Федеральное государственное автономное образовательное учреждение

высшего образования «Российский университет транспорта (МИИТ)»

Институт транспортной техники и систем управления

Кафедра «Управление и защита информации»

Практическая работа на тему:

«АС от НСД класса защищенности 1Г»

По дисциплине:

«Организационное и правовое обеспечение ИБ»

Выполнил:

Студент группы ТКИ-342

Дроздов Антон Дмитриевич

Проверил:

к.т.н.

Привалов Александр Андреевич

Москва 2023

Оглавление

1. Перечень сокращений и определений

АС – Автоматизированная система – система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций;

ИБ – Информационная безопасность — состояние сохранности информационных ресурсов и защищённости законных прав личности и общества в информационной сфере;

ИС – Информационная система - совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств;

НСД – Несанкционированный доступ – это доступ к информации или к ресурсам автоматизированной информационной системы, осуществляемый с нарушением установленных прав и (или) правил доступа;

РД – Руководящий документ - нормативно-технический документ, устанавливающий нормы, правила, требования организационно-методического и общетехнического характера;

ФЗ – Федеральный закон — закон, установленный федеральными законодательными органами федеративного государства.

ФСТЭК − Федеральная служба по техническому и экспортному контролю − федеральный орган исполнительной власти России, осуществляющий реализацию государственной политики, организацию межведомственной координации и взаимодействия, специальные и контрольные функции в области государственной безопасности по вопросам:

1) обеспечения безопасности (некриптографическими методами) информации в системах информационной и телекоммуникационной инфраструктуры, оказывающих существенное влияние на безопасность государства в информационной сфере, в том числе в функционирующих в составе критически важных объектов Российской Федерации информационных системах и телекоммуникационных сетях,

деструктивные информационные воздействия на которые могут привести к значительным негативным последствиям;

2) противодействия иностранным техническим разведкам на территории Российской Федерации;

3) обеспечения защиты (некриптографическими методами) информации, содержащей сведения, составляющие государственную тайну, иной информации с ограниченным доступом, предотвращения ее утечки по техническим каналам, несанкционированного доступа к ней, специальных воздействий на информацию (носители информации) в целях ее добывания, уничтожения, искажения и блокирования доступа к ней на территории Российской Федерации;

4) защиты информации при разработке, производстве, эксплуатации и утилизации неинформационных излучающих комплексов, систем и устройств;

5) осуществления экспортного контроля.

2. Введение

Действующие и проектируемые АС, обрабатывающие конфиденциальную информацию, классифицируются в соответствии с пунктом 1.1. Руководящего документа Гостехкомиссии России "Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации".

А необходимость в классификации АС указывается в пункте 1.2.: "... необходимо в целях разработки и применения обоснованных мер по достижению требуемого уровня защиты информации."

В соответствии с пунктом 1.4., классификация АС включает следующие этапы:

"Основными этапами классификации АС являются:

- разработка и анализ исходных данных;
- выявление основных признаков АС, необходимых для классификации;
- сравнение выявленных признаков АС с классифицируемыми;
- присвоение АС соответствующего класса защиты информации от НСД."

Выбор класса АС производится заказчиком и разработчиком с привлечением специалистов по защите информации.

Определяющие признаки классификации АС рассматриваются в пункте 1.7.:

"К числу определяющих признаков, по которым производится группировка АС в различные классы, относятся:

- наличие в АС информации различного уровня конфиденциальности;
- уровень полномочий субъектов доступа АС на доступ к конфиденциальной информации;
- режим обработки данных в АС - коллективный или индивидуальный."

Классы характеризуются определённой минимальной совокупностью требований по защите.

В практической работе рассмотрен класс защищенности 1Г, которому соответствуют многопользовательские АС с обработкой и (или) хранением

информации разного уровня конфиденциальности и разграничением доступа пользователей к этой информации – в соответствии с пунктом 1.9. РД.

Цель данной практической работы – определение состава технических требований АС от НСД класса защищенности 1Г в соответствии с действующим законодательством Российской Федерации.

