Лекция №10

Основы защиты информации

План лекции

1. Защита информации как закономерность развития компьютерных систем
2. Объекты и элементы защиты в компьютерных системах обработки данных
3. Средства опознания и разграничения доступа к информации
4. Криптографический метод защиты информации
5. Защита программных продуктов
6. Обеспечение безопасности данных на автономном компьютере

Защита информации как закономерность развития компьютерных систем

Защита информации –это применение различных средств и методов, использование мер и осуществление мероприятий для того, чтобы обеспечить систему надежности передаваемой, хранимой и обрабатываемой информации.

Защита информации включает в себя:

- обеспечение физической целостности информации, исключение искажений или уничтожения элементов информации;
- недопущение подмены элементов информации при сохранении ее целостности;
- отказ в несанкционированном доступе к информации лицам или процессам, которые не имеют на это соответствующих полномочий;
- приобретение уверенности в том, что передаваемые владельцем информационные ресурсы будут применяться только в соответствии с обговоренными сторонами условиями.

Процессы по нарушению надежности информации подразделяют на **случайные** и **злоумышленные** (преднамеренные). Источниками случайных разрушительных процессов являются непреднамеренные, ошибочные действия людей, технические сбои. Злоумышленные нарушения появляются в результате умышленных действий людей.

Защита информации как закономерность развития компьютерных систем

Если в первые десятилетия активного использования ПК основную опасность представляли хакеры, подключившиеся к компьютерам в основном через телефонную сеть, то в последнее десятилетие нарушение надежности информации прогрессирует через программы, компьютерные вирусы, глобальную сеть Интернет.

Имеется достаточно много способов несанкционированного доступа к информации, в том числе:

- просмотр;
- копирование и подмена данных;
- ввод ложных программ и сообщений в результате подключения к каналам связи;
- чтение остатков информации на ее носителях;
- прием сигналов электромагнитного излучения и волнового характера;
- использование специальных программ.

Защита информации как закономерность развития компьютерных систем

- Для борьбы со всеми этими способами несанкционированного доступа необходимо разрабатывать, создавать и внедрять многоступенчатую непрерывную и управляемую архитектуру безопасности информации. Защищать следует не только информацию конфиденциального содержания. На объект защиты обычно действует некоторая совокупность дестабилизирующих факторов. При этом вид и уровень воздействия одних факторов могут не зависеть от вида и уровня других.

Объекты и элементы защиты в компьютерных системах обработки данных

Объект защиты –это такой компонент системы, в котором находится защищаемая информация. Элементом защиты является совокупность данных, которая может содержать необходимые защите сведения.

При деятельности компьютерных систем могут возникать:

- отказы и сбои аппаратуры;
- системные и системотехнические ошибки;
- программные ошибки;
- ошибки человека при работе с компьютером.

Объекты и элементы защиты в компьютерных системах обработки данных

- Несанкционированный доступ к информации возможен во время технического обслуживания компьютеров в процессе прочтения информации на машинных и других носителях. Незаконное ознакомление с информацией разделяется на пассивное и активное. При пассивном ознакомлении с информацией не происходит нарушения информационных ресурсов и нарушитель может лишь раскрывать содержание сообщений. В случае активного несанкционированного ознакомления с информацией есть возможность выборочно изменить, уничтожить порядок сообщений, перенаправить сообщения, задержать и создать поддельные сообщения.

Объекты и элементы защиты в компьютерных системах обработки данных

Для обеспечения безопасности проводятся разные мероприятия, которые объединены понятием «система защиты информации».

Система защиты информации –это совокупность организационных (административных) и технологических мер, программно-технических средств, правовых и морально-этических норм, которые применяются для предотвращения угрозы нарушителей с целью сведения до минимума возможного ущерба пользователям и владельцам системы.

Организационно-административными средствами защиты называется регламентация доступа к информационным и вычислительным ресурсам, а также функциональным процессам систем обработки данных. Эти средства защиты применяются для затруднения или исключения возможности реализации угроз безопасности. Наиболее типичными организационно-административными средствами являются:

- допуск к обработке и передаче охраняемой информации только проверенных должностных лиц;
- хранение носителей информации, которые представляют определенную тайну, а также регистрационных журналов в сейфах, недоступных для посторонних лиц;
- учет применения и уничтожения документов (носителей) с охраняемой информацией;
- разделение доступа к информационным и вычислительным ресурсам должностных лиц в соответствии с их функциональными обязанностями.

