ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«САНКТ-ПЕТЕРБУРГСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, МЕХАНИКИ И ОПТИКИ»

Факультет безопасности информационных технологий

Дисциплина:
«Теория информационной безопасности и методология защиты информации»

ОТЧЕТ ПО ЛАБОРАТОРНОЙ РАБОТЕ №2
РД ФСТЭК

Выполнил:
Студент гр. N3253
Пастухова А.А.

Проверил:
Якимова С.А.

Санкт-Петербург
2022г.

Цель: изучить основные руководящие документы ФСТЭК и научиться применять их для практических задач.

Задачи:

1. Ознакомиться с руководящими документами;
2. Решить представленные кейсы;
3. Сделать вывод о том, в каком порядке необходимо начинать решение различных задач.

Ход работы:

На основе описания предприятия предложить совокупность подходящих по требованиям безопасности Автоматизированной системы и Средств вычислительной техники. Также стоит описать класс защищенности от НСД для выбранных АС и СВТ. (необходимо аргументировать свой выбор, при выборе определенной АС кроме СВТ следует также выбрать и МЭ, соответствующий этой АС, и также описать требования по его безопасности).

НСД - несанкционированный доступ;
СЗИ НСД - система защиты информации от несанкционированного доступа;
- управления доступом;
- регистрации и учета;
- криптографической;
- обеспечения целостности.

АС - автоматизированные системы;
СВТ - средства вычислительной техники;
МЭ - межсетевые экраны;
КД – конструкторская документация;
КСЗ – комплекс средств защиты;
РД - руководящий документ;
КСЗ – комплекс средств защиты;
НДВ - недекларированные возможности.

Кейс 1

Является первой группой АС, класс защищенности 1Г, т.к. одновременно обрабатывается и (или) хранится информация разных уровней конфиденциальности. Не все пользователи имеют право доступа к информации, при этом они имеют доступ к ЭВМ.

Защищенность СВТ от НСД 5 класса - есть регистрация, но нет защиты ввода-вывода информации на носитель.

АС соответствует 4 классу защищенности МЭ, присутствует регистрация, но нет идентификации и аутентификации.

Считается необходимым четвертый уровень контроля для ПО, используемого при защите конфиденциальной информации.

Кейс 2

Вторая группа АС, класс защищенности 2А - несколько пользователей, директор архива и руководство города, которые имеют одинаковые права доступа ко всей информации. Присутствуют данные, составляющие гос. тайну под грифом СС. Выбор класса такой, потому что есть доступ к томам, каталогам, файлам, записям, полям записей; ведется регистрация и учет выдачи печатных (графических) выходных документов.

Защищенность СВТ от НСД 3 класса (нет контроля модификаций, дистрибуций и гарантии архитектуры, но есть взаимодействие пользователя с КСЗ).

Уровень МЭ 2 или 1 (обрабатывается информация с грифом СС).

Уровень контроля НДВ, достаточного для ПО, 2 (в архиве хранится информация под грифом совершенно секретно).

Кейс 3

Третья группа АС, класс защищенности 3Б (один пользователь, конфиденциальная информация, печатные документы).

Защищенность СВТ от НСД – 5 (требуется целостность КСЗ, но нет защиты ввода-вывода на отчуждаемый физический носитель информации)

Межсетевые экраны (МЭ) – 4 (есть регистрация, но нет идентификации и аутентификации). Для АС класса 3Б, 2Б должны применяться МЭ не ниже 5 класса.

Необходим самый низкий 4 уровень контроля для ПО, так как нет информации, относящейся к государственной тайне.

Кейс 4

Первая группа АС, класс защищенности 1Г (пользователи с разными доступами имеют права доступа к информации, но есть разграничение по каталогам, файлам, записям).

Защищенность СВТ от НСД – 5 (требуется целостность КСЗ, но нет изоляции модулей).

Межсетевые экраны (МЭ) – 4 (есть регистрация, но нет идентификации и аутентификации).

Необходим самый низкий 4 уровень контроля для ПО, так как нет информации, относящейся к государственной тайне.

Кейс 5

Вторая группа АС, класс защищенности 2Б (несколько пользователей имеют одинаковые права доступа ко всей информации, конфиденциальная информация). Должна быть обеспечена целостность программных средств СЗИ НСД, обрабатываемой информации, а также неизменность программной среды.

Защищенность СВТ от НСД – 5-6 (дискреционная защита).

Межсетевые экраны (МЭ) – 4 (присутствует регистрация).

Необходим самый низкий 4 уровень контроля для ПО, так как нет информации, относящейся к государственной тайне.

Кейс 6

Первая группа АС, класс защищенности 3А (один пользователь, в архиве находятся данные с грифами “совершенно секретно” и “секретно”).

Защищенность СВТ от НСД – 3 (есть взаимодействие пользователя с КСЗ, надежное восстановление).

Межсетевые экраны (МЭ) – 2 (грифы СС, С).

Необходим 2 уровень контроля для ПО, используемого для защиты информации (есть гостайна).

Кейс 7

Первая группа АС, класс защищенности не ниже 1В (не все пользователи имеют право доступа ко всей информации).

Защищенность СВТ от НСД – 4 (есть регистрация, но нет защиты ввода-вывода информации на носитель).

Межсетевые экраны (МЭ) – 3

Сотрудник не соблюдал требования о защищенности АС.

Подсистема обеспечения целостности:
должна быть обеспечена целостность программных средств СЗИ НСД, а также неизменность программной среды.
При этом:
- целостность СЗИ НСД проверяется при загрузке системы по контрольным суммам компонент СЗИ;
- целостность программной среды обеспечивается использованием трансляторов с языков высокого уровня и отсутствием средств модификации объектного кода программ в процессе обработки и (или) хранения защищаемой информации;
- должна осуществляться физическая охрана СВТ (устройств и носителей информации), предусматривающая контроль доступа в помещения АС посторонних лиц, наличие надежных препятствий для несанкционированного проникновения в помещения АС и хранилище носителей информации, особенно в нерабочее время;
- должно проводиться периодическое тестирование функций СЗИ НСД при изменении программной среды и персонала АС с помощью тест - программ, имитирующих попытки НСД;
- должны быть в наличии средства восстановления СЗИ НСД, предусматривающие ведение двух копий программных средств СЗИ НСД и их периодическое обновление и контроль работоспособности.

Вывод: решение кейсов стоит начинать с определения необходимого класса АС, СВТ, МЭ. Далее поэтапно можно представить себе проектирование АС, СВТ, МЭ на основе требований из ФСТЭК. для решения данной задачи нужно четко следовать пунктам, описывающим минимальные требования для классификации.