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 методологии защиты информации.

ОТЧЕТ ПО ЛАБОРАТОРНОЙ РАБОТЕ №2

Выполнил:

Студент гр. N3249

Шарифуллин Ильдан Айдарович

Проверил:

Якимова Софья Андреевна

Санкт-Петербург

2022г.

Лабораторная работа №2

РД ФСТЭК

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

Задачи:

1. Ознакомиться с руководящими документами:

- https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/382-rukovodyashchij-dokument-prikaz-predsedatelya-gostekhkomissii-rossii-ot-4-iyunya-1999-g-n-114
- Защита от НСД термины (https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/386-rukovodyashchij-dokument-reshenie-predsedatelya-gostekhkomissii-rossii-ot-30-marta-1992-g3) + Концепция защиты от НСД
- Автоматизированные системы. Защита от НСД https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/384-rukovodyashchij-dokument-reshenie-predsedatelya-gostekhkomissii-rossii-ot-30-marta-1992-g
- №187з
- Средства вычислительной техники. Защита от НСД (https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/385-rukovodyashchij-dokument-reshenie-predsedatelya-gostekhkomissii-rossii-ot-30-marta-1992-g2)
- СВТ. Межсетевые экраны. Защита от НСД (https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/383-rukovodyashchij-dokument-reshenie-predsedatelya-gostekhkomissii-rossii-ot-25-iyulya-1997-g)

- https://habr.com/post/311978/

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

Ход работы:

1) Кейс: 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.

1) Выбор АС

Классификация АС – 1Г (много пользователей имеют доступ не ко всей информации, при этом они имеют доступ к ЭВМ (поэтому 1Г, а не 1Д), информация конфиденциальная)

А) Подсистема обеспечения целостности:
должна быть обеспечена целостность программных средств СЗИ НСД, а также неизменность программной среды.

Б) Подсистема управления доступом:
должна осуществляться идентификация и проверка подлинности субъектов доступа при входе в систему по идентификатору (коду) и паролю условно-постоянного действия, длиной не менее шести буквенно-цифровых символов;

В) Подсистема регистрации и учета:
должна осуществляться регистрация входа (выхода) субъектов доступа в систему (из системы), либо регистрация загрузки и инициализации операционной системы и ее программного останова. Регистрация выхода из системы или останова не проводится в моменты аппаратурного отключения АС.

2) Выбор СВТ:

Класс защищенности СВТ от НСД: 4 (мандатная защита; поскольку информация конфиденциальная)

Можно воспользоваться продуктами компании “Код безопасности”. Их продукт Панцирь-С сертифицирован по требованиям ФСТЭК 4-й класс защищенности СВТ.

3) Выбор МЭ

Класс защищенности МЭ: 4-5 (АС 1Г)

Можно воспользоваться программным комплексом «Аркан».

Он соответствует требованиям документов: Требования к МЭ, Профиль защиты МЭ (ИТ.МЭ.Д4.ПЗ — тип «Д», четвёртый класс защиты), Требования к СОВ, Профили защиты СОВ (ИТ.СОВ.С4.ПЗ — уровень сети, четвёртый класс защиты).

2) Кейс: 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.

1) Выбор АС

Классификация АС – 3А (1 пользователь, гриф СС)

А) Подсистема обеспечения целостности:

физическая охрана СВТ может обеспечиваться СКУДом и службой охраны городского архива.

Б) Подсистема управления доступом:

должны осуществляться идентификация и проверка подлинности субъектов доступа при входе в систему по паролю условно-постоянного действия длиной не менее шести буквенно-цифровых символов.

В) Подсистема регистрации и учета:

В АС должны сохраняться все необходимые данные (дата и время входа (выхода) сбъектов, результаты попыток входа и тд)

2) Выбор СВТ:

Класс защищенности СВТ от НСД: 1 (верифицированная защита)

Нет готовых продуктов под СВТ 1, слишком индивидуальны характеристики

3) Выбор МЭ

Класс защищенности МЭ: 2 (АС 3А + СС)

Можно воспользоваться программно-аппаратным комплексом “Рубикон-К”

Он соответствует требованиям документов: Требования к МЭ, Профиль защиты МЭ (ИТ.МЭ.А2.ПЗ — тип «А», второй класс защиты; ИТ.МЭ.А4.ПЗ — тип «А», четвёртый класс защиты; ИТ.МЭ.Б4.ПЗ — тип «Б», четвёртый класс защиты), Требования к СОВ, Профили защиты СОВ (ИТ.СОВ.С4.ПЗ — уровень сети, четвёртый класс защиты).

3) Кейс: 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.

1) Выбор АС

Классификация АС – 3Б (1 пользователь, конфиденциальная информация)

А) Подсистема обеспечения целостности:

должна быть обеспечена целостность программных средств СЗИ НСД, обрабатываемой информации, а также неизменность программной среды.

Б) Подсистема управления доступом:

должны осуществляться идентификация и проверка подлинности субъектов доступа при входе в систему по паролю условно-постоянного действия длиной не менее шести буквенно-цифровых символов.