Объекты и элементы защиты в компьютерных системах обработки данных

Технические средства защиты применяются для создания некоторой физически замкнутой среды вокруг объекта и элементов защиты. При этом используются такие мероприятия, как:

- ограничение электромагнитного излучения через экранирование помещений, в которых осуществляется обработка информации;
- реализация электропитания оборудования, отрабатывающего ценную информацию, от автономного источника питания или общей электросети через специальные сетевые фильтры.

Программные средства и методы защиты являются более активными, чем другие применяемые для защиты информации в ПК и компьютерных сетях. Они реализуют такие функции защиты, как разграничение и контроль доступа к ресурсам; регистрация и изучение протекающих процессов; предотвращение возможных разрушительных воздействий на ресурсы; криптографическая защита информации.

Объекты и элементы защиты в компьютерных системах обработки данных

Под технологическими средствами защиты информации понимаются ряд мероприятий, органично встраиваемых в технологические процессы преобразования данных. В них также входят:

- создание архивных копий носителей;
- ручное или автоматическое сохранение обрабатываемых файлов во внешней памяти компьютера;
- автоматическая регистрация доступа пользователей к различным ресурсам;
- выработка специальных инструкций по выполнению всех технологических процедур и др.

Правовые и морально-этические меры и средства защиты включают в себя действующие в стране законы, нормативные акты, регламентирующие правила, нормы поведения, соблюдение которых способствует защите информации.

Средства опознания и разграничения доступа к информации

Средства опознания и разграничения доступа к информации

Идентификацией называется присвоение тому или иному объекту или субъекту уникального имени или образа. Аутентификация – это установление подлинности объекта или субъекта, т. е. проверка, является ли объект (субъект) тем, за кого он себя выдает.

Конечная цель процедур идентификации и аутентификации объекта (субъекта) заключается в допуске его к информации ограниченного пользования в случае положительной проверки либо отказе в допуске при отрицательном результате проверки.

Объекты идентификации и аутентификации включают в себя: людей (пользователей, операторов); технические средства (мониторы, рабочие станции, абонентские пункты); документы (ручные, распечатки); магнитные носители информации; информацию на экране монитора.

К наиболее распространенным методам аутентификации относятся присвоение лицу или другому имени пароля и хранение его значения в вычислительной системе. Паролем называется

Средства опознания и разграничения доступа к информации

Пароль как средство обеспечения безопасности способен использоваться для идентификации и установления подлинности терминала, с которого входит в систему пользователь, а также для обратного установления подлинности компьютера по отношению к пользователю.

С учетом важности пароля как средства повышения безопас – ности информации от несанкционированного использования необходимо соблюдать следующие меры предосторожности:

1) не хранить пароли в вычислительной системе в незашифрованном месте;

2) не печатать и не отображать пароли в открытом виде на терминале пользователя;

3) не применять в качестве пароля свое имя или имена родственников, а также личную информацию (дата рождения, номер домашнего или служебного телефона, название улицы);

4) не применять реальные слова из энциклопедии или толкового словаря;

5) использовать длинные пароли;

6) применять смесь символов верхнего и нижнего регистров клавиатуры;

7) применять комбинации из двух простых слов, соединенных специальными символами (например, +,=,<);

8) использовать несуществующие новые слова (абсурдные или даже бредового содержания);

9) как можно чаще менять пароль.

Средства опознания и разграничения доступа к информации

Для идентификации пользователей могут использоваться сложные в плане технической реализации системы, которые обеспечивают установление подлинности пользователя на основе анализа его индивидуальных параметров: отпечатков пальцев, рисунка линий руки, радужной оболочки глаз, тембра голоса. Наиболее широкое применение имеют физические методы идентификации, которые используют носители кодов паролей. Такими носителями могут быть пропуск в контрольно-пропускных системах; пластиковые карты с именем владельца, его кодом, подписью; пластиковые карточки с магнитной полосой, которая считывается специальным считывающим устройством; пластиковые карты, содержащие встроенную микросхему; карты оптической памяти.

Одним из наиболее интенсивно разрабатываемых направлений по обеспечению безопасности информации является идентификация и определение подлинности документов на основе электронной цифровой подписи. При передаче информации по каналам связи используется факсимильная аппаратура, но при этом к получателю приходит не подлинник, а только копия документа с копией подписи, которая в процессе передачи может быть подвергнута повторному копированию для использования ложного документа.