Для достижения данной цели необходимо выполнение следующих задач:

1. Провести сбор и анализ нормативно - методических документов, связанных с обеспечением безопасности АС;
2. Определить состав и содержание организационных и технических мер и требований по обеспечению безопасности АС от НСД 1Г класса.
3. Определить требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий.

3. Анализ нормативных документов

При обеспечении безопасности АС от НСД необходимо опираться на следующие нормативно-правовые документы:

1. ФЗ РФ № 149 «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 г.

> Статья 9 пункт 2 – " Обязательным является соблюдение конфиденциальности информации, доступ к которой ограничен федеральными законами."
>
> Статья 16 пункт 4 – "Обладатель информации, оператор информационной системы в случаях, установленных законодательством Российской Федерации, обязаны обеспечить:
>
> 1) предотвращение несанкционированного доступа к информации и (или) передачи ее лицам, не имеющим права на доступ к информации;
>
> 2) своевременное обнаружение фактов несанкционированного доступа к информации; ..."

2. Положение ФСТЭК по аттестации объектов информатизации по требованиям безопасности информации от 25 ноября 1994 г.

> Пункт 1.4. – "… Наличие на объекте информатизации действующего "Аттестата соответствия" дает право обработки информации с уровнем секретности (конфиденциальности) и на период времени..."
>
> Пункт 1.6. – " При аттестации объекта информатизации подтверждается его соответствие требованиям по защите информации от несанкционированного доступа ..."

3. Указ Президента Российской Федерации от 06.03.1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера».

> Включает в себя перечень сведений конфиденциального характера.

4. Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР–К).

Пункт 5.1.1. – "Система (подсистема) защиты информации, обрабатываемой в автоматизированных системах различного уровня и назначения, должна предусматривать комплекс организационных, программных, технических …"

Пункт 5.1.2. – "Основными направлениями защиты информации являются:

- обеспечение защиты информации от хищения, утраты, утечки, уничтожения, искажения и подделки за счет НСД и специальных воздействий; ..."

Пункт 5.1.3. – "В качестве основных мер защиты информации рекомендуются:

- разграничение доступа пользователей и обслуживающего персонала к информационным ресурсам, программным средствам обработки (передачи) и защиты информации;
- регистрация действий пользователей АС и обслуживающего персонала, контроль за несанкционированным доступом и действиями пользователей, обслуживающего персонала и посторонних лиц;
- использование сертифицированных средств защиты информации;"

Пункт 5.1.9. – "В случае, когда признаки классифицируемой АС (п. 1.7. РД Гостехкомиссии России "Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации") не совпадают с предложенными в РД (п. 1.9) группами по особенностям обработки информации в АС, то при классификации выбирается наиболее близкая группа защищенности с предъявлением к АС соответствующих дополнительных требований по защите информации."

Пункт 5.2.3. – "В соответствии с РД Гостехкомиссии России "Автоматизированные системы. Защита от несанкционированного

доступа к информации. Классификация автоматизированных систем и требования по защите информации" устанавливается следующий порядок классификации АС в зависимости от вида сведений конфиденциального характера:

- АС, обрабатывающие информацию, составляющую служебную тайну, должны быть отнесены по уровню защищенности к классам 3Б, 2Б и не ниже 1Г;
- АС, обрабатывающие персональные данные, должны быть отнесены по уровню защищенности к классам 3Б, 2Б и не ниже 1Д."

Пункт 5.3.3. – "Рекомендуется относить АС, обрабатывающие информацию, составляющую коммерческую тайну, режим защиты которой определяет ее собственник, по уровню защищенности к классам 3Б, 2Б и не ниже 1Д (если по решению руководителя предприятия не предъявляются более высокие требования)."

5. Выписка из Требований по безопасности информации, утвержденных приказом ФСТЭК России от 30 июля 2018 г. № 131.

Пункт 1 – "Настоящие Требования являются обязательными требованиями в области технического регулирования к продукции (работам, услугам), используемой в целях защиты сведений, составляющих государственную тайну или относимых к охраняемой в соответствии с законодательством Российской Федерации иной информации ограниченного доступа ..."

