

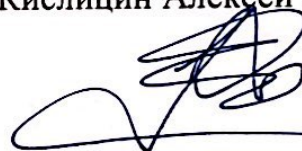
**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«САНКТ-ПЕТЕРБУРГСКИЙ НАЦИОНАЛЬНЫЙ
ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИНФОРМАЦИОННЫХ
ТЕХНОЛОГИЙ,
МЕХАНИКИ И ОПТИКИ»**

Факультет информатики и вычислительной техники

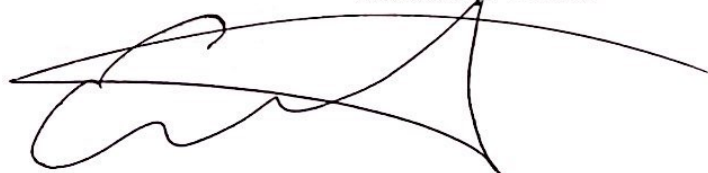
Дисциплина:
«Теория информационной безопасности и методология защиты информации»

ОТЧЕТ ПО ЛАБОРАТОРНОЙ РАБОТЕ №2

Выполнил:
Студент гр. Р3231
Кислицин Алексей Андреевич



Проверил:
Есипов Дмитрий Андреевич,
инженер ФБИТ



Санкт-Петербург
2022г.

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

Задачи:

1. Ознакомиться с руководящими документами:

<https://fstec.ru/tekhnicheskayazashchitainformatsii/dokumenty/114spetsialnyenormativnyedokumenty/382rukovodyashchijdokumentprikazpredsedatelyagostekhhkomissiirossiiot4iyunya1999gn114>

Защита от НСД термины

(<https://fstec.ru/tekhnicheskayazashchitainformatsii/dokumenty/114spetsialnyenormativnyedokumenty/386rukovodyashchijdokumentresheniepredsedatelyagostekhhkomissiirossiiot30marta1992g3>) + Концепция защиты от

НСД

Автоматизированные системы. Защита от НСД

<https://fstec.ru/tekhnicheskayazashchitainformatsii/dokumenty/114spetsialnyenormativnyedokumenty/384rukovodyashchijdokumentresheniepredsedatelyagostekhhkomissiirossiiot30marta1992g>

№187з

Средства вычислительной техники. Защита от НСД

(<https://fstec.ru/tekhnicheskayazashchitainformatsii/dokumenty/114spetsialnyenormativnyedokumenty/385rukovodyashchijdokumentresheniepredsedatelyagostekhhkomissiirossiiot30marta1992g2>)

СВТ. Межсетевые экраны. Защита от НСД (

<https://fstec.ru/tekhnicheskayazashchitainformatsii/dokumenty/114spetsialnyenormativnyedokumenty/383rukovodyashchijdokumentresheniepredsedatelyagostekhhkomissiirossiiot25iyulya1997g>)

<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 защищённости 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, причём 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 – многопользовательская 1Г персональные данные (конфиденциальная информация – не все пользователи имеют право доступа ко всей информации)

Защищённость СВТ от НСД – 5

Межсетевые экраны (МЭ) – 4

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.

Классификация АС – один пользователь – 3А (гос. тайна)

Защищённость СВТ от НСД – 3

Межсетевые экраны (МЭ) – 2

Требования к классу защищённости 1Г

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;
- должна осуществляться идентификация терминалов, ЭВМ, узлов сети ЭВМ, каналов связи, внешних устройств ЭВМ по логическим именам;
- должна осуществляться идентификация программ, томов, каталогов, файлов, записей, полей записей по именам;
- должен осуществляться контроль доступа субъектов к защищаемым ресурсам в соответствии с матрицей доступа.

