МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ
ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ ГРАЖДАНСКОЙ АВИАЦИИ

А.А. Антонов

СЕРТИФИКАЦИЯ И АТТЕСТАЦИЯ ОБЪЕКТОВ ИНФОРМАЦИОННОЙ ЗАЩИТЫ

**Учебно-методическое пособие
по выполнению лабораторных работ**

**для студентов V курса
специальности 10.05.02
очной формы обучения**

Москва · 2022

ФЕДЕРАЛЬНОЕ АГЕНТСТВО ВОЗДУШНОГО ТРАНСПОРТА
(РОСАВИАЦИЯ)

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ
УНИВЕРСИТЕТ ГРАЖДАНСКОЙ АВИАЦИИ» (МГТУ ГА)

Кафедра основ радиотехники и защиты информации

А.А. Антонов

СЕРТИФИКАЦИЯ И АТТЕСТАЦИЯ ОБЪЕКТОВ ИНФОРМАЦИОННОЙ ЗАЩИТЫ

Учебно-методическое пособие
по выполнению лабораторных работ

для студентов V курса
специальности 10.05.02
очной формы обучения

Москва
ИД Академии Жуковского
2022

УДК 004.056
ББК 001.8
А72

Рецензент:

Петров В.И. – канд. техн. наук, доцент

Антонов А.А.

А72 Сертификация и аттестация объектов информационной защиты [Текст] : учебно-методическое пособие по выполнению лабораторных работ / А.А. Антонов. – М.: ИД Академии Жуковского, 2022. – 32 с.

Учебно-методическое пособие соответствует рабочей программе учебной дисциплины «Методы программирования» по специальности 10.05.02 для студентов V курса очной формы обучения и предназначено для получения практических навыков защиты информации в информационных системах авиапредприятий.

В учебно-методическом пособии рассматриваются методические основы обеспечения качества и сертификации; методы оценки несоответствия средств защиты информации; сертификация программного обеспечения; сертификация средств криптографической защиты информации; требования к защите персональных данных и к системам обнаружения вторжений; особенности аттестации объектов критической информационной инфраструктуры.

Рассмотрено и одобрено на заседаниях кафедры 19.04.2022 г. и методического совета 21.04.2022 г.

УДК 004.056
ББК 001.8

В авторской редакции

Подписано в печать 13.07.2022 г.
Формат 60х84/16 Печ. л. 2 Усл. печ. л. 1,86
Заказ № 904/0603-УМП15 Тираж 30 экз.

Московский государственный технический университет ГА
125993, Москва, Кронштадтский бульвар, д. 20

Издательский дом Академии имени Н. Е. Жуковского
125167, Москва, 8-го Марта 4-я ул., д. 6А
Тел.: (495) 973-45-68
E-mail: zakaz@itsbook.ru

Лабораторная работа № 1

Проведение оценки соответствия в форме сертификации.

1. Цель работы – ознакомиться с нормативными документами, регламентирующими работу испытательной лаборатории и уяснить процесс сертификации программного обеспечения в системе сертификации ФСТЭК.

2. Краткие теоретические сведения

2.1 Понятие сертификации

Под сертификацией понимается комплекс действий с целью подтверждения соответствия третьей стороной, относящийся к продукции, процессам, системам или персоналу.

Ключевые особенности сертификации:

1. Сертификация проводится на соответствие заданным требованиям, а именно техническим регламентам, положениям стандартов, сводов правил, условиям договоров и другим требованиям, определенным в нормативных документах и соответствующей документации.

Поэтому область сертификации и ее результат однозначно определены конкретными нормативными документами, а не требованиями и рекомендациями по повышению качеству или защищенности вообще.

2. В случае положительно результата процесс сертификации заканчивается выдачей официального письменно оформленного удостоверения – сертификата соответствия, а сертифицированная продукция подлежит маркировке знаком соответствия системы сертификации.

В некоторых системах сертификации можно встретить еще одно официальное удостоверение – заключение, которое применяется для случаев, когда орган по сертификации затрудняется выдать общепринятый сертификат соответствия.

3. Сертификация является деятельностью третьей стороны, т.е. должна быть обеспечена независимость оценки соответствия, максимально исключающая любые формы сговора.

4. Сертификация может быть добровольной и обязательной.

Сертификация средств защиты информации по требованиям безопасности информации является обязательной.

5. Так как в стране действует несколько систем сертификации, то эти системы определяют некоторые свои правила и процедуры проведения оценки соответствия, включая аккредитацию органов по сертификации и испытательных лабораторий, разумеется, в рамках российского законодательства и своей компетенции.

Таким образом, сертификация средств защиты информации по требованиям безопасности информации представляет собой обязательное, независимое подтверждение соответствия СЗИ требованиям нормативных

документов по защите информации с учетом правил федеральных органов (Минобороны, ФСБ, ФСТЭК) в рамках их компетенции.

Следует отметить, что федеральные органы по сертификации трактуют СЗИ в широком смысле, как средство защиты от угроз информационной безопасности и ее составных свойств: целостности, доступности, конфиденциальности и др.

В этом смысле под понятие СЗИ при самой общей модели угроз подпадает любое изделие в защищенном исполнении, например, «безопасное» от программных закладок ПО.

В таблице 1 приведены примеры объектов сертификации в области информационной безопасности, к которым определены требования в открытых нормативных документах.

Таблица 1.1 Требования к объектам сертификации

Объекты сертификации по требованиям безопасности информации	Объект сертификации средств защиты информации
Продукция	Средства защиты информации Средства вычислительной техники Профили защиты Межсетевые экраны Средства обнаружения вторжений Средства антивирусной защиты Средства криптографической защиты информации Средства защиты персональных данных
Системы	Автоматизированные системы
Системы менеджмента	Системы менеджмента (управления) безопасности

Процесс сертификации включает несколько уровней независимых проверок:

экспертизу заявки в федеральном органе,

проведение испытаний в аккредитованной испытательной лаборатории,

проверку материалов испытаний в аккредитованном органе по сертификации и др.

При этом обеспечивается независимость между участниками сертификации: аккредитованным органом по сертификации, аккредитованной испытательной лабораторией и другими заинтересованными сторонами

2.2 Правила и участники сертификации

Руководство системами сертификации возложено на федеральные органы по сертификации: Минобороны России, ФСБ России и ФСТЭК России.

В общегражданском плане регулирование рынка не криптографических СЗИ в стране возложено на ФСТЭК России, а рынка криптографических СЗИ - на ФСБ России.

Участниками сертификации являются:

федеральный орган по сертификации,

аккредитованный орган по сертификации,

аккредитованная испытательная лаборатория,

заявитель на сертификацию, которым может быть разработчик, изготовитель или поставщик.

Порядок проведения сертификации выглядит следующим образом.

1. Заявитель подает в федеральный орган заявку на проведение сертификационных испытаний. Заявителем может являться организация-разработчик, изготовитель, поставщик СЗИ или потребитель.