Пункт 5 – "Средства, соответствующие 4 уровню доверия, применяются в значимых объектах критической информационной инфраструктуры 1 категории*, в государственных информационных системах 1 класса защищенности**, в автоматизированных системах управления производственными и технологическими процессами 1 класса защищенности***, в информационных системах персональных данных при необходимости обеспечения 1 уровня защищенности персональных

данных****, в информационных системах общего пользования II класса****."

1? – рассматриваем в практической работе, АС тогда в соответствии с ГОСТ 34.003 пункт 1.1. АС – это либо АСУ (далее АСУТП/АСУП), либо САПР, либо АНСИ – подходит ли нам пункт 5 ФСТЭК № 131?

2? – в состав АС входит ИС?

3? – в каком документе указанно о категории для гос тайны?

4. Состав мер и требований к объектам информатизации в соответствие с действующим законодательством Российской Федерации

Для обеспечения класса защищенности 1Г должны быть реализованы следующие требования, приведенные в Таблице 1, на основании Руководящего документа "Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требований по защите информации".

Таблица 1. Содержание требований по защите информации в АС класса защищенности 1Г

Условное обозначение и номер меры	Содержание мер по обеспечению безопасности персональных данных
1. Подсистема управления доступом (УД)	
УД.1	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
УД.2	Должна осуществляться идентификация терминалов, ЭВМ, узлов сети ЭВМ, каналов связи, внешних устройств ЭВМ по логическим именам
УД.3	Должна осуществляться идентификация программ, томов, каталогов, файлов, записей, полей записей по именам
УД.4	Должен осуществляться контроль доступа субъектов к защищаемым ресурсам в соответствии с матрицей доступа
2.1. Подсистема регистрации и учёта – регистрация и учет (РУ)	
РУ.1	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

РУ.2	Должна осуществляться регистрация выдачи печатных (графических) документов на "твердую" копию
РУ.3	Должна осуществляться регистрация запуска (завершения) программ и процессов (заданий, задач), предназначенных для обработки защищаемых файлов
РУ.4	Должна осуществляться регистрация попыток доступа программных средств (программ, процессов, задач, заданий) к защищаемым файлам
РУ.5	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
2.2. Подсистема регистрации и учёта – учёт носителей информации (УНИ)	
УНИ.1	Должен проводиться учет всех защищаемых носителей информации с помощью их маркировки и с занесением учетных данных в журнал (учетную карточку)
2.3. Подсистема регистрации и учёта – очистка освобождаемых областей оперативной памяти ЭВМ и внешних накопителей (ОП)	
ОП.1	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)
3. Подсистема обеспечения целостности (ОЦ)	
ОЦ.1	Должна быть обеспечена целостность программных средств СЗИ НСД, а также неизменность программной среды
ОЦ.2	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
ОЦ.3	Должно проводиться периодическое тестирование функций СЗИ НСД при изменении программной среды и персонала АС с помощью тест - программ, имитирующих попытки НСД
ОЦ.4	Должны быть в наличии средства восстановления СЗИ НСД, предусматривающие ведение двух копий программных средств СЗИ НСД и их периодическое обновление и контроль работоспособности

Далее в Таблице 2 рассмотрены основные рекомендации по защите информации, составляющей коммерческую тайну.

Таблица 2. Рекомендации по защите информации, составляющей коммерческую тайну, на основании документа "СТР-К"

№	Меры по обеспечению безопасности коммерческой тайны
1.	Следует документально оформлять "Перечень сведений, составляющих коммерческую тайну". Все исполнители должны быть ознакомлены с данным перечнем
2.	Рекомендуется оформить порядок разработки и эксплуатации таких автоматизированных систем документально
3.	Рекомендуется относить АС, обрабатывающие информацию, составляющую коммерческую тайну, режим защиты которой определяет ее собственник, по уровню защищенности к классам 3Б, 2Б и не ниже 1Д (если по решению руководителя предприятия не предъявляются более высокие требования).
4.	Рекомендуется для обработки информации, составляющей коммерческую тайну, использовать средства вычислительной техники, удовлетворяющие требованиям стандартов Российской Федерации по электромагнитной совместимости, по безопасности и эргономическим требованиям к средствам отображения информации, по санитарным нормам, предъявляемым к видеодисплейным терминалам ПЭВМ (ГОСТ 29216-91, ГОСТ Р 50948-96, ГОСТ Р 50949-96, ГОСТ Р 50923-96, СанПиН 2.2.2.542-96).

