Лекция 8. **Проблемы защиты информации.**

8.1. Актуальность проблемы защиты информации.

8.2. Виды угроз безопасности систем.

8.3. Оценка безопасности ИС

8.4. Методы и средства защиты информации.

8.1. Актуальность проблемы защиты информации

В 21 веке все большую роль в любой сфере жизни человека приобретает информация. И поэтому нашему веку суждено стать «информационным». Нематериальная составляющая производственных процессов несет в себе информационную компоненту, которая в любом производстве с течением времени заметно возрастает.

В связи с возрастанием роли информации на первый план выходит защита информации. Прежде, чем установить защиту, нужно определить степень важности и значимости этой информации.

Домашний пользователь не станет применять криптографические меры с целью уберечь скрытую информацию от посторонних лиц. Даже, если у него и есть такая информация, максимум, он может ограничиться маскировкой личных файлов или установкой пароля на систему, более «продвинутые» пользователи применяют пароли или шифры к конкретным каталогам с ценной информацией.

- **Малые** предприятия также используют систему паролей. Доступ к ценной информации разрешен, естественно, только обладателям паролей. Часто в целях предотвращения утечки информации персонал фирмы лишается возможности ее копирования на гибкие и лазерные диски из-за отсутствия соответствующих дисководов в системном блоке. Выходом из такого положения может стать флэшка, подключаемая к USB- порту. Следует упомянуть о коммерческой тайне, которую обязан блюсти каждый работник предприятия. Эффективность данной меры в действительности довольно слабый барьер на пути к добыче ценной информации.
- **Крупным** компаниям, особенно разработчикам продукции, в условиях непрекращающейся конкуренции в доминировании на различных рынках недостаточна система ограничения доступа. Такие компании нуждаются в комплексных мерах защиты информации.

- В этот комплекс входят криптографическая, физическая, электромагнитная и другие типы защиты, в том числе человеческий фактор. Выстраивая комплексную защиту, всегда нужно помнить о принципе «слабейшего звена», который утверждает, что устойчивость всей системы защиты равна устойчивости ее слабейшего звена. Принимая меры по защите той или иной информации, следует подумать, имеет ли это смысл, прежде всего - с экономической точки зрения. Например, известная компания Microsoft тратит много средств на защиту своего программного продукта. Качество выпускаемой продукции, разумно построенная система защиты информации позволяют оставаться ей лидером на рынке программных продуктов.
- Абсолютно надёжной защиты не существует. Любую защиту «в принципе» можно преодолеть. Это может потребовать таких затрат сил, средств или времени, что добытая информация их не окупит. Надежной признается та защита, преодоление которой потребует от противника затрат, значительно превышающих ценность информации. Таким образом, руководитель любого предприятия, будь то малого, среднего или крупного, должен руководствоваться следующим принципом – на защиту информации потратить средств не свыше необходимого.

- Безопасность сайтов и систем, открытых для всеобщего доступа через сеть Интернет, уже не один год является проблемой для специалистов, отвечающих за их безопасность. Уже в начальный период существования Интернета практика показала, что нельзя недооценивать существующие в этой сфере угрозы.
- Так, в 1994 г. в результате взлома через Интернет американского СитиБанка, который приписывают русскому хакеру Владимиру Левину, было украдено более 12 млн. долларов. Вскоре были успешно взломаны и сайты НАТО, ЦРУ и Минюста США.
- В настоящее время владельцы сайтов также не чувствуют себя в безопасности. Например, в 2007 году были взломаны сайты Газпрома, компании Nokia, сайты Утро.ру и РБК, сайты партии "Яблоко" и лаборатории Касперского и т. д.
- В значительной мере защищённость сайтов зависит от правильной настройки и конфигурирования сервера с установленной на нём операционной системой, а также дополнительного сетевого оборудования.

- В связи с тем, что подавляющее большинство веб-мастеров размещают свои сайты на виртуальном хостинге, влияние на данные факторы оказывается за пределами их возможностей.
- Как правило, если сайт расположен у известного и надёжного хостера, то сервера администрируются достаточно грамотно и их взлом требует значительных усилий и высокой квалификации самих хакеров.
- В то же время, даже если сайт расположен на абсолютно защищённом сервере, он никак не застрахован от элементарных ошибок, которые часто допускают сами плохо осведомлённые в вопросах безопасности владельцы сайтов, открывая своими руками ворота для взломщиков.

