8.5. Основные меры и способы защиты информации в информационных технологиях

В практической деятельности в информационных технологиях применение мер и способов защиты информации включает следующие самостоятельные направления,

Для каждого направления определены основные цели и задачи.

1. Защита конфиденциальной информации от несанкционированного доступа и модификации призвана обеспечить решение одной из наиболее важных задач - защиту хранимой и обрабатываемой в вычислительной технике информации от всевозможных злоумышленных покушений, которые могут нанести существенный экономический и другой материальный и нематериальный ущерб. Основной целью этого вида защиты является обеспечение конфиденциальности, целостности и доступности информации.

Требования по защите информации от несанкционированного доступа в информационных технологиях направлены на достижение трех основных свойств защищаемой информации:

1.	Конфиденциальность	Засекреченная информация должна быть доступна только тому, кому она предназначена
2.	Целостность	Информация, на основе которой принимаются важные решения, должна быть достоверной и точной и должна быть защищена от возможных непреднамеренных и злоумышленных искажений
3.	Готовность	Информация и соответствующие информационные службы ИТ должны быть доступны, готовы к обслуживанию всегда, когда в них возникает необходимость

В части технической реализации защита от несанкционированного доступа в информационных технологиях сводится к задаче разграничения функциональных полномочий и доступа к данным с целью не только использования информационных ресурсов, но и их модификации.

2. Защита информации в каналах связи направлена на предотвращение возможности несанкционированного доступа к конфиденциальной информации, циркулирующей по каналам связи различных видов между различными уровнями управления экономическим объектом или внешними органами. Данный вид защиты преследует достижение тех же целей: обеспечение конфиденциальности и целостности информации. Наиболее эффективным средством защиты информации в неконтролируемых каналах связи является применение криптографии и специальных связных протоколов.

3. Защита юридической значимости электронных документов оказывается необходимой при использовании систем и сетей для обработки, хранения и передачи информационных объектов, содержащих в себе приказы и другие распорядительные, договорные, финансовые документы. Их общая особенность заключается в том, что в случае возникновения споров (в том числе и судебных), должна быть обеспечена возможность доказательства истинности факта того, что автор действительно фиксировал акт своего волеизъявления в отчуждаемом электронном документе. Для решения данной проблемы используются современные криптографические методы проверки подлинности информационных объектов, связанные с применением электронных подписей (цифровых

подписей). На практике вопросы защиты значимости электронных документов решаются совместно с вопросами защиты ИТ экономического объекта.

4. Защита информации от утечки по каналам побочных электромагнитных излучений и наводок является важным аспектом защиты конфиденциальной и секретной информации в вычислительной технике от несанкционированного доступа со стороны посторонних лиц. Данный вид защиты направлен на предотвращение возможности утечки информативных электромагнитных сигналов за пределы охраняемой территории экономического объекта. При этом предполагается, что внутри охраняемой территории применяются эффективные режимные меры, исключающие возможность бесконтрольного использования специальной аппаратуры перехвата, регистрации и отображения электромагнитных сигналов. Для защиты от побочных электромагнитных излучений и наводок широко применяется экранирование помещений, предназначенных для размещения средств вычислительной техники, а также технические меры, позволяющие снизить интенсивность информативных излучений самого оборудования персональных компьютеров и каналов связи.

В некоторых ответственных случаях может быть необходима дополнительная проверка вычислительной техники на предмет возможного выявления специальных закладных устройств промышленного шпионажа, которые могут быть внедрены туда с целью регистрации или записи информативных излучений персонального компьютера, а также речевых и других несущих уязвимую информацию сигналов.

5. Защита от несанкционированного копирования и распространения программ и ценной компьютерной информации является самостоятельным видом защиты прав, ориентированных на проблему охраны интеллектуальной собственности, воплощенной в виде программ и ценных баз данных. Данная защита обычно осуществляется с помощью специальных программных средств, подвергающих защищаемые программы и базы данных предварительной обработке (вставка парольной защиты, проверок по обращениям к устройствам хранения ключа и ключевым дискетам, блокировка отладочных прерываний, проверка рабочего персонального компьютера по его уникальным характеристикам и т. д.), которая приводит исполнимый код защищаемой программы и базы данных в состояние, препятствующее его выполнению на "чужих" ПК.

Общим свойством средств защиты программ и баз данных в ИТ от несанкционированного копирования является ограниченная стойкость такой защиты, т. к. в конечном случае исполнимый код программы поступает на выполнение в центральный процессор в открытом виде и может быть прослежен с помощью аппаратных отладчиков. Однако это обстоятельство не снижает потребительских свойств средств защиты до минимума, т. к. основная цель их применения - максимально затруднить, хотя бы временно, возможность несанкционированного копирования ценной информации.