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

Выполнил:
Студент гр. P32151
Соловьев Артемий Александрович

Проверил:
Кондратенко С. С.,
аспирант ФБИТ

Санкт-Петербург 2023г.

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:

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)

Расшифровки:

НСД – несанкционированный доступ.

ПРД – правила разграничения доступа.

СРД – среда разграничения доступа.

КСЗ – комплекс системы защиты.

АС – автоматизированные системы.

СВТ – средства вычислительной техники

МЭ – межсетевой экран.

СЗИ – средства защиты информации.

Кейсы:

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.

   АС относится к первой группе: многопользовательские АС, в которых одновременно обрабатывается и (или) хранится информация разных уровней конфиденциальности. Не все пользователи имеют право доступа ко всей информации АС. Группа содержит пять классов - 1Д, 1Г, 1В, 1Б и 1А.

   Необходимы следующие уровни защиты:

   1) Классификация АС 1Г: Идентификация, проверка подлинности и контроль доступа субъектов: в систему, к программам, каталогам и файлам. (Класс АС 1Г согласно руководящему документу по решению председателя Гостехкомиссии России от 30 марта 1992 г.)
   2) Защищенность СВТ от НСД: Защищенность от НСД: 5. Необходим дискретный принцип контроля доступа, аутентификация и идентификация и т. д. (согласно руководящему документу по решению председателя Гостехкомиссии России от 30 марта 1992 г.)

3) Межсетевой экран: Межсетевой экран: 4. Необходимо: управление доступом (фильтрация данных и трансляция адресов), регистрация, аутентификация и идентификация, целостность, восстановление, тестирование и т.д. (согласно руководящему документу по решению председателя Гостехкомиссии России от 25 июля 1997 г.)

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, так же, 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.

   У одного человека есть доступ ко всей информации, которая может содержать гос.тайну, значит необходимы уровни защиты:

   1) Классификация АС. Классификация АС: 3Б. 1) Идентификация, проверка подлинности и контроль доступа субъектов: в систему, к терминалам (Класс АС 2А согласно руководящему документу по решению председателя Гостехкомиссии России от 30 марта 1992 г.) 2) Регистрация и учет: входа (выхода) субъектов доступа в (из) систему (Класс АС 2А согласно руководящему документу по решению председателя Гостехкомиссии России от 30 марта 1992 г.)
   2) Защищенность от НСД. Защищенность СВТ от НСД: 3. очистка памяти, изоляция модулей, маркировка документов и т.д. (согласно руководящему документу по решению председателя Гостехкомиссии России от 30 марта 1992 г.)
   3) Межсетевой экран. Так как на некоторой информации есть гриф совершенно секретно МЭ 1 или 2. Управление доступом (фильтрация данных и трансляция адресов), идентификация и аутентификация,

тестирование и т.д. (согласно руководящему документу по решению председателя Гостехкомиссии России от 25 июля 1997 г.)

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.

   У одного человека есть доступ ко всей информации, в информации не содержится гос.тайны. Значит необходимы следующие уровни защиты:

   1) Классификация АС. Классификация АС:3Б. Идентификация, проверка подлинности и контроль доступа субъектов: в систему, к программам, каталогам и файлам и т. д. (Класс АС 3Б согласно руководящему документу по решению председателя Гостехкомиссии России от 30 марта 1992 г.)
   2) Защищенность от НСД. Защищенность СВТ от НСД: 6. Дискретный принцип контроля доступа, аутентификация и идентификация и т. д. (согласно руководящему документу по решению председателя Гостехкомиссии России от 30 марта 1992 г.)
   3) Межсетевой экран. Межсетевой экран: 4. Управление доступом (фильтрация данных и трансляция адресов), регистрация, аутентификация и идентификация, целостность, восстановление, тестирование и т. д. (согласно руководящему документу по решению председателя Гостехкомиссии России от 25 июля 1997 г.)

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.

Так как это многопользовательская система с минимальной конфиденциальной информацией, необходимы следующие уровни защиты:

1) Классификация АС. классификация АС: 1Д. Идентификация, проверка подлинности и контроль доступа субъектов: в систему, к программам, каталогам и файлам. (Класс АС 1Г согласно руководящему документу по решению председателя Гостехкомиссии России от 30 марта 1992 г.)
2) Защищенность от НСД. Защищенность СВТ от НСТ: 7. Дискретный принцип контроля доступа, аутентификация и идентификация и т.д. (согласно руководящему документу по решению председателя Гостехкомиссии России от 30 марта 1992 г.)
3) Межсетевой экран. Межсетевой экран: 4. Управление доступом (фильтрация данных и трансляция адресов), регистрация, аутентификация и идентификация, целостность, восстановление, тестирование и т.д. (согласно руководящему документу по решению председателя Гостехкомиссии России от 25 июля 1997 г.)

