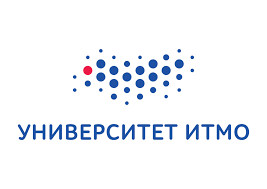
**Министерство науки и высшего образования Российской Федерации**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ  
**НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИТМО**



**Факультет безопасности информационных технологий**

**Дисциплина:**

«Теория информационной безопасности и методология защиты

информации»

**ОТЧЕТ ПО ЛАБОРАТОРНОЙ РАБОТЕ №2**

«РД ФСТЭК»

**Выполнили:**

Нгуен Тхи Маи, студент группы: N3245

*\_\_\_\_\_\_\_\_\_\_*

(подпись)

**Проверил:**

Есипов Дмитрий Андреевич, ассистент ФБИТ

*\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*

(отметка о выполнении)

*\_\_\_\_\_\_\_\_\_\_\_\_\_*

(подпись)

# СОДЕРЖАНИЕ

В[ведение 2](#_heading=h.gjdgxs)

[1. РД ФСТЭК 3](#_heading=h.y10pjzpe32i2)

[1.1 Классификации СЗИ на основании требований ФСТЭК России 3](#_heading=h.bpz8x0jjvfll)

[2. Решение кейсов 5](#_heading=h.3jlshhhzcmrj)

[2.1 Кейс 1: 5](#_heading=h.cqeiq9w1clbw)

[2.2 Кейс 2: 6](#_heading=h.s3r4wsaqqq0)

[2.3 Кейс 3: 6](#_heading=h.5i1n47gtpvvj)

[2.4 Кейс 4: 7](#_heading=h.et0ezp7phoqi)

[2.5 Кейс 5: 7](#_heading=h.kueycadt04tf)

[2.6 Кейс 6: 8](#_heading=h.35xrh9umbh8s)

[2.7 Кейс 7: 9](#_heading=h.cs8glhjve42i)

[Вывод по работе. 10](#_heading=h.t0p55bvsw0th)

# ВВЕДЕНИЕ

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

Для достижения поставленной цели необходимо решить следующие задачи:

* Ознакомиться с руководящими документами;
* Решить представленные кейсы;
* Сделать вывод о том, в каком порядке необходимо начинать решение различных задач.

# РД ФСТЭК

На территории Российской Федерации обладатели информации и операторы информационных систем обязаны блокировать попытки несанкционированного доступа к информации, а также осуществлять мониторинг состояния защищенности ИТ-инфраструктуры на постоянной основе. При этом защита информации обеспечивается за счет принятия различных мер, включая технические.

Средства защиты информации, или СЗИ обеспечивают защиту информации в информационных системах, по сути представляющих собой совокупность хранимой в базах данных информации, информационных технологий, обеспечивающих ее обработку, и технических средств.

Для современных информационных систем характерно использование различных аппаратно-программных платформ, территориальная распределенность компонентов, а также взаимодействие с открытыми сетями передачи данных.

Структурой, определяющей порядок и координирующей действия обеспечения не криптографическими методами ИБ, является ФСТЭК России (ранее — Государственная техническая комиссия при Президенте Российской Федерации, Гостехкомиссия).

## 1.1 Классификации СЗИ на основании требований ФСТЭК России

Проникая в систему, злоумышленник преодолевает выстроенную систему защиты информации, осуществляет несанкционированный доступ. НСД. ФСТЭК России под системой защиты информации от НСД понимает совокупность мер организационного характера и программно-технических СЗИ от НСД. Функциональность СЗИ от НСД должна предотвращать или существенно затруднять несанкционированное проникновение в обход правил разграничения доступа, реализованных штатными средствами. Эти средства входят в состав средств вычислительной техники и автоматизированных систем в виде совокупности программного и технического обеспечения

При этом, регулятор полагает, что средства вычислительной техники являются элементами, из которых строятся автоматизированные системы. Поэтому, не решая прикладных задач, СВТ не содержат пользовательской информации. Совокупность требований в части защиты СВТ и АС образуют т. н. класс защищенности.

