Угрозы ИБ

Определения

Угроза информационной безопасности – это потенциальная возможность нарушения режима информационной безопасности

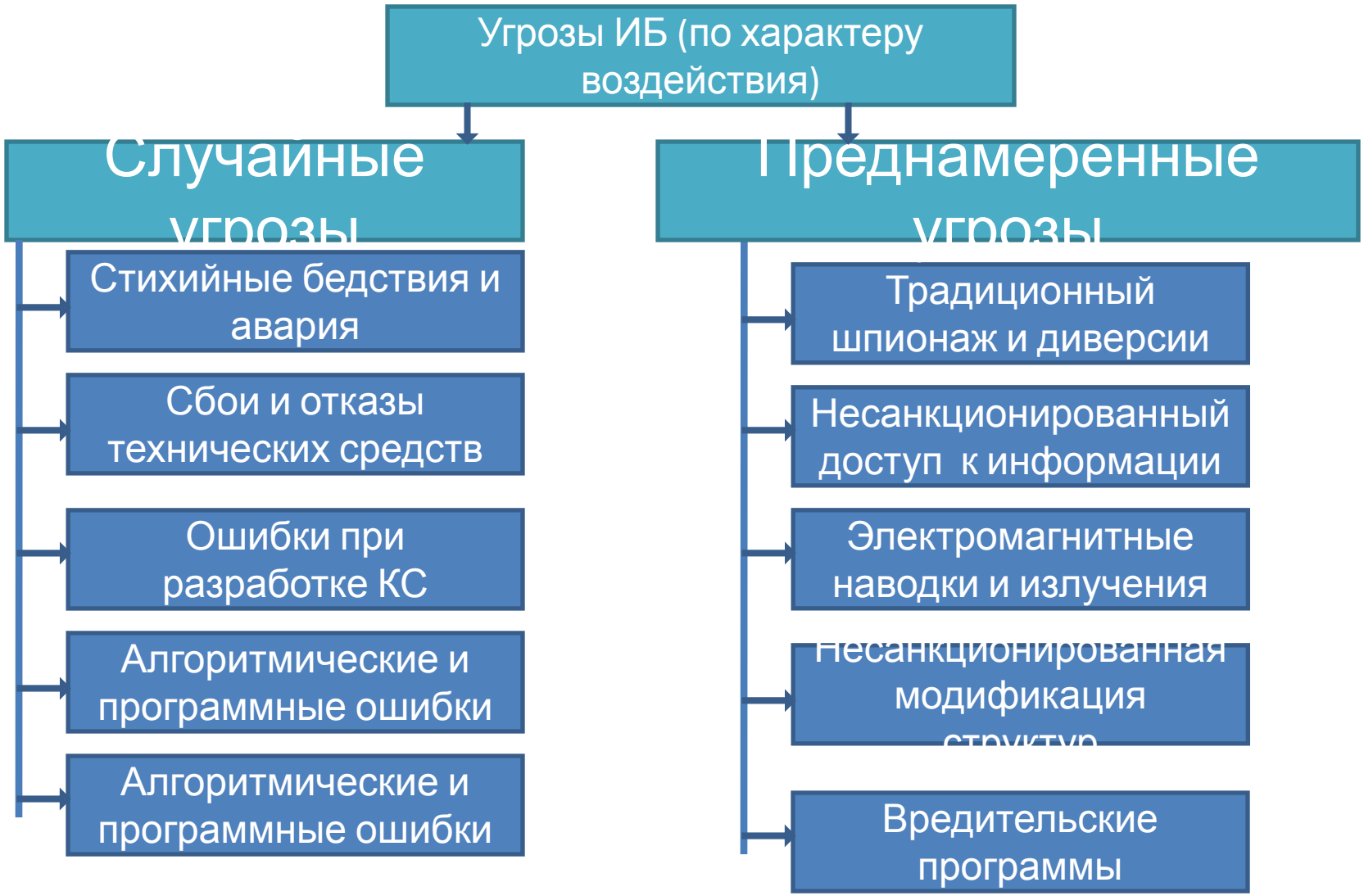
Преднамеренная реализация угрозы называется атакой

Лица, преднамеренно реализующие угрозы, являются злоумышленниками

Угрозы ИБ классифицируются по признакам:

- **По составляющим** ИБ (К, Ц, Д)
- **По компонентам** ИС , на которые угрозы нацелены(данные, программы, аппаратура, персонал)
- **По характеру воздействия** (случайные, преднамеренные)
- **По расположению** источника угроз (внутри или вне информационной системы)

Угрозы по характеру воздействия



Соотношение случайных/преднамеренных

Случайные угрозы

- **Стихийные бедствия и аварии** - наиболее разрушительны для КС (компьютерных систем)
- **Сбои и отказы сложных систем неизбежны**. В результате нарушается работоспособность технических средств, уничтожаются и искажаются данные и программы. Возможны нарушения конфиденциальности информации
- **Ошибки при разработке КС, алгоритмические и программные ошибки.** Могут использоваться злоумышленниками для воздействия на ресурсы КС. Особую опасность представляют ошибки в ОС и программных средствах защиты информации

