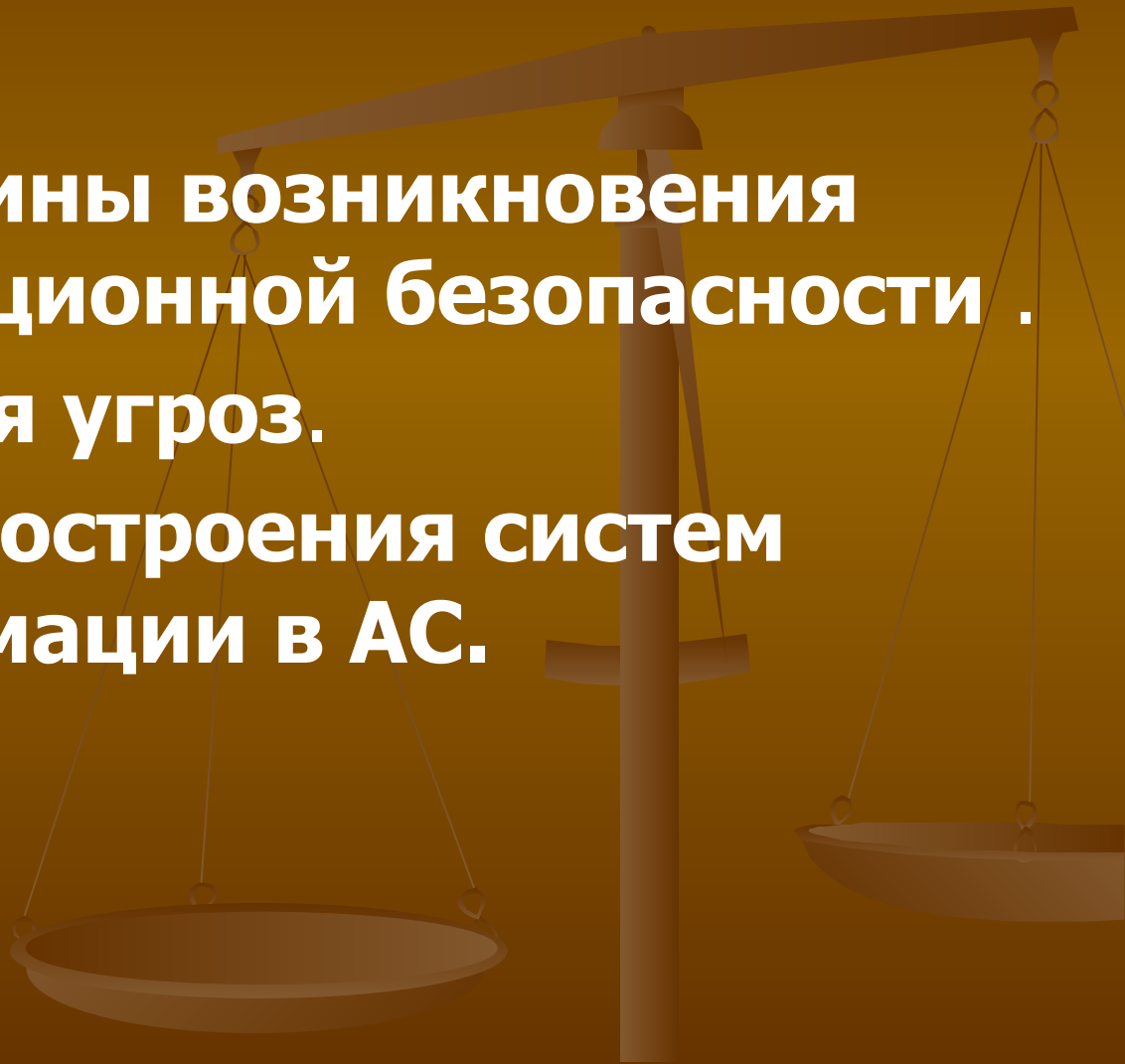
ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Тема 4. Информационные угрозы

Учебные вопросы



1. **Анализ и причины возникновения угроз информационной безопасности .**
2. **Классификация угроз.**
3. **Методология построения систем защиты информации в АС.**

1. Анализ угроз информационной безопасности

Под угрозой вообще понимают потенциально возможное событие, действие процесс или явление, которое может принести ущерб чьим-либо интересам.

Под **угрозой информационной безопасности АС** будем понимать:

- возможность **реализации воздействия на информацию**, приводящего к ее искажению, уничтожению, копированию, блокированию доступа;

-**возможность реализации воздействия на компоненты АС**, приводящего к утрате, уничтожению или сбою функционирования носителя информации, средства взаимодействия с носителем или средства его управления.

В настоящее время перечень угроз насчитывает **более ста пунктов**.

При разработке системы защиты необходимо составлять полный перечень требований к ней, в который входят:

- **перечень угроз,**
- **оценки вероятности их реализации,**
- **модель нарушителя.**

Перечень типовых угроз информационной безопасности

- Следующий перечень содержит некоторые примеры угроз и уязвимостей, связанных с целями и механизмами контроля из ISO/IEC 27002:2005. Этот перечень не является исчерпывающим и должен рассматриваться только в качестве примера, однако его более чем достаточно для проведения высокоуровневой оценки рисков.
- Один из наиболее важных принципов заключается в том, что организация должна самостоятельно выбрать подходы к оценке и управлению рисками, которые должным образом учитывают и идентифицируют полный диапазон угроз и уязвимостей, имеющих отношение к ее бизнес-окружению и могут включать все или часть угроз и уязвимостей, приведенных в следующем перечне.

Физические угрозы

- • Физический несанкционированный доступ в помещения организации, в кабинеты и серверные комнаты, к оборудованию, бумажным документам, запоминающим устройствам, носителям информации и т.п.
- • Кража или повреждение компьютерного оборудования и носителей информации инсайдерами.
- • Кража или повреждение компьютерного оборудования и носителей информации внешними злоумышленниками.
- • Постороннее лицо может получить физический доступ к комплексу средств защиты с целью переконфигурирования либо создания возможности обхода средств защиты.
- • Кража бумажных документов инсайдерами.
- • Кража бумажных документов внешними злоумышленниками.

Нецелевое использование компьютерного оборудования и сети Интернет сотрудниками организации

- • Злоупотребление средствами аудита.
- • Злоупотребление средствами обработки информации.
- • Злоупотребление ресурсами или активами.
1. • Несанкционированное использование программного обеспечения.
- • Использование сетевых средств несанкционированным образом.
- • Неосторожное или умышленное злоупотребление оборудованием по причине отсутствия разделения обязанностей или их неисполнения.

Угрозы утечки конфиденциальной информации

- • Утечка конфиденциальной информации из сети по каналам связи (e-mail, web, chat/IM и т.п.).
- • Утечка конфиденциальной информации на мобильных устройствах, носителях информации, ноутбуках и т.п.
- • Прослушивание внешних каналов связи злоумышленниками.
- • Нарушение конфиденциальности данных, передаваемых по линиям связи, проходящим вне контролируемой зоны, осуществляемого внешними нарушителями путем пассивного прослушивания каналов связи (подключение к каналам связи и перехват информации возможен во многих местах).
- • Нарушение конфиденциальности данных, передаваемых по линиям связи, проходящим внутри контролируемой зоны, осуществляемого внутренними нарушителями путем пассивного прослушивания каналов связи с использованием специализированных программных средств.
- • Аутентификационная информация или конфиденциальные данные могут быть модифицированы либо перехвачены вследствие активного или пассивного прослушивания в системе внешних коммуникаций либо во внутренней сети.
- • Перехват информации на линиях связи путем использования различных видов анализаторов сетевого трафика.
- • Замена, вставка, удаление или изменение данных пользователей в информационном потоке.

- • Перехват информации, например пользовательских паролей, передаваемой по каналам связи, с целью ее последующего использования для обхода средств сетевой аутентификации.
- • Статистический анализ сетевого трафика (например, наличие или отсутствие определенной информации, частота передачи, направление, типы данных и т. п.
- • Неумышленное раскрытие конфиденциальной информации сотрудниками компании.
- • Несанкционированное раскрытие информации о местонахождении площадок/зданий/офисов,
- содержащих критичные или конфиденциальные средства обработки информации.
- • Раскрытие конфиденциальной информации подрядчиками или партнерами компании.

Угрозы утечки информации по техническим каналам

- • Побочные электромагнитные излучения информативного сигнала от технических средств и линий передачи информации.
- Наводки информативного сигнала, обрабатываемого техническими средствами, на провода и линии, выходящие за пределы контролируемой зоны предприятия (учреждения), в том числе на цепи заземления и электропитания.
- Изменения тока потребления, обусловленные обрабатываемыми техническими средствами информативными сигналами
- Изменения тока потребления, обусловленные обрабатываемыми техническими средствами, информативными сигналами.

- Радиоизлучения, модулированные информативным сигналом, возникающие при работе различных генераторов, входящих в состав технических средств, или при наличии паразитной генерации в узлах (элементах) технических средств.
- Электрические сигналы или радиоизлучения, обусловленные воздействием на технические средства высокочастотных сигналов, создаваемых с помощью разведывательной аппаратуры, и модуляцией их информативным сигналом (облучение, навязывание»).
- Радиоизлучения или электрические сигналы от внедренных в технические средства и выделенные помещения специальных электронных устройств перехвата информации (-закладок»), модулированные информативным сигналом.
- Радиоизлучения или электрические сигналы от электронных устройств перехвата информации, подключенных к каналам связи или техническим средствам обработки информации.
- Акустическое излучение информативного речевого сигнала или сигнала, обусловленного функционированием технических средств обработки информации.
- Электрические сигналы, возникающие посредством преобразования информативного сигнала из акустического в электрический за счет микрофонного эффекта и распространяющиеся по проводам и линиям передачи информации.