В качестве СЗИ регулятором рассматриваются т.н. межсетевые экраны — средства, реализующее контроль за информацией, направленной в АС или исходящей из нее. Межсетевые экраны выполняют фильтрацию информации по заданным критериям.

К СЗИ также относят т.н. средства обнаружения вторжений. Они представляют собой средства, автоматизирующие процесс контроля событий в системе (сети) с проведением анализа этих событий с целью поисках признаков инцидента ИБ.

Антивирусные СЗИ должны выявлять и соответствующим образом реагировать на средства несанкционированного уничтожения, блокирования, модификации, копирования информации или нейтрализации СЗИ.

В рамках реализации мер по управлению доступом предусмотрено обеспечение так называемой доверенной загрузки. Для этого применяются также соответствующие СЗИ.

Меры по защите машинных носителей информации в части обеспечения контроля за их использованием реализуются с помощью средств контроля съемных носителей.

# РЕШЕНИЕ КЕЙСОВ

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)

## 2.1 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.

* Классификация АС - 1Г: Потому что в системе работает
* Пользователи имеют разные права доступа к информации. Уровень информационной безопасности также разный. Конкурирующие компании также направили своих сотрудников на фабрики, чтобы попытаться украсть информацию, необходимо внедрить систему идентификации, аутентификации и контроля доступа пользователей к различным информационным объектам. Это означает, что требуется автоматизированная система не ниже 1-го класса (Г) по требованиям информационной безопасности.
* Поскольку сотрудники конкурирующих компаний могут получить несанкционированный доступ к данным, необходимо защитить данные от несанкционированного доступа. Также требуется контроль ввода-вывода конфиденциальной информации. Поэтому класс защищенности системы от несанкционированного доступа должен быть не ниже 4-го и уровень защищенности СВТ
* Класс защищенности МЭ: 4. Межсетевые экраны 4 класса требуются в случае защиты взаимодействия автоматизированных систем класса 1Г с внешней средой.

## 2.2 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.

* Классификация АС - 3A: Потому что это засекреченная информация, являющаяся государственной тайной, необходимо использовать сертифицированные средства защиты информации. Следовательно, класс защищенности автоматизированной системы должен быть не ниже 3А.
* Поскольку обрабатывается информация с грифом "совершенно секретно", требуется надежное восстановление системы после сбоев и аварийных ситуаций. Также необходимо организовать эффективное взаимодействие пользователей с комплексной системой защиты информации. Следовательно, класс защищенности системы от несанкционированного доступа должен быть не ниже 3-го и уровень защищенности СВТ
* Класс защищенности МЭ: 2. Информация под грифом «совершенно секретно», обрабатываемая в системах уровня 3А и 2А, требует использования межсетевого экрана не ниже указанного типа.

## 2.3 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. 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.

* Классификация АС - 3Б: В этом случае речь идет об однопользовательских системах. Пользователь допущен ко всей информации. Уровень конфиденциальности носителей — одинаковый. 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;
* Кроме того, необходимо предусмотреть: идентификацию и аутентификацию пользователей, регистрацию запросов на доступ к ресурсам, создание и удаление объектов, изменение настроек безопасности. Такая конфигурация обеспечит защищенность системы от несанкционированного доступа 5-го уровня в соответствии с требованиями и и уровень защищенности СВТ 5.
* Класс защищенности МЭ: 5.

## 2.4 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.

* Классификация АС - 1Г: потому что АС является обеспечением разных прав по доступу и информация разных уровней конфиденциальности, то необходимо АС первой группы. Для предотвращения несанкционированного доступа сотрудников к информационным ресурсам других пользователей необходимо внедрить систему контроля доступа к таким объектам, как тома, каталоги, файлы, записи и поля записей.
* Поскольку достаточно обеспечить регистрацию фактов доступа пользователей к защищаемым информационным ресурсам, класс защищенности системы от несанкционированного доступа может быть определен как 5-й и уровень защищенности СВТ 5. Реализация более высокого класса защиты не требуется.
* Класс защищенности МЭ: 4.