Он: подаёт во ФСТЭК России заявку на сертификацию; указывает в технической документации сведения о сертифицируемой технике защиты информации, нормативных документах, которым она должна соответствовать, обеспечивает доведение этой информации до потребителя.

Заявитель, если он выступает в качестве организации-разработчика или изготовителя СЗИ, должен иметь лицензию ФСТЭК России на соответствующий вид деятельности.

Поставщик СЗИ или потребитель, в рамках работ по сертификации, иметь соответствующие лицензии не обязаны.

2. Федеральный орган определяет аккредитованную испытательную лабораторию и орган по сертификации, что фиксируется в решении на сертификацию.

По отношению к Заявителю ФСТЭК России выполняет следующие практически важные функции:

рассматривает заявки на сертификацию, принимает по ним решения, определяет схему проведения сертификации средств защиты информации и испытательный центр (лабораторию) с учётом предложений Заявителя и назначает орган по сертификации; в

выдаёт сертификаты и, в зависимости от схемы сертификации, знаки соответствия.

3. Испытательная лаборатория проводит сертификационные испытания.

ФСТЭК России ведёт реестр аккредитованных органов по сертификации и испытательных лабораторий.

Основные выполняемые функции испытательной лаборатории:

осуществляет отбор образцов средств защиты информации для проведения сертификационных испытаний;

разрабатывает программы и методики сертификационных испытаний, осуществляет сертификационные испытания средств защиты информации, оформляет протоколы сертификационных испытаний и технические заключения.

На практике встречается, что организация может являться одновременно и органом по сертификации и испытательной лабораторией. Однако в процессе сертификации конкретного продукта организация может выступать только в одной ипостаси – одновременно совмещать и ту и другую роль при сертификации запрещено.

4. Материалы испытаний (программа и методика, протоколы испытаний, техническое заключение) передаются в орган по сертификации, который проводит их независимую экспертизу.

Орган по сертификации выполняет контрольные функции и проверяет корректность работ, проведённых испытательной лабораторией. Таким образом, реализуется принцип невозможности выполнения критичных функций одним субъектом.

Основные функции, выполняемые органом по сертификации:

проводит экспертизу технической, эксплуатационной документации на средства защиты информации и материалов сертификационных испытаний;

оформляет экспертное заключение по сертификации средств защиты информации и представляет их в федеральный орган по сертификации – ФСТЭК России.

5. Федеральный орган по сертификации на основании положительного технического заключения органа по сертификации оформляет сертификат соответствия.

В случае выявления каких-либо несоответствий федеральный орган может провести дополнительную экспертизу с привлечением экспертов из различных аккредитованных лабораторий и органов по сертификации.

2.3 Схемы сертификационных испытаний

В области защиты информации применяются следующие схемы сертификации СЗИ:

сертификация единичного образца СЗИ;

сертификация партии СЗИ;

сертификация серии (типового образца) с предварительной проверкой производства.

Сертификационные испытания можно классифицировать по методу тестирования:

функциональное тестирование продукта или системы по методу «черного ящика»;

структурное тестирование исходного кода ПО.

В первом случае при испытаниях используются:

традиционные нормативные документы (например, руководящие документы Гостехкомисии России);

документация (например, ТУ);

задание по безопасности - документ, разрабатываемый в соответствии с метастандартом ГОСТ ИСО 15408.

Особенность структурного тестирования состоит в том, что оно проводится в форме статического и динамического анализа исходного кода программ и касается только вопросов внутренней безопасности продукта (контроля отсутствия недекларированных возможностей).

Законодательные и правовые требования определяют, когда сертификация необходима, а также ответственность за несоблюдение этих требований.

При определении обязательности сертификации СЗИ удобно провести классификацию защищаемого информационного ресурса и объектов информатизации.

В качестве признаков классификации информационного ресурса выделяют два: принадлежность к государственному информационному ресурсу и уровень ограниченности доступа. Для государственного информационного ресурса требования устанавливает и контролирует сам собственник (государство). В других случаях могут быть неоднозначности.

Основные случаи, когда сертификации СЗИ в нашей стране обязательна:

защищаемая информация составляет сведения, отнесенные к государственной тайне;

защищаемая информация ограниченного доступа, но не отнесенная к государственной тайне, при условии, что она относится к государственному информационному ресурсу;

защищаемая информация относится к персональным данным и составляет личную и семейную тайну;

к защите объектов информатизации (систем, комплексов) определены требования по оценке соответствия независимо от видов тайн.

Следует сказать, что с практической точки зрения обязательность сертификации СЗИ диктуется обычно двумя обстоятельствами.

Первое связано с требованиями заказчика, который формулирует их к разработке, поставке, внедрению защищенной информационной системы.

Другой случай связан с необходимостью быть уверенным в защищенности объекта с формальной точки зрения, когда требуется заполучить какой-нибудь официальный документ о подтверждении соответствия информационной системы требованиям российского законодательства.

2.4 Подготовка к проведению сертификационных испытаний программного обеспечения в системе сертификации ФСТЭК

1. Отбор образца.

Отбор образцов для проведения сертификационных испытаний является важной операцией, направленной на обеспечение достоверности и обоснованности результатов обязательного подтверждения соответствия продукции (получения сертификата).

2. Требования законодательства.

3. Полноту предоставленных материалов – их достаточность для проведения сертификационных испытаний. Например, отсутствие программных компонентов, отдельных типов документов и др.

4. Соответствие материалов требованиям испытательной лаборатории и органа по сертификации – присутствие иностранного языка в документации, соответствие ГОСТам и т.д.

Подходы по обеспечению доступа испытательной лаборатории к материалам образца заключаются в:

полном проведении сертификации на территории испытательной лаборатории в РФ;

доступе к материалам образца на территории российской компании или филиала иностранной компании;

доступе к материалам образца на территории иностранной компании.

3.Порядок выполнения работы

а) Изучаете необходимые теоретические сведения и уясняете их.

б) Получаете индивидуальное задание на выполнение лабораторной работы.

в) Выполнение работы:

составляете блок схему процесса сертификации программного обеспечения согласно указанной схемы сертификации;

оформляете соглашение о неразглашении (NDA) между испытательной лабораторией и заявителем;

уточняете исходные данные согласно вашего варианта;

составляете заявку на сертификацию в федеральный орган по сертификации;

оформляете решение от федерального органа по сертификации;

заполняете сертификат соответствия на СЗИ.

г) составляете отчет

4. Содержание отчета

1. Титульный лист, с указанием темы лабораторной работы.
2. Цель работы и вариант выполнения.
3. Оформленные, согласно вашего варианта, документы для проведения сертификации средства защиты информации.
4. Вывод.

