

Лабораторная работа

Определение состава защищаемой информации

Цель работы: изучить перечень нормативных документов на основе которых осуществляется построение системы защиты информации.

Теоретическая часть

Защита информации является составной частью работ по созданию и эксплуатации объектов информатизации различного назначения и осуществляется в соответствии с установленными руководящими документами

порядком в виде системы (подсистемы) защиты информации. Защите подлежит информация, как речевая, так и обрабатываемая техническими средствами, а также представленная в виде информативных электрических сигналов, физических полей, носителей на бумажной, магнитной, оптической и иной основе в виде информационных массивов и баз данных в автоматизированной системе.

Защита конфиденциальной информации осуществляется на основании федеральных законов «Об информации, информатизации и защите информации», «Об участии в международном информационном обмене», Указа Президента Российской Федерации от 06.03.1997 г. № 188 «Перечень сведений конфиденциального характера», «Доктрины информационной безопасности Российской Федерации», утвержденной Президентом Российской Федерации 09.09.2000 г. № Пр.-1895, других нормативных правовых актов по защите информации, а также опыта реализации мер защиты информации в министерствах и ведомствах, в учреждениях и на предприятиях.

В качестве примера рассмотрим одну из наиболее важных задач, решаемых в области защиты информации, – обеспечение безопасности персональных данных граждан. Для того чтобы ее решить, необходимо не только придерживаться порядка, установленного нормативными и методическими документами, но и хорошо ориентироваться в том, что касается классификации информационных систем и категорий персональных данных, применяемых технологий и средств защиты.

Основным законодательным актом в области защиты персональных данных является Федеральный закон № 152-ФЗ «О персональных данных» от 27.07.2006 г. Федеральным законом регулируются отношения, связанные с обработкой персональных данных, осуществляемой органами государственной власти, иными государственными органами, юридическими лицами и физическими лицами с использованием средств автоматизации, в том числе в информационно-телекоммуникационных сетях, или без использования таких средств.

В соответствии с законом «О персональных данных» уполномоченные органы с учетом возможного вреда субъекту персональных данных, объема и содержания обрабатываемых персональных данных, вида деятельности, при

осуществлении которого обрабатываются персональные данные, актуальности угроз безопасности персональных данных устанавливают:

- 1) уровни защищенности персональных данных при их обработке в информационных системах персональных данных в зависимости от угроз безопасности этих данных;
- 2) требования к защите персональных данных при их обработке в информационных системах персональных данных, исполнение которых обеспечивает установленные уровни защищенности персональных данных;
- 3) требования к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных.

Уровень защищенности персональных данных определяется на этапе классификации информационной системы персональных данных в соответствии с Постановлением Правительства № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» от 01.11.2012 г. Устанавливаются 4 уровня защищенности персональных данных в зависимости от категории данных, количества субъектов персональных данных и типа угроз безопасности персональных данных, актуальных для системы. К каждому из четырех уровней предъявляются общие требования к защите данных.

Формирование конкретных требований к системе защиты информации (персональных данных) осуществляют в соответствии с приказом ФСТЭК № 21 «Об утверждении Состав и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» от 18.02.2013 г.

Требования к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных описаны в Постановлении Правительства № 512 от 06.07.2008 г. «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных».

Требования к процессу обработки персональных данных, осуществляемому без использования средств автоматизации, установлены Постановлением Правительства № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» от 15.09.2008 г.

Все описанные выше законодательные акты и нормативные документы в области защиты персональных данных содержат описание организационных и технических мер обеспечения безопасности персональных данных за исключением требований, предъявляемых в случае использования криптографических (шифровальных) средств.

В случае применения криптографических средств защиты информации, их разработка, внедрение и эксплуатация осуществляется в соответствии с «Методическими рекомендациями по обеспечению с помощью криптосредств

безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации», утвержденными приказом ФСБ № 149/54-144 от 21.02.2008 г., а также в соответствии с «Типовыми требованиями по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденными приказом ФСБ № 149/6/6-622 от 21.02.2008 г.

При построении модели угроз и модели вероятного нарушителя безопасности информации (персональных данных) применяют «Методику определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных», а также «Базовую модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных».

Практическое задание

Составить перечень мероприятий необходимых для построения комплексной системы защиты информации (на примере хозяйствующего субъекта) с учётом нормативно-методических актов.

Содержание отчета

1. Титульная страница отчета.
2. Цель лабораторной работы.
3. Описание выполненной работы.
4. Заключение