

Вопрос 4. Методы защиты информации в КИС и сетях.

Для решения задачи противодействия угрозам безопасности необходим соответствующий набор методов и средств защиты, определение и разработка которых являются неотъемлемой частью работ по защите информации в КИС и сетях.

К настоящему времени разработан весьма широкий набор методов и средств защиты, с помощью которых обеспечивается требуемый уровень защищенности информации. Разнообразие возможных методов и средств защиты определяется, прежде всего, способами воздействия на угрозы безопасности или порождающие их причины, причем воздействия в направлении, способствующем повышению значений показателей защищенности или сохранению прежних их значений.

Методами обеспечения защиты информации являются: препятствие, управление доступом, маскировка, регламентация, принуждение, побуждение.

Препятствие заключается в создании на пути возникновения и распространения угрозы безопасности барьера, не позволяющего соответствующей угрозе реализоваться. Примерами препятствий являются блокировка, создание физических препятствий на пути нарушителей и т.п.

Управление доступом — метод защиты, регулирующий использование всех ресурсов КИС. Управление доступом включает в себя такие функции защиты, как идентификация пользователей, персонала и ресурсов КИС посредством присвоения персонального идентификатора; аутентификация (установление подлинности) объекта или субъекта по предъявленному идентификатору; проверка полномочий на работу в системе; разрешение и создание условий работы в пределах установленного регламента; протоколирование обращений к защищаемым ресурсам; реагирование при попытках несанкционированных действий.

Маскировка представляет собой преобразование информации, вследствие которого она становится недоступной и непонятной для нарушителей.

Регламентация как метод защиты заключается в разработке и реализации в процессе функционирования КИС комплексов мероприятий, создающих условия обработки информации, затрудняющих проявление и воздействие угроз безопасности.

Принуждение — метод защиты, при котором субъекты системы вынуждены соблюдать правила создания, обработки, передачи, использования защищаемой информации под угрозой материальной, административной, уголовной ответственности.

Побуждение есть метод защиты, при котором субъекты системы внутренне (материальными, моральными, этическими, психологическими мотивами) побуждаются к соблюдению всех правил работы с информацией.