5. Литература

1. Федеральный закон от 27.12.2002 № 184-ФЗ «О техническом регулировании».
2. Постановление Правительства РФ от 26 июня 1995 г. № 608 "О сертификации средств защиты информации".
3. Постановление Правительства РФ от 3 февраля 2012 г. № 79 "О лицензировании деятельности по технической защите конфиденциальной информации".
4. Приказ Федеральной службы по техническому и экспортному контролю России от 3.04.2018 г. № 55 «Об утверждении положения о системе сертификации средств защиты информации».

Лабораторная работа № 2

Построение модели угроз информационной системы

1. Цель работы - изучить нормативные документы ФСТЭК по построению модели угроз. Построить модель угроз информационной системы.

2. Краткие теоретические сведения

При подготовке объекта информатизации к аттестации всё это нужно документально оформить.

Первый документ — это перечень объектов информатизации, утверждённый руководителем организации.

Далее издается некоторое количество приказов, здесь указан один приказ о назначении ответственного. В приказе ставиться задача о подготовке документации, провести необходимые работе по защите информации, в этом приказе может быть сформирована комиссия по классификации объектов информатизации. Приказ доводится до исполнителей.

Результатом работы комиссии является акт классификации объекта информатизации. Если обрабатываем государственную тайну нужен еще акт категорирования. Типовой пример акта есть в СТР-К.

Следующий документ, который нужно разработать это модель угроз. Необходимость модели угроз описана в приказах ФСТЭК.

Рисунок 2.1 – Этапы моделирования угроз

На рисунке 2.1 представлены этапы моделирования угроз. Методика разбита на этапы. Главные нововведения — это появление негативных последствий, ранее только учитывался ущерб.

Модель нарушителя не изменилась. Основное новшество — это сценарный подход. По сути эту схему можно привести к трем вопросам: для чего, кто и как?

Рассмотрим схему поэтапно на примере.

Рисунок 2.2 – Исходные данные

Рассмотрим коммерческую страховую компанию, занимающуюся урегулированием убытков. Информационная система обрабатывает персональные данные.

На ИС используется средства защиты, представленные на рисунке 2.2. СКЗИ, межсетевой экран, антивирусные средства защиты, внедрены меры по безопасные разработки программного обеспечения и другие.

Далее идет определение негативных последствий – рисунок 2.3.

У1 в части персональных данных. Возможные ущербы персональным данным.

У2 относится к организации. Может быть простой информационной системы, утрата доверия и потеря клиентов, поставщиков, которые оказывают какие-то услуги.

У3 соответственно возникновение ущерба.

Рисунок 2.3 – Определение негативных последствий

Другие виды последствий также могут быть, но как правило они несут на несколько порядков меньший ущерб

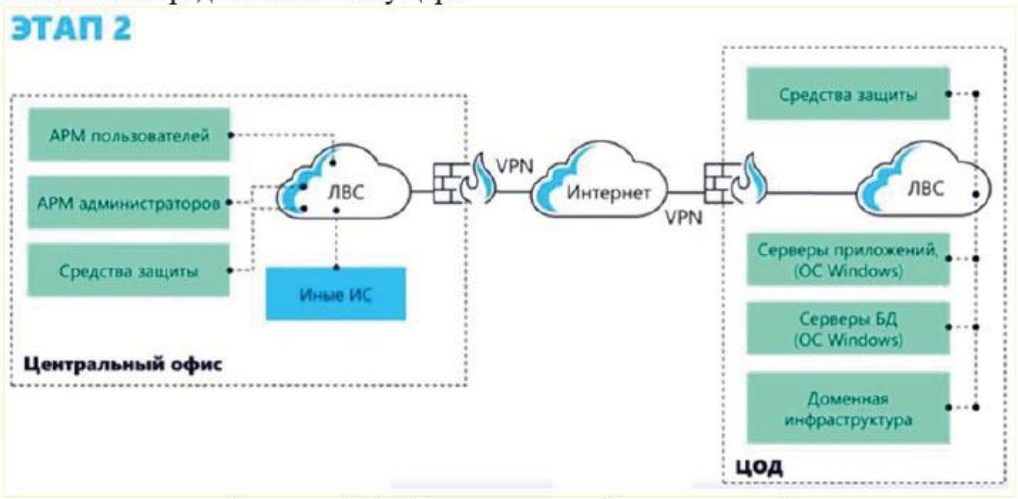

Рисунок 2.4 – Определение объектов воздействия

Следующий шаг определяем объекты воздействия, как представлено на рисунке 2.4. В рамках ЦОД есть наша система с серверами приложений и баз данных, а также всякие вспомогательные элементы.

(2/3) ЭТАП 2

Негативные последствия	Объекты воздействия	Виды воздействия
Утечка персональных данных	Серверы БД	• Модификация данных • Несанкционированный доступ
Простой информационной системы или сети	• Серверы инфраструктуры • Серверы БД • Серверы приложений	Отказ в обслуживании

Рисунок 2.5 – Определение видов воздействия на объекты

Далее определяем виды воздействия на объекты, как представлено на рисунке 2.5. Здесь рассматриваем объекты прямого воздействия.

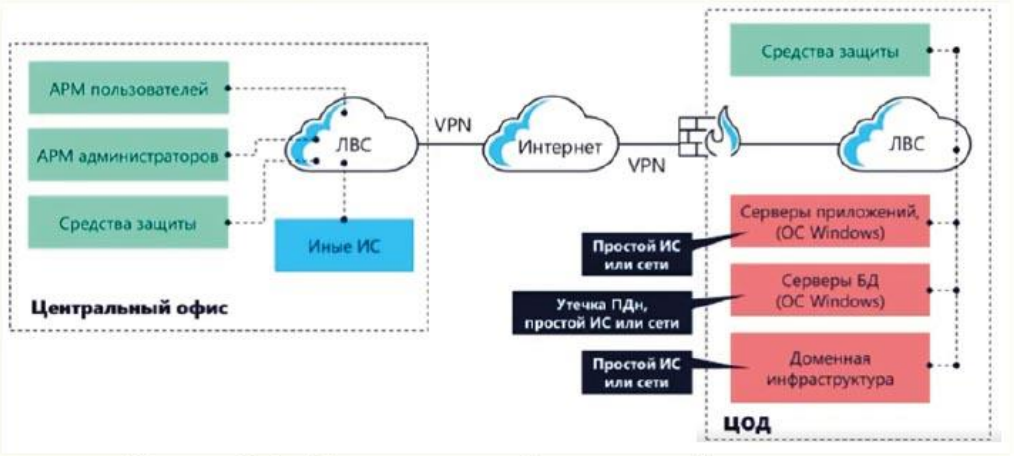

Рисунок 2.6 – Сопоставление объектов воздействия и негативных последствий

На рисунке 2.6 таблицу рисунка 2.5 перевели в схему о сопоставлении последствий и объектов воздействия. Если нарушитель достигнет своих целей организация получит данные негативные последствия.

