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.

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;

Причины возникновения угроз

- 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.

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 (распечаток, 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), обеспечивающее 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 раскр. парам.:

W- основная система;

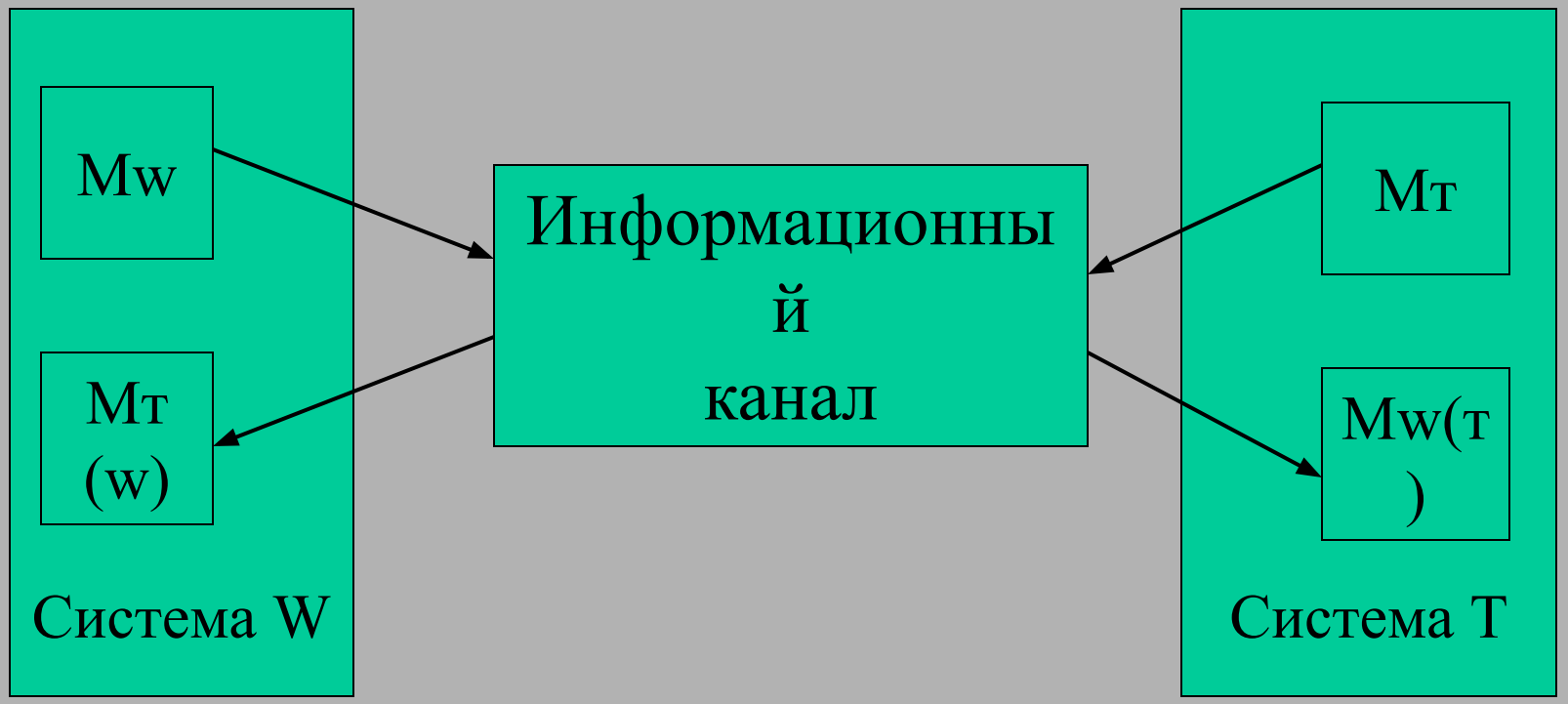
M_W - ее модель, оптимизирующая затраты на управление системой и ее качество;

Объем информационных ресурсов - один из параметров модели (под ИР понимают фактические 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 $M_{T(W)}$ и $M_{W(T)}$.

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 существующих 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, быстродействие ...).

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

6. Защита АС обязательно предусматривает периодический 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 требований 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 распространения 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 .