## 8.2. Система защиты данных в информационных технологиях

На современном этапе существуют следующие предпосылки сложившейся кризисной ситуации обеспечения безопасности информационных технологий:

- современные ПК за последние годы приобрели большую вычислительную мощность, но одновременно с этим стали гораздо проще в эксплуатации;
- прогресс в области аппаратных средств сочетается с еще более бурным развитием ПО;
- развитие гибких и мобильных технологий обработки информации привело к тому, что практически исчезает грань между обрабатываемыми данными и исполняемыми программами за счет появления и широкого распространения виртуальных машин и интерпретаторов;
- несоответствие бурного развития средств обработки информации и медленной проработки теории информационной безопасности привело к появлению существенного разрыва между теоретическими моделями безопасности, оперирующими абстрактными понятиями типа "объект", "субъект" и реальными категориями современных информационных технологий;
- необходимость создания глобального информационного пространства и обеспечение безопасности протекающих в нем процессов потребовали разработки международных стандартов, следование которым может обеспечить необходимый уровень гарантии обеспечения защиты.

Вследствие совокупного действия всех перечисленных факторов перед разработчиками современных информационных технологий, предназначенных для обработки конфиденциальной информации, стоят следующие задачи, требующие немедленного и эффективного решения:

- обеспечение безопасности новых типов информационных ресурсов;
- организация доверенного взаимодействия сторон (взаимной идентификации / аутентификации) в информационном пространстве;
- защита от автоматических средств нападения;
- интеграция в качестве обязательного элемента защиты информации в процессе автоматизации ее обработки.

Таким образом, организация информационной технологии требует решения проблем по защите информации, составляющей коммерческую или государственную тайну, а также безопасности самой информационной технологии.

Современные автоматизированные информационные технологии обладают следующими основными признаками:

1. Наличие информации различной степени конфиденциальности;
2. Необходимость криптографической защиты информации различной степени конфиденциальности при передаче данных между различными подразделениями или уровнями управления;
3. Иерархичность полномочий субъектов доступа и программ к АРМ специалистов, каналам связи, информационным ресурсам, необходимость оперативного изменения этих полномочий;

4. Организация обработки информации в интерактивном (диалоговом) режиме, в режиме разделения времени между пользователями и в режиме реального времени;
5. Обязательное управление потоками информации как в локальных вычислительных сетях, так и при передаче данных на большие расстояния;
6. Необходимость регистрации и учета попыток несанкционированного доступа, событий в системе и документов, выводимых на печать;
7. Обязательное обеспечение целостности программного обеспечения и информации в автоматизированных информационных технологиях;
8. Наличие средств восстановления системы защиты информации;
9. Обязательный учет магнитных носителей информации;
10. Наличие физической охраны средств вычислительной техники и магнитных носителей.

В этих условиях проблема создания системы защиты информации в информационных технологиях включает в себя две взаимодополняющие задачи:

1. Разработка системы защиты информации (ее синтез).
2. Оценка разработанной системы защиты информации путем анализа ее технических характеристик с целью установления, удовлетворяет ли система защиты информации комплексу требований к таким системам.

Вторая задача является задачей классификации, которая в настоящее время решается практически исключительно экспертным путем с помощью сертификации средств защиты информации и аттестации системы защиты информации в процессе ее внедрения.

Создание базовой системы защиты информации в организациях и на предприятиях основывается на следующих принципах,

1. **Комплексный подход к построению системы защиты при ведущей роли организационных мероприятий.** Он означает оптимальное сочетание программно-аппаратных средств и организационных мер защиты, подтвержденное практикой создания отечественных и зарубежных систем защиты.
2. **Разделение и минимизация полномочий по доступу к обрабатываемой информации и процедурам обработки.** Специалистам экономического объекта предоставляется минимум строго определенных полномочий, достаточных для успешного выполнения ими своих служебных обязанностей, с точки зрения автоматизированной обработки доступной им конфиденциальной информации.
3. **Полнота контроля и регистрация попыток несанкционированного доступа, т. е.** необходимость точного установления идентичности каждого специалиста и протоколирования его действий для проведения возможного расследования, а также невозможность совершения любой операции обработки информации в ИТ без ее предварительной регистрации.
4. **Обеспечение надежности системы защиты**, т. е. невозможность снижения ее уровня при возникновении в системе сбоев, отказов, преднамеренных действий нарушителя или непреднамеренных ошибок специалистов экономического объекта и обслуживающего персонала.
5. **Обеспечение контроля за функционированием системы защиты**, т. е. создание средств и методов контроля работоспособности механизмов защиты.
6. **"Прозрачность" системы защиты информации для общего, прикладного программного обеспечения и специалистов экономического объекта.**
7. **Экономическая целесообразность использования системы защиты.** Она выражается в том, что стоимость разработки и эксплуатации системы защиты

информации должна быть меньше стоимости возможного ущерба, наносимого объекту в случае разработки и эксплуатации информационной технологии без системы защиты информации.

В процессе организации системы защиты информации в информационных технологиях решаются следующие вопросы:

- устанавливается наличие конфиденциальной информации, оценивается уровень конфиденциальности и объемы такой информации;
- определяются режимы обработки информации (интерактивный, реального времени и т. д.), состав комплекса технических средств, общесистемные программные средства и т. д. ;
- анализируется возможность использования имеющихся на рынке сертифицированных средств защиты информации;
- определяется степень участия персонала, функциональных служб, научных и вспомогательных работников объекта автоматизации в обработке информации, характер их взаимодействия между собой и со службой безопасности;
- вводятся мероприятия по обеспечению режима секретности на стадии разработки системы.

Важным организационным мероприятием по обеспечению безопасности информации является охрана объекта, на котором расположена защищаемая автоматизированная информационная технология (территория здания, помещения, хранилища информационных ресурсов). При этом устанавливаются соответствующие посты охраны, технические средства, предотвращающие или существенно затрудняющие хищение средств вычислительной техники, информационных носителей, а также исключающие несанкционированный доступ к автоматизированным информационным технологиям и каналам связи.

Функционирование системы защиты информации от несанкционированного доступа предусматривает:

- учет, хранение и выдачу специалистам организации или предприятия информационных носителей, паролей, ключей;
- ведение служебной информации (генерация паролей, ключей, сопровождение правил разграничения доступа);
- оперативный контроль за функционированием системы защиты секретной и конфиденциальной информации;
- контроль соответствия общесистемной программной среды эталону;
- приемку и карантин включаемых в информационные технологии новых программных средств;
- контроль за ходом технологического процесса обработки информации путем регистрации анализа действий специалистов экономического объекта;
- сигнализацию в случаях возникновения опасных событий и т. д.