2. Угрозы информационной безопасности, их классификация. Основные методы реализации угроз, этапы осуществления атаки на информационную систему

ПОНЯТИЕ УГРОЗЫ БЕЗОПАСНОСТИ

С позиции обеспечения безопасности информации в ИВС целесообразно рассматривать в виде трех связных взаимовлияющих друг на друга компонент:

1. информация;
2. технические и программные средства;
3. обслуживающий персонал и пользователи.

Целью создания любой ИВС является удовлетворение потребностей пользователей в своевременном получении достоверной информации и сохранении ее конфиденциальности. При этом задача обеспечения информации должна решаться путем защиты от внешних и внутренних неразрешенных(несанкционированных) воздействий.

Под угрозой обычно понимают потенциально возможно событие, действие(воздействие), процесс или явление, которое может привести к нанесению ущерба чьим-либо интересам. В дальнейшем изложении угрозой информационной безопасности АС будем называть возможность реализации воздействия на информацию, обрабатываемую АС, приводящего к искажению, уничтожению, копированию, блокированию, доступа к информации, а также возможность воздействия на компоненты АС, приводящего к утрате, уничтожению или сбою функционирования носителя информации, средства взаимодействия с носителем или средства его управления.

Утечка информации рассматривается как бесконтрольный и неправомерный выход конфиденциальной информации за пределы организации или круга лиц, которым эта информация была доверена.

Существует три разновидности угроз:

1. Угроза нарушения конфиденциальности заключается в том, что информация становится известной тому, кто не располагает полномочиями доступа к ней. Она имеет место всякий раз, когда получен доступ к некоторой секретной информации, хранящейся в вычислительной системе или передаваемой от одной системы к другой. Иногда, в связи с угрозой нарушения конфиденциальности, используется термин «утечка».

2. Угроза нарушения целостности включает в себя любое умышленное изменение информации, хранящейся в вычислительной системе или передаваемой из одной системы в другую. Когда злоумышленники преднамеренно изменяют информацию, говорится, что целостность информации нарушена. Целостность также будет нарушена, если к несанкционированному изменению приводит случайная ошибка программного или аппаратного обеспечения. Санкционированными изменениями являются те, которые сделаны уполномоченными лицами с обоснованной целью (например, санкционированным изменением является периодическая запланированная коррекция некоторой базы данных).

Целостность информации – существование информации в неискаженном виде (неизменном по отношению к некоторому фиксированному ее состоянию). Чаще субъектов интересует обеспечение более широкого свойства – достоверности информации, которое складывается из адекватности (полноты и точности) отображения состояния предметной области и непосредственно целостности информации, т.е. ее не искаженности.

3. Угроза отказа служб возникает всякий раз, когда в результате преднамеренных действий, предпринимаемых другим пользователем или злоумышленником, блокируется доступ к некоторому ресурсу вычислительной системы. Реально блокирование может быть постоянным – запрашиваемый ресурс никогда не будет получен, или оно может вызывать только задержку запрашиваемого ресурса, достаточно долгую для того чтобы он стал бесполезным. В этих случаях говорят, что ресурс исчерпан.

Доступность информации – свойство системы (среды, средств и технологии обработки), в которой циркулирует информация, характеризующееся способностью обеспечивать своевременный беспрепятственный доступ субъектов к интересующей их

информации и готовность соответствующих автоматизированных служб к обслуживанию поступающих от субъектов запросов всегда, когда в обращении к ним возникает необходимость.

КЛАССИФИКАЦИЯ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Классификация всех возможных угроз информационной безопасности АС может быть проведена по ряду базовых признаков:

1. По природе возникновения.
   1.1. **Естественные угрозы** – угрозы, вызванные воздействиями на АС и ее компоненты объективных физических процессов или стихийных природных явлений, независящих от человека.
   1.2. **Искусственные угрозы** – 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.
   2.2. Угрозы, не связанные с преднамеренными действиями злоумышленников и реализуемые в случайные моменты времени, называют случайными или непреднамеренными.

Реализация угроз этого класса приводит к наибольшим потерям информации (до 80 % ущерба). При этом может происходить уничтожение, нарушение целостности, доступности и конфиденциальности информации, например:

- проявление 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 (неумышленная порча оборудования, удаление, искажение файлов с важной информацией или программ, в том числе системных и т.п.);
- 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.