Угрозы несанкционированного доступа

- • Маскарад (присвоение идентификатора пользователя), использование чужих пользовательских идентификаторов, раскрытие паролей и другой аутентификационной информации.
- • Несанкционированный доступ (НСД) к ресурсам -ЛВС компании со стороны внутренних злоумышленников.
- • НСД к ресурсам ЛВС компании со стороны внешних злоумышленников.
- • НДС к журналам аудита.
- • НДС к средствам аудита.
- • Внешний нарушитель может выдавать себя за легального пользователя путем подделывания адресов в заголовках сетевых пакетов либо информации канального уровня.
- • Сбои в работе средств защиты могут предоставить возможность реализации попытки НСД для потенциального нарушителя (переход в небезопасное состояние). Кроме того, при восстановлении системы безопасное состояние может быть восстановлено некорректно либо может быть утеряна часть данных аудита.
- • НСД к веб-сайту компании и внешним хостам со стороны внешних злоумышленников.
- • НСД к беспроводной сети компании.
- • НСД к резервным копиях данных.

Причины возникновения угроз

- недостаточная квалификация (некомпетентность) использующего технические средства обработки информации (ТСОИ) персонала;
- несовершенство программного обеспечения средств и систем информатизации и АСУ;
- несовершенство технических решений, реализованных при проектировании ТСОИ и монтаже систем информатизации и АСУ;
- естественное старение технических средств и систем в процессе эксплуатации, приводящее к изменению их свойств и характеристик;
- экстремальные нагрузки, испытываемые ТСОИ в процессе эксплуатации;
- неисправности ТСОИ и вспомогательного оборудования;
- действия спецслужб, конкурентов и злоумышленников.

2. Классификация угроз.

1. По природе возникновения.

- 1.1. Естественные – угрозы, вызванные воздействием на АС и её компоненты объективных физических процессов или стихийных природных явлений, независящих от человека.
- 1.2. Искусственные – угрозы, информационной безопасности АС, вызванные деятельностью человека.

2. По степени преднамеренности проявления.

2.1 Угрозы случайного действия и/или угрозы, вызванные ошибками или халатностью персонала.

Например:

- появление ошибок программно-аппаратных средств АС;
- некомпетентное использование, настройка или неправомерное отключение средств защиты персоналом службы безопасности;
- неумышленные действия, приводящие к частичному или полному отказу системы или разрушению аппаратных, программных, информационных ресурсов системы.
- неправомерное включение оборудования или изменение режимов работы устройств и программ;
- неумышленная порча носителей информации;
- пересылка данных по ошибочному адресу абонента (устройства);
- ввод ошибочных данных;
- неумышленное повреждение каналов связи.

2.2. Угрозы преднамеренного действия (например, угрозы действий злоумышленника для хищения информации).

3. По непосредственному источнику угроз.

3.1. Угрозы, непосредственным источником которых является природная среда (стихийные бедствия, магнитные бури, радиоактивное излучение и т.п.).

3.2. Угрозы, непосредственным источником которых является человек.

Например:

- внедрение агентов в число персонала системы (в том числе, возможно, и в административную группу, отвечающую за безопасность);
- вербовка (путём подкупа, шантажа и т.п.) персонала или отдельных пользователей, имеющих определённые полномочия;
- угроза несанкционированного копирования секретных данных пользователем АС;
- разглашение, передача или утрата атрибутов разграничения доступа (паролей, ключей шифрования, идентификационных карточек, пропусков и т.п.).

3.3. Угрозы, непосредственным источником которых являются санкционированные программно-аппаратные средства.

Например:

- запуск технологических программ, способных при некомпетентном использовании вызывать потерю работоспособности системы (зависание) или необратимые изменения в ней (форматирование или реструктуризацию носителей информации, удаление данных);

- возникновение отказа в работе ОС.

3.4. Угрозы, непосредственным источником которых являются несанкционированные программно-аппаратные средства.

Например:

- нелегальное внедрение и использование неучтенных программ (игры, обучалки и т.д.) с последующим необоснованным расходованием ресурсов;

- заражение компьютера вирусами с деструктивными функциями.

4. По положению источника угроз.

4.1. Угрозы, источник которых расположен вне контролируемой зоны территории, на которой находится АС. Например:

- перехват побочных электромагнитных, акустических и других излучений устройств и линий связи;

- перехват данных, передаваемых по каналам связи, и их анализ с целью выяснения протоколов обмена, правил вхождения в связь и авторизации пользователя и последующих попыток их имитации для проникновения в систему;

- дистанционная фото- и видеосъёмка.

4.2. Угрозы, источник которых расположен в контролируемой зоне территории, на которой находится АС. Например:

- хищение производственных отходов (рас-печаток, записей, списанных носителей информации и т.п.);

- отключение или вывод из строя подсистем функционирования ВС (электропитания, линий связи и т.п.);

- применение подслушивающих устройств.

4.3. Угрозы, источник которых имеет доступ к периферийным устройствам АС (терминалам).

4.4. Угрозы, источник которых расположен в АС.

Например:

- проектирование архитектуры системы и технологии обработки данных, разработка прикладных программ, которые представляют опасность для работоспособности системы и безопасности информации;

- некорректное использование ресурсов АС.

5. По степени зависимости от активности АС.

5.1. Угрозы, которые могут непосредственно проявляться независимо от активности АС. Например:

- вскрытие шифров криптозащиты информации;
- хищение носителей информации (магнитных дисков, лент, микросхем памяти, запоминающих устройств).

5.2. Угрозы, которые могут проявляться только в процессе автоматизированной обработки данных (например, угрозы выполнения и распространения программных вирусов).

6. По степени воздействия на АС.

6.1. Пассивные угрозы, которые при реализации ничего не меняют в структуре и содержании АС (например, угроза копирования секретных данных).

6.2. Активные угрозы, которые при воздействии вносят изменения в структуру и содержание АС. Например:

внедрение аппаратных спецвложений, программных “закладок” и “вирусов” (“троянских коней” и “жучков”), то есть таких участков программ, которые позволяют преодолеть систему защиты;

- действия по дезорганизации функционирования системы (изменение режимов работы устройств или программ, забастовка персонала, установка мощных активных радиопомех на частотах работы устройств системы);

- угрозы умышленной модификации информации.

7. По этапам доступа пользователей или программ к ресурсам АС.

7.1. Угрозы, которые могут проявляться на этапе доступа к ресурсам АС (например, несанкционированный доступ).

7.2. Угрозы, которые могут проявляться после разрешения доступа к ресурсам АС (некорректное использование ресурсов АС).

8. По способу доступа к ресурсам АС.

8.1. Угрозы, направленные на использования прямого стандартного доступа к ресурсам АС. Например:

- незаконное получение паролей и других реквизитов разграничения доступа с последующей маскировкой под зарегистрированного пользователя (“маскарад”);
- несанкционированное использование терминалов пользователей, имеющих уникальные физические характеристики (номер рабочей станции сети, физический адрес, адрес в системе связи);

8.2. Угрозы, направленные на использование скрытого нестандартного пути доступа к

ресурсам АС.

Например:

- вход в систему в обход средств защиты (загрузка посторонней ОС со сменных МД);
- угроза несанкционированного доступа к ресурсам АС путём использования недокументированных возможностей ОС.

9. По текущему месту расположения информации, хранимой и обрабатываемой в АС.

9.1. Угрозы доступа к информации на внешних запоминающих устройствах (например копирование секретной информации с ЖД).

9.2. Угрозы доступа к информации в ОП:

- чтение остаточной информации из ОП;

- чтение информации из областей ОП, используемых ОС в асинхронном режиме, используя недостатки мультизадачных АС и систем программирования;

- угроза доступа к системной области ОП со стороны прикладных программ.

9.3. Угрозы доступа к информации, циркулирующей в линиях связи:

- незаконное подключение к линиям связи с целью работы “между строк”, использованием пауз в действиях законного пользователя от его имени, с вводом ложных сообщений или модификацией передаваемых сообщений;

- подключение к линиям связи с целью прямой подмены законного пользователя путём его физического отключения после входа в систему, с вводом дезинформации и ложных сообщений;

- перехват всего потока данных с целью дальнейшего анализа не в реальном масштабе времени.

9.4. Угрозы доступа к информации, отображаемой на терминале или печатаемой на принтере (запись отображаемой информации на скрытую видеокамеру).

Однако, вне зависимости от конкретных видов угроз считается, что АС удовлетворяет требованиям безопасности **эксплуатирующих ее лиц**, если обеспечиваются следующие свойства информации и систем ее обработки:

- **Конфиденциальность** – субъективно определяемая характеристика, указывающая на необходимость введения ограничений на круг субъектов, имеющих доступ к данной информации. Это свойство обеспечивается способностью системы (среды) сохранять указанную информацию в тайне от субъектов, не имеющих полномочий доступа к ней.

- **Целостность** – существование информации в некотором неискаженном виде (фиксированном относительно определенного состояния).

- **Достоверность** – адекватность (полнота, точность) отображения состояния предметной области. Эта проблема более широкая и выходит за рамки проблем безопасности.

- **Доступность** - свойство системы (среды, средств и технологии обработки), обеспечиваю-щее своевременный беспрепятственный доступ субъектов к интересующей их информации и готовность всех служб к обслуживанию поступающих запросов.

Три вида основных угроз для АС:

- **Угроза нарушения конфиденциальности** заключается в том, что информация становится известна лицу, не обладающему соответствующими полномочиями. Часто используется термин “утечка”.

- **Угроза нарушения целостности** - есть любое умышленное изменение информации, хранящейся или передаваемой по каналам связи из одной АС в другую.

- **Угроза отказа служб** – возникает всякий раз, когда в результате преднамеренных действий, предпринимаемых другим пользователем или злоумышленником, блокируется доступ к некоторому ресурсу ВС. В случае блокирования ресурса навсегда либо на продолжительное время

говорят, что ресурс исчерпан.