Подсистема регистрации и учёта:

- 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 аппаратного отключения АС. В параметрах регистрации указываются:

- дата и время входа (выхода) субъекта доступа в систему (из системы) или загрузки (останова) системы;

- результат попытки входа: успешная или неуспешная несанкционированная;

- идентификатор (код или фамилия) субъекта, предъявленный при попытке доступа;

- код или пароль, предъявленный при неуспешной попытке;

- должна осуществляться регистрация выдачи печатных (графических) документов на "твёрдую" копию. В параметрах регистрации указываются:

- дата и время выдачи (обращения к подсистеме вывода);

- спецификация устройства выдачи [логическое имя (номер) внешнего устройства];

- краткое содержание (наименование, вид, шифр, код) и уровень конфиденциальности документа;

- идентификатор субъекта доступа, запросившего документ;

- должна осуществляться регистрация запуска (завершения) программ и процессов (заданий, задач), предназначенных для обработки защищаемых файлов. В параметрах регистрации указываются:

- дата и время запуска;

- имя (идентификатор) программы (процесса, задания);

- идентификатор субъекта доступа, запросившего программу (процесс, задание);

- результат запуска (успешный, неуспешный несанкционированный);

- должна осуществляться регистрация попыток доступа программных средств (программ, процессов, задач, заданий) к защищаемым файлам.

В параметрах регистрации указываются:

- дата и время попытки доступа к защищаемому файлу с указанием ее результата: успешная, неуспешная несанкционированная;

- идентификатор субъекта доступа;

- спецификация защищаемого файла;

- должна осуществляться регистрация попыток доступа программных средств к следующим дополнительным защищаемым объектам доступа: терминалам, ЭВМ, узлам сети ЭВМ, линиям (каналам) связи, внешним устройствам ЭВМ, программам, томам, каталогам, файлам, записям, полям записей.

В параметрах регистрации указываются:

- дата и время попытки доступа к защищаемому объекту с указанием ее результата: успешная, неуспешная несанкционированная;

- идентификатор субъекта доступа;

- спецификация защищаемого объекта [логическое имя (номер)];

- должен проводиться учёт всех защищаемых носителей информации с помощью их маркировки и с занесением учётных данных в журнал (учётную карточку);

- учёт защищаемых носителей должен проводиться в журнале (картотеке) с регистрацией их выдачи (приёма);

- должна осуществляться очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти ЭВМ и внешних накопителей. Очистка осуществляется однократной произвольной записью в освобождаемую область памяти, ранее использованную для хранения защищаемых данных (файлов);

- 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 надёжных 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.

Требования к показателям пятого класса защищённости:

- Дискреционный принцип контроля доступа.
- Данные требования включает в себя аналогичные требования шестого класса.
- Дополнительно должны быть предусмотрены средства управления, ограничивающие распространение прав на доступ.
- Очистка памяти.
- При первоначальном назначении или при перераспределении внешней памяти КСЗ должен предотвращать доступ субъекту к остаточной информации.
- Идентификация и аутентификация.

- Данные требования полностью совпадают с аналогичными требованиями шестого класса.

- Гарантии проектирования.

- На начальном этапе проектирования СВТ должна быть построена модель защиты. Модель должна включать в себя ПРД к объектам и непротиворечивые правила изменения ПРД.

- Регистрация.

- КСЗ должен быть в состоянии осуществлять регистрацию следующих событий:

- использование идентификационного и аутентификационного механизма;

- запрос на доступ к защищаемому ресурсу (открытие файла, запуск программы и т.д.);

- создание и уничтожение объекта;

- действия по изменению ПРД.

- Для каждого из этих событий должна регистрироваться следующая информация:

- дата и время;

- субъект, осуществляющий регистрируемое действие;

- тип события (если регистрируется запрос на доступ, то следует отмечать объект и тип доступа);

- успешно ли осуществилось событие (обслужен запрос на доступ или нет).

- КСЗ должен содержать средства выборочного ознакомления с регистрационной информацией.

- Целостность КСЗ.

- В СВТ пятого класса защищённости должны быть предусмотрены средства периодического контроля за целостностью программной и информационной части КСЗ.

- Тестирование.