5.	Для передачи информации по каналам связи, выходящим за пределы контролируемой зоны, необходимо использовать защищенные каналы связи, в том числе защищенные волоконно-оптические линии связи или предназначенные для этого криптографические средства защиты информации.
6.	Следует установить на предприятии порядок учета, хранения и уничтожения носителей информации на магнитной (магнитно-оптической) и бумажной основе в научных, производственных и функциональных подразделениях, а также разработать и ввести в действие разрешительную систему допуска исполнителей документам и сведениям, составляющим коммерческую тайну.

Следующий этап, приведенный в Таблице 4 – рассмотрение требований к разработке и производству средства, проведению испытаний средства, поддержке безопасности средства 4 уровня доверия, на основании Выписки из Требований по безопасности информации, утвержденной приказом ФСТЭК России от 30 июля 2018 г. № 131.

Таблица 4. Требования к средству 4 уровня доверия

Наименование требования	Описание требования
Требование к разработке и производству средства	При разработке средства разработчиком должны быть выполнены процедуры, предусматривающие: Разработку модели безопасности средства – пункт 28. "При разработке модели безопасности средства должны быть отражены следующие сведения: реализуемые политики управления доступом (если применимо); реализуемые политики фильтрации информационных потоков (если применимо). Модель безопасности должна включать описание условий безопасности, выполнение которых указывает на реализацию

	политик. Доверие к модели безопасности должно быть достигнуто формальным (математическим) доказательством того, что в ней не содержится противоречий, то есть выполняются условия безопасности. Для условий безопасности неформально (нематематически) должна быть показана их взаимосвязь с режимами функционирования средства. Язык описания модели безопасности должен быть математическим или формализованным (машиночитаемым) и допускать полную независимую от разработчика модели проверку корректности её описания, заданных в ней условий безопасности, а также всех выполненных в модели доказательств." Проектирование архитектуры безопасности средства – пункт 9,29. "Спроектированная архитектура безопасности средства должна обеспечивать: невозможность обхода функций безопасности средства; защиту функций безопасности средства от несанкционированного доступа к ним. На средство должно быть разработано описание архитектуры безопасности средства с обоснованием: безопасности процесса инициализации средства; обеспечения собственной защиты средства от несанкционированного доступа; невозможности обхода функций безопасности средства." Разработку функциональной спецификации средства – пункт 10, 20,30. "Разработка функциональной спецификации средства должна предусматривать:

	разработку описания назначения и способов использования каждого интерфейса функций безопасности (при наличии функций безопасности); идентификацию параметров, связанных с каждым интерфейсом функций безопасности (при наличии функций безопасности); идентификацию интерфейсов, не влияющих на функции безопасности средства (при наличии функций безопасности и наличии таких интерфейсов). В функциональную спецификацию средства должны быть включены: описание назначения и способов использования каждого интерфейса функций безопасности (при наличии функций безопасности) и иных функций средства; описание параметров, связанных с каждым интерфейсом функций безопасности (при наличии функций безопасности) и иных функций средства; перечень интерфейсов, не влияющих на функции безопасности средства (при наличии функций безопасности и наличии таких интерфейсов). При разработке функциональной спецификации средства наряду с требованиями, установленными пунктом 10 настоящих Требований, должны быть разработаны описания: всех функций безопасности (при наличии функций безопасности); действий с каждым интерфейсом функций безопасности (при наличии функций безопасности);

	сообщений о возможных ошибках, связанных с действиями по выполнению функции безопасности (при наличии функций безопасности). Разработка функциональной спецификации средства наряду с требованиями, установленными пунктом 20 настоящих Требований, должна предусматривать разработку описаний: действий с каждым интерфейсом функций безопасности, не влияющим на выполнение требований, предъявляемых к средству; сообщений обо всех ошибках, которые могут возникнуть при вызове каждого интерфейса функций безопасности. В функциональную спецификацию дополнительно должны быть включены описания: действий с каждым интерфейсом функций безопасности, не влияющим на выполнение требований, предъявляемых к средству; сообщений обо всех ошибках, которые могут возникнуть при вызове каждого интерфейса функций безопасности." Проектирование средства – пункт 11,31. "Проектирование средства должно предусматривать: определение перечня подсистем, реализующих функции безопасности средства; определение перечня подсистем, поддерживающих выполнение функций безопасности; определение перечня подсистем, не влияющих на выполнение функций безопасности; проектирование подсистем, реализующих функции безопасности средства;