Впервые перечисленные угрозы сформулированы в конце 60-х годов для открытых UNIX- подобных систем

Данные виды угроз считаются первичными или непосредственными.

В настоящее время информация не предъявляется в чистом виде, на пути к ней ставится хотя бы какая- то система защиты.

Для **защищенных систем** рассматривается четвертый вид угрозы – **угроза раскрытия параметров** АС, включающей в себя систему защиты. (Это этап разведки и выбора технических средств).

Угроза раскрытия параметров есть опосредованная угроза, т.к. ее реализация не причиняет непосредственного ущерба обрабатываемой информации.

С точки зрения владельца информации и в зависимости от цели воздействия:

1.Уничтожение. При уничтожении информационных объектов или их элементов они утрачиваются или разрушаются (например, в результате стихийного бедствия, неквалифицированных действий пользователей, преднамеренного введения в программное обеспечение определенного типа вирусов и т.п.).

2. Утечка. При утечке информационные объекты не утрачиваются, однако становятся доступными посторонним лицам .

3. Искажение. Результатом искажения является преднамеренное или непреднамеренное изменение информационного объекта (например, изменение информации в процессе обработки и передаче).

4. Блокирование. В результате блокирования информационный объект не утрачивается, но становится недоступным для его собственника, владельца или пользователя (потребителя) в результате физического или логического блокирования этого элемента.

Принято считать, что защищенные ИС это такие, для которых существует угроза раскрытия параметров.

Открытые системы считаются **прозрачными** для атакующих систем.

Модель осуществления угроз раскрытия параметров:

W- основная система;

MW - ее модель, оптимизирующая затраты на управление системой и ее качество;

Объем информационных ресурсов - один из параметров модели (под ИР понимают факти-ческие сведения, отражающие восприятие как самих себя, так и окружающего мира);

Т- противник, Мт - его модель.

Между моделями противоборство через информационные каналы. Каждый участник строит модель противника: соответственно $М_{т(w)}$ и $М_{w(т)}$.

Имеем симметричную модель взаимодействия:

Сопоставим угрозы с моделью.

Угроза нарушения конфиденциальности системы W- это возможность системы T добавлять инф. ресурсы системы W к собственным инф. ресур., используя для этого информационный канал.

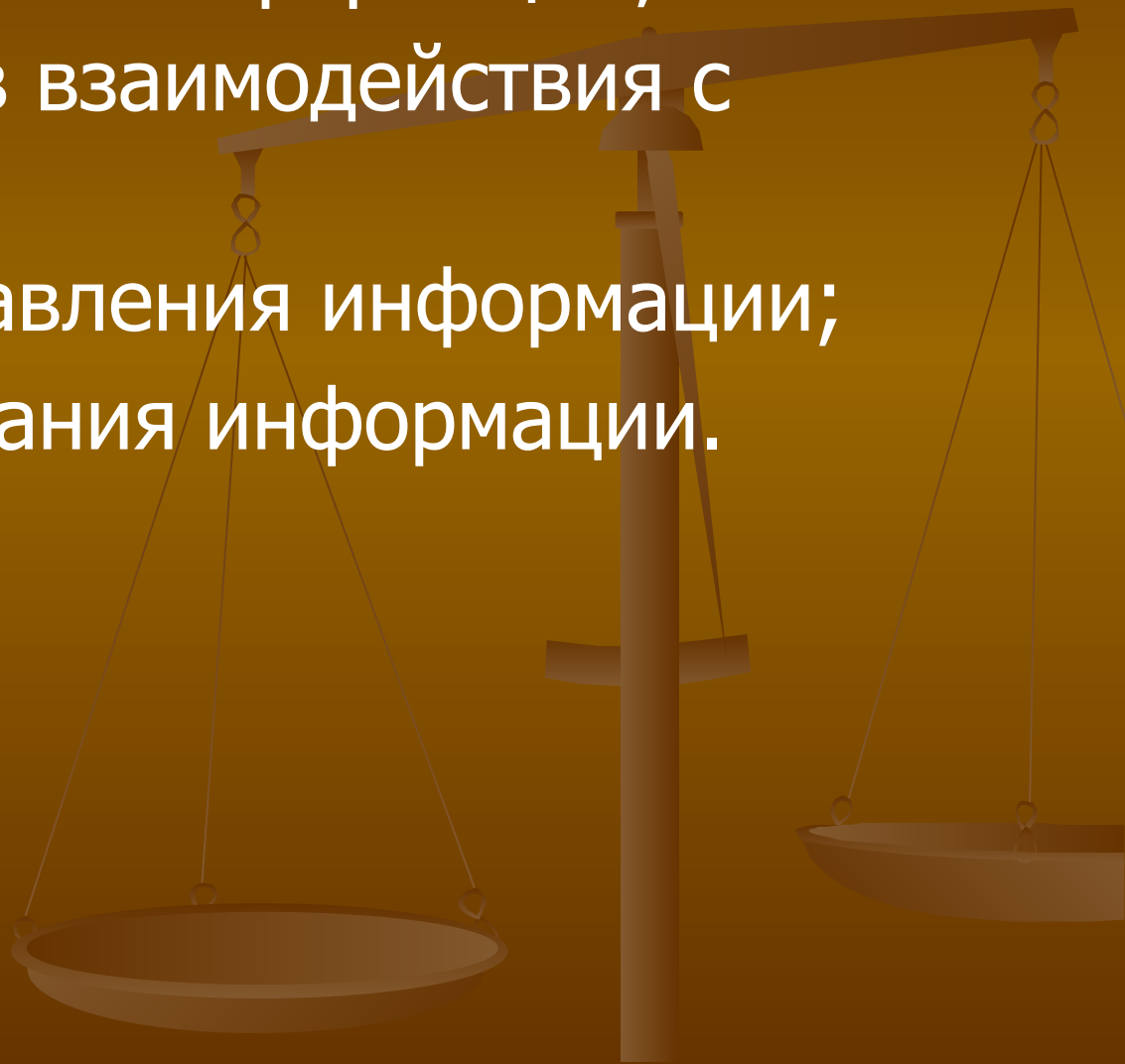
Угроза нарушения целостности W - это возможность T внедрять собственные инфор. ресурсы в инфор. ресурсы системы W через информационный канал.

Угроза отказа служб системы W - это возможность системы T разорвать существующий информацион-ный канал.

Угроза разведки параметров W- это возможность сист. T организовать инф. канал с целью реализации угроз нарушения конф. и целостности.

Уровни градации доступа к защищаемой информации:

- уровень носителей информации;
- уровень средств взаимодействия с носителем;
- уровень представления информации;
- уровень содержания информации.



Основные направления реализации инф. угроз:

- непосредственное обращение к объектам доступа;
- обход защиты с помощью создания программных и технических средств;
- модификация средств защиты;
- внедрение в АС специальных прогр. или технич. средств, нарушающих структуру и функции АС.

Далее по всем видам угроз ...

Положения гостехкомиссии по защите АС:

1. Инф. безопасность АС основывается на существу-ющих законах, стандартах, нормативных документах.

2. Инф. безопасность АС обеспечивается комплексом программных, технических и организационных мер.

3. Инф. безопасность АС должна обеспечиваться на всех технологических этапах обработки информации.

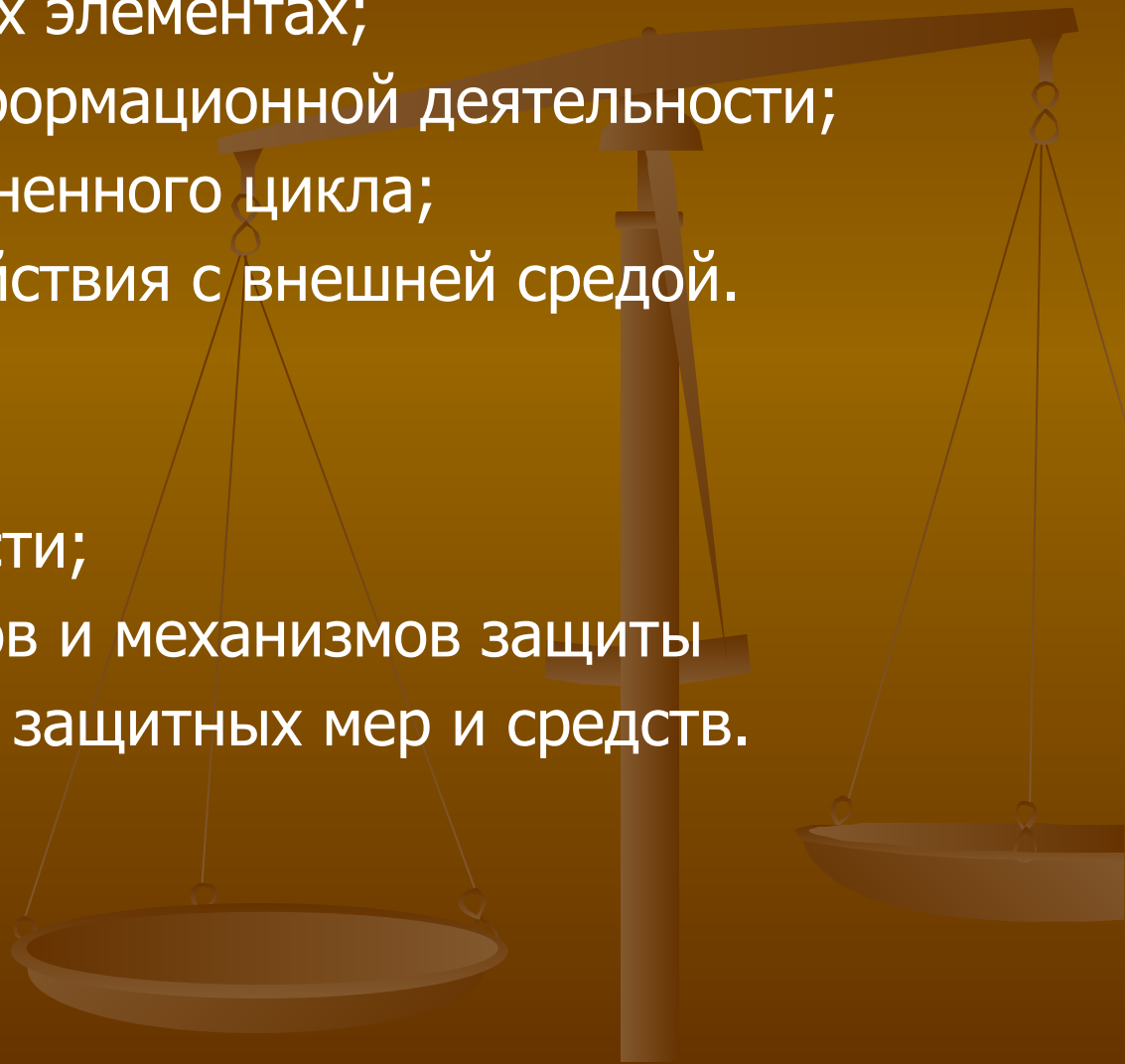
4. Средства защиты не должны существенно ухудшать основные характеристики АС (надежность, быстродей-ствие …).