Тип нарушителя	У1	У2	У3	Оценка актуальности
Специальные службы иностранных государств	–	–	–	Неактуальный
Преступные группы (криминальные структуры)	+	+	–	Актуальный
Отдельные физические лица (хакеры)	+	+	–	Актуальный
Конкурирующие компании	–	+	–	Актуальный

Рисунок 2.7 – Моделирование возможных нарушителей

Следующий шаг представлен на рисунке 2.7 - это моделирование нарушителей. Здесь использованы цели по аналогии с мотивацией. Т.к. информационная система не представляет интерес для специальных служб, то данный нарушитель неактуален. Остальные нарушители могут иметь какой-то интерес, с точки зрения обрабатываемых данных. Исключить больше нарушителей по данной методике не представляется возможным.

Также актуальны разработчики, администраторы, бывшие работники и сами пользователи.

Актуальный тип нарушителя	Объекты воздействия	Доступные интерфейсы	Способы реализации
Отдельные физические лица (хакеры)	Серверы БД: утечка ПДн	Внешние сетевые интерфейсы	• Использование уязвимостей • Внедрение ВПО
		Внутренние сетевые интерфейсы	• Использование уязвимостей • Внедрение ВПО
		Интерфейсы для использования съемных носителей	Внедрение ВПО

Рисунок 2.8 – Способы реализации угроз

Следующий шаг представлен на рисунке 2.8 - это способы реализации угроз. Комбинация информации полученной предыдущих этапах. Т.е. мы определили актуальных нарушителей, определили объекты воздействия, теперь определяем доступные интерфейсы и способы реализации. Здесь приведен пример для одного вида нарушителя.

Рисунок 9 – Определение сценария реализации угрозы

Следующий этап определение сценария реализации угрозы. Рассмотрим на примере утечки персональных данных. Выбираем для примера три сценария, которые хотим рассмотреть, они представлены внизу на рисунке 2.9.

ТАКТИКА	ТЕХНИКИ	ВОЗМОЖНОСТЬ РЕАЛИЗАЦИИ ТЕХНИКИ И ОБОСНОВАНИЙ В СЛУЧАЕ НЕВОЗМОЖНОСТИ	УГРОЗЫ ИЗ БДУ ФСТЭК	АКТУАЛЬНОСТЬ УГРОЗЫ
Т1 (Сбор информации о системах и сетях)	Т1.12 (Сбор личной идентификационной информации)	Реализация возможна	-	-
	Т1.15 (Поиск и покупка баз данных, скомпрометированных паролей и ключей)	Реализация возможна	-	-
Т2 (Получение первоначальног о доступа)	Т2.1 (Использование внешних сервисов в сети Интернет)	Внешний сервис рассматриваемого объекта в ЦОД доступен по VPN. В центральном офисе отсутствуют внешние сервисы в сеть Интернет. Выполняется проверка паролей по умолчанию автоматизированным способом по словарям. Также проводятся внутренние проверки	-	-

Рисунок 2.10 – Определение сценария реализации угрозы

Каждый сценарий рассматриваем в отношении тактик и техник (Рисунок 10).

Рассматриваем тактику Т1 - сбор информации в рамках которой возможны техники Т1.12 и Т1.15.

Считаем их реализацию возможной. В БДУ допустим ничего не нашли.

Следующая тактика это Т2. Система доступна только через VPN, поэтому считаем данную технику реализовать нельзя.

Далее сопоставляем техники и БДУ ФСТЭК.

Т.к. нет вероятности, то третий пункт оценивается исходя из текущих мер, которые есть в ИС.

Аналогично рассматриваем второй сценарий распространения вредоносного программного обеспечения через съемный носитель. Т1 возможны, Т2 не реализуема.

Затем третий сценарий. Здесь начинаем с Т6, т.к. обычно пользователю не нужно зарегистрироваться, чтобы получать доступ. Пользователь пытается что-то эксплуатировать до учетной записи администратора.

Из общего состава техник и тактик, приведенных в Методике, исключаем те, которые не связаны с используемыми у нас технологиями, не применимы к нашим процессам (например, связанные с АСУ ТП, так как у нас клиент ФО), не приводящие к ущербу или недоступные актуальным нарушителям. Все актуальные сценарии должны быть подмножествами их этого ограниченного набора тактик.

И в конце проверяем, какие из этих техник ещё не закрыты применяющимися у вас мерами защиты.

Далее уже исходя из этих применимых тактик, возможностей нарушителей, объектов воздействия и их интерфейсов и способов реализации мы определяем актуальные угрозы (в данном примере угрозы из БДУ объединены в общие группы угроз).

Таким образом составляется модель угроз информационной системы.

4. Порядок выполнения работы.

а) Изучаете необходимые теоретические сведения и уясняете их.

б) Получаете индивидуальное задание на выполнение лабораторной работы, справочные материалы и шаблоны документов.

в) Выполнение работы:

- определяете негативные последствия от реализации угроз безопасности, заполняется таблица 2.1;

Таблица 2.1

Вид риска(ущерба)	Актуальность	Негативные последствия
У1		
У2	Возможны *(пример)*	П2.2 Потеря (хищение) денежных средств *(пример)*
У3		

- определяете объекты воздействия угроз безопасности информации, заполняется таблица 2.2. Типовые примеры объектов, интерфейсов и видов воздействий приводятся в методике ФСТЭК;

Таблица 2.2

Негативные последствия	Наименование объекта воздействия	Интерфейсы доступа						Виды воздействия					
		ИНТ 1	ИНТ 2	ИНТ 3	ИНТ 4	ИНТ 5	ИНТ 6	В 1	В 2	В 3	В 4	В 5	В 6
П2.2	Носитель информации *(пример)*	-	-	-	да	-	-	да	да	-	да	-	-
...	...												

- определяете источники угроз безопасности информации, заполняется таблица 2.3. Определяем актуальные цели нарушителей, примеры целей берем в Методике ФСТЭК;

Таблица 2.3

Негативные последствия	Вид актуального нарушителя	Цель нарушителя				Категория нарушителя	Уровень возможностей нарушителя
		Ц1	Ц2	⋮	Ц12		
П2.2	Преступные группы *(пример)*	-	-	…	-	внешний	Н2
...	...			…			

- определяете способы реализации угроз безопасности информации, заполняется таблица 2.4. (примеры способов берем из Методики ФСТЭК);

Таблица 2.4

Вид актуального нарушителя	Категория нарушителя	Способ реализации/доступный интерфейс											
		С1	С2	С3	С4	С5	С6	С7	С8	С9	С10	С11	С12
Преступные группы *(пример)*	Внешний	1,2, 3, 4,5	1,2, 3, 4,5, 6	-	-	1, 4	-	-	-	-	-	-	-
...	...												

- из общего состава техник и тактик, приведенных в методике ФСТЭК, исключаем те, которые не связаны с используемыми у нас технологиями, не применимы к нашим процессам, не приводящие к ущербу или недоступные актуальным нарушителям, заполняется таблица 2.5.

