Министерство науки и высшего образования Российской Федерации
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 группы N3246,

Суханкулиев Мухаммет

(подпись)

Проверила:

Коржук Виктория Михайловна,

доцент (квалификационная категория "ординарный доцент")

(отметка о выполнении)

(подпись)

Санкт-Петербург

2024 г.

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

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

Для достижения поставленной цели необходимо решить следующие задачи:

1. Ознакомиться с руководящими документами:
    - **Защита от НСД термины** (Руководящий документ от 30 марта 1992 г. - ФСТЭК России (fstec.ru)) + **Концепция защиты от НСД** (Руководящий документ от 30 марта 1992 г. - ФСТЭК России (fstec.ru))
    - **Автоматизированные системы. Защита от НСД** Руководящий документ от 30 марта 1992 г. - ФСТЭК России (fstec.ru)
    - **Средства вычислительной техники. Защита от НСД (**Руководящий документ от 30 марта 1992 г. - ФСТЭК России (fstec.ru)**)**
    - **СВТ. Межсетевые экраны. Защита от НСД (**Руководящий документ от 25 июля 1997 г. - ФСТЭК России (fstec.ru)**)**
    - Сводная таблица РД ФСТЭК (до профилей защиты) по порядку и в разрезе грифов / Хабр (habr.com)
2. Решить представленные кейсы.
3. Сделать вывод о том, в каком порядке необходимо начинать решение различных задач.

1 ОЗНАКОМИТЬСЯ С РУКОВОДЯЩИМИ ДОКУМЕНТАМИ

1.1 Защита от НСД термины. Концепция защиты от НСД

АС - автоматизированная система

КСЗ - комплекс средств защиты

НСД - несанкционированный доступ

НДВ - недекларированные возможности

ПЗ - профиль защиты

ОС - операционная система

ППП - пакет прикладных программ

ПРД - правила разграничения доступа

РД - руководящий документ

СВТ - средства вычислительной техники

СЗИ - система защиты информации

СЗИ НСД - система защиты информации от несанкционированного доступа

СЗСИ - система защиты секретной информации

СНТП - специальное научно-техническое подразделение

СРД - система разграничения доступа

СУБД - система управления базами данных

ТЗ - техническое задание

ЭВМ - электронно-вычислительная машина

ЭВТ - электронно-вычислительная техника

2.2. НСД — это доступ к информации, нарушающий правила доступа с использованием штатных средств АС или СВТ.

4.1. Нарушители классифицируются по возможностям штатных средств АС и СВТ, выделяются четыре уровня.

5. К основным способам НСД относятся:

- Прямое обращение к объектам.

- Создание программ и средств для обхода защиты.

- Модификация средств защиты.

- Внедрение механизмов, нарушающих работу АС или СВТ.

6.1. Защита осуществляется системой разграничения доступа (СРД).

9.1. Организация защиты должна быть частью общей системы безопасности информации.

1.2 Автоматизированные системы. Защита от НСД

1.1. Классификация распространяется на все АС, обрабатывающие конфиденциальную информацию.

1.8. Существует девять классов защищенности АС от НСД.

1.9. Третья группа включает однопользовательские АС с доступом к информации одного уровня (классы 3Б и 3А).

Вторая группа включает АС с равным доступом пользователей к данным разного уровня конфиденциальности (классы 2Б и 2А).

Первая группа включает многопользовательские АС с различными уровнями доступа к информации (классы 1Д, 1Г, 1В, 1Б, 1А).

2.2. Защита от НСД включает четыре подсистемы:

- управление доступом;
- регистрация и учет;
- криптографическая защита;
- обеспечение целостности.

1.3 Средства вычислительной техники. Защита от НСД

1.4. Устанавливается семь классов защищенности СВТ от НСД к информации. Самый низкий класс – седьмой, самый высокий – первый.

Классы подразделяются на четыре группы, отличающиеся качественным уровнем защиты:

- первая группа содержит только один седьмой класс;
- вторая группа характеризуется дискреционной защитой и содержит шестой и пятый классы;
- третья группа характеризуется мандатной защитой и содержит четвертый, третий и второй классы;
- четвертая группа характеризуется верифицированной защитой и содержит только первый класс.

1.4 СВТ. Межсетевые экраны. Защита от НСД

МЭ — это локальное (однокомпонентное) или функционально-распределенное (комплекс) средство, контролирующее информацию, поступающую в АС или выходящую из нее. Оно обеспечивает защиту через фильтрацию информации, анализируя ее по критериям и принимая решение о ее передаче.

1.5. Устанавливается пять классов защищенности МЭ.

Каждый класс характеризуется определенной минимальной совокупностью требований по защите информации.