5. Оценка эффективности средств защиты обязательно учитывает всю совокупность техн. характ. объекта.

6. Защита АС обязательно предусматривает периоди-ческий или инициативный контроль эффективности.

Принципы обеспечения инфор. безопасности АС:

- системности:
  - при всех режимах функционирования;
  - во всех структурных элементах;
  - при всех видах информационной деятельности;
  - на всех этапах жизненного цикла;
  - с учетом взаимодействия с внешней средой.
- комплексности;
- непрерывности;
- разумной достаточности;
- открытости алгоритмов и механизмов защиты
- простоты применения защитных мер и средств.



Причины утечки информации:

- несоблюдение персоналом правил, норм и требова-ний эксплуатации АС;
- ошибки в проектировании АС и ее системы защиты;
- ведение технической и агентурной разведки.

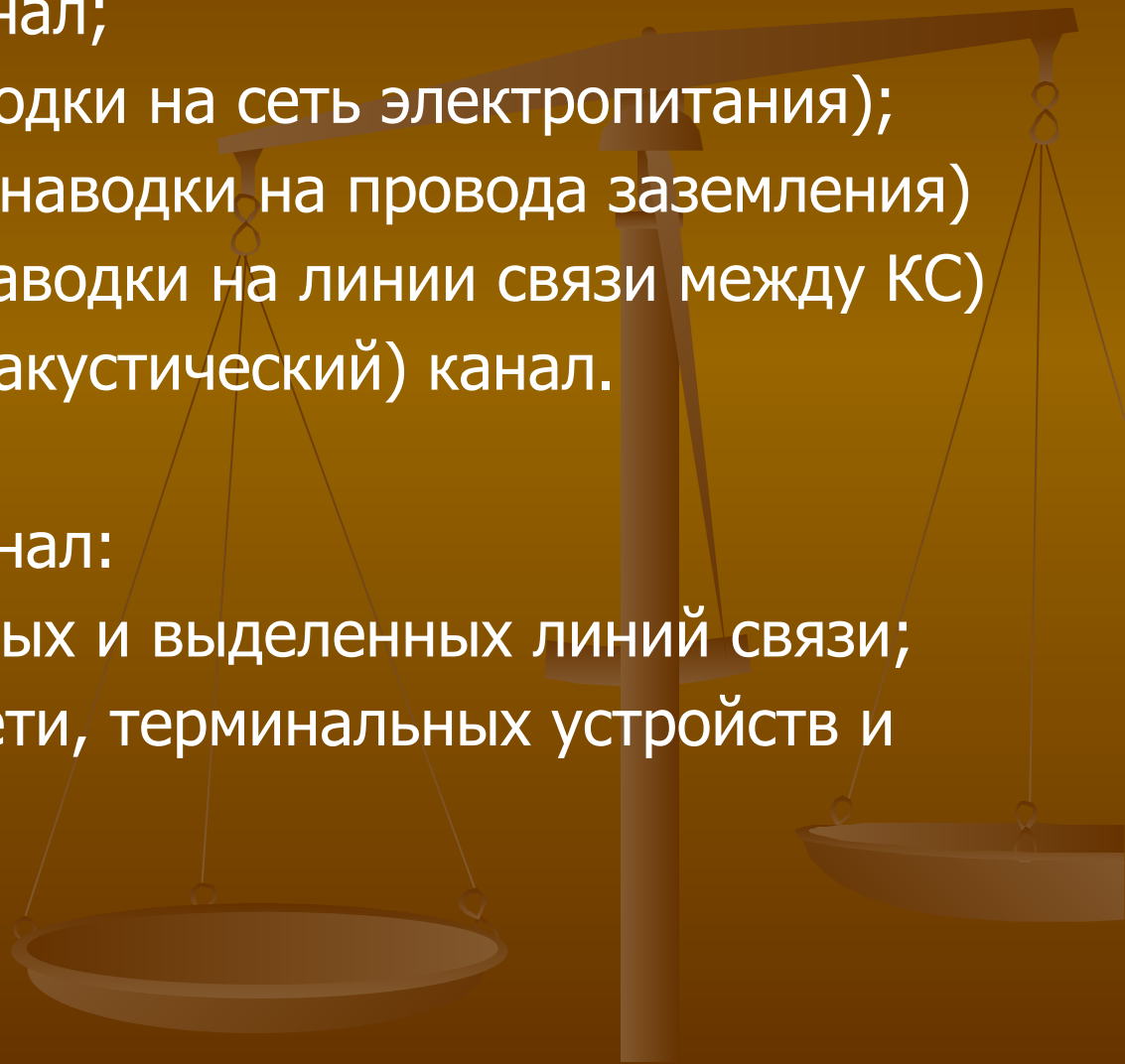
Три вида утечки (в соответствии с ГОСТ):

- разглашение;
- несанкционированный доступ;
- получение защищаемой информации разведками.

Канал утечки информации - совокупность источника информации, материального носителя или среды рас-пространения и средства выделения информации из сигнала или среды.

Типы каналов утечки:

1. Электромагнитный канал:
   - радиоканал (высокочастотное излучение);
   - низкочастотный канал;
   - сетевой канал (наводки на сеть электропитания);
   - канал заземления (наводки на провода заземления)
   - линейный канал (наводки на линии связи между КС)
2. Акустический (виброакустический) канал.
3. Визуальный канал.
4. Информационный канал:
   - канал коммутируемых и выделенных линий связи;
   - канал локальной сети, терминальных устройств и машинных носителей .



3. МЕТОДОЛОГИЯ ПОСТРОЕНИЯ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ В АС

1.Защита от угрозы нарушения конфиденциальности

Защита машинных носителей информации (МНИ).

Особенности:

- последовательный либо прямой метод доступа;
- различные физические принципы реализации;
- различие объемов хранимой информации;
- многообразие вариантов реализации фирмами.

Задача злоумышленника:

1) выбор соответствующего данному носителю привода;

2) запуск соответствующего комплекта программ (операционных средств, драйверов и т.п.);

3) осуществление (организация) считывания в па- мять КС содержимого носителей.

Отсюда тактика защиты. Существуют носители (накопители) со встроенными средствами защиты, требующими специальных паролей.

Парольные системы для защиты от НСД.

Под НСД в руководящих документах понимают до-ступ к информации, нарушающий установленные правила разграничения доступа и осуществляемый с использованием **штатных** средств. НСД может быть случайным либо преднамеренным.

Категории методов защиты от НСД:

- организационные (мероприятия и регламентирующие инструкции);
- технологические (программно-аппаратные средства идентификации, аутентификации и охранной сигнализации);
- правовые (меры контроля за исполнением нормативных актов).

Идентификация - присвоение пользователям идентификаторов и проверка предъявляемых идентификаторов по списку присвоенных.

Аутентификация - проверка принадлежности пользователю предъявленного им идентификатора.

Безопасность (стойкость) системы идентификации и аутентификации это степень обеспечиваемых ею гарантий того, что злоумышленник не способен пройти аутентификацию от имени другого пользователя.

Методы **аутентификации** основаны на наличии у каждого пользователя:

- индивидуального объекта заданного типа (про-пуск, магнитная карта и т.п.);
- знаний некоторой информации (пароля), известного только ему и проверяющей стороне;
- индивидуальных биометрических характеристик (тембра голоса, рисунка папилярных линий, структуры радужной оболочки глаза и т.п.).

Если в процедуре аутентификации участвуют только две стороны, то это **непосредственная аутентификация** (direct password authentication).

Если в этой процедуре участвует третья *доверенная* сторона, то ее называют **сервером аутентификации,** а метод называют с *участием доверенной стороны* (trusted third party authentication).

Общие подходы к построению парольных систем.

