ОСОБЕННОСТЬ ЭТАПОВ ПОСТРОЕНИЯ ИНТЕГРИРОВАННОЙ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ

М.М. Каримов, А.А. Ганиев, Б.Э.Элмуродова

Узбекистан, Ташкент, ТУИТ

Как известно, цель защиты информации (ЗИ) - предотвращение утечки или нарушения целостности информации. Эта цель может быть достигнута, с помощью построением интегрированной системы зашиты информации, которая представляет собой организованную совокупность методов и средств обеспечения ЗИ.

Процесс построения ИСЗИ осуществляется поэтапно в последующей последовательности:

- определение и анализ угроз;
- разработка интегрированной системы зашиты информации;
- реализация плана зашиты информации;
- контроль функционирования и управление интегрированной системой зашиты информации.

Определение и анализ угроз. На этом этапе необходимо осуществить анализ объектов ЗИ, ситуационного плана, условий функционирования предприятия, учреждения, организации, оценить вероятность проявления угроз и ожидаемый ущерб от их реализации, подготовить исходные данные для построения частной модели угроз.

Угрозы могут осуществляться:

- по техническим каналам, включающим каналы побочных электромагнитных излучений и наводок, акустические, оптические, радио-, радиотехнические, химические и другие каналы;
- по каналам специального воздействия путем формирования полей и сигналов в целях разрушения системы зашиты или нарушения целостности информации;
- несанкционированным доступом в результате подключения к аппаратуре и линиям связи, маскировки под зарегистрированного пользователя, преодоления мер защиты для использования информации или навязывания ложной информации, применения закладных устройств и программ и внедрения компьютерных вирусов.

Разработка интегрированной системы защиты информации. На этом этапе следует осуществить разработку плана ЗИ, включающего организационные, первичные и основные технические меры зашиты информации, определить зоны безопасности информации.

Организационные меры регламентируют порядок информационной деятельности с учетом норм и требований по ЗИ для всех периодов жизненного цикла объекта ЗИ.

Технические меры предусматривают защиту информации блокированием угроз с использованием технических средств обеспечения ЗИ.

Меры зашиты информации должны:

- быть адекватны угрозам;
- быть разработаны с учетом возможного ущерба от их реализации и стоимости защитных мер и вносимых ими ограничений;
- обеспечивать заданную эффективность зашиты информации в течение периода ограничения доступа к ней.

Уровень защиты информации определяется системой количественных и качественных показателей, обеспечивающих решение задачи зашиты информации на основе норм и требований по ЗИ.

Минимально необходимый уровень зашиты информации обеспечивается ограничительными и фрагментарными мерами противодействия наиболее опасной угрозе.

Повышение уровня зашиты информации достигается наращиванием технических мер противодействия множеству угроз.

Реализация плана защиты информации. На третьем этапе следует реализовать организационные и основные технические меры зашиты информации, установить необходимые зоны безопасности информации, провести аттестацию технических средств обеспечения информационной деятельности, технических средств зашиты информации, рабочих мест (помещений) на соответствие требованиям по безопасности информации.

Техническая зашита информации обеспечивается применением защищенных программ и технических средств обеспечения информационной деятельности, программных и технических средств зашиты информации контроля эффективности зашиты, а также применением специальных инженерно-технических сооружений, средств и систем.

Средства ЗИ могут функционировать автономно или совместно с техническими средствами обеспечения информационной деятельности в виде отдельных устройств или встроенных в них составных элементов.

Состав средств обеспечения ЗИ, перечень их поставщиков, а также услуг по установке, монтажу, наладке и обслуживанию определяются лицами, которые владеют, пользуются и распоряжаются информацией самостоятельно или по рекомендациям специалистов по ЗИ в соответствии с нормативными документами системы ЗИ.

Предоставление услуг по ЗИ, аттестацию и обслуживание средств обеспечения ЗИ могут осуществлять юридические и физические лица, имеющие соответствующую лицензию.

Контроль функционирования и управление интегрированной системой зашиты информации. На заключительном этапе следует провести анализ функционирования интегрированной системы зашиты информации, проверку выполнения мер ЗИ, контроль эффективности зашиты, подготовить и выдать исходные данные для управления интегрированной системой зашиты информации.

Управление интегрированной системой защиты информации заключается в адаптации мер ЗИ к текущей задаче. По фактам изменения условий осуществления или выявления новых угроз меры ЗИ реализуются в кратчайший срок.

В случае необходимости повышения уровня защиты информации необходимо выполнить работы по модернизации интегрированной системы зашиты информации.