- В СВТ пятого класса защищённости должны тестироваться:

- реализация ПРД (перехват явных и скрытых запросов на доступ, правильное распознавание санкционированных и несанкционированных запросов, средства защиты механизма разграничения доступа, санкционированные изменения ПРД);

- успешное осуществление идентификации и аутентификации, а также их средства защиты;

- очистка памяти;

- регистрация событий, средства защиты регистрационной информации и возможность санкционированного ознакомления с ней;

- работа механизма, осуществляющего контроль за целостностью КСЗ.

- Руководство пользователя.

- Данное требование совпадает с аналогичным требованием шестого класса.

- Руководство по КСЗ.

- Данный документ адресован администратору защиты и должен содержать:

- описание контролируемых функций;

- руководство по генерации КСЗ;

- описания старта СВТ, процедур проверки правильности старта, процедур работы со средствами регистрации.

- Тестовая документация.

- Должно быть предоставлено описание тестов и испытаний, которым подвергалось СВТ (в соответствии с требованиями п.2.3.7), и результатов тестирования.

- Конструкторская и проектная документация.
- Должна содержать:
 - описание принципов работы СВТ;
 - общую схему КСЗ;
 - описание интерфейсов КСЗ с пользователем и интерфейсов модулей КСЗ;
 - модель защиты;
 - описание механизмов контроля целостности КСЗ, очистки памяти, идентификации и аутентификации.

Требования к четвёртому классу защищённости МЭ:

- Управление доступом.
- Данные требования полностью включают аналогичные требования пятого класса.
 - Дополнительно МЭ должен обеспечивать:
 - фильтрацию пакетов служебных протоколов, служащих для диагностики и управления работой сетевых устройств;
 - фильтрацию с учётом входного и выходного сетевого интерфейса как средство проверки подлинности сетевых адресов;
 - фильтрацию с учётом любых значимых полей сетевых пакетов.
 - Регистрация.
 - МЭ должен обеспечивать возможность регистрации и учёта фильтруемых пакетов. В параметры регистрации включаются адрес, время и результат фильтрации.
- Администрирование: идентификация и аутентификация.
- Данные требования полностью совпадают с аналогичными требованиями пятого класса.
 - Администрирование: регистрация.
 - Данные требования включают аналогичные требования пятого класса.

- Дополнительно МЭ должен обеспечивать регистрацию запуска программ и процессов (заданий, задач).

- Целостность.

- Данные требования полностью совпадают с аналогичными требованиями пятого класса.

- Восстановление.

- Данные требования полностью совпадают с аналогичными требованиями пятого класса.

- Тестирование.

- В МЭ должна обеспечиваться возможность регламентного тестирования:

- реализации правил фильтрации;

- процесса регистрации;

- процесса идентификации и аутентификации администратора МЭ;

- процесса регистрации действий администратора МЭ;

- процесса контроля за целостностью программной и информационной части МЭ;

- процедуры восстановления.

- Руководство администратора МЭ.

- Данные требования полностью совпадают с аналогичными требованиями пятого класса.

- Тестовая документация.

- Должна содержать описание тестов и испытаний, которым подвергался МЭ, и результаты тестирования.

- Конструкторская (проектная) документация.

- Данные требования полностью совпадают с аналогичными требованиями пятого класса по составу документации.

Требования к классу защищённости 3А:

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.

Подсистема регистрации и учёта:

- 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. В параметрах регистрации указываются:

- дата и время входа (выхода) субъекта доступа в систему (из системы) или загрузки (останова) системы;

- результат попытки входа: успешная или неуспешная (при НСД);

- должна осуществляться регистрация выдачи печатных (графических) документов на "твёрдую" копию. Выдача должна сопровождаться автоматической маркировкой каждого листа (страницы) документа порядковым номером и учётными реквизитами АС с указанием на последнем листе документа общего количества листов (страниц).

В параметрах регистрации указываются:

- дата и время выдачи (обращения к подсистеме вывода);

- краткое содержание документа (наименование, вид, код, шифр) и уровень его конфиденциальности;

- спецификация устройства выдачи [логическое имя (номер) внешнего устройства];

- должен проводиться учёт всех защищаемых носителей информации с помощью их маркировки и с занесением учётных данных в журнал (учётную карточку);

- должно проводиться несколько видов учёта (дублирующих) с регистрацией выдачи (приёма) носителей информации;

- должна осуществляться очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти ЭВМ и внешних накопителей.

Очистка осуществляется двукратной произвольной записью в освобождаемую область памяти, ранее использованную для хранения защищаемых данных (файлов).

- Подсистема обеспечения целостности:

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

- целостность СЗИ НСД проверяется при загрузке системы по наличию имён (идентификаторов) компонент СЗИ;

- целостность программной среды обеспечивается отсутствием в АС средств разработки и отладки программ;

- должны осуществляться физическая охрана СВТ (устройств и носителей информации), предусматривающая постоянное наличие охраны территории и здания, где размещается АС, с помощью технических средств охраны и специального персонала, использование строгого пропускного режима, специальное оборудование помещений АС;

- 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;

- должны использоваться сертифицированные средства защиты. Их сертификацию проводят специальные сертификационные центры или специализированные предприятия, имеющие лицензию на проведение сертификации средств защиты СЗИ НСД.

Требования к показателям третьего класса защищённости:

- Дискреционный принцип контроля доступа.
- Данные требования полностью совпадают с требованиями пятого и четвёртого классов.
- Мандатный принцип контроля доступа.
- Данные требования полностью совпадают с аналогичным требованием четвёртого класса.
- Очистка памяти.
- Для СВТ третьего класса защищённости КСЗ должен осуществлять очистку оперативной и внешней памяти. Очистка должна производиться путём записи маскирующей информации в память при ее освобождении (перераспределении).
- Изоляция модулей.
- Данные требования полностью совпадают с аналогичным требованием четвёртого класса.
- Маркировка документов.
- Данные требования полностью совпадают с аналогичным требованием четвёртого класса.
- Защита ввода и вывода на отчуждаемый физический носитель информации.
- Данные требования полностью совпадают с аналогичным требованием четвёртого класса.
- Сопоставление пользователя с устройством.
- Данные требования полностью совпадают с аналогичным требованием четвёртого класса.
- Идентификация и аутентификация.
- Данные требования полностью совпадают с аналогичным требованием четвёртого класса.
- Гарантии проектирования.

• На начальном этапе проектирования КСЗ должна строиться модель защиты, задающая принцип разграничения доступа и механизм управления доступом. Эта модель должна содержать:

- непротиворечивые правила изменения ПРД;
- правила работы с устройствами ввода и вывода;
- формальную модель механизма управления доступом.

• Должна предлагаться высокоуровневая спецификация части КСЗ, реализующего механизм управления доступом и его интерфейсов. Эта спецификация должна быть верифицирована на соответствие заданных принципов разграничения доступа.

• Регистрация.

• Данные требования полностью совпадают с аналогичным требованием четвёртого класса.

• Взаимодействие пользователя с КСЗ.

• Для обеспечения возможности изучения, анализа, верификации и модификации КСЗ должен быть хорошо структурирован, его структура должна быть модульной и чётко определенной. Интерфейс пользователя и КСЗ должен быть определен (вход в систему, запросы пользователей и КСЗ и т.п.). Должна быть обеспечена надёжность такого интерфейса. Каждый интерфейс пользователя и КСЗ должен быть логически изолирован от других таких же интерфейсов.

• Надёжное восстановление

• Процедуры восстановления после сбоев и отказов оборудования должны обеспечивать полное восстановление свойств КСЗ.

• Целостность КСЗ.

• Необходимо осуществлять периодический контроль за целостностью КСЗ.

• Программы должны выполняться в отдельной части оперативной памяти. Это требование должно подвергаться верификации.

