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. P32141, поток ТИБ 2.3

Полуянов Александр Михайлович

Проверила:

Доцент ФБИТ

Коржук Виктория Михайловна

Санкт-Петербург

2023 г.

Цель работы:

Ознакомиться с основными руководящими документами ФСТЭК и научиться применять их для практических задач.

Объекты:

- Защита от НСД термины + Концепция защиты от НСД
- Автоматизированные системы. Защита от НСД
- Средства вычислительной техники. Защита от НСД
- СВТ. Межсетевые экраны. Защита от НСД
- Федеральный закон "О безопасности критической информационной инфраструктуры Российской Федерации" от 26.07.2017 N 187-ФЗ

Аббревиатуры:

- АС – автоматизированная система
- СВТ – средства вычислительной техники
- НСД – несанкционированный доступ
- КСЗ – комплекс средств защиты
- МЭ – межсетевой экран

Ход работы:

Кейс 1:

На заводе, производящем автомобильные детали, хотят произвести модернизацию и перейти от бумажного документооборота к электронному. Рассматриваемое предприятие не является государственным, однако в архивах отдела кадров хранятся некоторые сведения составляющие персональные данные сотрудников. Компьютерами на предприятии могут пользоваться сотрудники, работающие в бухгалтерии и отделе кадров, а также директор предприятия, причем бухгалтера имеют доступ только с “числам”, а кадровики - только к “характеристикам”. Новая система должна обеспечивать защиту от утечек информации о поставщиках, так как в этом заинтересованы заводы-конкуренты, которые не раз пытались произвести кражу такой информации на бумажных носителях, устраивая на завод работать своих сотрудников.

Класс АС – 1Г
Класс защищенности СВТ – 5 класс
Класс МЭ – 4 класс

Данная группа выбрана для того, чтобы знать, кто распечатал документ, если произойдет утечка корпоративной информации.
От МЭ необходима фильтрация на сетевом уровне, документирование действий администратора. Обеспечение целостности и возможности восстановления. Также осуществляется регистрация событий.

Кейс 2:

В городском архиве необходимо заменить АС и СВТ в связи с сокращением штата сотрудников до одного человека (содержание архива было полностью перенесено на электронные носители несколько лет назад, поэтому для обеспечения корректной его работы не требуется много сотрудников). Единственным сотрудником архива является его директор, который, также как и руководство города имеет доступ ко всей информации в архиве и даже такой, которая составляет государственную тайну и хранится в архиве под грифом совершенно секретно.

Класс АС – 3А
Класс защищенности СВТ – 3 класс
Класс МЭ – 2 класс

Доступ к АС будет иметь только один сотрудник. Также в ней содержатся совершенно секретные документы.
От МЭ необходима фильтрация на сетевом уровне, документирование действий администратора. Обеспечение целостности и возможности восстановления. Также осуществляется регистрация событий. Администратор должен иметь возможность централизованного управления МЭ.

Кейс 3:

ИП, занимающийся производством ручных изделий, имеет собственные секреты производства. Он хочет сохранить всю информацию о производимом товаре и также автоматизировать весь документооборот. Он занимается всем этим один. Несмотря на то, что он один должен иметь доступ ко всей информации о фирме, он переживает, что кто-то все-таки может воспользоваться его отсутствием в арендованном кабинете и все узнать.

Класс АС – 3Б
Класс защищенности СВТ – 5 класс
Класс МЭ – 4 класс

Доступ к АС имеет один человек, в системе содержится информация о производственной тайне.
От МЭ необходима фильтрация на сетевом уровне, документирование действий администратора. Обеспечение целостности и возможности восстановления. Также осуществляется регистрация событий.

Кейс 4:

В компании, имеющей штат сотрудников более 100 человек, используется единая система для передачи всех данных, связанных с компанией, однако у данной системы нет свободного выхода в сеть интернет. В небольших офисных помещениях сотрудники могут без особого труда получить доступ к компьютерам других сотрудников. Высокопоставленные сотрудники при передаче данных имеют доступ к информации, к которой не все сотрудники имеют право доступа. Конфиденциальная информация в системе не передается.

Класс АС – 1Д
Класс защищенности СВТ – 6 класс
Класс МЭ – 5 класс

К системе имеют доступ все сотрудники, но руководство владеет дополнительной информацией, конфиденциальных данных нет.
От МЭ необходима фильтрация на сетевом уровне, документирование действий администратора. Обеспечение целостности и возможности восстановления.

Кейс 5:

На предприятии, состоящем из нескольких сотрудников, было решено реализовать “информационную сеть”, позволяющую производить документооборот. При реализации данного проекта было решено, что через “сеть” можно передавать любую информацию любому из пользователей, даже составляющие производственную тайну. Доступ к “сети” можно получить с любого устройства, подключенного к сети интернет, авторизовавшись в специальном приложении.

Класс АС – 2Б
Класс защищенности СВТ – 5 класс
Класс МЭ – 4 класс

Доступ к любой информации в системе имеют все сотрудники. Информация составляет производственную тайну.
От МЭ необходима фильтрация на сетевом уровне, документирование действий администратора. Обеспечение целостности и возможности восстановления. Также осуществляется регистрация событий.

Кейс 6:

На государственном предприятии используется закрытая от внешней среды система передачи данных. Данной системой пользуется исключительно один рабочий (заведующий архивом). Известно, что в архиве находятся данные с грифами “совершенно секретно” и “секретно”, при этом может осуществляться их дистрибуция. Доступ к данной системе можно осуществить исключительно со специального ПК в архиве при помощи авторизации пользователя.

Класс АС – 3А
Класс защищенности СВТ – 2 класс
Класс МЭ – 1 класс

Один сотрудник имеет доступ к секретной и совершенно секретной информации. Так как он осуществляет её дистрибуцию был дан 2 класс СВТ.
От МЭ необходима фильтрация на сетевом уровне, документирование действий администратора. Обеспечение целостности и возможности восстановления. Также осуществляется регистрация событий. Администратор должен иметь возможность централизованного управления МЭ.

Кейс 7:

Государственная энергетическая компания обеспечивает электроэнергией страну. Но, похоже, сотрудники компании имеют очень туманное представление об информационной безопасности. В начале текущей недели новый ИБ-специалист обнаружил, что данные этой компании были похищены трояном-стилером. Дело в том, что ИБ специалист до этого постоянно искал зараженные корпоративные машины и старался предупредить о компрометации их владельцев. Так он поступил и в этом случае. ИБ специалист сказал руководству, что машина сотрудника оказалась заражена из-за того, что тот, кто занимался автоматизацией и скачал фейковый установщик IDE. В итоге допустили утечку данных своих клиентов. Любому желающему «видны» личные данные клиентов, внутренние метрики, платежные данные (включая номера карт и CVV) и так далее.

Класс АС – 1Г
Класс защищенности СВТ – 5 класс
Класс МЭ – 4 класс

Сотрудник запустил на своём компьютере нелицензированное компанией ПО, не задокументировал свои действия.

Вывод:

При планировании архитектуры АС и СВТ надо начать с определения грифа секретности информации и того, сколько людей и как будут иметь к ним доступ. На основании этого и дополнительных данных необходимо планировать остальные шаги по защите.