	проектирование иных подсистем таким образом, чтобы они не оказывали влияния на выполнение функций безопасности средства; определение способов взаимодействия подсистем, реализующих функции безопасности, с иными подсистемами, обеспечивающих невозможность влияния на выполнение функций безопасности средства; определение и проектирование для каждой подсистемы, реализующей функции безопасности, перечня входящих в ее состав модулей, осуществляющих выполнение функций безопасности; определение способов взаимодействия модулей, осуществляющих выполнение функций безопасности, с иными модулями, обеспечивающих невозможность влияния на выполнение функций безопасности средства. Проектная документация средства должна включать: проект на уровне подсистем средства (эскизный проект); проект на уровне модулей средства (технический проект). Эскизный проект должен включать: описание структуры средства на уровне подсистем средства; описание всех подсистем средства; сопоставление функций средства и интерфейсов, описанных в функциональной спецификации, с подсистемами средства; описание взаимодействия подсистем средства между собой. Технический проект должен включать: описание структуры средства на уровне модулей; описание всех модулей средства (для модулей средства, реализующих функции безопасности, – описание интерфейсов, возвращаемых ими в ответ на запросы

	значений, взаимодействий с другими модулями и вызываемыми интерфейсами этих модулей; для модулей средства, не влияющих на выполнение функций безопасности, – описание назначения и взаимодействия с другими модулями); сопоставление подсистем средства, описанных в эскизном проекте, с модулями." Разработка представлений реализации средства – пункт 12, 22, 32. "Формуляр средства должен содержать контрольные суммы дистрибутива и исполняемых файлов программного обеспечения средства. Контрольные суммы должны уточняться при обновлении средства в соответствии с настоящими Требованиями. Для аппаратной платформы программно-технического средства должен быть представлен перечень аппаратных устройств (микросхем), которые влияют на выполнение функций безопасности и (или) могут быть использованы для реализации угроз безопасности информации. Представление реализации средства наряду с требованием, установленным пунктом 12 настоящих Требований, должно включать: для аппаратной платформы средства (при наличии аппаратной платформы) – структурные схемы и техническая документация аппаратных средств (даташит на микросхемы), входящих в аппаратную платформу; для программного обеспечения – исходные тексты программного обеспечения, входящего в состав средства, с указанием значений контрольных сумм файлов с исходными

	текстами программного обеспечения, за исключением программного обеспечения, не реализующего функции безопасности и не влияющего на реализацию функций безопасности, заимствованного у сторонних изготовителей. Представление реализации средства наряду с требованиями, установленными пунктом 22 настоящих Требований, должно включать для аппаратной платформы средства (при наличии аппаратной платформы) – функциональные схемы аппаратных средств (микросхем), входящих в аппаратную платформу, и представление (код) на языке описания аппаратных средств." Требования к средствам, применяемым для разработки средства – пункт 13, 33. "На средства, применяемые для разработки средства, должна быть разработана документация включающая описания: средств, применяемых для разработки средства; использованных опций средств, применяемых для разработки средства." Требования к управлению конфигурацией средства – пункт 14, 24, 34. "Управление конфигурацией средства должно предусматривать управление изменениями средства и документации и обеспечение их уникальной маркировки. Документация по управлению конфигурацией средства должна включать: описание уникальной маркировки средства; список элементов конфигурации средства, включающий в том числе документацию; порядок управления изменениями средства и документации.