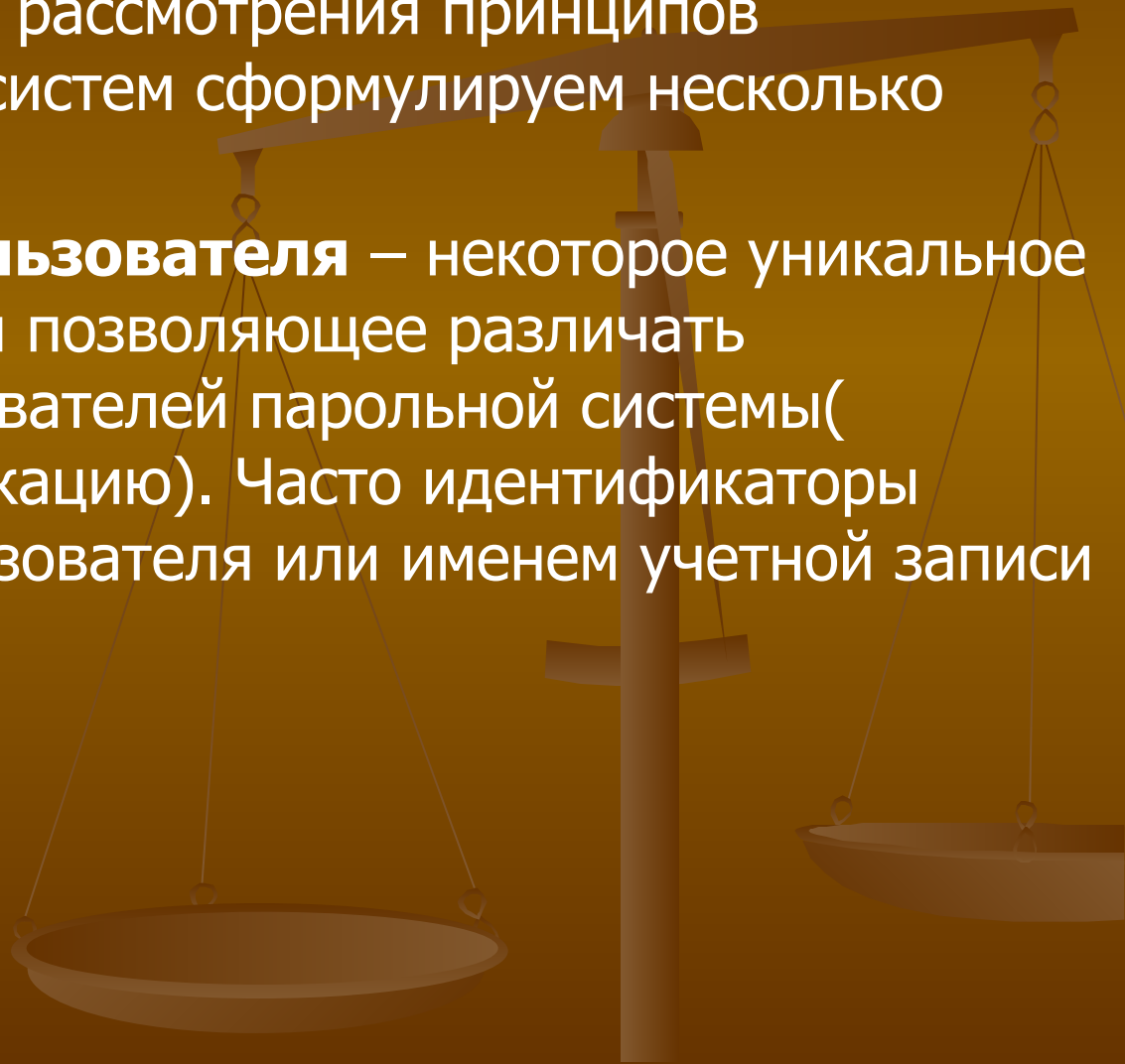
Наиболее распространенные методы аутентификации основаны на применении многоразовых и одноразовых паролей. Из-за своего широкого распространения и простоты реализации парольные системы часто становятся мишенью атак злоумышленников. Эти методы включают следующие разно-видности способов аутентификации:

- по хранимой копии пароля или его свёртке **(plaintext- equivalent)**;
- по некоторому проверочному значению **(verifier-based) ;**

- Без непосредственной передачи информа-ции о пароле проверяющей стороне (zero- knowledge);
- С использованием пароля для получения криптографического ключа (cryptographic).

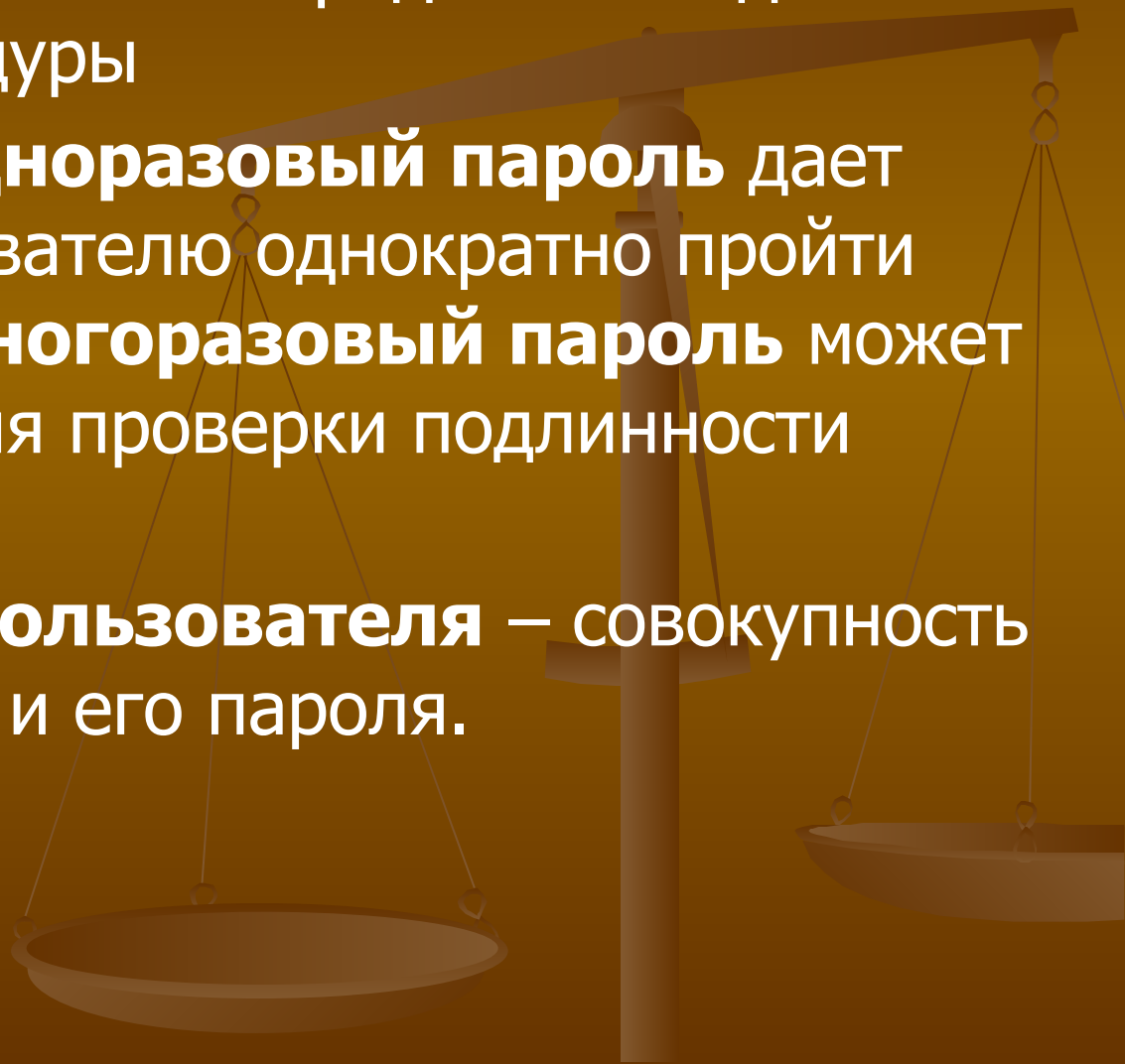
Для более детального рассмотрения принципов построения парольных систем сформулируем несколько основных определений.

Идентификатор пользователя – некоторое уникальное количество информации позволяющее различать индивидуальных пользователей парольной системы(проводить их идентификацию). Часто идентификаторы также наз. именем пользователя или именем учетной записи пользователя .



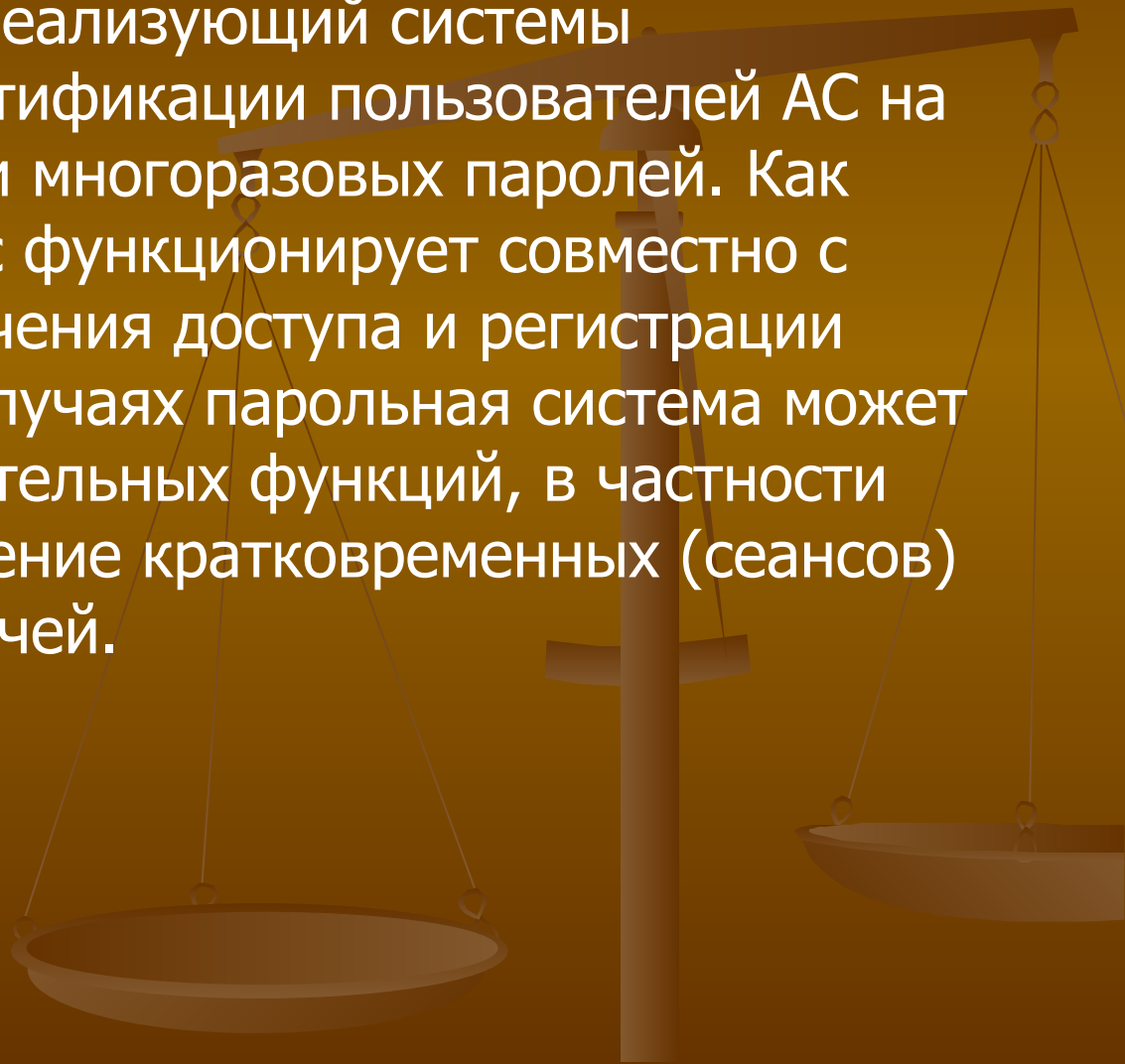
Пароль пользователя – некоторое секретное кол-во информации известное только пользователю и парольной системе, которая может быть запомнена пользователем и предъявлена для прохождения процедуры аутентификации. **Одноразовый пароль** дает возможность пользователю однократно пройти аутентификацию. **Многоразовый пароль** может быть использован для проверки подлинности повторно.

