**Понятия информационных угроз и их виды**

Угроза это потенциальная возможность определенным образом нарушить информационную безопасность, попытка реализации угрозы называется атакой, а тот кто предпринимает такую попытку – злоумышленником. Потенциальные злоумышленники – источники угроз. Чаще всего угроза является следствием наличия уязвимостей в защите информационных систем (например возможность доступа посторонних лиц к критически важному оборудованию или ошибки в ПО).

Промежуток времени от момента, когда появляется возможность использовать слабое место до момента, когда пробел ликвидируется – окно опасности связанным с данным опасным местом, пока существует окно опасности, возможны успешные атаки на ИС. Если речь идет об ошибках В ПО, то окно опасности открывается с появлением средств использования ошибки и ликвидируется с наложением заплат её исправляющих.

Для большинства уязвимых мест окно опасности существует долго от нескольких дней до нескольких недель, поскольку за это время должны произойти след события:

1. должно стать известно о средствах использования пробелов в защите;
2. должны быть выпущены заплаты;
3. заплаты должны быть установлены в защищаемой ИС.

Новые уязвимые места и средства их использования появляются постоянно, это значит:

1. что всегда существуют окна опасности;
2. отслеживание таких окон должно происходить постоянно, а выпуск и наложение заплат – оперативно;

Понятия угроза в разных ситуациях трактуется по разному, на пример для открытой организации угроз конфиденциальности не существует – вся информация общедоступна, однако в большинстве случаев представляется серьезной опасностью, поэтому многое зависит от субъектов информационных отношений.

Угрозы можно классифицировать по нескольким критериям:

1. по аспекту ИБ (доступность, целостность, конфиденциальность) против которых угрозы направленны в первую очередь;
2. по компонентам ИС на которые направлены угрозы (данные, программы, аппаратура, поддерживающая инфраструктура);
3. по способу осуществления (случайные, преднамеренные, действия природного или техногенного характера);
4. по расположению источника угроз (внутри или вне рассматриваемой ИС.

Самыми опасными являются (с точки зрения ущерба) непреднамеренные ошибки штатных пользователей.

По некоторым данным до 65% потерь информации – следствия непреднамеренных ошибок. Радикальным способом борьбы с непреднамеренными ошибками – автоматизация и строгий контроль.

Другие угрозы доступности классифицируем по компонентам ИС на которые нацелены угрозы:

1. внутренний отказ ИС;
2. отказ поддерживающей инфраструктуры;
3. отказ пользователей.

Обычно применительно к пользователям рассматриваются следующие угрозы:

1. не желание работать с ИС (отказ от совершенствования);
2. невозможность работать с системой в силу отсутствия подготовки;
3. невозможность работать с системой в силу отсутствия технической поддержки.

Основными источниками внутренних отказов являются:

1. выход системы из штатного режима эксплуатации в силу случайных или преднамеренных действий пользователей;
2. ошибки при пере конфигурации системы;
3. отказы ПО, АО;
4. отступление от установленных правил эксплуатации;
5. разрушение данных;
6. разрушение/повреждение аппаратуры.

По отношению к поддерживающей инфраструктуры рекомендуется рассматривать угрозы:

1. нарушение работ систем связи, электрики, водо- и теплоснабжения, кондиционирования;
2. разрушение или повреждение помещений;
3. невозможность выполнять обязанности;

**Вредоносное ПО**

Одним из опаснейших способов проведения атак является внедрение вредоносного ПО.

Грани ВПО:

1. вредоносная функция;
2. способ распространения;
3. внешнее представление.

Осуществление разрушительной функции предназначается для:

1. внедрение ВПО;
2. получение контроля над атакуемой системой;
3. агрессивное потребление ресурсов;
4. изменение/разрушение программ или данных.

По механизму распространения ВПО:

1. вирусы – код обладающий способность к распространению, путем внедрения в другие программы;
2. черви – код способный самостоятельно без внедрения в другие программы вызывать распространение своих копий и их выполнение;

Вирусы распространяются локально в пределах узла сети для передачи по сети им требуется внешняя помощь, черви наоборот ориентированы на путешествие по сети.

Окно опасности для вредоносного ПО появляется с выпуском новой разновидности вирусов или червей и перестаёт существовать с обновлением БД антивирусных программ