**5. Организационные меры по защите информации**

**Организационно-административные методы защиты информации**

Они регламентируют процессы создания и эксплуатации информационных объектов, а также взаимодействие пользователей и систем таким образом, чтобы несанкционированный доступ к информации становился либо невозможным, либо существенно затруднялся.

Организационно-административные методы защиты информации охватывают все компоненты автоматизированных информационных систем на всех этапах их жизненного цикла: проектирования систем, строительства зданий, помещений и сооружений, монтажа и наладки оборудования, эксплуатации и модернизации систем. К организационно-административным мероприятиям защиты информации относятся:

выделение специальных защищенных помещений для размещения ЭВМ и средств связи и хранения носителей информации;

выделение специальных ЭВМ для обработки конфиденциальной информации;

организация хранения конфиденциальной информации на специальных промаркированных магнитных носителях;

использование в работе с конфиденциальной информацией технических и программных средств, имеющих сертификат защищенности и установленных в аттестованных помещениях;

организация специального делопроизводства для конфиденциальной информации, устанавливающего порядок подготовки, использования, хранения, уничтожения и учета документированной информации;

организация регламентированного доступа пользователей к работе на ЭВМ, средствам связи и к хранилищам носителей конфиденциальной информации;

установление запрета на использование открытых каналов связи для передачи конфиденциальной информации;

разработка и внедрение специальных нормативно-правовых и распорядительных документов по организации защиты конфиденциальной информации, которые регламентируют деятельность всех звеньев объекта защиты в процессе обработки, хранения, передачи и использования информации;

постоянный контроль за соблюдением установленных требований по защите информации.

**Организационно-технические методы защиты информации.**

Они охватывают все структурные элементы автоматизированных информационных систем на всех этапах их жизненного цикла. Организационно-техническая защита информации обеспечивается осуществлением следующих мероприятий:

ограничение доступа посторонних лиц внутрь корпуса оборудования за счет установки механических запорных устройств или замков;

отключение ЭВМ от локальной вычислительной сети или сети удаленного доступа (региональные и глобальные вычислительные сети) при обработке на ней конфиденциальной информации, кроме случаев передачи этой информации по каналам связи;

использование для отображения конфиденциальной информации жидкокристаллических, а для печати — струйных принтеров или термопечати с целью снижения утечки информации по электромагнитному каналу. При использовании обычных дисплеев и принтеров с этой же целью рекомендуется включать устройства, создающие дополнительный шумовой эффект (фон), — генераторы шума, кондиционер, вентилятор, или обрабатывать другую информацию на рядом стоящей ЭВМ;

установка клавиатуры и печатающих устройств на мягкие прокладки с целью снижения утечки информации по акустическому каналу;

размещение оборудования для обработки конфиденциальной информации на расстоянии не менее 2,5 м от устройств освещения, кондиционирования, связи, металлических труб, теле- и радиоаппаратуры;

организация электропитания ЭВМ от отдельного блока питания (с защитой от побочных электромагнитных излучений или от общей электросети через фильтр напряжения);

использование бесперебойных источников питания (БИП) персональных компьютеров для силовых электрических сетей с неустойчивым напряжением и плавающей частотой. Основное назначение бесперебойных источников питания — поддержание работы компьютера после исчезновения напряжения в электрической сети. Это обеспечивается за счет встроенных аккумуляторов, которые подзаряжаются во время нормальной работы. БИП мгновенно предупредит своего владельца об аварии электропитания и позволит ему в течение некоторого времени (от нескольких минут до нескольких часов) аккуратно закрыть файлы и закончить работу. Кроме обычных для БИП функций они могут выполнять функцию высококлассного стабилизатора напряжения и электрического фильтра. Важной особенностью устройства является возможность непосредственной связи между ним и сетевой операционной системой.