В) Подсистема регистрации и учета:

В АС должны сохраняться все необходимые данные (дата и время входа (выхода) сбъектов, результаты попыток входа и тд)

2) Выбор СВТ:

Класс защищенности СВТ от НСД: 1 (поскольку информация конфиденциальная)

Нет готовых продуктов под СВТ 1, слишком индивидуальны характеристики

3) Выбор МЭ

Класс защищенности МЭ: 4-5 (АС 3Б)

Можно воспользоваться программным комплексом «Аркан».

Он соответствует требованиям документов: Требования к МЭ, Профиль защиты МЭ (ИТ.МЭ.Д4.ПЗ — тип «Д», четвёртый класс защиты), Требования к СОВ, Профили защиты СОВ (ИТ.СОВ.С4.ПЗ — уровень сети, четвёртый класс защиты).

4) Кейс: 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.

4) Выбор АС

Классификация АС – 1Г (пользователи с разными доступами, конфиденциальная информация)

А) Подсистема обеспечения целостности:

должна быть обеспечена целостность программных средств СЗИ НСД, обрабатываемой информации, а также неизменность программной среды.

Б) Подсистема управления доступом:

должны осуществляться идентификация и проверка подлинности субъектов доступа при входе в систему по паролю условно-постоянного действия длиной не менее шести буквенно-цифровых символов.

В) Подсистема регистрации и учета:

В АС должны сохраняться все необходимые данные (дата и время входа (выхода) сбъектов, результаты попыток входа и тд)

5) Выбор СВТ:

Класс защищенности СВТ от НСД: 3 (мандатная защита)

Можно воспользоваться продуктами компании “Код безопасности”. Их продукт Secret Net Studio - С сертифицирован по требованиям ФСТЭК 3-й класс защищенности СВТ.

6) Выбор МЭ

Класс защищенности МЭ: 4-5 (АС 1Г)

Можно воспользоваться программным комплексом «Аркан».

Он соответствует требованиям документов: Требования к МЭ, Профиль защиты МЭ (ИТ.МЭ.Д4.ПЗ — тип «Д», четвёртый класс защиты), Требования к СОВ, Профили защиты СОВ (ИТ.СОВ.С4.ПЗ — уровень сети, четвёртый класс защиты).

5) Кейс: 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.

7) Выбор АС

Классификация АС – 2Б (несколько сотрудников, одинаковые доступы, конфиденциальная информация)

А) Подсистема обеспечения целостности:

должна быть обеспечена целостность программных средств СЗИ НСД, обрабатываемой информации, а также неизменность программной среды.

Б) Подсистема управления доступом:

должны осуществляться идентификация и проверка подлинности субъектов доступа при входе в систему по паролю условно-постоянного действия длиной не менее шести буквенно-цифровых символов.

В) Подсистема регистрации и учета:
В АС должны сохраняться все необходимые данные (дата и время входа (выхода) сбъектов, результаты попыток входа и тд)

8) Выбор СВТ:

Класс защищенности СВТ от НСД: 5-6 (дискреционная защита)
Можно воспользоваться продуктами компании “Код безопасности”. Их продукт SecretNet-К 6 сертифицирован по требованиям ФСТЭК 5-й класс защищенности СВТ.

9) Выбор МЭ

Класс защищенности МЭ: 4-5 (АС 2Б)
Можно воспользоваться программным комплексом «Аркан».
Он соответствует требованиям документов: Требования к МЭ, Профиль защиты МЭ (ИТ.МЭ.Д4.ПЗ — тип «Д», четвёртый класс защиты), Требования к СОВ, Профили защиты СОВ (ИТ.СОВ.С4.ПЗ — уровень сети, четвёртый класс защиты).

6) Кейс: 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.

1) Выбор АС

Классификация АС – 3А (1 пользователь, гриф СС)

А) Подсистема обеспечения целостности:
физическая охрана СВТ может обеспечиваться СКУДом и службой охраны архива.

Б) Подсистема управления доступом:
должны осуществляться идентификация и проверка подлинности субъектов доступа при входе в систему по паролю условно-постоянного действия длиной не менее шести буквенно-цифровых символов.

В) Подсистема регистрации и учета:
В АС должны сохраняться все необходимые данные (дата и время входа (выхода) сбъектов, результаты попыток входа и тд)

2) Выбор СВТ:

Класс защищенности СВТ от НСД: 1 (верифицированная защита)
Нет готовых продуктов под СВТ 1, слишком индивидуальны характеристики

3) Выбор МЭ

Класс защищенности МЭ: 2 (СС + АС 3А)
Можно воспользоваться программно-аппаратным комплексом “Рубикон-К”
Он соответствует требованиям документов: Требования к МЭ, Профиль защиты МЭ (ИТ.МЭ.А2.ПЗ — тип «А», второй класс защиты; ИТ.МЭ.А4.ПЗ — тип «А», четвёртый класс защиты; ИТ.МЭ.Б4.ПЗ — тип «Б», четвёртый класс защиты), Требования к СОВ, Профили защиты СОВ (ИТ.СОВ.С4.ПЗ — уровень сети, четвёртый класс защиты).

7) Кейс: 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.

Какие требования РД ФСТЭК не соблюдал сотрудник?

Он 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.