## 2.5 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.

* Классификация АС - 2Б: Пользователи имеют равные права на всю информацию. Сама информация размещается на носителях с разным уровнем безопасности. Требуется обеспечить идентификацию, проверку подлинности и контроль доступа субъектов только в систему. Кроме того, необходима регистрация и учет только фактов входа (выхода) субъектов доступа в (из) систему (узел сети).
* Необходимо контролировать, какие пользователи имеют доступ к сети. Не требуется контролировать действия пользователей после аутентификации, а также регистрировать другие события безопасности. Требуемый минимальный уровень защиты с упрощенным контроллером и уровнем безопасности и регистрации SVT 5.
* Межсетевые экраны (МЭ) – 4: Межсетевые экраны 4 класса требуются в случае защиты взаимодействия автоматизированных систем класса 1Г с внешней средой.

## 2.6 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.

* Классификация АС - 3A: потому что один пользователь допущенный ко всей информации и у него одинаковый уровень конфиденциальности информации,следовательно будет 3- гр.Требуется обеспечить защиту информации обрабатываемой в системе с учетом следующих факторов: информация имеет грифы Секретно и Совершенно секретно. Необходимо использовать только сертифицированные средства защиты. Обязательна очистка, обнуление, обезличивание оперативной памяти ЭВМ и внешних накопителей после работы с информацией. Учитывая эти требования, рекомендуется применить класс защиты АС 3A.
* Уровень защищенности от несанкционированного доступа: информация имеет гриф Совершенно секретно. Необходимо взаимодействие пользователя с комплексом защиты информации. Должна обеспечиваться надежная регистрация событий. Следовательно, требуется 3 уровень защищенности от несанкционированного доступа и уровень защищенности СВТ 3.
* Межсетевые экраны (МЭ) – 3: если в автоматизированных системах классов 3А, 2А происходит обработка информации с грифом «секретно», потребуется межсетевой экран не ниже 3 класса.

## 2.7 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-стиллером. 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.

* Сотрудники государственной энергетической компании нарушили следующие требования РД ФСТЭК:
* Требования к обеспечению безопасности информационных систем от несанкционированного доступа (НСД). Согласно РД ФСТЭК, сотрудники должны использовать только официальные источники программного обеспечения и не скачивать установщики из непроверенных источников. В данном случае сотрудник скачал фейковый установщик IDE, который содержал троян-стиллер.
* Требования к обеспечению безопасности персональных данных. Согласно РД ФСТЭК, сотрудники должны обеспечивать конфиденциальность персональных данных клиентов. В данном случае в результате утечки данных к злоумышленникам попали личные данные клиентов, внутренние метрики, платежные данные, включая номера карт и CVV.
* Требования к обеспечению безопасности информационных систем от вредоносного программного обеспечения. Согласно РД ФСТЭК, сотрудники должны использовать антивирусное программное обеспечение и регулярно обновлять антивирусные базы данных. В данном случае сотрудник не использовал антивирусное программное обеспечение или не обновлял его антивирусные базы данных, что позволило трояну-стиллеру проникнуть в систему.

# ЗАКЛЮЧЕНИЕ

* В процессе выполнения лабораторной работы я изучил нормативные документы ФСТЭК России, регламентирующие требования к защите информации от несанкционированного доступа. Было решено 7 практических кейсов, в каждом из которых определялись класс защищённости автоматизированной системы и средств вычислительной техники от НСД, а также выбиралось межсетевое экранирование.
* В результате выявил, что при решении подобных задач наиболее рационально сначала определить класс защищённости автоматизированной системы от НСД. На основе полученного класса выбрать соответствующее межсетевое экранирование. После этого определить класс защищённости средств вычислительной техники от несанкционированного доступа. Такой подход позволяет последовательно и обоснованно подойти к выбору мер защиты информации.