Таблица 2.5

№ п/п	Т1 - Сбор информации о системах и сетях	Т2 - Получение первоначального доступа к компонентам систем и сетей	...	Т10 - Несанкционированный доступ и (или) воздействие
1	Т1.1. Сбор информации из публичных источников: официальный сайт (сайты) организации, СМИ, социальные сети, фотобанки, сайты поставщиков и вендоров, материалы конференций/ УБИ006 *(пример)*	Т2.3. Эксплуатация уязвимостей сетевого оборудования и средств защиты вычислительных сетей для получения доступа к компонентам систем и сетей при удаленной атаке / УБИ020	...	Т10.3. Несанкционированное воздействие на программные модули прикладного программного обеспечения / УБИ201
2	...	...	...	...

- последним пунктом выделяете актуальные угрозы безопасности информации и заполняете таблицу 2.6. Исходя применимых тактик, возможностей нарушителей, объектов воздействия и их интерфейсов и способов реализации мы определяем актуальные угрозы (в данном примере угрозы из БДУ объединены в общие группы угроз).

Таблица 2.6

Группа актуальных угроз	**Уровень возможностей нарушителя**	**Объекты воздействия**	**Способы реализации**	**Негативные последствия**
Угроза атаки на клиентов беспроводной сети *(пример)*	Н2	Точка беспроводного доступа	С1, С12	П2.2
...	...	...	...	...

г) По окончании занятия представляете оформленный отчет.

4. Содержание отчета

1. Титульный лист.

2. Описание разделов модели безопасности «Общие положения» и «Описание систем и сетей и их характеристика как объектов защиты», заполненные таблицы со 2.1 по 2.6.

3. Вывод

5. Литература

1. База данных угроз ФСТЭК РОССИИ.

2. Методический документ методика оценки угроз безопасности информации, утвержден ФСТЭК РОССИИ 5 февраля 2021 г.

3. Банк данных угроз безопасности информации ФСТЭК.

Лабораторная работа № 3

Изучение построения системы защиты информации персональных данных на основе нормативных актов и методических указаний

1. Цель работы - закрепить теоретические знания построения системы защиты информации, изучить перечень нормативных документов, определить тип угроз и уровень защищенности информационной системы.

2. Краткие теоретические сведения

Аттестация объектов информатизации осуществляется федеральными органами государственной власти, органами государственной власти субъектов Российской Федерации, органами местного самоуправления, организациями, которым на праве собственности или ином законном основании принадлежат объекты информатизации, а также лицами, заключившими контракт на создание объектов информатизации, или лицами, осуществляющими эксплуатацию объектов информатизации.

Аттестацию на соответствие требованиям по защите информации необходимо проводить для следующих объектов информатизации:

государственных и муниципальных информационных систем, в том числе государственных, муниципальных информационных систем персональных данных;

информационных систем управления производством, используемых организациями оборонно-промышленного комплекса, в том числе автоматизированных систем станков с числовым программным управлением;

помещений, предназначенных для ведения конфиденциальных переговоров;

значимых объектов критической информационной инфраструктуры Российской Федерации;

информационных систем персональных данных (за исключением государственных, муниципальных информационных систем персональных данных);

автоматизированных систем управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды.

Аттестация объекта информатизации проводится на этапе его создания или развития (модернизации) и предусматривает проведение комплекса организационных и технических мероприятий и работ (аттестационных испытаний), в результате которых подтверждается соответствие объекта информатизации требованиям по защите информации в условиях его эксплуатации. Допускается проведение аттестации объекта информатизации на этапе его эксплуатации в случае, если владельцем объекта принято решение об

обработке защищаемой информации после ввода в эксплуатацию объекта информатизации.

Аттестационные испытания включают следующие мероприятия и работы:

а) оценку соответствия технического паспорта объекта информатизации, акта классификации информационной (автоматизированной) системы, акта категорирования значимого объекта, состава и содержания эксплуатационной документации на систему защиты информации объекта информатизации и документов по защите информации владельца объекта информатизации требованиям по защите информации;

б) проверку наличия и согласования с ФСТЭК России, модели угроз безопасности информации, технического задания на создание (развитие, модернизацию) объекта информатизации (только для государственных информационных систем);

в) обследование объекта информатизации на предмет оценки соответствия объекта информатизации и условий его эксплуатации требованиям по защите информации;

г) проверку наличия документов, содержащих результаты анализа уязвимостей, проведенного на этапах предварительных или приемочных испытаний системы защиты информации объекта информатизации;

д) проверку наличия сведений о средствах защиты информации, установленных на объекте информатизации, в реестре сертифицированных средств защиты информации, ведение которого осуществляет ФСТЭК России;

е) проверку наличия у владельца объекта информатизации работников, ответственных за обеспечение защиты информации в ходе эксплуатации объекта информатизации, в том числе за проведение оценки угроз безопасности информации, управление (администрирование) системой защиты информации (администраторов безопасности), управление конфигурацией объекта информатизации, реагирование на инциденты, информирование и обучение персонала, контроль за обеспечением уровня защиты информации, а также проверку достаточности установленных для них обязанностей в соответствии с требованиями по защите информации;

ж) оценку уровня знаний и умений работников владельца объекта информатизации, ответственных за обеспечение защиты информации, в соответствии с установленными для них обязанностями в эксплуатационной документации и документах по защите информации владельца объекта информатизации;

з) оценку соответствия принятых на объекте информатизации организационных мер требованиям по защите информации и их достаточности для защиты от актуальных для объекта информатизации угроз безопасности информации;

и) оценку соответствия принятых на объекте информатизации технических мер по защите информации от несанкционированного доступа (воздействия на информацию) требованиям по защите информации и их

достаточности для защиты от актуальных для объекта информатизации угроз безопасности информации;

к) оценку эффективности защиты (защищенности) информации от утечки по техническим каналам.

При проведении аттестационных испытаний органом по аттестации проводятся:

а) при проведении мероприятий и работ оценка соответствия системы защиты информации объекта информатизации требованиям по защите информации на основе анализа экспертами органа по аттестации документов;

б) при проведении работ испытания системы защиты информации путем осуществления тестирования ее функций безопасности (функциональное тестирование), анализ уязвимостей с использованием средств контроля эффективности защиты информации от несанкционированного доступа, а также испытания системы защиты информации путем осуществления попыток несанкционированного доступа (воздействия) в обход системы защиты информации с использованием средств тестирования;

в) при проведении работ оценка показателей эффективности защиты информации с применением контрольно-измерительного и испытательного оборудования.

В ходе аттестационных испытаний объекта информатизации владельцем объекта информатизации могут вноситься изменения в объект информатизации, в том числе в архитектуру его системы защиты информации, в целях приведения объекта информатизации в соответствие с требованиями по защите информации.

