ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ. ВИДЫ ВОЗМОЖНЫХ УГРОЗ.

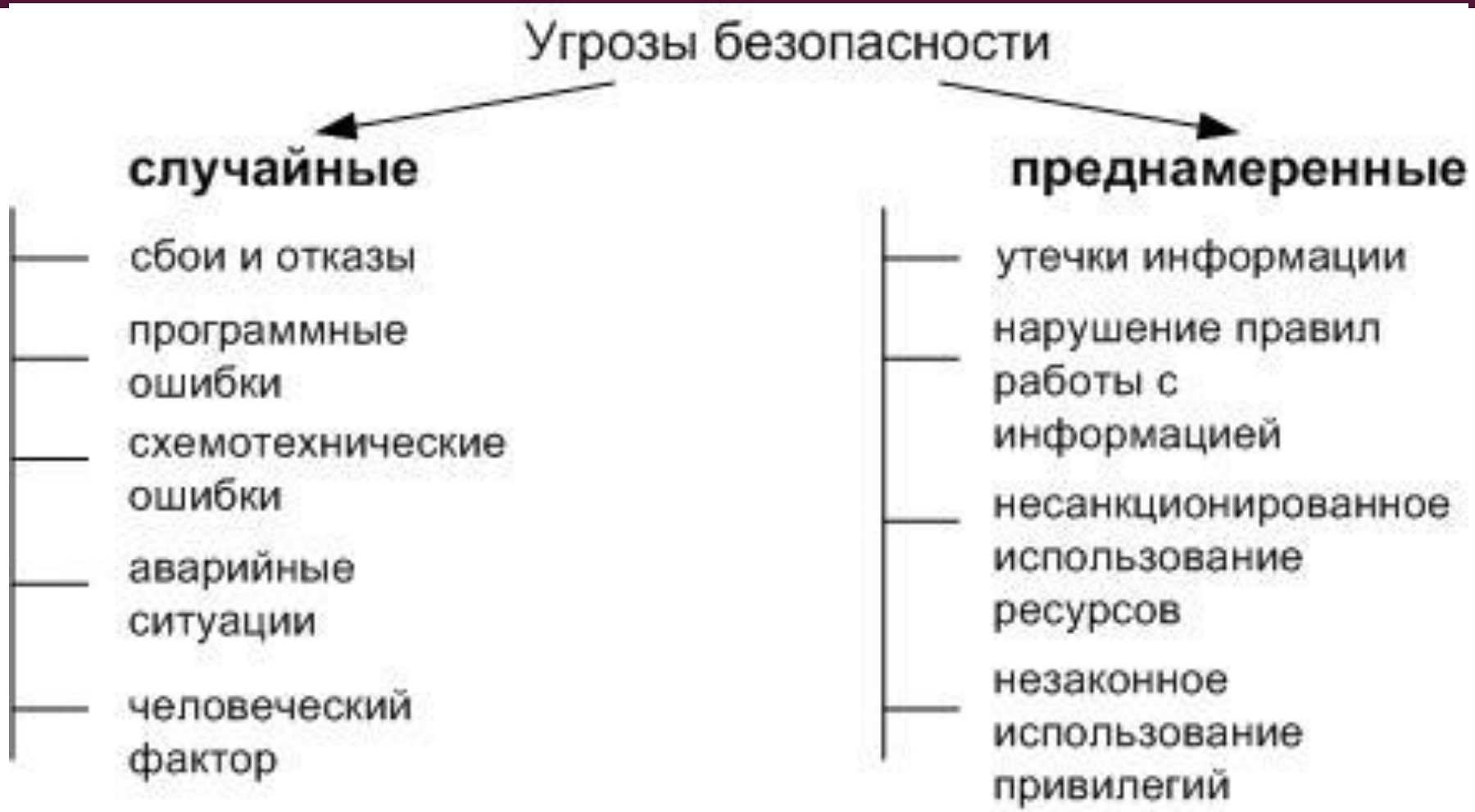
ОСНОВНОЕ ПОНЯТИЕ

Информационная безопасность – это защита информации от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести ущерб ее владельцу или пользователю.

ОСНОВНЫЕ ПРИНЦИПЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

1. **Целостность данных** - такое свойство, в соответствии с которым информация сохраняет свое содержание и структуру в процессе ее передачи и хранения. Создавать, уничтожать или изменять данные может только пользователь, имеющий право доступа.
2. **Конфиденциальность** — свойство, которое указывает на необходимость ограничения доступа к конкретной информации для обозначенного круга лиц. Таким образом, конфиденциальность дает гарантию того, что в процессе передачи данных, они могут быть известны только авторизованным пользователям
3. **Доступность информации** - это свойство характеризует способность обеспечивать своевременный и беспрепятственный доступ полноправных пользователей к требуемой информации.
4. **Достоверность** – данный принцип выражается в строгой принадлежности информации субъекту, который является ее источником или от которого она принята.

ВИДЫ ИНФОРМАЦИОННЫХ УГРОЗ



ИСТОЧНИКИ УГРОЗ

- *Угрозы, источник которых находятся вне контролируемой группы компьютерной системы (пример – перехват данных, передаваемых по каналам связи)*
- *Угрозы, источник которых – в пределах контролируемой зоны системы (это может быть хищение носителей информации)*
- *Угрозы, находящиеся непосредственно в самой системе (например, некорректное использование ресурсов).*

Угрозы способны по-разному воздействовать на компьютерную систему. Это могут быть **пассивные воздействия**, реализация которых не влечет за собой изменение структуры данных (например, копирование). **Активные угрозы** — это такие, которые, наоборот, меняют структуру и содержание компьютерной системы (внедрение специальных программ).

В соответствии с разделением угроз **по этапам доступа пользователей или программ к ресурсам системы** существуют такие опасности, которые проявляются на этапе доступа к компьютеру и обнаружимые после разрешения доступа (несанкционированное использование ресурсов).

Классификация **по месту расположения в системе** подразумевает деление на три группы: угрозы доступа к информации, находящейся на внешних запоминающих устройствах, в оперативной памяти и к той, что циркулирует в линиях связи.

Случайными, или **непреднамеренными** называются такие угрозы, которые не связаны с действиями злоумышленников. Механизм их реализации изучен достаточно хорошо, поэтому существуют разработанные методы противодействия.

Выделяют также **преднамеренные угрозы**, которые связаны с целенаправленными действиями нарушителя. Изучение этого класса затруднено, так как он имеет очень динамичный характер и постоянно пополняется новыми видами угроз. Выделяют также **преднамеренные угрозы**, которые связаны с целенаправленными действиями нарушителя. Изучение этого класса затруднено, так как он имеет очень динамичный характер и постоянно пополняется новыми видами угроз.

СПЕЦИАЛЬНЫЕ ВРЕДОНОСНЫЕ ПРОГРАММЫ

- **«компьютерные вирусы»** — это небольшие программы, способные самостоятельно распространятся после внедрения в компьютер путем создания своих копий. При определенных условиях вирусы оказывают негативное воздействие на систему;
- **«черви»** – утилиты, которые активируются при каждой загрузке компьютера. Они обладают способностью перемещаться в пределах системы или сети и размножаться аналогично вирусам. Лавинообразное размножение программ приводит к перегрузке каналов связи, памяти, а затем к блокировке работы;
- **«троянские кони»** — такие программы «скрываются» под видом полезного приложения, а, на самом деле, наносят вред компьютеру: разрушают программное обеспечение, копируют и пересылают злоумышленнику файлы с конфиденциальной информацией и т.д.

Спасибо за внимание!!!