Учетная запись пользователя – совокупность его идентификатора и его пароля.



База данных пользователей парольной системы содержит учетные записи всех пользователей данной парольной системы.

Под парольной системой будем понимать программно-аппаратный комплекс, реализующий системы идентификации и аутентификации пользователей АС на основе одноразовых или многоразовых паролей. Как правило такой комплекс функционирует совместно с подсистемами разграничения доступа и регистрации событий. В отдельных случаях парольная система может выполнять ряд дополнительных функций, в частности генерацию и распределение кратковременных (сеансов) криптографических ключей.



Основными компонентами парольной системы являются:

- интерфейс пользователя;
- интерфейс администратора;
- модуль сопряжения с другими подсистемами безопасности;
- база данных учетных записей.

Парольная система представляет собой “перед-ний край обороны” всей системы безопасности. Некоторые ее элементы(в частности реализую-щие интерфейс пользователя) могут быть расположены в местах, открытых для доступа потенциальному злоумышленнику.

Поэтому парольная система становиться одним из первых объектов атаки при вторжении злоумышленника в защищенную систему.

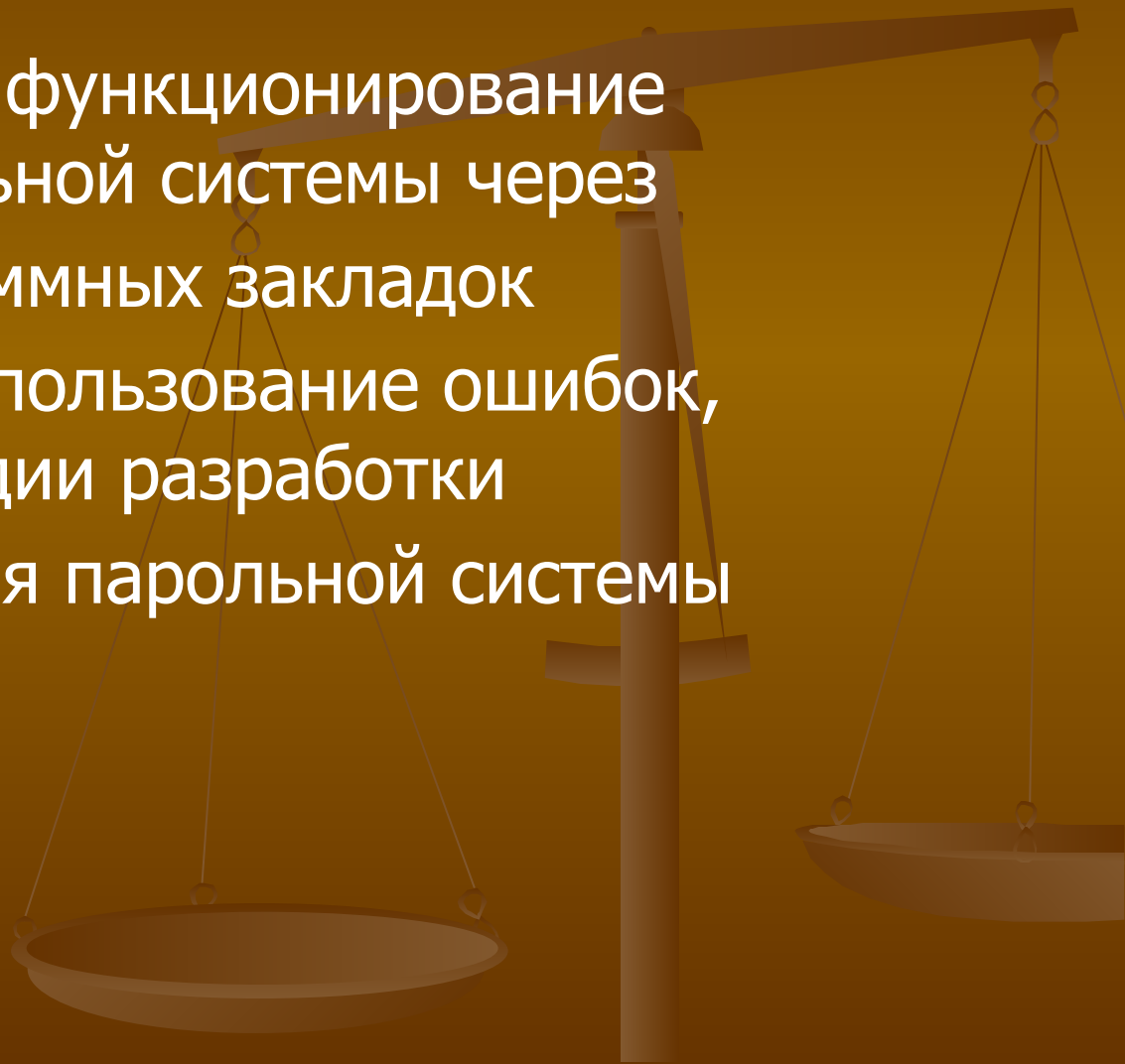
Типы угроз безопасности парольных систем.

1.Разглашение параметров учетной записи через :

- Подбор в интерактивном режиме
- Подсматривание
- Преднамеренную передачу пароля ее владельцем другому лицу
- Захват базы данных парольной системы с дальнейшей дешифрацией

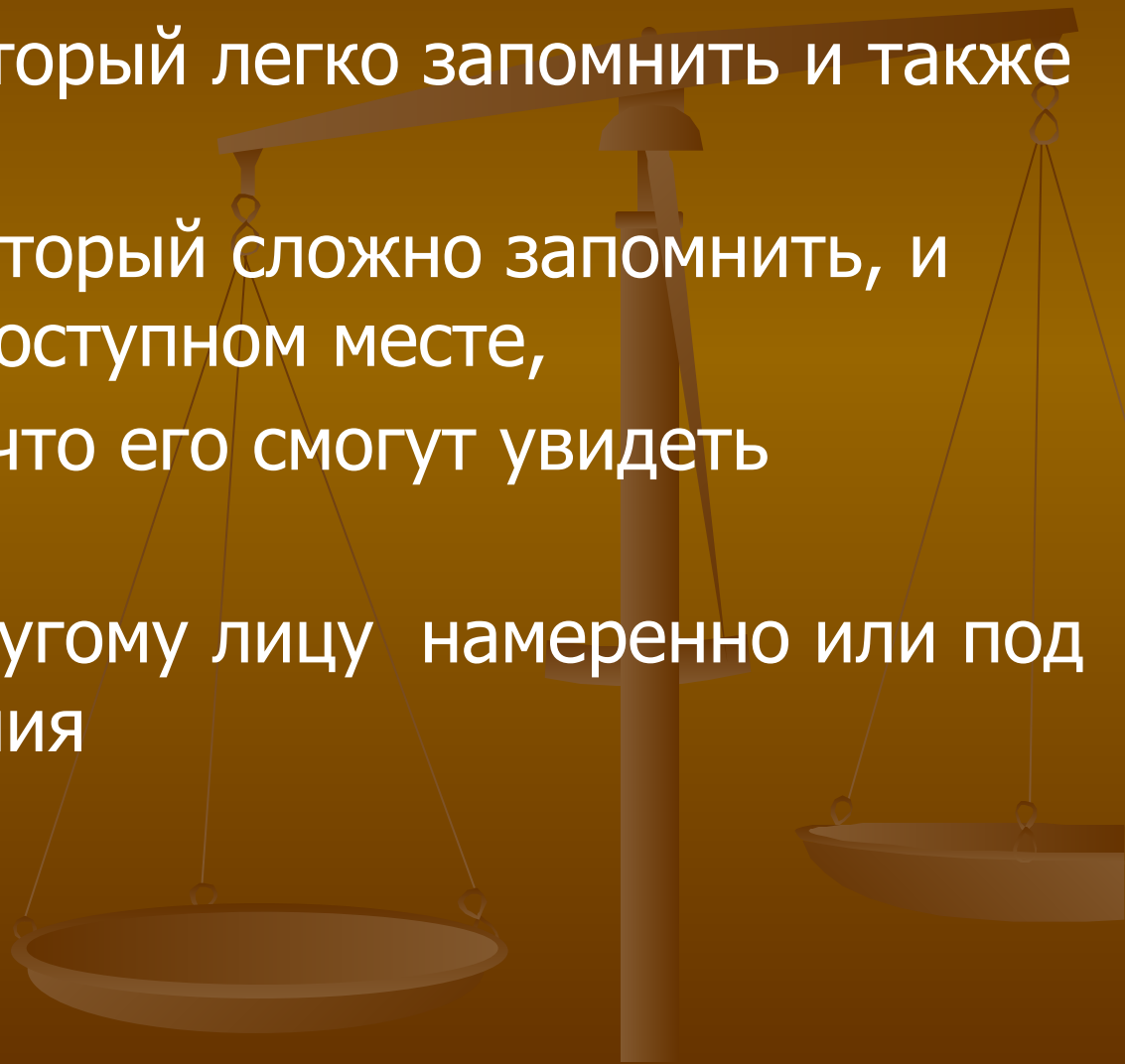
- Перехват переданной по сети информации о пароле
- Хранение пароля в доступном месте

2. Вмешательство в функционирование компонентов парольной системы через
- Внедрение программных закладок
- Обнаружение и использование ошибок, допущенных на стадии разработки
- Выведение из строя парольной системы



Некоторые из перечисленных типов угроз связанны с наличием так называемого **человеческого фактора**, проявляющегося в том, что пользователь может:

- Выбрать пароль, который легко запомнить и также легко подобрать,
- Записать пароль, который сложно запомнить, и положить запись в доступном месте,
- Ввести пароль так, что его смогут увидеть посторонние,
- Передать пароль другому лицу намеренно или под влиянием заблуждения



Выбор паролей

Для уменьшения влияния человеческого фактора при выборе и использовании паролей необходимо выполнить ряд требований:

- установить оптимальную длину пароля;
- использовать в паролях различные группы символов;
- проверка и отбраковка паролей по словарю;
- установить максимальный и минимальный срок действия пароля;
- ведение журнала истории паролей;
- применять алгоритмы, бракующие пароли на основании данных журнала историй;

- ограничение числа попыток ввода пароля;
- поддержка режима принудительной смены пароля пользователя;
- использование вопросо-ответного диалога при вводе неправильного пароля (для замедления цикла подбора);
- запрет на выбор пароля самим пользователем и автоматическая генерация паролей;
- принудительная смена пароля при первой регистрации пользователя в системе (для защиты от неправомерных действий системного администратора, имеющего доступ к паролю в момент создания учетной записи).

Оценка стойкости парольных систем осуществляется по формуле:

P = V*T/S, где $S = A^L$

Здесь A - мощность алфавита паролей;

L - длина пароля;

S - мощность пространства паролей;

V - скорость подбора паролей;

T - срок действия пароля;

P - вероятность подбора пароля в течение его срока действия.

ПРИМЕР:

Пусть задано P = 0.000001. Найти минимальную длину пароля, обеспечивающую его стойкость в течение одной недели непрерывных попыток подобрать пароль. Пусть скорость интерактивного подбора паролей V = 10паролей/мин. Тогда в течение недели можно подобрать:

10*60*24*7=100800 паролей.

Тогда из формулы 1 имеем:

S = 100800/0.000001 = 1.008*E+11

Полученному значению S соответствуют пары:

A = 26, L = 8 и A = 36, L = 6.

Хранение паролей

Важным аспектом стойкости парольной системы, является способ хранения паролей в базе данных учетных записей. Варианты хранения паролей:

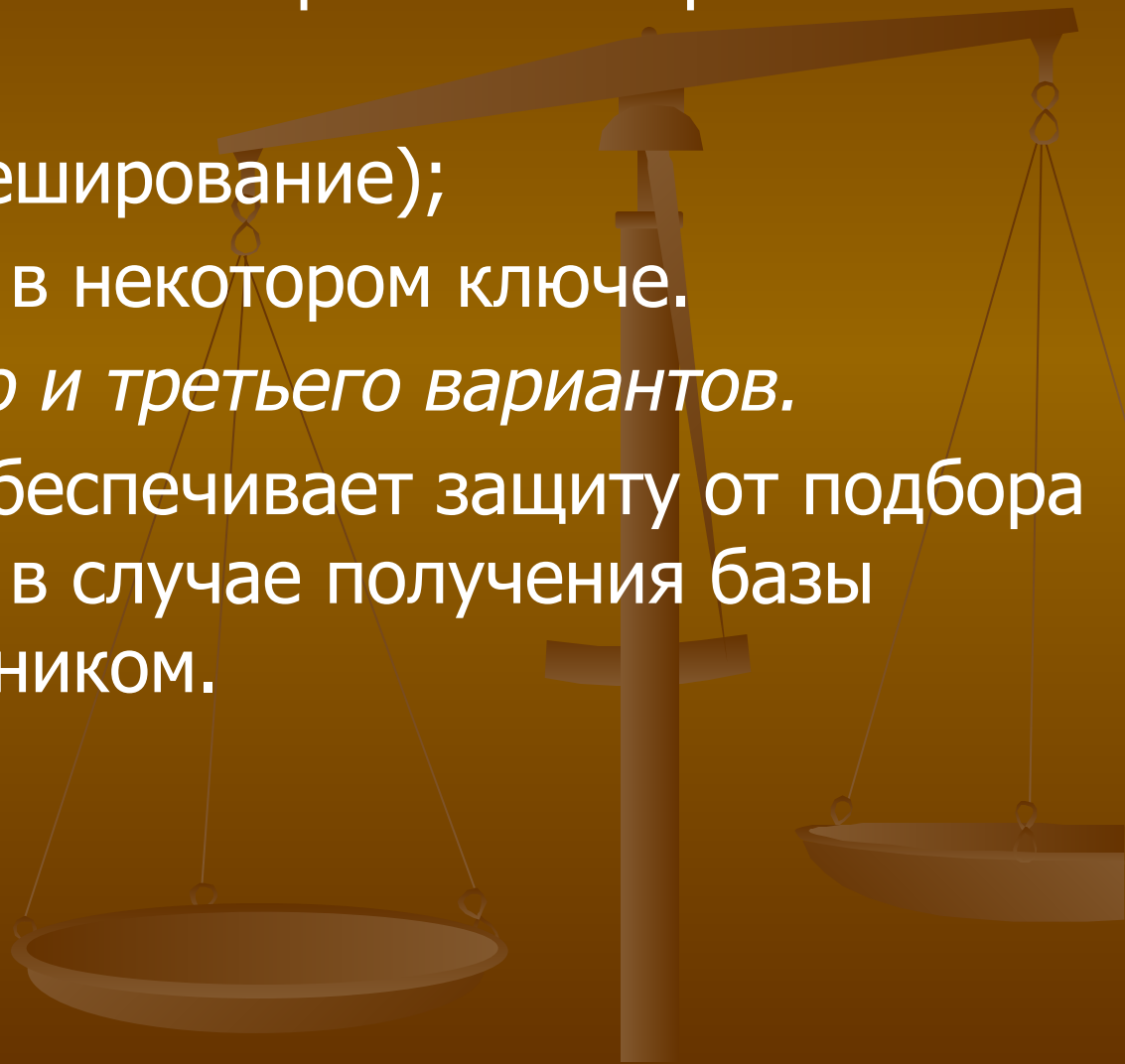
1) в открытом виде;

2) в виде сверток (хеширование);

3) зашифрованными в некотором ключе.

Особенности второго и третьего вариантов.

Хеширование не обеспечивает защиту от подбора паролей по словарю в случае получения базы данных злоумышленником.



При выборе алгоритма хеширования необходимо: - гарантировать несовпадение значений сверток, полученных на основе различных паролей пользователей;

- предусмотреть механизм, обеспечивающий уникальность сверток в том случае, если два пользователя выбирают одинаковые пароли, предусмотрев некоторое количество “случайной” информации.

Варианты шифрования базы данных учетных записей:

1) ключ генерируется программно и хранится в системе, обеспечивая возможность ее автоматической перезагрузки;

2) ключ генерируется программно и хранится на внешнем носителе, с которого считывается при каждом запуске;

3) ключ генерируется на основе выбранного администратором пароля, который вводится в систему при каждом запуске.

Наиболее безопасное хранение паролей обеспечивается при комбинации второго и третьего способов.

Стойкость парольной системы определяет ее способность противостоять атаке противника, а также зависит от криптографических свойств алгоритма шифрования или хеширования.

Передача пароля по сети.

Если передаваемая по сети в процессе аутентификации информация не защищена надлежащим образом, возникает угроза ее перехвата и использования для нарушения защиты парольной системы.

Многие компьютерные системы позволяют переключать сетевой адаптер в режим прослушивания адресованного другим получателям сетевого трафика.

Основные виды защиты сетевого трафика:

- физическая защита сети;
- оконечное шифрование;
- шифрование пакетов.

Способы передачи паролей по сети :

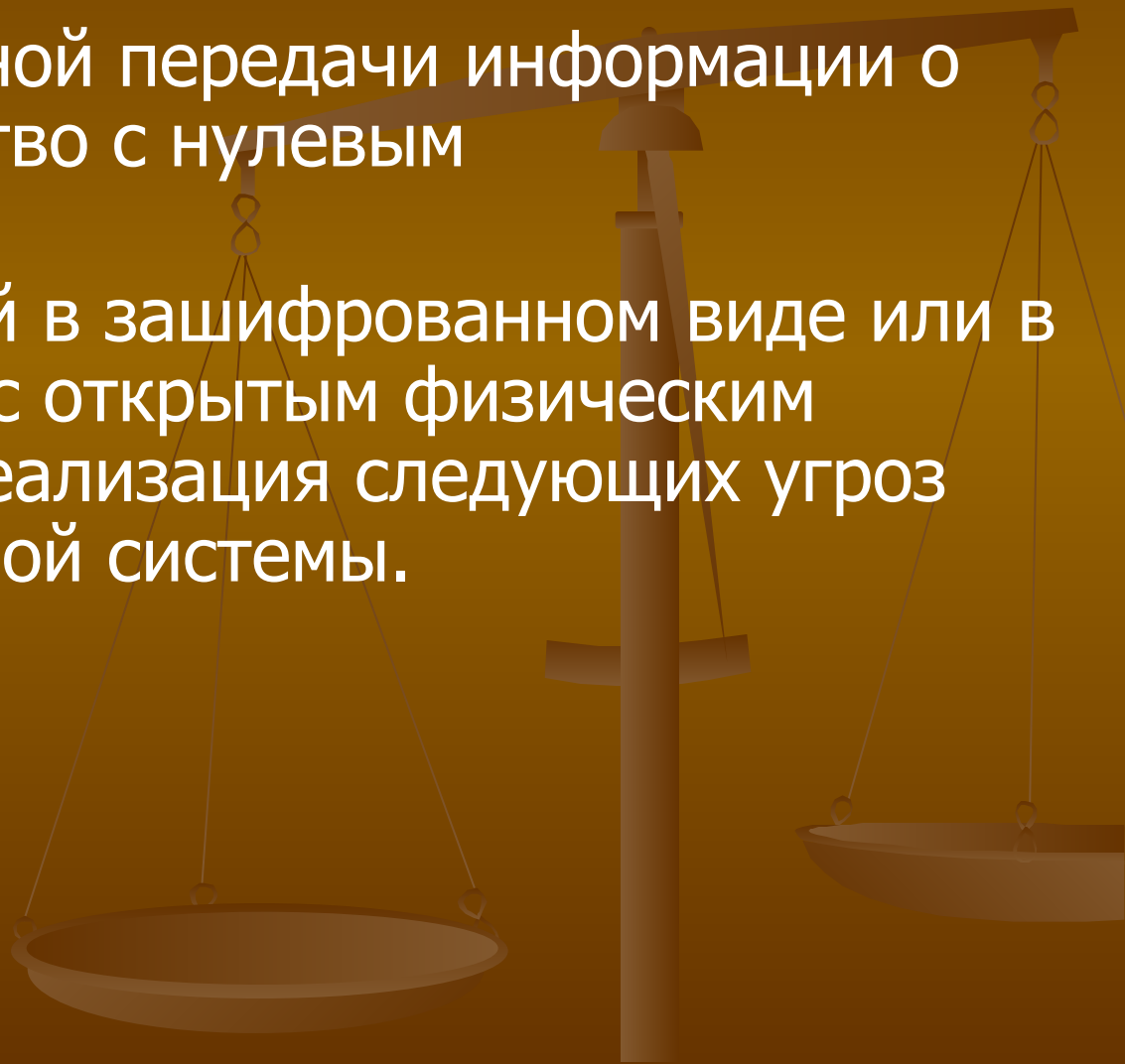
1) в открытом виде; (TELNET, FTP и других)

2) зашифрованными;

3) в виде сверток;

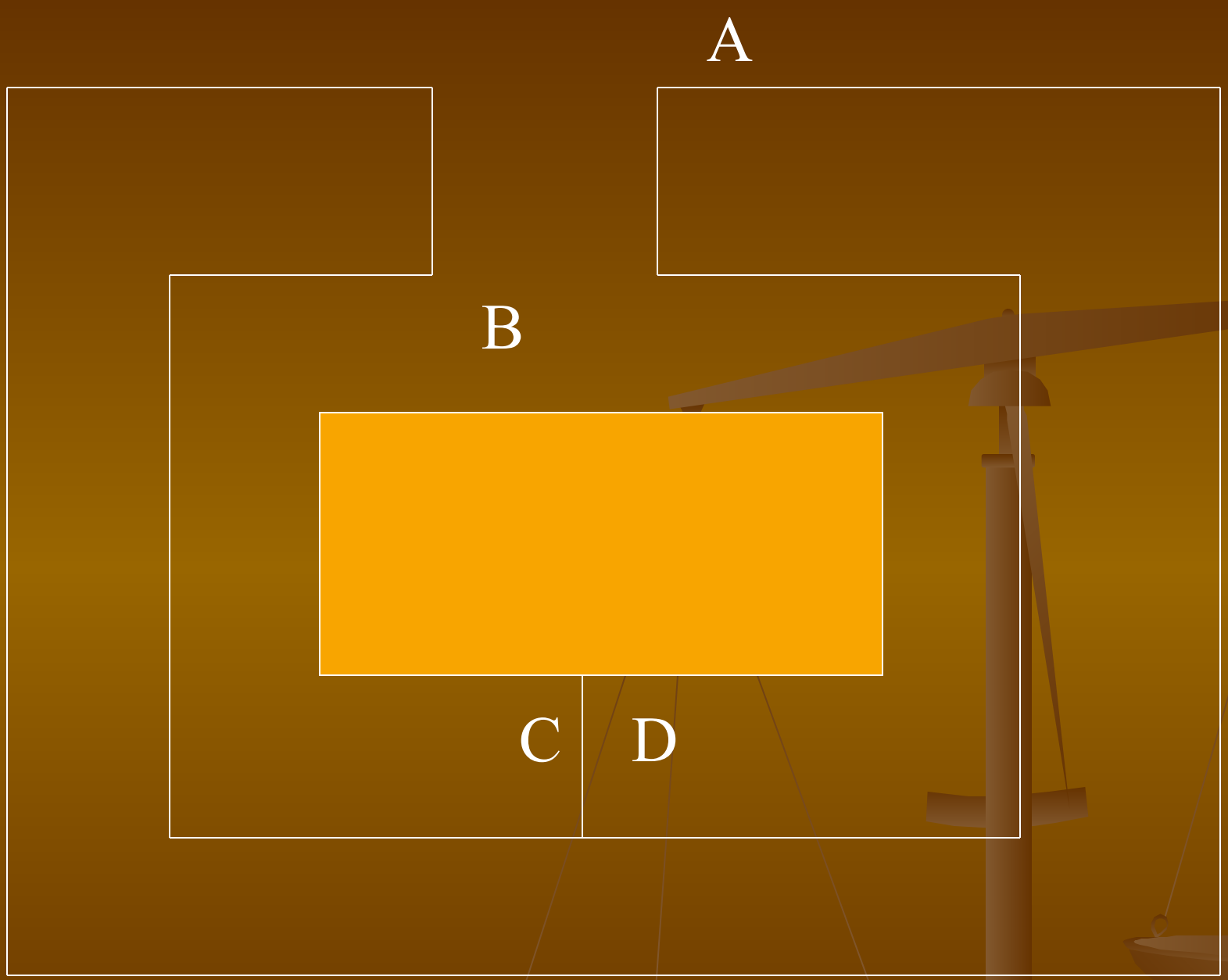
4) без непосредственной передачи информации о пароле (“доказательство с нулевым разглашением”).

При передаче паролей в зашифрованном виде или в виде сверток по сети с открытым физическим доступом возможна реализация следующих угроз безопасности парольной системы.



- - перехват и повторное использование инфор-мации;
- - перехват и восстановление паролей;
- - модификация информации с целью введения в заблуждение проверяющей стороны;
- - имитация злоумышленником действий проверяющей стороны для введения в заблуждение пользователя.
- Схемы с **нулевым разглашением** впервые появи-лись в на рубеже 80-90-х годов. **Идея**: обеспечить возможность одному из пары субъектов доказать истинность некоторого утверждения второму, умал-чивая при этом о содержании самого утверждения.

- Общая схема процедуры **аутентификации с нулевым разглашением** состоит из последовательности информационных обменов (итераций) между двумя участниками процедуры, по завершению которой проверяющий **с заданной вероятностью** делает правильный вывод об истинности проверяемого утверждения. С увеличением числа итераций возрастает вероятность правильного распознавания истинности (или ложности) утверждения.
- Классическим примером неформального описания системы аутентификации с нулевым разглашением служит так называемая пещера АЛИ-БАБЫ.


A
B
C
D

Пещера имеет один вход, путь от которого разветвляется в глубине пещеры на два коридора, сходящихся затем в одной точке, где установлена дверь с замком. Каждый, кто имеет ключ от замка, может переходить из од- ного коридора в другой в любом направлении. Одна итерация алгоритма состоит из последо- вательности шагов:

1. Проверяющий становится в точку A.

2. Доказывающий проходит пещеру и добира- ется до двери (оказывается в точке C или D). Проверяющий не видит, в какой из двух кори- доров тот свернул.

3. Проверяющий приходит в точку B и в соответствии со своим выбором просит доказывающего выйти из определенного коридора.

4.Доказывающий, если нужно, открывает дверь ключом и выходит из названного проверяющим коридора.

Итерация повторяется столько раз, сколько требуется для распознания истинности утверждения «доказывающий владеет ключом от двери» с заданной вероятностью. После i-той итерации вероятность того, что проверяющий попросит доказывающего выйти из того же коридора, в который вошел доказывающий, равна $(1\backslash 2)^i$.

Еще один способ повышения стойкости парольных систем в сети - применение одноразовых **(one-time)** паролей. Общий подход к их применению основан на последовательном использовании **хеш-функции** для вычисления **одноразового пароля на основе предыдущего:**

Вначале пользователь получает упорядоченный список одноразовых паролей, последний из кото-рых также сохраняется в системе аутентификации. При каждой регистрации пользователь вводит очередной пароль, а система вычисляет его свойства и сравнивает с хранимым у себя эталоном.