По результатам аттестационных испытаний орган по аттестации оформляет заключение по результатам аттестационных испытаний объекта информатизации, включающее следующие сведения:

а) наименование объекта информатизации и его назначение, состав программно-технических, программных средств и средств защиты информации;

б) класс защищенности информационной (автоматизированной) системы, категория значимости значимого объекта;

в) фамилии, имена, отчества (при наличии), должности экспертов органа по аттестации, проводивших аттестацию объекта информатизации;

г) дату утверждения программы и методик аттестационных испытаний объекта информатизации;

д) срок проведения аттестационных испытаний;

д) наименования и реквизиты документов ФСТЭК России, устанавливающих требования по защите информации, на соответствие которым проводилась аттестация объекта информатизации;

е) результаты испытаний с описанием состава проведенных работ и испытаний в соответствии с программой и методикой испытаний, указанием сроков выполнения каждого испытания и экспертов органа по аттестации,

ответственных за проведение каждого испытания, используемых экспертами при испытаниях средств, а также заключение о соответствии (несоответствии) требованиям по защите информации по каждой проведенной работе и испытанию;

ж) рекомендации по устранению несоответствий системы защиты информации объекта информатизации требованиям по защите информации в случае их выявления при проведении аттестационных испытаний;

з) вывод о возможности или невозможности выдачи аттестата соответствия или о необходимости доработки системы защиты информации объекта информатизации.

Заключение подписывается экспертами органа по аттестации, проводившими аттестацию объекта информатизации, и утверждается руководителем органа по аттестации.

По результатам испытаний органом по аттестации наряду с заключением по результатам аттестационных испытаний оформляются протоколы аттестационных испытаний объекта информатизации, содержащие:

а) наименование испытания в соответствии с программой и методикой испытаний;

б) дату утверждения программы и методик аттестационных испытаний объекта информатизации;

в) дату и место проведения аттестационных испытаний;

г) критерии выполнения требований по защите информации, в отношении которых проводились испытания;

д) условия и исходные данные для проведения испытаний;

е) применяемые при проведении испытаний средства контроля эффективности защиты информации от несанкционированного доступа, а также контрольно-измерительное и испытательное оборудование;

ж) описание порядка испытаний по оценке критериев выполнения требований по защите информации;

з) результаты испытаний по каждому оцениваемому критерию выполнения требований по защите информации.

Протоколы подписываются экспертами органа по аттестации, проводившими аттестационные испытания объекта информатизации.

Заключение и протоколы в течение 5 рабочих дней после утверждения органом по аттестации направляются владельцу объекта информатизации.

В случае выявления в ходе аттестационных испытаний недостатков, которые можно устранить в процессе аттестации объекта информатизации, владелец объекта информатизации обеспечивает их устранение, а орган по аттестации оценивает качество такого устранения.

По результатам устранения недостатков орган по аттестации повторно оформляет заключение, включаются сведения об устранении владельцем объекта информатизации всех выявленных недостатков, а также делается вывод

о возможности выдачи аттестата соответствия требованиям по защите информации на объект информатизации.

Аттестат соответствия оформляется органом по аттестации. Аттестат соответствия подписывается руководителем органа по аттестации и заверяется печатью органа по аттестации (при наличии).

Аттестат соответствия вручается органом по аттестации владельцу объекта информатизации или направляется ему заказным почтовым отправлением с уведомлением о вручении.

При подготовке объекта информатизации к аттестации всё это нужно документально оформить. На рисунке 3.1 представлена последовательность действий для подготовки и проведения аттестации.

Рисунок 3.1 – алгоритм аттестации

Первый документ – перечень объектов информатизации, утверждённый руководителем организации.

Далее издается некоторое количество приказов, здесь указан один – назначении ответственного. В приказе ставиться задача о подготовке документации, провести необходимые работе по защите информации, в этом приказе может быть сформирована комиссия по классификации объектов информатизации. Приказ доводится до исполнителей.

Результатом работы комиссии является акт классификации объекта информатизации. Если обрабатываем государственную тайну нужен еще акт категорирования. Типовой пример акта есть в СТР-К.

Следующий документ, который нужно разработать это модель угроз. Необходимость модели угроз описана в приказах ФСТЭК.

Затем необходим технический паспорт. Может быть подготовлен и для автоматизированных систем и помещений, т.е. состав оборудования, схемы размещения средств, схема электропитания и заземления, перечень программных средств и т.д.

Необходимо подготовить положение по защите конфиденциальной информации. Далее перечень сведений конфиденциального характера, перечень защищаемых ресурсов. Следующее это описание технологического процесса обработки информации.

Далее идут инструкция администратора, инструкция пользователя и инструкция по проведению антивирусного контроля.

Завершает последовательность журнал учета машинных носителей, список пользователей или называется матрица доступа. Т.е. это таблица, в которой расписаны права пользователей.

По завершении издается приказ о вводе в эксплуатации объекта информатизации.

Сертификаты соответствия на СВТ, данные о подготовке кадров, трудовые книжки, план прокладки инженерных коммуникаций и другие документы.

Аттестация объекта информатизации может быть проведена на соответствии требованиям различным документам. Исходя из этого возникают требования к категорированию и классификации автоматизированных систем.

Первоначально выбирают класс защищенности – определенную совокупность требований по защите информации, переделяемых к автоматизированной системе. Определение класса защищенности определяется заказчиком, потом проверяется комиссий по аттестации.

Затем по определенной таблице ФСТЭК определяются необходимые меры (Рисунок 3.2).

Категория	Гриф	Многопользовательский		Однопользовательский
		с разными правами доступа	с равными правами доступа	
1	ОВ	1А	2А	3А
2	СС	1Б		
3	С	1В		
4	ДСП	1Г	2Б	3Б
	ПДн	1Д		

Рисунок 3.2 – Классификация автоматизированных систем

Существует 4 категории. Т.е. от ОВ до конфиденциальной информации.

Классификация касается только автоматизированных систем, к помещениям не относится. Она закрепляется актом.

Рассмотрим классификацию по РД-АС. Самая простая группа однопользовательская. Крайний столбец в таблице. И соответственно два класса 3А - секретно и 3Б – конфиденциальная информация, т.е. работает один человек, почти не встречается (нет отпуска, болезни, командировке).

Следующая группа многопользовательская с равными правами доступа 2А и 2Б – наиболее популярна в организациях.

Следующая группа многопользовательская с разными правами доступа 1А … 1Д. Каждый пользователь может работать со своей папкой и уровнем допуска. 5 классов защищенности. Данная классификация может быть использована для коммерческих структур.

Уровень значимости информации	Масштаб информационной системы		
	Федеральный	Региональный	Объектовый
УЗ1	К1	К1	К1
УЗ2	К1	К2	К2
УЗ3	К2	К3	К3

Рисунок 3.3 – Классификация по уровню значимости информации

Следующий вариант классификации по приказу ФСТЭК (Рисунок 3.3), который используется для государственных и коммерческих информационных систем.