	Управление конфигурацией средства наряду с требованиями, установленными пунктом 14 настоящих Требований, должно предусматривать: управление изменениями частей (элементов, компонентов) средства; обеспечение уникальной идентификации всех элементов конфигурации. Документация по управлению конфигурацией средства дополнительно должна включать: описание метода, используемого для уникальной идентификации элементов конфигурации; описание уникальных идентификаторов всех элементов конфигурации; части (элементы, компоненты) средства в списке элементов конфигурации. Для каждого элемента конфигурации в списке элементов конфигурации должен быть указан разработчик. Управление конфигурацией средства наряду с требованиями, установленными пунктом 24 настоящих Требований, должно предусматривать: управление изменениями представления реализации средства; применение автоматизированных мер контроля, обеспечивающих внесение в элементы конфигурации только санкционированных изменений; организацию процедур приемки модифицированных или вновь созданных элементов конфигурации. Документация по управлению конфигурацией средства дополнительно должна включать:

	представление реализации средства в списке элементов конфигурации; описание автоматизированных мер контроля, которые применяются для обеспечения внесения в элементы конфигурации только санкционированных изменений; план управления конфигурацией, содержащий описание процедур, используемых для приемки модифицированных или вновь созданных элементов конфигурации." Требования к разработке документации по безопасной разработке средства – пункт 15, 35. "Требования к разработке документации по безопасной разработке средства. На средство должна быть разработана документация по безопасности разработки средства, которая должна включать: описание всех физических, процедурных, организационных и других мер безопасности, применяемых в среде разработки средства для защиты конфиденциальности и целостности проектной документации и реализации средства; применяемые меры безопасности, направленные на снижение вероятности возникновения в средстве уязвимостей и иных недостатков, и их обоснование."» Требования к разработке руководства пользователя средства – пункт 16, 36. "Требования к разработке руководства пользователя средства. На средство должно быть разработано руководство пользователя средства (при наличии пользователей средства) с описанием: режимов работы средства;

	принципов безопасной работы средства; функций и интерфейсов функций средства, доступных каждой роли пользователей; параметров (настроек) безопасности средства, доступных каждой роли пользователей, и их безопасных значений; типов событий безопасности, связанных с доступными пользователю функциями средства; действий после сбоев и ошибок эксплуатации средства." Требования к разработке руководства администратора средства – пункт 17, 37. "Требования к разработке руководства администратора средства. На средство должно быть разработано руководство администратора средства с описанием: действий по приемке поставленного средства; действий по безопасной установке и настройке средства; действий по реализации функций безопасности среды функционирования средства."
Требование к проведению испытаний средства	Тестирование средства – пункт 69, 72, 75 "Для подтверждения выполнения требований по безопасности информации, предъявляемых к средству, средство должно быть протестировано в соответствии с разработанными для этой цели тестами. Тестовая документация должна включать: план тестирования, содержащий тесты, которые необходимо выполнить, описание сценариев проведения каждого теста, учитывающее зависимости последовательности выполнения тестов от результатов других тестов, описание ресурсов, необходимых для проведения тестирования;

	описание сопоставления тестов с интерфейсами функций безопасности средства (при наличии функций безопасности), описанными в функциональной спецификации, демонстрирующее их полное покрытие тестами; описание ожидаемых результатов тестирования, свидетельствующих об успешности выполнения тестов; описание фактических результатов тестирования, их сопоставление с ожидаемыми результатами тестирования и на его основе – выводы об успешности тестов. При проведении тестирования средства наряду с требованиями, установленными пунктом 69 настоящих Требований, тестовая документация должна включать описание сопоставления тестов с подсистемами средства, описанными в эскизном проекте, демонстрирующее их полное покрытие тестами. При проведении тестирования средства проводится оценка влияния (невлияния) на подсистемы средства, реализующие функции безопасности, иных подсистем средства. При проведении тестирования средства наряду с требованиями, установленными пунктом 72 настоящих Требований, тестовая документация должна включать описание сопоставления тестов с модулями средства, реализующими функции безопасности (при наличии функций безопасности) и описанными в техническом проекте, демонстрирующее полное покрытие тестами функций безопасности. При проведении тестирования средства проводится оценка влияния (невлияния) на модули средства, реализующие функции безопасности, иных модулей средства."

