

**Абдулханов Хамзат**

**П-20**

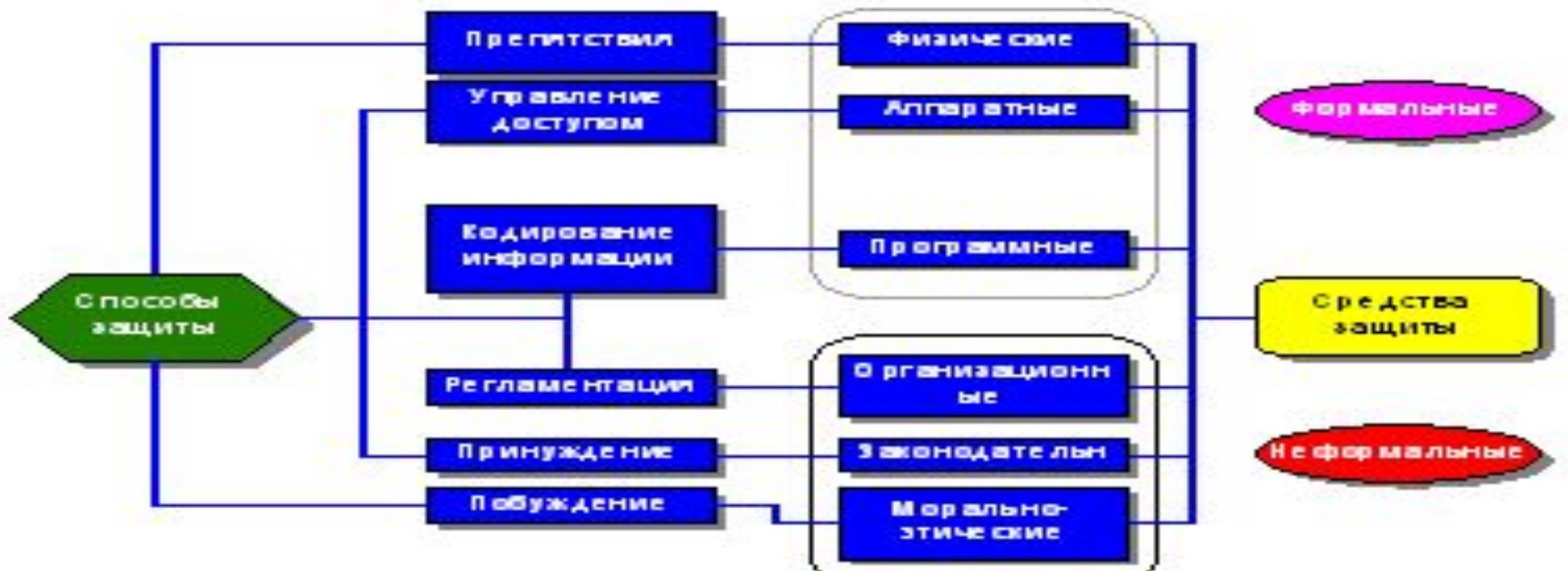
# Пути и методы защиты информации в локальных сетях:

- 
- Архитектура ЛС и технология ее функционирования позволяет злоумышленнику находить или специально создавать лазейки для скрытого доступа к информации, причем многообразие и разнообразие даже известных фактов злоумышленных действий дает достаточные основания предполагать, что таких лазеек существует или может быть создано много.

# Средства и способы защиты информации

- Для решения проблемы защиты информации основными средствами, используемыми для создания механизмов защиты принято считать:
  - 1. Технические средства - реализуются в виде электрических, электромеханических, электронных устройств. Технические средства подразделяются.