Здесь класс защищённости определяется от уровня значимости информации и масштаба информационной системы. Уровень значимости – степень возможного ущерба от нарушения целостности, доступности и значимости.

Далее по таблице определяется класс защищенности информационной системы. Инструкция по определению класса защищенности есть в 17 приказе ФСТЭК. Затем открываются требования, которые приложены приказу и по таблице реализуются меры по данному классу.

152-ФЗ «О персональных данных» повторяет общемировые тенденции в части защиты персональных данных.

Исходя из определения персональных следует, что к этой информации можно отнести очень многое. В целом под этим понимают информацию необходимую для идентификации человека.

В 2019 году вышло постановление правительства Российской Федерации № 1197, которое касалось биометрической системы персональных данных. Согласно него номер телефона и адрес электронной почты также отнесены к персональным данным.

Возвращаясь к федеральному закону следует, что организация может сама и не обрабатывать персональные данные, передавать другой организации. Но в целом, не может сбросить с себя название оператор.

Тип ИСПДн	Категории субъектов	Количество субъектов	Тип актуальных угроз		
			1 тип	2 тип	3 тип
ИСПДн-С	Не сотрудников	Более 100 000	УЗ 1	УЗ 1	УЗ 2
		Менее чем 100 000	УЗ 1	УЗ 2	УЗ 3
	Сотрудников	Любое	УЗ 1	УЗ 2	УЗ 3
ИСПДн-Б	Не сотрудников	Более 100 000	УЗ 1	УЗ 2	УЗ 3
		Менее чем 100 000	УЗ 1	УЗ 2	УЗ 3
	Сотрудников	Любое	УЗ 1	УЗ 2	УЗ 3
ИСПДн-И	Не сотрудников	Более 100 000	УЗ 1	УЗ 2	УЗ 3
		Менее чем 100 000	УЗ 1	УЗ 3	УЗ 4
	Сотрудников	Любое	УЗ 1	УЗ 3	УЗ 4
ИСПДн-О	Не сотрудников	Более 100 000	УЗ 2	УЗ 2	УЗ 4
		Менее чем 100 000	УЗ 2	УЗ 3	УЗ 4
	Сотрудников	Любое	УЗ 2	УЗ 3	УЗ 4

Рисунок 3.4 – Классификация информационных систем в части персональных данных

Таким образом, еще один вариант классификации по уровни защищенности в части персональных данных Рисунок 3.4.

Для того, чтобы пользоваться данным приказом необходимо определить уровни защищенности в соответствии с Постановлением Правительства Российской Федерации № 1119.

Необходимо определиться с типом персональных данных, их всего четыре: специальные (национальная, здоровье), биометрические, общедоступные и иные категории ПДн (не представлены в трех предыдущих группах).

Далее идет определение категории субъектов. Сотрудники или нет. Важным является их количество – ограничено 100000.

Кроме того, уделяется внимание типам актуальных угроз. 1 тип не декларированные возможности в ОС, системном ПО. 2 тип не декларированные возможности в прикладном ПО. 3 тип не декларированные возможности в ПО не связанном с обработкой ПДн.

Таким образом, происходит определение уровня защищенности, затем по приказу ФСТЭК № 21реализуются все необходимые меры защиты.

3. Порядок выполнения работы.

1. Изучаете необходимые теоретические сведения и уясняете их.
2. Получаете индивидуальное задание на выполнение лабораторной работы, справочные материалы и шаблоны документов.
3. Выполняете пункты индивидуального задания лабораторной работы:

составляете исходные для формирования заявки на объект информатизации;

подготавливаете проект приказа с приложениями о назначении ответственного за защиту информации и классификацию объекта (шаблоны документов прилагаются);

определяете уровень защищенности информационной системы, опираясь на нормативно-правовые акты;

составляете акт определения уровня защищенности информационной системы (акт классификации);

составляете базовый набор мер для определенного вами уровня защищенности, согласно нормативно-методической документации;

определяете соответствие каждому пункту базового набора мер вашей информационной системы и документального или программного его исполнения.

4. По окончании занятия представляете оформленный отчет.

4. Содержание отчета

1. Титульный лист.
2. Задание.
3. Исходные для формирования заявки на объект информатизации, акт определения уровня защищенности информационной системы, базовый набор мер для определенного вами уровня защищенности.
4. Вывод.

5. Литература

1. Федеральный закон от 27 июля 2006 г. N 152-ФЗ "О персональных данных".
2. Постановление Правительства Российской Федерации от 1 ноября 2012 г. N 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных"
3. Приказ Федеральной службы по техническому и экспортному контролю от 18 февраля 2013 г. N 21 "Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных".
4. Приказ Федеральной службы по техническому и экспортному контролю от 29 апреля 2021 г. № 77 “Об утверждении Порядка организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну”
5. Материалы лекций.

Лабораторная работа № 4

Методика выбора оптимальных средств защиты информационной системы

1. Цель работы - изучить экспертную методику выбора средств защиты информации.

2. Краткие теоретические сведения

Последним этапом после определения требований приказа ФСТЭК, которым определены требования к аттестации объекта информатизации, моделированная угроз и уточнения мер защиты – является выбор средств защиты информационной системы.

Выбор любых других средств является достаточно сложной задачей, потому что как правило средства защиты информации от разных производителей достаточно разные и обладают разными характеристиками.

Найти какую-либо линейку одинаковых средств, которые выполняют примерно одни и те же функции, но от разных производителей очень сложно.

Есть различные методы для выбора СЗИ, но мы рассмотрим на лабораторной работе анализ средств защиты информации методом анализа иерархий.

Данный метод предоставляет математический инструмент, в котором сравниваются количественные и качественные характеристики СЗИ.

Для примера рассмотрим аппаратно-программные модули доверенной загрузки.

«Соболь» – Код безопасности

«Криптон –замок» - Анкад

«Аккорд-АМДЗ» - ОКБ САПР

«Максим-М1» - НПО «РусБИТех»

Выберем четыре критерия оценки аппаратно-программных модулей доверенной загрузки.

Количественные:

1. Срок действия сертификата (должен быть максимальный -выгодней)
2. Требования к СДЗ ФСТЭК России (чем меньше, тем лучше - надёжнее).

Качественные:

3. Функциональный набор СДЗ.
4. Поддерживаемые файловые системы

Критерии 1 и 2 количественные – можно измерить, критерии 3 и 4 качественные, определяются экспертами.

На сайте ФСТЭК уточняем сроки действия сертификатов аппаратно-программных модулей доверенной загрузки и заполняем таблицу 4.1.