8.2. Виды угроз безопасности систем

Под ***безопасностью ИС*** понимается защищенность системы от случайного или преднамеренного вмешательства в нормальный процесс ее функционирования, от попыток хищения (несанкционированного получения) информации, модификации или физического разрушения ее компонентов.

Под ***угрозой безопасности информации*** понимаются события или действия, которые могут привести к искажению, несанкционированному воздействию, или даже к разрушению информационных ресурсов управляемой системы, а также программных и аппаратных средств.

Угрозы делят на ***случайные*** и ***умышленные***.

Умышленные угрозы разделяются на пассивные и активные.

Пассивные угрозы, как правило, направлены на несанкционированное использование информационных ресурсов, без оказания действия на их функционирование.

Активные угрозы имеют целью нарушение нормального функционирования системы посредством целенаправленного воздействия на аппаратные, программные и информационные ресурсы.

Умышленные угрозы подразделяются также на ***внутренние*** (возникающие внутри управляемой организации) и ***внешние***.

К основным угрозам безопасности информации относят:

- утечку конфиденциальной информации;

- несанкционированное использование информационных ресурсов;

- компрометацию информации;

- ошибочное использование информационных ресурсов;

- несанкционированный обмен информацией между абонентами;

- отказ от информации;

- нарушение информационного обслуживания;

- незаконное использование привилегий.


Компьютерные вирусы
По среде обитания
загрузочные
Файловые
Файлово - загрузочные
сетевые
системные
По степени воздействия
безвредные
Неопасные
опасные
разрушительные
По алгоритмической особенности
репликаторные
Троянский конь
Логическая бомба
мутанты
невидимки
макровирусы
По способу заражения
резидентные
нерезидентные

Логические бомбы используются для искажения или уничтожения информации, реже с их помощью осуществляются кража или мошенничество.

Троянский конь – программа, выполняющая в дополнение к основным, дополнительные действия, не предусмотренные в документации. Троянский конь представляет собой дополнительный блок команд, тем или иным образом вставленный в исходную безвредную программу, которая затем передается (дарится, продается, подменивается) пользователям ИС. Этот блок команд начинает действовать при наступлении некоторого условия (даты, времени, по команде извне и т.п.). радикальным способом защиты от этой угрозы является создание замкнутой среды использования программ.

Мутанты - (призраки, полиморфные вирусы, полиморфики) очень трудно обнаружить, поскольку они не имеют практически совпадающих участков кода (вставка пустых команд)

Вирус – программа, которая может заражать другие программы путем включения в них модифицированной копии, обладающей способностью к дальнейшему размножению. Считается, что вирус обладает двумя основными особенностями:

- 1) способностью к саморазмножению;
- 2) способностью к вмешательству в вычислительный процесс (т.е. к получению возможности управления).
- ***Червь (репликатор)*** – программа, распространяющаяся через сеть и не оставляющая своей копии на магнитном носителе. Червь использует механизмы поддержки сети для определения узла, который может быть заражен. Затем с помощью тех же механизмов передает свое тело или его часть на этот узел и либо активизируется, либо ждет для этого подходящих условий.

Захватчик паролей – это программы, специально предназначенные для воровства паролей. При попытке обращения пользователя к терминалу системы на экран выводится информация, необходимая для окончания сеанса работы. При повторной попытке входа, пользователь вводит имя и пароль, которые пересылаются владельцу программы-захватчика, после чего выводится сообщение об ошибке, а ввод передается операционной системе.

Атака – злонамеренные действия взломщика (попытки реализации им любого вида угроз). Среди таких атак часто выделяют «маскарад» и «взлом системы», которые могут быть результатом реализации разнообразных угроз.

Под ***«маскарадом»*** понимается выполнение каких-либо действий одним пользователем ИС от имени другого пользователя, которому эти действия разрешены.

Под ***взломом системы*** понимают умышленное проникновение в систему, когда взломщик не имеет санкционированных параметров для входа. Способы взлома могут быть различными, иногда используются рассмотренные ранее угрозами. Противостоять взлому может ограничение попыток неправильного ввода пароля, с последующей блокировкой терминала и уведомлением администратора в случае нарушения.

Люк – скрытая, недокументированная точка входа в программный модуль. Люки вставляются в программу обычно на этапе отладки для облегчения работы: модуль можно вызывать в разных местах, что позволяет отлаживать отдельные части программы независимо. Наличие люка позволяет вызывать программу нестандартным образом, что отражается на системе защиты.

