

Угроза безопасности данных

Выполнил Зайнуллин Богдан ИБ

31-19

Угроза – это потенциальная возможность определенным образом нарушить информационную безопасность.

Попытка реализации угрозы называется **атакой**, а тот, кто предпринимает такую попытку, – **злоумышленником**. Потенциальные злоумышленники называются **источниками угрозы**.

Чаще всего угроза является следствием наличия **уязвимых** мест в защите информационных систем (таких, например, как возможность доступа посторонних лиц к критически важному ошибке в программном



УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

СВОЙСТВА УГРОЗЫ

Избирательность

нацеленность угрозы на нанесение вреда тем или иным конкретным свойствам объекта безопасности

Предсказуемость

наличие признаков возникновения, позволяющих прогнозировать возможность появления угрозы и определять конкретные объекты безопасности, на которые она будет направлена

Вредоносность

возможность нанесения вреда различной тяжести объекту безопасности

- **Цель деятельности по обеспечению безопасности:** ликвидация угроз объектам информационной безопасности и минимизация возможного ущерба, который может быть нанесен вследствие реализации данных угроз.

Основные определения и критерии классификации угроз

Чаще всего угроза является следствием наличия **уязвимых мест** в защите информационных систем

Для большинства **уязвимых мест** *окно опасности* существует сравнительно долго, поскольку за это время должны произойти **следующие события**:

- должно стать известно о средствах использования пробела в защите;
- должны быть выпущены соответствующие заплаты;
- заплаты должны быть установлены в защищаемой ИС.

Основные определения и критерии классификации угроз

Для характеристики **угрозы информационной безопасности** используются следующие **параметры**:

- Источник угрозы.
- Метод воздействия на объект.
- Уязвимости, которые могут быть использованы.
- Ресурсы, которые могут пострадать от реализации.

Основные определения и критерии классификации угроз

Угроза безопасности информации –

совокупность условий и факторов, создающих потенциальную или реально существующую опасность, в результате которой возможны утечка информации, неправомерное модифицирование (искажение, подмена), уничтожение информации или неправомерное блокирование доступа к ней

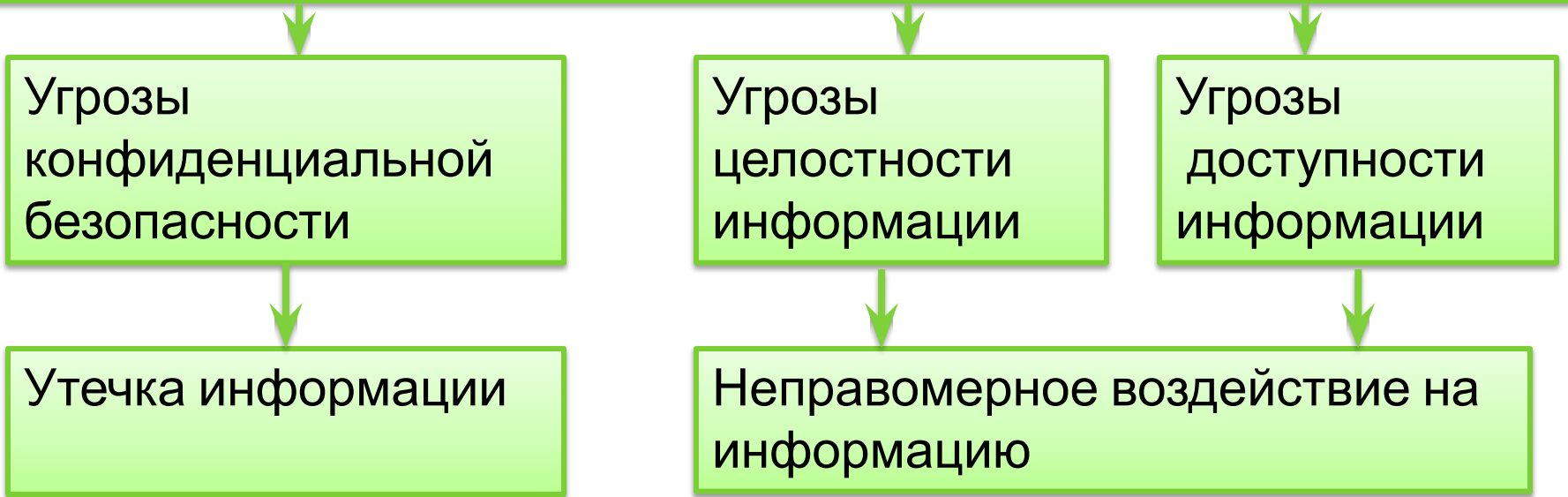
Угрозы
конфиденциальной
безопасности

Утечка информации

Угрозы
целостности
информации

Неправомерное воздействие на
информацию

Угрозы
доступности
информации



КЛАССИФИКАЦИЯ УГРОЗ

Угрозы

По характеру ущерба	Расположение источника	По характеру воздействия	По величине ущерба
Материальный Моральный	Внутренние Внешние	Активные Пассивные	Предельный Значительный Незначительный

Наиболее распространенные угрозы доступности

Самыми частыми и самыми опасными (с точки зрения размера ущерба) являются ***непреднамеренные ошибки штатных пользователей***, операторов, системных администраторов и других лиц, обслуживающих информационные системы.

Основной способ борьбы с непреднамеренными ошибками - максимальная автоматизация и строгий контроль.

Наиболее распространенные угрозы доступности

Опасны так называемые **сотрудники** - нынешние и бывшие.

Как правило, они стремятся нанести вред организации-"обидчику", например:

- испортить оборудование;
- встроить логическую бомбу, которая со временем разрушит программы и/или данные;
- удалить данные.

Необходимо следить за тем, чтобы при увольнении сотрудника его права доступа (логического и физического) к информационным ресурсам аннулировались.

1) Кражи и подлоги

С целью нарушения **статической целостности** **злоумышленник** (как правило, штатный сотрудник) может:

- ввести неверные данные;
- изменить данные.

2) Внедрение вредоносного ПО

Угрозами динамической целостности являются переупорядочение, кража, дублирование данных или внесение дополнительных сообщений (сетевых пакетов и т.п.).

Соответствующие действия в сетевой среде

Основные угрозы конфиденциальности

Угрозы конфиденциальности информации могут носить **некомпьютерный и вообще нетехнический характер.**

- 1. Неправильное хранение данных на резервных носителях.**
- 2. Перехват данных** (данные передаются по многим каналам, их защита может оказаться весьма сложной и дорогостоящей)
- 3. Злоупотребление полномочиями.**