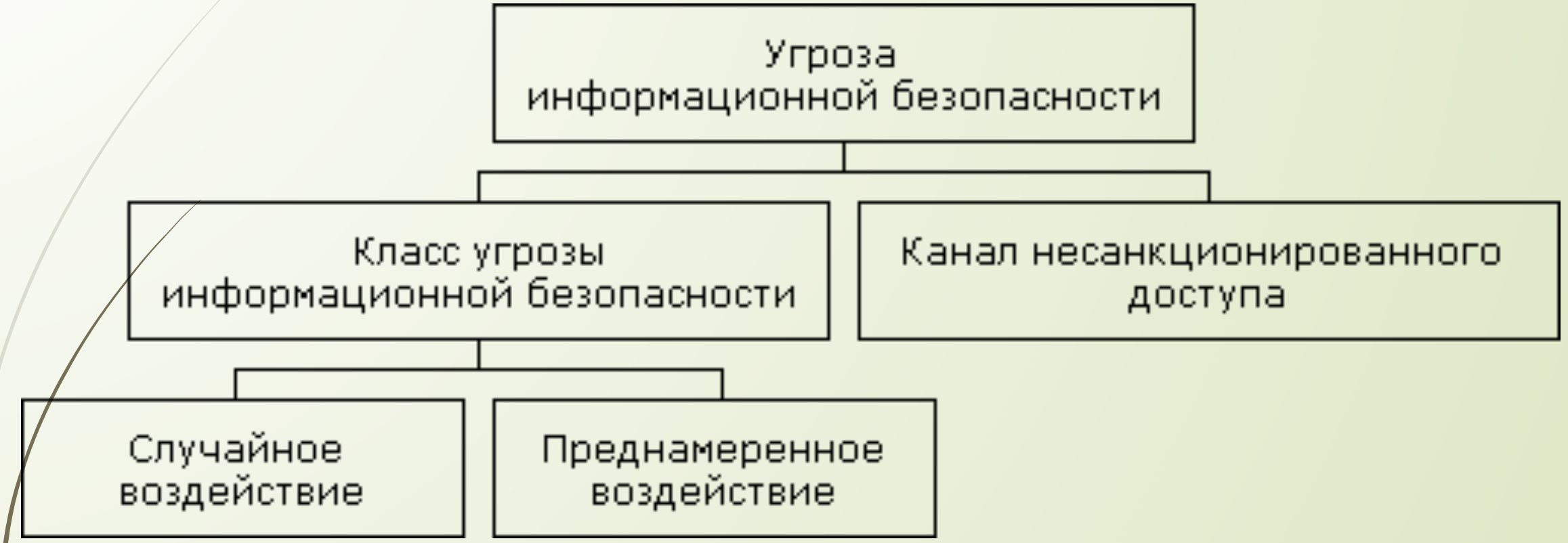
Тема 7: Классификация угроз "информационной безопасности"

Классы угроз информационной безопасности

- **Угроза информационной безопасности** – это потенциальная возможность нарушения режима информационной безопасности. Преднамеренная реализация угрозы называется **атакой** на информационную систему. Лица, преднамеренно реализующие угрозы, являются **злоумышленниками**.
- Чаще всего угроза является следствием наличия уязвимых мест в защите информационных систем, например, неконтролируемый доступ к персональным компьютерам или нелицензионное программное обеспечение (к сожалению даже лицензионное программное обеспечение не лишено уязвимостей).

- Угрозы информационной безопасности классифицируются по нескольким признакам:
- **по составляющим информационной безопасности** (доступность, целостность, конфиденциальность), против которых, в первую очередь, направлены угрозы;
- **по компонентам информационных систем**, на которые угрозы нацелены (данные, программы, аппаратура, персонал);
- **по характеру воздействия** (случайные или преднамеренные, действия природного или техногенного характера);
- **по расположению источника угроз** (внутри или вне рассматриваемой информационной системы).

Все виды угроз, классифицируемые по другим признакам



По характеру воздействия угрозы делятся на случайные и преднамеренные

- Причинами *случайных воздействий* при эксплуатации могут быть:
- аварийные ситуации из-за стихийных бедствий и отключений электропитания (природные и техногенные воздействия);
- отказы и сбои аппаратуры;
- ошибки в программном обеспечении;
- ошибки в работе персонала;
- помехи в линиях связи из-за воздействий внешней среды.

- ***Преднамеренные воздействия*** – это целенаправленные действия злоумышленника. В качестве злоумышленника могут выступать служащий, посетитель, конкурент, наемник. Действия нарушителя могут быть обусловлены разными мотивами, например:
- недовольством служащего служебным положением;
- любопытством;
- конкурентной борьбой;
- уязвленным самолюбием и т. д.

- Угрозы, классифицируемые **по расположению источника угроз**, бывают внутренние и внешние.
- *Внешние угрозы* обусловлены применением вычислительных сетей и создание на их основе информационных систем.
- Основная особенность любой вычислительной сети состоит в том, что ее компоненты распределены в пространстве. Связь между узлами сети осуществляется физически с помощью сетевых линий и программно, с помощью механизма сообщений. При этом управляющие сообщения и данные, пересылаемые между узлами сети, передаются в виде пакетов обмена. Особенность данного вида угроз заключается в том, что местоположение злоумышленника изначально неизвестно.

Каналы несанкционированного доступа к информации

- Одним из наиболее распространенных и многообразных способов воздействия на информационную систему, позволяющим нанести ущерб любой из составляющих информационной безопасности является **несанкционированный доступ**. Несанкционированный доступ возможен из-за ошибок в системе защиты, нерационального выбора средств защиты, их некорректной установки и настройки.

- **Каналы НСД** классифицируются по компонентам автоматизированных информационных систем:

Через человека:

- хищение носителей информации;
- чтение информации с экрана или клавиатуры;
- чтение информации из распечатки.

Через программу:

- перехват паролей;
- расшифровка зашифрованной информации;
- копирование информации с носителя.

Через аппаратуру:

- подключение специально разработанных аппаратных средств, обеспечивающих доступ к информации;
- перехват побочных электромагнитных излучений от аппаратуры, линий связи, сетей электропитания и т. д.

Составляющие информационной безопасности