8.3. Оценка безопасности ИС

Показатель защищенности ИС – характеристика средств системы, влияющая на защищенность и описываемая определенной группой требований, варьируемых по уровню и глубине в зависимости от класса защищенности. Для оценки реальной безопасности ИС могут применяться различные критерии.

В США вопросами стандартизации и разработки нормативных требований на защиту информации занимается ***Национальный центр компьютерной безопасности министерства обороны*** США (NCSC – National Computer Security Center). Центр еще в 1986 г. издал критерии безопасности компьютерных систем (TCSEC – Trusted Computer System Evaluation Criteria). Этот документ обычно называют Оранжевой книгой.

NCSC считает безопасной систему, которая посредством специальных механизмов защиты контролирует доступ информации таким образом, что только имеющие соответствующие полномочия лица или процессы, выполняющиеся от их имени, могут получить доступ на чтение, запись, создание или удаление информации.

В Оранжевой книге приняты следующие уровни безопасности систем:

А – высший класс;

В – промежуточный класс;

С – низкий уровень безопасности;

Д – класс систем, не прошедших испытания на более высокий уровень безопасности систем.

В России документы по безопасности систем разработаны Государственной технической комиссией при Президенте РФ.

Установлены 9 классов защищенности, каждый из которых характеризуется минимальной совокупностью требований по защите. Защитные мероприятия охватывают:

- управление доступом;

- регистрацию и учет (ведение журналов и статистики);

- криптографию (использование различных механизмов шифрования);

- законодательные меры;

- физические меры.

8.4. Методы и средства защиты информации

Защита информации представляет собой систему, состоящую из комплекса программно-технических средств и организационных решений.

Меры по защите информации делятся на способы защиты и средства защиты.

Способы защиты информации:

Препятствие - метод физического преграждения пути нарушителю к защищаемым ресурсам системы.

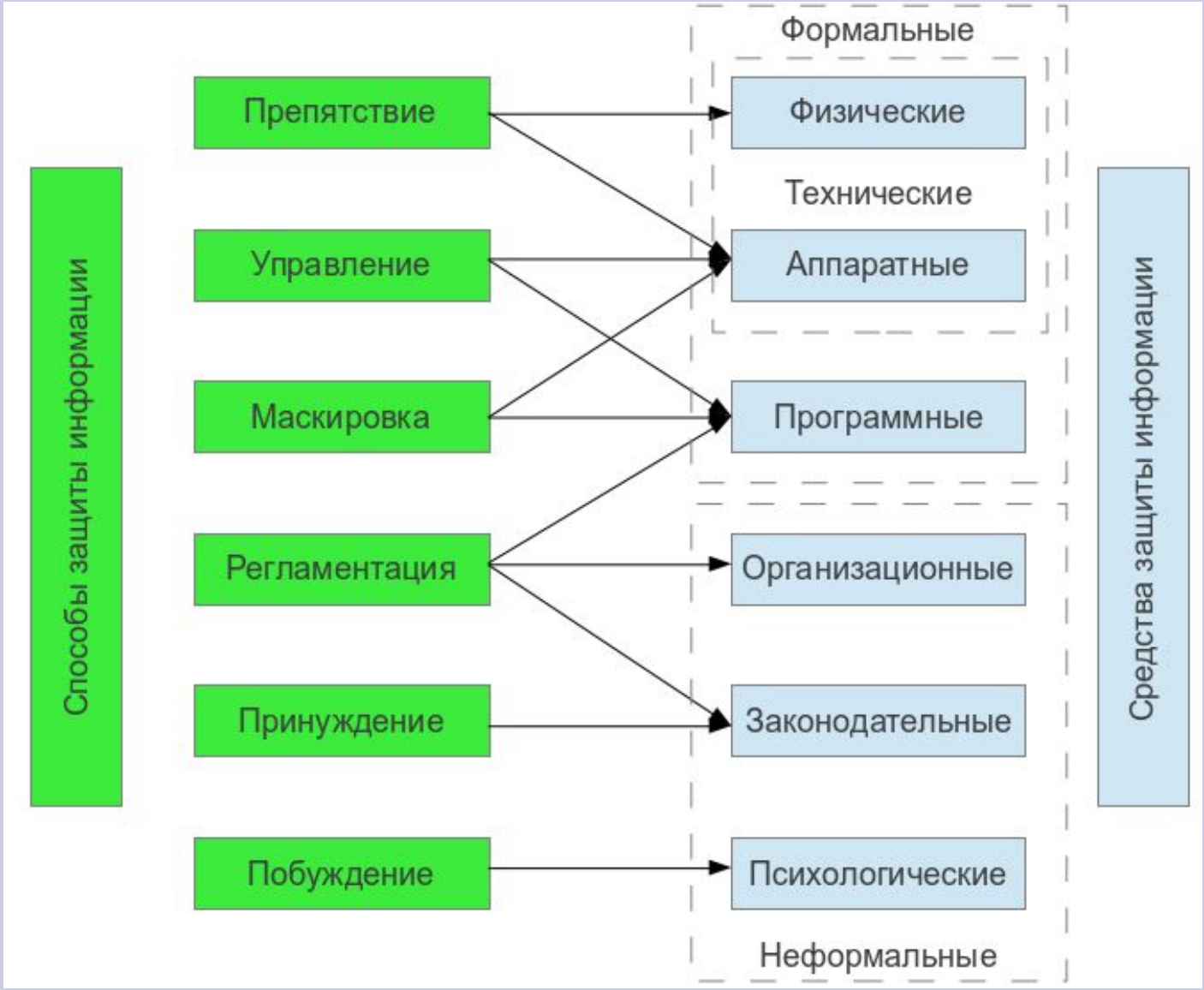
Управление доступом – совокупность мер, включая проверку полномочий, установление подлинности и пр.