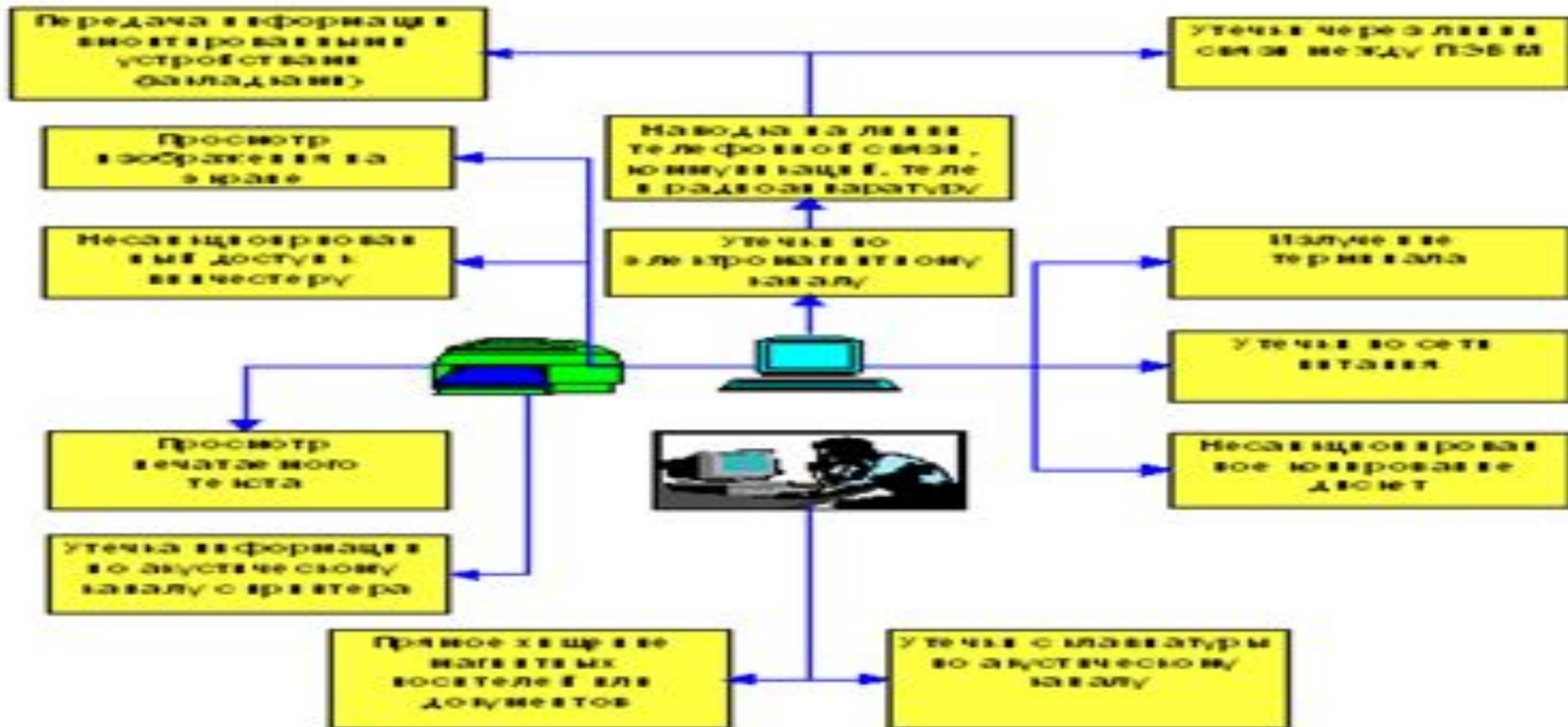
# Способы защиты информации



# Анализ методов защиты информации в ЛС

- 
- Обеспечение надежной защиты информации предполагает:
- Обеспечение безопасности информации в ЛС это есть процесс непрерывный, заключающийся в систематическом контроле защищенности, выявлении узких и слабых мест в системе защиты, обосновании и реализации наиболее рациональных путей совершенствования и развития системы защиты.

# Основные каналы утечки информации при ее обработке на ПЭВМ



# .1 Меры непосредственной защиты ПЭВМ

- Важным аспектом всестороннего подхода к защите ЭВМ являются меры защиты вычислительных устройств от прямых угроз, которые можно разбить на две категории:
- Меры защиты от стихийных бедствий.
- Меры защиты от злоумышленников.
- Наиболее опасным из стихийных бедствий можно считать пожар. Соблюдение элементарных пожарных норм позволяет решить эту проблему. Наиболее важен и интересен второй пункт.

## 2.2 Идентификация и установление личности

- Так как функционирование всех механизмов ограничения доступа, использующих аппаратные средства или средства математического обеспечения основано на предположении, что пользователь представляет собой конкретное лицо, то должен существовать некоторый механизм установления его подлинности. Этот механизм может быть основан на выявлении того, что знает только данный пользователь или имеет при себе, или на выявлении некоторых особенностей самого пользователя.

# Типы разрушающих программных средств



# Заключение

- 
- В ближайшее время прогресс в области развития средств вычислительной техники, программного обеспечения и сетевых технологий даст толчок к развитию средств обеспечения безопасности, что потребует во многом пересмотреть существующую научную парадигму информационной безопасности. Основными положениями нового взгляда на безопасность должны являться: