## 8.3. Методы и средства обеспечения безопасности информации

Методы и средства обеспечения безопасности информации в автоматизированных информационных технологиях. К ним относятся: **препятствие, управление доступом, маскировка, регламентация, принуждение, побуждение.**

Методы защиты информации представляют собой основу механизмов защиты.

**Препятствие** - метод физического преграждения пути злоумышленнику к защищаемой информации (к аппаратуре, носителям информации и т. д.).

**Управление доступом** - метод защиты информации с помощью использования всех ресурсов информационной технологии. Управление доступом включает следующие функции защиты:

- идентификация специалистов, персонала и ресурсов информационной технологии (присвоение каждому объекту персонального идентификатора);
- опознание (установление подлинности) объекта или субъекта по предъявленному им идентификатору;
- проверка полномочий (соответствие дня недели, времени суток, запрашиваемых ресурсов и процедур установленному регламенту);
- разрешение и создание условий работы в пределах установленного регламента;
- регистрация (протоколирование) обращений к защищаемым ресурсам;
- реагирование (сигнализация, отключение, задержка работ, отказ в запросе) при попытке несанкционированных действий.

**Маскировка** - метод защиты информации путем ее криптографического закрытия. Этот метод сейчас широко применяется как при обработке, так и при хранении информации, в том числе на дискетах. При передаче информации по каналам связи большой протяженности данный метод является единственно надежным.

**Регламентация** - метод защиты информации, создающий по регламенту в информационных технологиях такие условия автоматизированной обработки, хранения и передачи защищаемой информации, при которых возможности несанкционированного доступа к ней сводились бы к минимуму.

**Принуждение** - метод защиты, когда специалисты и персонал информационной технологии вынуждены соблюдать правила обработки, передачи и использования защищаемой информации под угрозой материальной, административной или уголовной ответственности.

**Побуждение** - метод защиты, побуждающий специалистов и персонал автоматизированной информационной технологии не разрушать установленные порядки за счет соблюдения сложившихся моральных и этических норм.

Рассмотренные методы обеспечения безопасности в информационных технологиях реализуются на практике за счет применения различных средств защиты.

Все средства защиты информации делятся на следующие виды:

| | |
|---|---|
| **Формальные средства защиты** - это средства, выполняющие защитные функции строго по заранее предусмотренной процедуре непосредственного участия человека | **Неформальные средства защиты** - это средства защиты, которые определяются целенаправленной деятельностью человека, либо регламентируют эту деятельность |

К основным формальным средствам защиты, которые используются в информационных технологиях для создания механизмов защиты, относятся следующие:

**Технические средства** реализуются в виде электрических, электромеханических и электронных устройств. Все технические средства делятся на следующие виды:

| | |
|---|---|
| Аппаратные, представляющие собой устройства, встраиваемые непосредственно в вычислительную технику, или устройства, которые сопрягаются с подобной аппаратурой по стандартному интерфейсу | Физические, представляющие собой автономные устройства и системы, создающие физические препятствия для злоумышленников (замки, решетки, охранная сигнализация и т. д.) |

Программные средства представляют собой программное обеспечение, специально предназначенное для выполнения функций защиты информации.

К основным неформальным средствам защиты относятся:

**Организационные средства.** Представляют собой организационно-технические и организационно-правовые мероприятия, осуществляемые в процессе создания и эксплуатации вычислительной техники, аппаратуры телекоммуникаций для обеспечения защиты информации в информационных технологиях. Организационные мероприятия охватывают все структурные элементы аппаратуры на всех этапах их жизненного цикла (строительство и оборудование помещений экономического объекта, проектирование информационной технологии, монтаж и наладка оборудования, испытания, эксплуатация и т. д.).

**Морально-этические средства.** Реализуются в виде всевозможных норм, которые сложились традиционно или складываются по мере распространения вычислительной техники и средств связи. Эти нормы большей частью не являются обязательными как законодательные меры, однако несоблюдение их ведет к утечке информации и нарушению секретности.

**Законодательные средства** определяются законодательными актами страны, в которых регламентируются правила пользования, обработки и передачи информации ограниченного доступа и устанавливаются меры ответственности за нарушения этих правил.