Угрозы преднамеренного действия, например:

- традиционный или универсальный шпионаж и диверсии (подслушивание, визуальное наблюдение; хищение документов и машинных носителей, хищение программ и атрибутов системы защиты, подкуп и шантаж сотрудников, сбор и анализ отходов машинных носителей, поджоги, взрывы);
- несанкционированный доступ к информации (реализуется посредством отсутствия системы разграничения доступа(СРД), сбоями или отказами технических средств), ошибками в СРД, фальсификацией полномочий);
- побочные электромагнитные излучения и наводки(ПЭМИН);
- несанкционированная модификация структур (алгоритмической, программной, технической);
- информационные инфекции (вредительские программы).

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, источником которых является человек, например:
      3.2.1. внедрение агентов в число персонала системы (в том числе, возможно, и в административную группу, отвечающую за безопасность);

3.2.2. вербовка (путем подкупа, шантажа и т.п.) персонала или отдельных пользователей, имеющих определенные полномочия;
3.2.3. угроза несанкционированного копирования данных пользователем АС;
3.2.4. 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:
3.3.1. запуск технологических программ, способных при некомпетентном пользовании вызывать потерю работоспособности системы (зависания или зацикливания) или необратимые изменения в системе (форматирование или реструктуризацию носителей информации, удаление данных и т.п.);
3.3.2. возникновение отказа в работе операционной системы.

3.4. Угрозы, непосредственным источником которых являются несанкционированные программно-аппаратные средства, например:
3.4.1. нелегальное внедрение и использование неучтенных программ (игровых, обучающих, технологических и других, не являющихся необходимыми для выполнения нарушителем своих служебных обязанностей) с последующим необоснованным расходованием ресурсов (загрузка процессора, захват оперативной памяти и памяти на внешних носителях);
3.4.2. заражение компьютера вирусами с деструктивными функциями.

4. По положению источника угроз.
4.1. Угрозы, источник которых расположен вне контролируемой зоны территории (помещения), на которой находится АС, например:
4.1.1. перехват побочных электромагнитных, акустических и других излучений устройств и линий связи, а также наводок активных излучений на вспомогательные технические средства, непосредственно не участвующие в обработке информации (телефонные линии, сети питания, отопления и т.п.);
4.1.2. 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;
4.1.3. дистанционная фото и видеосъемка.

4.2. Угрозы, источник которых расположен в пределах контролируемой зоны территории(помещения), на которой находится АС, например:
4.2.1. хищение производственных отходов (распечаток, записей, списанных носителей информации и т.п.);
4.2.2. отключение или вывод из строя подсистем обеспечения функционирования вычислительных систем (электропитания, охлаждения и вентиляции, линий связи и т.д.);
4.2.3. применение подслушивающих устройств.

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

4.4. Угрозы, источник которых расположен в АС, например:
4.4.1. проектирование архитектуры системы и технологии обработки данных, разработка прикладных программ, которые представляют опасность для работоспособности системы и безопасности информации;
4.4.2. некорректное использование ресурсов АС.

5. По степени зависимости от активности АС.
5.1. Угрозы, которые могут проявляться независимо от активности АС, например:
5.1.1. вскрытие шифров криптозащиты информации;
5.1.2. хищение носителей информации (магнитных дисков, лент, микросхем памяти, запоминающих устройств и компьютерных систем).