Самый низкий класс защищенности - пятый, применяемый для безопасного взаимодействия АС класса 1Д с внешней средой, четвертый - для 1Г, третий - 1В, второй - 1Б, самый высокий - первый, применяемый для безопасного взаимодействия АС класса 1А с внешней средой.

1.5 Сводная таблица РД ФСТЭК

<table>
<tr><td colspan="2" rowspan="3">доп. параметры</td><td colspan="7">Грифы</td></tr>
<tr><td colspan="4">Гос. тайна</td><td colspan="3">Конфиденциальная информация</td></tr>
<tr><td>ОС (особой важности)</td><td colspan="2">СС (совершенно секретно)</td><td>С (секретно)</td><td colspan="3">…</td></tr>
<tr><td rowspan="3">Классификация АС</td><td>один пользователь</td><td colspan="4">3А</td><td colspan="3">3Б</td></tr>
<tr><td>пользователи имеют одинаковые права доступа ко всей информации</td><td colspan="4">2А</td><td colspan="3">2Б</td></tr>
<tr><td>не все пользователи имеют право доступа ко всей информации</td><td>1А</td><td colspan="2">1Б</td><td>1В</td><td>1Г</td><td colspan="2">1Д</td></tr>
<tr><td colspan="2">Защищенность СВТ от НСД</td><td>1, 2</td><td colspan="2">3</td><td>4</td><td>5</td><td>6</td><td>7</td></tr>
<tr><td colspan="2">Межсетевые экраны
* Будет заменен профилями защиты с декабря 2016г.</td><td>1</td><td colspan="2">2</td><td>3</td><td>4</td><td colspan="2">5</td></tr>
<tr><td colspan="2">Контроль НДВ</td><td>1</td><td colspan="2">2</td><td>3</td><td colspan="3">4</td></tr>
<tr><td colspan="2">Профили защиты</td><td>1</td><td colspan="2">2</td><td>3</td><td colspan="3">4 и т. д.</td></tr>
</table>

2 РЕШЕНИЕ КЕЙСОВ

На основе описания предприятия предложить совокупность подходящих по требованиям безопасности Автоматизированный 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).

2.1 №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 к “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.

Решение:

АС	СВТ	МЭ	Контроль НДВ	ПЗ
1Г	4	4	4	4

- Выбираем класс 1, т. к. нужно определить различным пользователям различный доступ к конфиденциальной информации. Чтобы избежать краж определяем класс 1Г, т. к. в него входит «2.1. Регистрация и учет: выдачи печатных (графических) выходных документов».
- Согласно АС определяем необходимую защищенность СВТ от НСД 5-го класса, хотя в данном случаю лучше выбрать 4-й класс с мандатным принципов контроля доступа и защитой ввода и вывода на отчуждаемый физический носитель информации.
- Согласно АС определяем МЭ 4-го класса защищенности, содержащий регистрацию но не требующий идентификацию и аутентификацию.
- Контроль НДВ, как и ПЗ определим 4-й, т. к. он достаточен для ПО, используемого при защите конфиденциальной информации.

2.2 №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.

Решение:

АС	СВТ	МЭ	Контроль НДВ	ПЗ
2А	3	2	2	2

- Выбираем класс 2, т. к. хоть работает один сотрудник, в архиве содержится гос. тайна доступ к которой имеет и руководство города – определим класс 2А.
- В архиве хранится информация под грифом совершенно секретно – определяем необходимую защищенность СВТ – 3 класс, отличающийся требованием взаимодействия пользователя с КСЗ и надежным восстановлением.
- Согласно АС и грифу совершенно секретно - определяем МЭ 2-го класса защищенности.
- Контроль НДВ, как и ПЗ определим 2-й, отличающимся анализом алгоритма работы функциональных объектов, построенных по исходным текстам контролируемого ПО и динамическим анализ исходных текстов программ.

2.3 №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.

Решение:

АС	СВТ	МЭ	Контроль НДВ	ПЗ
3Б	6	5	4	4

- Выбираем класс 3Б, т. к. работает один сотрудник, желающий защитить свою конфиденциальную информацию, Регистрация и учет выдачи печатных выходных документов и использование сертифицированных средств защиты не требуется.
- Защищенность СВТ определим 6-го класса. Очистка памяти, Гарантии проектирования, Регистрация в нашем случае не требуются.
- Согласно АС и СВТ определим МЭ 5-го класса защищенности.
- Контроль НДВ, как и ПЗ определим 4-й.

2.4 №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.

Решение:

АС	СВТ	МЭ	Контроль НДВ	ПЗ
1Д	6	5	4	4

- Выбираем класс 1Д, т. к. различные пользователи имеют различный доступ к информации. Конфиденциальная информация в системе не передается поэтому более высокая степень защиты не требуется.
- Защищенность СВТ определим 6-го класса. Можно даже 7-й класс, т. к. пренебрегая такими показателями как «Тестирование», «Тестовая документация», мы особо ничего не потеряем.
- Согласно АС и СВТ определим МЭ 5-го класса защищенности.
- Контроль НДВ, как и ПЗ определим 4-й.