- Тестирование.
- СВТ должны подвергаться такому же тестированию, что и СВТ

четвёртого класса.

- Дополнительно должны тестироваться:
- очистка памяти;
- работа механизма надёжного восстановления.
- Руководство для пользователя.
- Данные требования полностью совпадают с аналогичным требованием

четвёртого класса.

- Руководство по КСЗ.
- Документ адресован администратору защиты и должен содержать:
- описание контролируемых функций;
- руководство по генерации КСЗ;
- описание старта СВТ, процедур проверки правильности старта, процедур работы со средствами регистрации;
- руководство по средствам надёжного восстановления.
- Тестовая документация
- В документации должно быть представлено описание тестов и испытаний, которым подвергалось СВТ, а также результатов тестирования.
- Конструкторская (проектная) документация.
- Требуется такая же документация, что и для СВТ четвёртого класса.

Дополнительно необходимы:

- высокоуровневая спецификация КСЗ и его интерфейсов;
- верификация соответствия высокоуровневой спецификации КСЗ модели

защиты.

Требования ко второму классу защищённости МЭ:

- Управление доступом.
- Данные требования включают аналогичные требования третьего класса.
- Дополнительно МЭ должен обеспечивать:

- возможность сокрытия субъектов (объектов) и/или прикладных функций защищаемой сети;

- возможность трансляции сетевых адресов.

- Идентификация и аутентификация.

- Данные требования полностью совпадают с аналогичными требованиями третьего класса.

- Регистрация.

- Данные требования включают аналогичные требования третьего класса.

- Дополнительно МЭ должен обеспечивать:

- дистанционную сигнализацию попыток нарушения правил фильтрации;

- регистрацию и учёт запрашиваемых сервисов прикладного уровня;

- программируемую реакцию на события в МЭ.

- Администрирование: идентификация и аутентификация.

- МЭ должен обеспечивать идентификацию и аутентификацию администратора МЭ при его запросах на доступ. МЭ должен предоставлять возможность для идентификации и аутентификации по идентификатору (коду) и паролю временного действия. МЭ должен препятствовать доступу неидентифицированного субъекта или субъекта, подлинность идентификации которого при аутентификации не подтвердилась.

- При удалённых запросах на доступ администратора МЭ идентификация и аутентификация должны обеспечиваться методами, устойчивыми к пассивному и активному перехвату информации.

- Администрирование: регистрация.

- Данные требования полностью совпадают с аналогичными требованиями третьего класса.

- Администрирование: простота использования.

- Данные требования полностью совпадают с аналогичными требованиями третьего класса.

- Целостность.

- МЭ должен содержать средства контроля за целостностью своей программной и информационной части по контрольным суммам как в процессе загрузки, так и динамически.

- Восстановление.

- МЭ должен предусматривать процедуру восстановления после сбоев и отказов оборудования, которые должны обеспечивать оперативное восстановление свойств МЭ.

- Тестирование.

- В МЭ должна обеспечиваться возможность регламентного тестирования

- реализации правил фильтрации;

- процесса идентификации и аутентификации;

- процесса регистрации;

- процесса идентификации и аутентификации администратора МЭ;

- процесса регистрации действий администратора МЭ;

- процесса контроля за целостностью программной и информационной части МЭ;

- процедуры восстановления.

- Руководство администратора МЭ.

- Данные требования полностью совпадают с аналогичными требованиями пятого класса.

- Тестовая документация.

- Должна содержать описание тестов и испытаний, которым подвергался МЭ, и результаты тестирования.

- Конструкторская (проектная) документация.

- Данные требования полностью совпадают с аналогичными требованиями третьего класса по составу документации.

Вывод

В ходе лабораторной работы я изучил основные руководящие документы ФСТЭК и научилась применять их для практических задач. Рассмотрел требования защиты от НСД, исходя из типа АС, СВТ и межсетевого экрана. Для решения различных задач необходимо определить проблему задачи, найти необходимую информацию и составить план для ее дальнейшего решения.