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.

Так как у всех пользователей разные права, а информация не содержит гос. тайну, необходимы следующие уровни защиты:

1) Классификация АС. Классификация АС: 2Б. Идентификация, проверка подлинности и контроль доступа субъектов в систему, к программам, каталогам и файлам и т.д. (Класс АС 2Б согласно руководящему документу по решению председателя Гостехкомиссии России от 30 марта 1992 г.)
2) Защищенность СВТ от НСД: 6. дискретный принцип контроля доступа, аутентификация и идентификация и т.д. (согласно руководящему документу по решению председателя Гостехкомисси России от 30 марта 1992 г.)
3) Межсетевой экран. Межсетевой экран: 4. Управление доступом (фильтрация данных и трансляция адресов), регистрация, аутентификация и идентификация, целостность, восстановление, тестирование и т.д. (согласно руководящему документу по решению председателя Гостехкомиссии России от 25 июля 1997 г.)

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.

   Так как один пользователь имеет доступ ко всей информации, в которой может содержаться гос.тайна, необходимы следующие уровни защиты:

1) классификация АС: 3А. Идентификация, проверка подлинности и контроль доступа субъектов: в систему, к терминалам, ЭВМ, узлам сети ЭВМ, каналам связи, внешним устройствам ЭВМ, к программам, к томам, каталогам, файлам, записям, полям записей. (Класс АС 3А согласно руководящему документу по решению председателя Гостехкомиссии России от 30 марта 1992 г.), Регистрация и учет: входа (выхода) субъектов доступа в (из) систему (узел сети), выдачи печатных (графических) выходных документов, запуска (завершения) программ и процессов (заданий, задач) и т.д. (Класс АС 3А согласно руководящему документу по решению председателя Гостехкомиссии России от 30 марта 1992 г.)
2) Защищенность от НСД. защищенность СВТ от НСТ: 3. Очистка памяти, изоляция модулей, маркировка документов и т.д. (согласно руководящему документу по решению председателя Гостехкомиссии России от 30 марта 1992 г.)
3) Межсетевой экран : 2. Управление доступом (фильтрация данных и трансляция адресов), идентификация и аутентификация, тестирование и т.д. (согласно руководящему документу по решению председателя Гостехкомиссии России от 25 июля 1997 г.)

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.

Так как это многопользовательская система, в которой содержится конфиденциальная информация, необходимы следующие уровни защиты:

1) Классификация АС. классификация АС: 1Г. Идентификация, проверка подлинности и контроль доступа субъектов: в систему, к программам, каталогам и файлам. (Класс АС 1Г согласно руководящему документу по решению председателя Гостехкомиссии России от 30 марта 1992 г.)
2) Защищенность СВТ от НСД: 5. Дискретный принцип контроля доступа, аутентификация и идентификация и т.д. (согласно руководящему документу по решению председателя Гостехкомиссии России от 30 марта 1992 г.)
3) Межсетевой экран: 4. Управление доступом (фильтрация данных и трансляция адресов), регистрация, аутентификация и идентификация, целостность, восстановление, тестирование и т.д. (согласно руководящему документу по решению председателя Гостехкомиссии России от 25 июля 1997 г.)

Какие требования РД ФСТЭК не соблюдал сотрудник?

Сотрудник не соблюдал требования РД «Средства вычислительной техники. Защита от несанкционированного доступа к информации». А именно, установил нелицензионное ПО, в котором оказался троян-стиллер, из-за чего была заражена система, и произошла утечка данных пользователей.

Вывод: в ходе работы были получены знания по работе с некоторыми руководящими документами ФСТЭК, а также на рассматриваемых кейсах были получены навыки в классифицировании АС, определении защищенности СВТ от НСД и классификации защищенности межсетевых экранов по следующему принципу: 1) нужно определить группы и количество пользователей 2)определить уровень тайны 3) исходя из выше определенных данных, определить следующие характеристики.