	Испытания по выявлению уязвимостей и недекларированных возможностей средства – пункт 70, 73, 76. "Испытания по выявлению уязвимостей и недекларированных возможностей средства должны быть проведены по 6 уровню контроля. Для аппаратной платформы программно-технического средства должна быть выполнена проверка перечня аппаратных устройств (микросхем), которые влияют на выполнение функций безопасности и (или) могут быть использованы для реализации угроз безопасности информации. Для аппаратной платформы программно-технического средства наряду с требованиями, установленными пунктом 70 настоящих Требований, должна быть выполнена проверка соответствия аппаратной платформы его структурной схеме. Для аппаратной платформы программно-технического средства наряду с требованиями, установленными пунктом 74 настоящих Требований, должны быть выполнены: проверка соответствия аппаратной платформы его функциональной схеме; проверка применения микросхем в устройстве по назначению, а также параметров микросхем в соответствии с технической документацией." Проведение анализа скрытых каналов в средстве – пункт 74, 77. " В средстве должны быть проведены идентификация и анализ скрытых каналов по памяти, основанных на использовании ресурсов памяти, в которые записывается защищаемая информация (сокрытие информации в структурированных и неструктурированных данных) и

	которые не учитываются разработчиками системы защиты информации информационной (автоматизированной) системы и не выявляются применяемыми средствами защиты информации. Анализ идентифицированных типов скрытых каналов должен включать: оценку потенциальной пропускной способности идентифицированных скрытых каналов с использованием формальных (математических), технических методов и (или) методов моделирования; разработку требований для среды функционирования средства с целью ограничения, мониторинга, полного или частичного устранения идентифицированных скрытых каналов, которые могут возникнуть в информационных (автоматизированных) системах вследствие использования в них средства. Документация анализа скрытых каналов должна включать: идентификацию скрытых каналов (если скрытые каналы выявлены); оценку пропускной способности идентифицированных скрытых каналов (если скрытые каналы выявлены); описание процедур, использованных для вынесения заключения о существовании и (или) отсутствии скрытых каналов, и информацию, использованную при анализе скрытых каналов; описание предположений (быстродействие процессора, системная конфигурация, объем памяти и (или) иных), сделанных при анализе скрытых каналов;

	описание способа, использованного для оценки пропускной способности канала для наиболее опасного сценария (если скрытые каналы выявлены); описание наиболее опасного сценария использования каждого идентифицированного скрытого канала (если скрытые каналы выявлены); сведения о включении в функциональную спецификацию и эскизный проект описание механизмов средства, направленных на ограничение, мониторинг, полное или частичное устранение идентифицированных скрытых каналов, которые могут возникнуть в информационных (автоматизированных) системах вследствие использования в них средства (если скрытые каналы выявлены и требуются соответствующие механизмы средства); сведения о включении в руководство администратора и (или) руководство пользователя требований для среды функционирования средства с целью ограничения, мониторинга, полного или частичного устранения идентифицированных скрытых каналов, которые могут возникнуть в информационных (автоматизированных) системах вследствие использования в них средства (если скрытые каналы выявлены)."
Требование к поддержке безопасности средства	Средство должно обеспечиваться поддержкой безопасности средств, которая предусматривает: Устранение недостатков и дефектов средства, в том числе устранение уязвимостей и недекларированных возможностей средства (далее – устранение недостатков средства) – пункт 88, 92, 96. " Устранение недостатков средства должно предусматривать:

	поиск в доступных источниках информации о недостатках средства, в том числе о недостатках в компонентах средства, заимствованных у сторонних изготовителей; получение сведений о недостатках средства от потребителей средства; проведение испытаний средства по выявлению недостатков в средстве, в том числе по выявлению уязвимостей и недекларированных возможностей средства; разработку компенсирующих мер по защите информации или ограничений по применению средства, снижающих возможность эксплуатации недостатков (уязвимостей); доведение информации о недостатках средства, а также о компенсирующих мерах по защите информации или ограничений по применению средства до потребителей средства, ФСТЭК России и банка данных угроз безопасности информации, ведение которого осуществляется ФСТЭК России в соответствии с подпунктом 21 пункта 8 Положения о Федеральной службе по техническому и экспортному контролю, утвержденного Указом Президента Российской Федерации от 16 августа 2004 г. N 1085; устранение недостатков средства путем доработки средства или его отдельных компонентов, принятие иных мер, снижающих возможность эксплуатации уязвимостей; тестирование (испытания) доработанного средства или его отдельных компонентов на предмет устранения влияния обновлений средства на его функции безопасности, подтверждения устранения уязвимостей, невнесения новых уязвимостей в средство.