Электронная цифровая подпись представляет собой способ шифрования с использованием криптографического преобразования и является паролем, зависящим от отправителя, получателя и содержания передаваемого сообщения. Для того чтобы предупредить повторное использование подписи, ее необходимо менять от сообщения к сообщению.

Криптографический метод защиты информации

Наиболее эффективным средством повышения безопасности является криптографическое преобразование. Для того чтобы повысить безопасность, осуществляется одно из следующих действий:

1) передача данных в компьютерных сетях;

2) передача данных, которые хранятся в удаленных устройствах памяти;

3) передача информации при обмене между удаленными объектами.

Защита информации методом криптографического преобразования состоит в приведении ее к неявному виду через преобразование составных частей информации (букв, цифр, слогов, слов) с применением специальных алгоритмов либо аппаратных средств и кодов ключей. Ключ является изменяемой частью криптографической системы, хранящейся в тайне и определяющей, какое шифрующее преобразование из возможных выполняется в данном случае.

Криптографический метод защиты информации

К методам криптографического преобразования предъявляются следующие необходимые требования:

1) он должен быть достаточно устойчивым к попыткам раскрытия исходного текста с помощью использования зашифрованного;

2) обмен ключа не должен быть тяжел для запоминания;

3) затраты на защитные преобразования следует сделать приемлемыми при заданном уровне сохранности информации;

4) ошибки в шифровании не должны вызывать явную потерю информации;

5) размеры зашифрованного текста не должны превышать размеры исходного текста.

Методы, предназначенные для защитных преобразований, подразделяют на четыре основные группы: перестановки, замены (подстановки), аддитивные и

Защита программных продуктов

Программные продукты являются важными объектами защиты по целому ряду причин:

1) они представляют собой продукт интеллектуального труда специалистов высокой квалификации, или даже групп из нескольких десятков или даже сотен человек;

2) проектирование этих продуктов связано с потреблением значительных материальных и трудовых ресурсов и основано на применении дорогостоящего компьютерного оборудования и наукоемких технологий;

3) для восстановления нарушенного программного обеспечения необходимы значительные трудозатраты, а применение простого вычислительного оборудования чревато негативными результатами для организаций или физических лиц.

Защита программных продуктов

Защита программных продуктов преследует следующие цели:

- ограничение несанкционированного доступа отдельных категорий пользователей к работе с ними;
- исключение преднамеренной порчи программ с целью нарушения нормального хода обработки данных;
- недопущение преднамеренной модификации программы с целью порчи репутации производителя программной продукции;
- препятствование несанкционированному тиражированию (копированию) программ;
- исключение несанкционированного изучения содержания, структуры и механизма работы программы.

Защита программных продуктов

Самый простой и доступный способ защиты программных продуктов заключается в ограничении доступа к ним с помощью:

- парольной защиты программ при их запуске;
- ключевой дискеты;
- специального технического устройства (электронного ключа), подключаемого к порту ввода-вывода компьютера.

Для того чтобы избежать несанкционированного копирования программ, специальные программные средства защиты должны:

- идентифицировать среду, из которой программа запускается;
- вести учет числа выполненных санкционированных инсталляций или копирования;
- противодействовать (вплоть до саморазрушения) изучению алгоритмов и программ работы системы.

Защита программных продуктов

Для программных продуктов действенными защитными мерами являются:

1) идентификация среды, из которой запускается программа;

2) ввод учета числа выполненных санкционированных инсталляций или копирования;

3) противодействие нестандартному форматированию запускающей дискеты;

4) закрепление месторасположения программы на жестком диске;

5) привязка к электронному ключу, вставляемому в порт ввода-вывода;

6) привязка к номеру BIOS.

При защите программных продуктов необходимо использовать и правовые методы. Среди них выделяются лицензирование соглашений и договоров, патентная защита, авторские права, технологическая и производственная секретность.

Обеспечение безопасности данных на автономном компьютере

используют общие ресурсы файлового сервера.

К методам обеспечения безопасности относят:

- использование атрибутов файлов и каталогов типа «скрытый», «только для чтения»;
- сохранение важных данных на гибких магнитных дисках;
- помещение данных в защищенные паролем архивные файлы;
- включение в защитную программу регулярной проверки на компьютерные вирусы.

Существует три основных способа применения антивирусных программ:

1) поиск вируса при начальной загрузке, когда команда запуска антивирусной программы включается в AUTOEXEC.bat;

2) запуск вирусной программы вручную;

3) визуальный просмотр каждого загружаемого файла.