Маскировка - защита информации путем ее криптографического закрытия.

Регламентация – минимизация несанкционированного доступа

Принуждение – угроза ответственности

Побуждение – мотивирование пользователей к защите информации


Способы защиты информации
Препятствие
Управление
Маскировка
Регламентация
Принуждение
Побуждение
Формальные
Физические
Технические
Аппаратные
Программные
Организационные
Законодательные
Психологические
Неформальные
Средства защиты информации

Средства защиты делятся на формальные (технические и программные) и неформальные.

Техническими, аппаратными средствами являются устройства, встраиваемые непосредственно в вычислительную технику или сопрягаемые с ней по стандартному интерфейсу (электронные ключи).

Программные средства, как правило, используют различные механизмы шифрования (криптографии). ***Криптография*** – это наука об обеспечении секретности и/или аутентичности (подлинности) передаваемых сообщений.

Организационные решения предусматривают:

- учет, хранение и выдачу пользователям информации, паролей и ключей;
- ведение служебной информации (генерация паролей, ключей, сопровождение правил разграничения доступа);
- оперативный контроль за функционированием системы защиты секретной информации;
- контроль соответствия общесистемной программной среды эталону;
- приемку включенных в автоматизированную технологию программных средств;
- регистрацию и анализ действий пользователей;
- сигнализацию опасных событий и т.п.

Сущность криптографии: готовое к передаче сообщение зашифровывается, преобразуется в закрытый текст. Санкционированный пользователь дешифрует его посредством обратного преобразования криптограммы. Наряду с шифрованием применяются следующие механизмы безопасности:

- ***цифровая (электронная) подпись*** – основана на формировании криптографической подписи отправителем и дешифровке ее получателем;

- ***контроль доступа*** – осуществление проверки полномочий программ и пользователей в конечной и промежуточных точках на доступ к ресурсам;

- ***обеспечение целостности данных*** – отправитель дополняет передаваемый блок данных криптографической суммой, а получатель сравнивает ее с криптографическим значением, соответствующим передаваемому блоку и др.

Виды антивирусных программ

- Программы – **детекторы** (сканеры) - основаны на сравнении характерной последовательности байтов (сигнатур или масок вирусов), содержащихся в теле вируса, с байтами проверяемых программ.
- Программы – **доктора** (или фаги, дезинфекторы) не только находят файлы, зараженные вирусами, но и лечат их, удаляя из файла тело программы – вируса. Программы – доктора, которые позволяет лечить большое число вирусов, называют полифагами.

- Программы – **ревизоры** анализируют текущее состояние файлов и системных областей диска и сравнивают его с информацией, сохраненной ранее в одном из файлов ревизора.
- Программы – **фильтры** (сторожа, мониторы) это резидентные программы (сторожа), которые оповещают пользователя обо всех попытках какой – либо программы выполнить подозрительные действия.
- Программы – **иммунизаторы** (вакцины) записывают в вакцинируемую программу признаки конкретного вируса так, что вирус считает ее уже зараженной, и поэтому не производит повторное инфицирование.