальности
  + расширение круга пользователей к информации, хранящейся в БД, и к ресурсам вычислительной сети
  + увеличение числа удаленных рабочих мест
  + широкое использование глобальной сети интернет и различных каналов связи
  + автоматизация обмена информацией между компьютерами пользователя

Самыми частыми и опасными с точки зрения размера ущерба являются непреднамеренные ошибки пользователей, операторов, администраторов, обслуживающих компьютерную информационную систему.

# Угрозы и уязвимости беспроводных сетей

# Метод обнаружения изменений

При реализации этого метода антивирусные программы, называемые ревизорами диска запоминают предварительно характеристики всех областей диска, которые могут подвергнутся нападению, а затем периодически проверяют их.

Метод встраивания антивирусов в БИОС компьютера