**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**](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**](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://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/>

1. Решить представленные кейсы;
2. 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)

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.

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.

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. Не смотря 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.

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.

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.

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.

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?