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:
6.2.1. внедрение аппаратных спец вложений, программных «закладок» и «вирусов» («троянских коней» и «жучков»), т.е. таких участков программ, которые не нужны для выполнения заявленных функций, но позволяют преодолеть систему защиты, скрытно и незаконно осуществить доступ к системным ресурсам с целью регистрации и передачи критической информации или дезорганизации функционирования системы;
6.2.2. действия по дезорганизации функционирования системы (изменение режимов работы устройств или программ, забастовка, саботаж персонала, постановка мощных активных радиопомех на частотах работы устройств системы и т.п.);
6.2.3. угроза 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, угрозы несанкционированного доступа в АС).
7.2. Угрозы, которые могут проявляться после разрешения доступа к ресурсам АС (например, угрозы несанкционированного или некорректного использования ресурсов АС).
8. По способу доступа к ресурсам АС.
8.1. Угрозы, направленные на использование прямого стандартного пути доступа к ресурсам АС. Например:
8.1.1. незаконное получение паролей и других реквизитов разграничения доступа (агентурным путем, используя халатность пользователей, подбором, имитацией интерфейса системы и т.д.) с последующей маскировкой под зарегистрированного пользователя(«маскарад»);
8.1.2. несанкционированное использование терминалов пользователей, имеющих уникальные физические характеристики, такие как номер рабочей станции в сети, физический адрес, адрес в системе связи, аппаратный блок кодирования и т.п.
8.2. Угрозы, направленные на использование скрытого нестандартного пути доступа к ресурсам АС, например:
8.2.1. вход в систему в обход средств защиты (загрузка посторонней операционной системы со сменных магнитных носителей и т.п.);
8.2.2. угроза несанкционированного доступа к ресурсам АС путем использования недокументированных возможностей ОС.
9. По текущему месту расположения информации, хранимой и обрабатываемой в АС.
9.1. Угрозы доступа к информации на внешних запоминающих устройства(например, угроза несанкционированного копирования секретной информации с жесткого диска).
9.2. Угрозы доступа к информации в оперативной памяти, например:
9.2.1. чтение остаточной информации из оперативной памяти;
9.2.2. чтение информации из областей оперативной памяти, используемых операционной системой (в том числе подсистемой защиты) или другими пользователями, в асинхронном режиме, используя недостатки мульти задачных АС и систем программирования;
9.2.3. угроза доступа к системной области оперативной памяти со сторон прикладных программ.
9.3. Угрозы доступа к информации, циркулирующей в линиях связи, например:
9.3.1. незаконное подключение к линиям связи с целью работы «между строк» с использованием пауз в действиях законного пользователя от его имени с последующим вводом ложных сообщений или модификацией передаваемых сообщений;

9.3.2. незаконное подключение к линиям связи с целью прямой подмены законного пользователя путем его физического отключения после входа в систему и успешной аутентификации с последующим вводом дезинформации и навязыванием ложных сообщений;

9.3.3. 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, например, угроза записи отображаемой информации на скрытую видеокамеру.

ОСНОВНЫЕ МЕТОДЫ РЕАЛИЗАЦИИ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

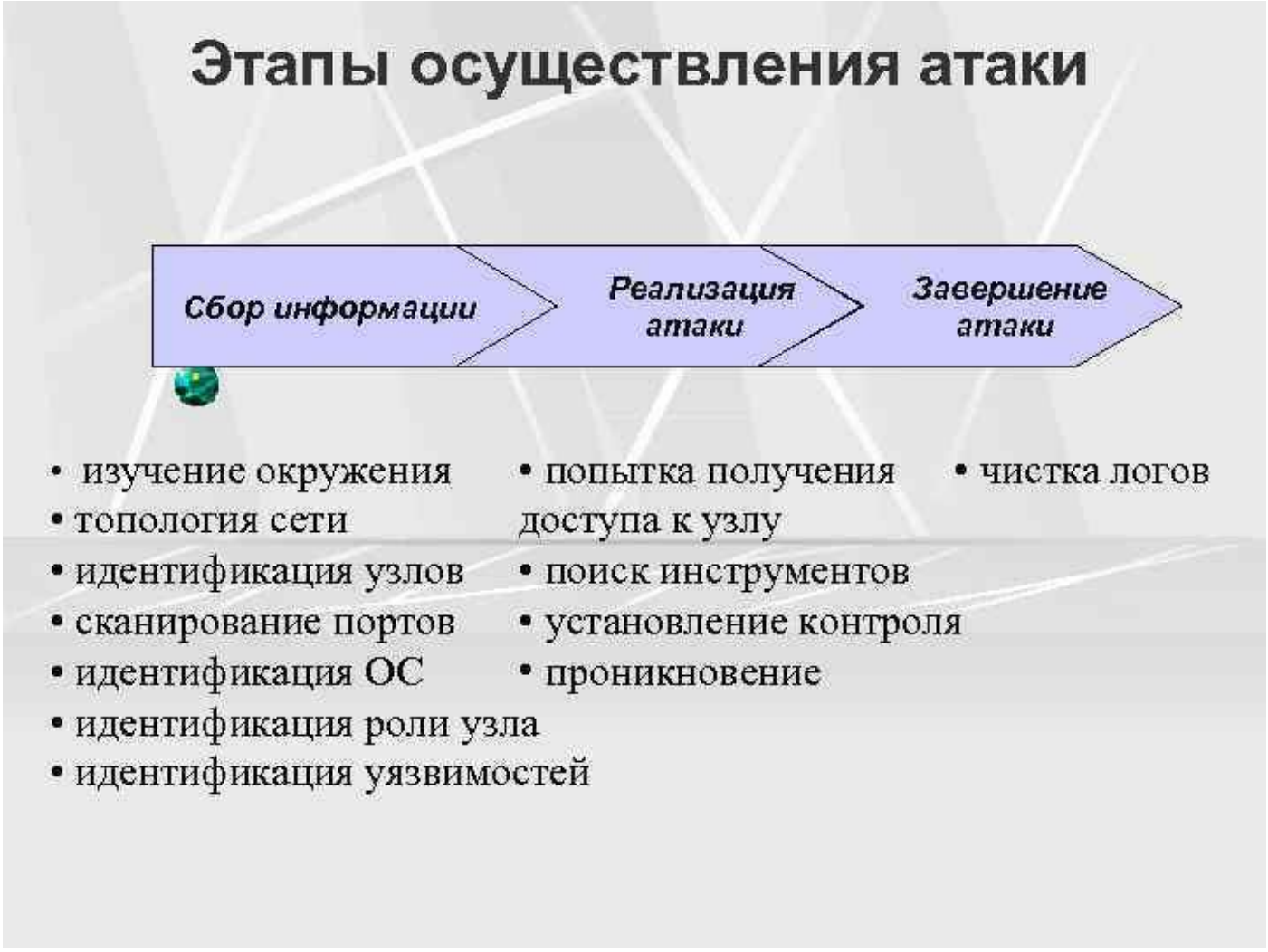
К основным направлениям реализации злоумышленником информационных угроз относятся:

- 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 информационной безопасности;
- внедрение в технические средства АС программных или технических механизмов, нарушающих предполагаемую структуру и функции АС.

К числу основных методов реализации угроз информационной безопасности АС относятся:

- определение злоумышленником типа и параметров носителей информации;
- получение злоумышленником информации о программно-аппаратной среде, типе и параметрах средств вычислительной техники, типе и версии операционной системы, составе прикладного программного обеспечения;
- получение злоумышленником детальной информации о функциях, выполняемых АС;
- получение злоумышленником данных о системах защиты;
- определение способа представления информации;
- определение злоумышленником содержания данных, обрабатываемых в АС, на качественном уровне (мониторинг дешифрования сообщений);
- хищение(копирование) машинных носителей информации, имеющих конфиденциальные данные;
- хищение(копирование) носителей информации;
- использование специальных технических средств для перехвата побочных электромагнитных излучений и наводок (ПЭМИН) – конфиденциальные данные перехватываются злоумышленником путем изменения информативных сигналов из электромагнитного излучения и наводок по цепям питания средств вычислительной техники, входящей в АС;
- уничтожение средств ВТ и носителей информации;
- несанкционированный доступ пользователя к ресурсам АС путем преодоления систем защиты с использованием спецсредств, приемов, методов;
- несанкционированное превышение пользователем своих полномочий;
- несанкционированное копирование программного обеспечения;
- перехват данных, передаваемых по каналам связи;
- визуальное наблюдение – конфиденциальные данные считываются с экранов терминалов, распечаток в процессе их печати и т.п.;
- раскрытие представления информации (дешифрование данных);
- раскрытие содержания информации на семантическом уровне к смысловой составляющей информации, хранящейся в АС;
- уничтожение машинных носителей информации;

- внесение пользователем несанкционированных изменений программно-аппаратные компоненты АС и обрабатываемых данных;
- установка и использование нештатного аппаратного и/или программного обеспечения;
- заражение программными вирусами;
- внесение искажений в представление данных, уничтожение на уровне представления, искажение информации при передаче по линиям связи;
- внедрение дезинформации;
- выведение из строя машинных носителей информации без уничтожения информации (выведение из строя электронных блоков жестких дисков и т.п.);
- проявление ошибок проектирования и разработки аппаратных программных компонентов АС;
- обход(отключение) механизмов защиты – загрузка злоумышленником нештатной операционной системы с дискеты, использование режимов программно-аппаратных компонент АС
- искажение соответствия синтаксических и семантических конструкций языка– установление новых значений слов, выражений и т.п.;
- запрет на использование информации – имеющаяся информация каким-либо причинам не может быть использована.



Подготовительный этап заключается в поиске злоумышленником предпосылок для осуществления той или иной атаки (поиск уязвимостей в системе). На этапе реализации атаки осуществляется использование найденных уязвимостей. На третьем, заключительном, этапе злоумышленник завершает атаку и старается скрыть следы вторжения.