Случайные угрозы

- **Ошибки пользователей и обслуживающего персонала** (65% всех случайных угроз)- некомпетентное, небрежное или невнимательное выполнение функциональных обязанностей. аиболее разрушительны для КС (компьютерных систем) Возможны нарушения конфиденциальности, целостности , а также компрометации механизмов защиты

Случайные угрозы. Вывод

Изучены достаточно хорошо, накоплен значительный опыт противодействия этим угрозам

Преднамеренные угрозы

Данный класс изучен недостаточно, очень динамичен и постоянно пополняется новыми угрозами

Традиционный шпионаж и диверсии

- Подслушивание
- Визуальное наблюдение
- Хищение документов и магнитных носителей
- Хищение программ и атрибутов системы защиты
- Подкуп и шантаж сотрудников
- Сбор и анализ отходов машинных носителей информации
- Поджоги
- Взрывы

Подслушивание

- До 1 км с помощью отраженного луча лазера от стекла окна помещения
- 50-100 м с помощью сверхчувствительных направленных микрофонов
- Съем информации возможен также со стекол, металлоконструкций зданий, труб водоснабжения и отопления
- Аудиоинформация может быть получена также пктем высокочастотного навязывания (воздействие электромагнитным полем или электрическими сигналами на элементы, способные модулировать эти поля)
- Прослушивание каналов связи (телефонных, радиоканалы)

Видеоразведка

- Видеоразведка для получения информации малопригодна и носит вспомогательный характер. В основном служит для выявления режимов работы и расположения механизмов защиты.

Закладные устройства

- Для КС (компьютерных систем) наиболее вероятными являются закладные устройства или **«жучки».**
- Закладные устройства делятся **на проводные и излучающие**
- **Проводные устройства** требуют значительного времени на установку и имеют существенный **демаскирующий признак – провода**
- Излучающие **«закладки»** («радиозакладки») быстро устанавливаются, но также имеют демаскирующий признак - **излучение в** радио или **оптическом диапазоне**
- Наиболее распространение получили **акустические «радиозакладки»**. Они воспринимают акустический сигнал, преобразуют его в электрический и передают в виде радиосигнала на дальность до 8 км. На **практике 90% радиозакладок работают в диапазоне 50-800м**.

НСД к информации

- **Определение**: **Несанкционированный доступ (НСД)** к информации – доступ к информации, **нарушающий правила разграничения доступа** с использованием штатных средств вычислительной техники или автоматизированных систем

НСД к информации **возможен только** с использованием штатных аппаратных и программных средств **в следующих случаях**:

- отсутствует система разграничения доступа
- сбой или отказ в КС
- ошибочные действия пользователей или обслуживающего персонала
- Ошибки в СРД
- **Фальсификация полномочий (наиболее вероятный канал НСД)**

Электромагнитные излучения и наводки (ПЭМИН)

- Процесс обработки и передачи информации техническими средствами КС сопровождается электромагнитными излучениями в окружающее пространство и **наведением электрических сигналов в линиях связи, сигнализации, заземления** и других проводниках. Они получили название побочных электромагнитных излучений и наводок **(ПЭМИН)**
- С помощью спец. оборудования сигналы принимаются, выделяются, усиливаются и могут либо просматриваться, либо записываться в запоминающих устройствах.
- Наибольший уровень электромагнитного излучения присущ устройствам на ЭЛТ(электронно-лучевых трубках). Дальность удовлетворительного приема до 50м.
- Электромагнитные излучения используются злоумышленниками **не только для получения информации, но и для ее уничтожения**

Несанкционированная модификация структур

- Несанкционированная модификация структур (программных, алгоритмических,технических) может осуществляться на любом жизненном цикле КС.
- **Несанкционированное изменение структуры** КС на этапе разработки и модернизации получило название **«закладка»**
- В процессе разработки КС «закладки» внедряются , как правило, **в специализированные системы**, предназначенные для эксплуатации в какой-либо фирме или государственных учреждениях.
- В универсальные КС «закладки» внедряются реже, в основном для дискредитации таких систем конкурентом

Вредительские программы

- В зависимости от механизма действия вредительские программы деляться на 4 класса:

- Логические бомбы
- Черви
- Троянские кони
- Компьютерные вирусы

Классификация злоумышленников

- Оцениваются возможности осуществления вредительских воздействий на КС. Злоумышленником может быть:
- Разработчик КС
- Сотрудник из числа обслуживающего персонала
- Пользователь
- Постороннее лицо

Наибольший вред могут нанести **работники службы безопасности** информации, далее идут **системные программисты, прикладные программисты и инженерно-технический персонал**