**анализ защищенности информационной системы**

1)Виды возможных угроз

— содержания (изменение блоков информации, внешнее навязывание ложной информации)

— конфиденциальности (разрушение защиты, уменьшение степени защищенности информации)

— прав собственности на информацию (несанкционированное копирование, использование).

2)Предпосылки появления угроз

— объективные (количественная или качественная недостаточность элементов системы) — не связанные непосредственно с деятельностью людей и вызывающие случайные по характеру происхождения угрозы;

— субъективные — непосредственно связанные с деятельностью человека и вызывающие как преднамеренные (деятельность разведок иностранных государств, промышленный шпионаж, деятельность уголовных элементов и недобросовестных сотрудников), так и непреднамеренные (плохое психофизиологическое состояние, недостаточная подготовка, низкий уровень знаний) угрозы информации.

3)Источники появления угроз

Субъективные преднамеренные.

- Диверсия (организация пожаров, взрывов, повреждений электропитания и др.).

- Непосредственные действия над носителем (хищение, подмена носителей, уничтожение информации).

- Информационное воздействие (электромагнитное облучение, ввод в компьютерные системы разрушающих программных средств, воздействие на психику личности психотропным оружием).

- Субъективные непреднамеренные.

- Отказы обслуживающего персонала (гибель, длительный выход из строя).

- Сбои людей (временный выход из строя).

- Ошибки людей.

- Объективные непреднамеренные.

- Отказы (полный выход из строя) аппаратуры, программ, систем питания и жизнеобеспечения.

- Сбои (кратковременный выход из строя) аппаратуры, программ, систем питания и жизнеобеспечения.

- Стихийные бедствия (наводнения, землетрясения, ураганы).

- Несчастные случаи (пожары, взрывы, аварии).

- Электромагнитная несовместимость.

- Конфиденциальность - способность системы обеспечивать целостность и сохранность информации ее законных пользователей.

4)Рекомендации повышения защищенности ИС

Защищенность является одним из важнейших показателей эффективности функционирования ИС, наряду с такими показателями как надежность, отказоустойчивость, производительность и т. п. Под защищенностью ИС обычно понимается степень адекватности реализованных в ней механизмов защиты информации существующим в данной среде функционирования рискам, связанным с осуществлением угроз безопасности, нарушающих такие свойства информации, как конфиденциальность, целостность и доступность.

Типовая методика включает использование следующих методов:

* Изучение исходных данных по ИС
* Оценка рисков, связанных с осуществлением угроз безопасности в отношении ресурсов ИС
* Анализ механизмов безопасности организационного уровня, политики безопасности организации и организационно-распорядительной документации по обеспечению режима информационной безопасности и оценка их соответствия требованиям существующих нормативных документов, а также их адекватности существующим рискам
* Ручной анализ конфигурационных файлов маршрутизаторов, МЭ и прокси-серверов, осуществляющих управление межсетевыми взаимодействиями, почтовых и DNS серверов, а также других критических элементов сетевой инфраструктуры
* Сканирование внешних сетевых адресов ЛВС из сети Интернет
* Сканирование ресурсов ЛВС изнутри
* Анализ конфигурации серверов и рабочих станций ЛВС при помощи специализированных программных агентов