	Наряду с требованиями к устранению недостатков средства, установленными пунктом 88 настоящих Требований, дополнительно предъявляются следующие требования: разработка компенсирующих мер по защите информации или ограничений по применению средства, а также доведение информации о недостатках и указанных мерах и ограничениях до потребителей должны осуществляться не позднее 72 часов с момента выявления недостатка; доработка средства, в том числе разработка обновлений программного обеспечения средства, или разработка мер по защите информации, нейтрализующих недостаток, должна осуществляться в срок не более 60 дней с момента выявления недостатка. Наряду с требованиями к устранению недостатков средства, установленными пунктом 92 настоящих Требований, дополнительно предъявляются следующие требования: разработка компенсирующих мер по защите информации или ограничений по применению средства, а также доведение информации о таких мерах и ограничениях до потребителей должны осуществляться в срок не более 48 часов с момента выявления недостатка; доведение информации о недостатках средства, а также о компенсирующих мерах по защите информации или ограничениях по применению должно осуществляться до каждого потребителя сертифицированного средства путем отправки сообщений на электронные адреса потребителей или за счет применения компонента средства, обеспечивающего доведение указанной информации до потребителя автоматически."

	Информирование потребителей об обновлении программного обеспечения средства и доведение до потребителей обновлений программного обеспечения средства, а также изменений в эксплуатационную документацию (далее – обновление средства) – пункт 89, 93, 97 "Обновление средства должно предусматривать: информирование потребителей средства о выпуске обновлений; обеспечение возможности получения обновления средства способами, обеспечивающими его целостность. Наряду с требованиями к обновлению средства, установленными пунктом 89 настоящих Требований, дополнительно предъявляются следующие требования: в случае получения обновления средства по сетям связи средство должно получать такие обновления с информационного ресурса заявителя; при доведении обновлений средства до потребителей должны обеспечиваться подлинность и целостность обновлений за счет применения электронной цифровой подписи. Наряду с требованиями к обновлению средства, установленными пунктом 93 настоящих Требований, доведение информации о выпуске обновлений средства должно осуществляться до каждого потребителя сертифицированного средства путем отправки сообщений на электронные адреса потребителей или за счет применения компонента средства, обеспечивающего доведение указанной информации до потребителя автоматически."

	Документирование процедур устранения недостатков и обновления средства – пункт 90, 98. "Документирование процедур устранения недостатков и обновления средства должно предусматривать: включение в программную и конструкторскую документацию на средство процедур устранения недостатков; разработку регламента обновления средства потребителем, включающего порядок получения, установки и контроля установки обновления программного обеспечения средства." Информирование об окончании производства и (или) поддержки безопасности средства – пункт 91, 99. "Об окончании производства и (или) поддержки безопасности средства потребители и ФСТЭК России должны быть проинформированы не позднее чем за 1 год до окончания производства и (или) поддержки безопасности средства."

5. Заключение

В данной практической работе была рассмотрена тема «АС от НСД класса защищенности 1Г».

В результате проделанной работы были получены следующие результаты:

1. Найдены и проанализированы нормативно-правовые документы, связанные с АС от НСД;
2. Определен состав мер и требований по обеспечению безопасности автоматизированным системам от НСД класса защищенности 1Г.

6. Список использованных источников

1. Учебно–методическое пособие к практической работе «Определение состава мер и требований к объектам информатизации в соответствии с действующим законодательством Российской Федерации.» А. А. Привалов.
2. ФЗ РФ № 149 «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 г.
3. Руководящий документ «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации».
4. Положение ФСТЭК по аттестации объектов информатизации по требованиям безопасности информации от 25 ноября 1994 г.
5. Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР–К).
6. Выписка из Требований по безопасности информации, утвержденных приказом ФСТЭК России от 30 июля 2018 г. N 131.
7. Руководящий документ по стандартизации РД 50-680-88 "Методические указания. Автоматизированные системы. Основные положения" (утвержден и внесен в действие постановлением Государственного комитета СССР по стандартам от 28 декабря 1988 г. N 4622)