**3. Классификация угроз информационной безопасности и методов защиты информации**

Под **угрозой информационной безопасности** объекта будем понимать возможные воздействия на него, приводящие к ущербу. К настоящему времени известно большое количество угроз. Приведем упрощенную их классификацию. Угрозы делятся виду на:

– конфиденциальности информации - нарушение свойства информации быть известной только определенным субъектам;

– целостности - несанкционированное изменение, искажение, уничтожение информации;

– доступности (работоспособности) - нарушаются доступ к информации, работоспособность объекта, доступ к которому получил злоумышленник.

По происхождению:

– случайные (отказы, сбои, ошибки, стихийные явления);

– преднамеренные (злоумышленные действия людей).

По источникам:

– люди (персонал, посторонние);

– технические устройства;

– модели, алгоритмы, программы;

– внешняя среда (состояние атмосферы, побочные шумы, сигналы и наводки).

**Случайные угрозы** обусловлены недостаточной надежностью аппаратуры и программных продуктов, недопустимым уровнем внешних воздействий, ошибок персонала. Методы оценки воздействия этих угроз рассматриваются в других дисциплинах (теории надежности, программировании, инженерной психологии и т. д.).

**Преднамеренные угрозы** связаны с действиями людей. Это и работники спецслужб, хакеры, работники самого объекта. Огромное количество разнообразных ИО делает бессмысленным перечисление всех возможных угроз для информационной безопасности, поэтому в дальнейшем при изучении того или иного раздела мы будем рассматривать основные угрозы для конкретных объектов.

Например, для несанкционированного доступа к информации вычислительной системы злоумышленник может воспользоваться штатными каналами доступа, если нет никаких мер защиты:

– через терминалы пользователей;

– через терминал администратора системы;

– через удаленные терминалы.

И через нештатные каналы:

– побочное электромагнитное излучение информации с аппаратуры системы;

– побочные наводки информации по сети электропитания и заземления;

– побочные наводки информации на вспомогательных коммуникациях;

– подключение к внешним каналам связи.

Все методы защиты информации по характеру проводимых действий можно разделить на: законодательные (правовые); организационные; технические; комплексные.

Для обеспечения защиты объектов информационной безопасности должны быть соответствующие **правовые акты**, устанавливающие порядок защиты и ответственность за его нарушение. Законы должны давать ответы на следующие вопросы: что такое информация, кому она принадлежит, как может с ней поступать собственник, что является посягательством на его права, как он имеет право защищаться, какую ответственность несет нарушитель прав собственника информации.

Установленные в законах нормы реализуются через комплекс **организационных мер**, проводимых прежде всего государством, ответственным за выполнением законов, и собственниками информации. К таким мерам относятся и издание подзаконных актов, регулирующих конкретные вопросы по защите информации (положения, инструкции, стандарты т. д.), и государственное регулирование сферы через систему лицензирования, сертификации, аттестации.

Поскольку в настоящее время основное количество информации генерируется, обрабатывается, передается и хранится с помощью технических средств, то для конкретной ее защиты в информационных объектах необходимы **технические устройства**. В силу многообразия технических средств нападения приходится использовать обширный арсенал технических средств защиты.

Наибольший положительный эффект достигается в том случае, когда все перечисленные способы применяются совместно, т. е**. комплексно**.