2.5 №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.

Решение:

АС	СВТ	МЭ	Контроль НДВ	ПЗ
2Б	5	4	4	4

- Выбираем класс 2Б, т. к. все пользователи будут иметь доступ ко всей информации.
- Защищенность СВТ определим 5-го класса. Регистрацию лучше вести в таком случае.
- Согласно АС и СВТ определим МЭ 4-го класса защищенности.
- Контроль НДВ, как и ПЗ определим 4-й.

2.6 №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.

Решение:

АС	СВТ	МЭ	Контроль НДВ	ПЗ
3А	3	2	2	2

- Выбираем класс 3А, т. к. работает один рабочий, При этом в архиве находятся данные с грифами «совершенно секретно».
- Согласно АС и грифу «совершенно секретно» защищенность СВТ определим 3-го класса.
- Согласно АС и СВТ определим МЭ 2-го класса защищенности.
- Контроль НДВ, как и ПЗ определим 2-й.

2.1 №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.

Какие требования РД ФСТЭК не соблюдал сотрудник?

Решение:

АС	СВТ	МЭ	Контроль НДВ	ПЗ
1Г	5	4	4	4

- Выбираем класс 1Г, т. к. он требует регистрацию и учет: доступа программ субъектов доступа к защищаемым файлам, включая их создание и удаление, передачу по линиям и каналам связи и доступа программ субъектов доступа к терминалам, ЭВМ, узлам сети ЭВМ, каналам связи, внешним устройствам ЭВМ, программам, томам, каталогам, файлам, записям, полям записей. Это поможет определить троян.
- Защищенность СВТ определим 5-го класса. Однако в данном случае лучше использовать мандатный принцип контроля доступа и изоляцию модулей, лучше подумать и, может быть, выбрать 4-й уровень защищенности.
- Согласно АС и СВТ определим МЭ 4-го класса защищенности.
- Контроль НДВ, как и ПЗ определим 4-й.

1. Сотрудник не проверял источники загрузки ПО, что привело к установке вредоносного программного обеспечения, т. к.
2. Не было проведено достаточное обучение сотрудников по вопросам информационной безопасности, что могло бы предотвратить скачивание вредоносного ПО.
3. Регулярное обновление антивирусных систем. Так же необходимы регулярные обновления и патчи для всех используемых программ.
4. Важно иметь механизмы для оперативного реагирования на инциденты безопасности и уведомления соответствующих служб о возможных угрозах.

ЗАКЛЮЧЕНИЕ

Я ознакомился с РД ФСТЭК, что позволило глубже изучить классификацию АС, СВТ и МЭ с учетом требований по безопасности.

Были рассмотрены различные сценарии защиты АС и СВТ. На основании представленных решений можно сделать следующий вывод:

Процесс обеспечения защиты информации следует начинать с определения категории АС на основе прав доступа пользователей к системе. Затем важно более точно определить необходимый класс защищенности внутри выбранной категории. Это позволит правильно подобрать класс защищенности для СВТ и МЭ, исходя из специфики задачи и требований безопасности.

Полученные знания и навыки будут полезны для дальнейшего развития в области информационной безопасности.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Руководящий документ от 30 марта 1992 г. - ФСТЭК России (fstec.ru)
2. Руководящий документ от 30 марта 1992 г. - ФСТЭК России (fstec.ru)
3. Руководящий документ от 30 марта 1992 г. - ФСТЭК России (fstec.ru)
4. Руководящий документ от 30 марта 1992 г. - ФСТЭК России (fstec.ru)
5. Руководящий документ от 25 июля 1997 г. - ФСТЭК России (fstec.ru)
6. Сводная таблица РД ФСТЭК (до профилей защиты) по порядку и в разрезе грифов / Хабр (habr.com)
7. Средства защиты информации (СЗИ) и их классификация от ФСТЭК и ФСБ (anti-malware.ru)
8. Руководящий документ от 4 июня 1999 г. N 114 - ФСТЭК России (fstec.ru)
9. Руководящий документ, 2003 год - FSTEC of Russia
10. Google-диск – 24/25 ТИБиМЗИ - Ретроспективный анализ подходов к формированию множества угроз информации - https://drive.google.com/file/d/11fXC8dlwv-krVRNaloXpFFVb6ZRS7q5_/view?usp=sharing
11. Google-диск – 24/25 ТИБиМЗИ – Методический документ: Методика оценки угроз безопасности информации – https://drive.google.com/file/d/12hfnnuQpKGi85KcCYPZX87DfLrLCGXbO/view?usp=sharing