Таблица 4.1

	Срок действия сертификата	Процентное соотношение	
«Соболь» – Код безопасности	До 05.12.2026 г. (2009 дней)	2009/5819	0,345
«Криптон –замок» - Анкад	До 04.09.2024 г. (1218 дней)	1218/5819	0,209
«Аккорд-АМДЗ» - ОКБ САПР»	До 13.02.2024 г (1287 дней)	1287/5819	0,221
«Максим-М1» - НПО «РусБИТех»	До 31.12.2024 (1305 дней)	1305/5819	0,224
	5819		0,999

Далее находим общую сумму дней и записываем внизу в этом столбце в последней строке. Затем процентное соотношение для каждого СЗИ, т.е. заполним следующий столбец.

Самый высокий коэффициент получился у аппаратно-программного модуля доверенной загрузки **«Соболь» – Код безопасности, до 2026 года.**

Расчет коэффициентов для срока действия сертификата завершен.

Следующий расчет коэффициентов для требований к СДЗ, заполняем таблицу 4.2.

Таблица 4.2

	Требования к СДЗ ФСТЭК России	Процентное соотношение		
«Соболь» – Код безопасности	2 класс защиты	2/13=0,153	1/0,153=6,535	6,535/21,463=**0,304**
«Криптон – замок» - Анкад	нет класса, присваиваем значение 7	7/13=0,538	1/0,538=1,858	1,858/21,463=**0,086**
«Аккорд-АМДЗ» - ОКБ САПР»	2 класс защиты	2/13=0,153	1/0,153=6,535	6,535/21,463=**0,304**
«Максим-М1» - НПО «РусБИТех»	2 класс защиты	2/13=0,153	1/0,153=6,535	6,535/21,463=**0,304**
	13		21,463	

Далее находим общую сумму и записываем внизу в этом столбце в последней строке. Теперь находим процентное соотношение для каждого СЗИ, т.е. заполним следующий столбец.

Но здесь мы знаем, что чем меньше класс защиты, тем лучше. Следовательно, необходимо привести к обратной форме.

Самый высокий коэффициент получился у трех аппаратно-программных модулей доверенной загрузки.

Расчет количественных критериев выбора завершен.

Рассмотрим функциональный набор СДЗ выбранных средств защиты, представленный в таблице 4.3.

Таблица 4.3

Параметр сравнения	**«Соболь»**	**«Криптон – замок»**	**«Аккорд-АМДЗ»**	**«Максим-М1»**
Доступ пользователя по паролю	да	да	да	да
Доступ пользователя по идентификатору и паролю	да	да	да	да
Блокировка загрузки ОС со сторонних носителей	да	да	да	да
Контроль целостности файлов и секторов накопителя	да	да	да	да
Контроль целостности системного реестра	да	да	да	да
Контроль целостности BIOS (UEFI)	да	да	да	да
Контроль целостности аппаратной части	да	да	да	да
Контроль целостности транзакций в журналах файловых систем	да	да	да	да
Самоконтроль средства (модуля) доверенной загрузки	да	да	да	да
Ограничение доступа к BIOS (UEFI)	да	да	**нет**	да
Регистрация событий безопасности	да	да	да	да
Программная инициализация комплекса	да	да	да	да
Удалённое управление	да	да	да	да
Энергонезависимая память	да	да	да	да
Сторожевой таймер	да	да	да	да
Датчик случайных чисел (аппаратный/программный)	да	да	да	да
Контроль вскрытия корпуса ПЭВМ	**нет**	да	да	да
Инициализация устройств шифрования	**нет**	да	да	да
Неизвлекаемость из ПЭВМ	**нет**	да	**нет**	**нет**

Из таблицы видно, что не по всем параметрам СДЗ имеют одинаковые свойства.

Далее составляем таблицу 4.4 для получения коэффициентов функционального набора СДЗ, в данном случае это качественный показатель.

Сначала заполняем первый столбец таблицы – экспертным методом, затем первую строку и диагональ.

Т.е. сравнили СДЗ «Соболь» с каждым – метод попарного сравнения.

Таблица 4.4

	«Соболь»	«Максим-М1»	«Аккорд-АМДЗ»	«Криптон – замок»		
«Соболь»	1	1/5	1/3	1/9	1,64	0,044
«Максим-М1»	5	1	3	1/5	9,20	0,247
«Аккорд-АМДЗ»	3	1/3	1	1/7	4,47	0,120
«Криптон – замок»	9	5	7	1	22	0,590
					37,31	

Далее экспертным путем, опираясь метод иерархий, заполняем нашу таблицу 4.4. Затем находим сумму в каждой строке, а также сумму столбца и находим коэффициенты. Соответственно СДЗ «Криптон-замок» занимает первое место с самым высоким коэффициентом.

Следующая характеристика — это поддерживаемые файловые системы, также качественная.

Таблица 4.5

«Соболь»	«Максим-М1»	«Аккорд-АМДЗ»	«Криптон – замок»
NTFS, FAT 16, FAT 32, UFS, UFS2, EXT2, EXT3, EXT4	FAT32, NTFS 3.0, NTFS 3.1, Ext2, Ext3 и Ext4	FAT12, FAT16, FAT32, NTFS, Ext2, Ext3 Ext4, FreeBSD UFS/UFS2, QNX4, QNX6, XFS	FAT12, FAT16, FAT32, NTFS, Ext2, Ext3, Ext4
8	**6**	**11**	**7**

Далее экспертным путем заполняем таблицу 4.6.

Таблица 4.6

	«Соболь»	«Аккорд-АМДЗ»	«Криптон –замок»	«Максим-М1»		
«Соболь»	1	1/3	5	9	15,33	0,39
«Аккорд-АМДЗ»	3	1	5	9	18	0,458
«Криптон – замок»	1/5	1/5	1	3	4,4	0,112
«Максим-М1»	1/9	1/9	1/3	1	1,55	0,039
					39,28	

Затем находим сумму в каждой строке, а также сумму столбца и находим коэффициенты. Соответственно СДЗ «Аккорд-АМДЗ» занимает первое место с самым высоким коэффициентом. Т.е. мы сделали расчет всех четырех критериев.

Далее выделяем критерии по важности те же способом, что и качественные критерии – таблица 4.7.

Таблица 4.7

	Поддерживаемые файловые системы	Срок действия сертификата	Функциональный набор СДЗ	Требования к СДЗ ФСТЭК		
Поддерживаемые файловые системы	1	1/5	1/7	1/3	1,67	0,055
Срок действия сертификата	5	1	1/3	1	7,33	0,243
Функциональный набор СДЗ	7	3	1	5	16	0,530
Требования к СДЗ ФСТЭК	3	1	1/5	1	5,2	0,172
				30,2		

Самый важный критерий — это функциональный набор СДЗ.

Далее составляем общую таблицу 4.8, в которую сводим все значения предыдущих таблиц.

Таблица 4.8

	Поддерживаемые файловые системы	Срок действия сертификата	Функциональный набор СДЗ	Требования к СДЗ ФСТЭК		
Значимость критерия	0,055	0,243	0,530	0,172		
«Соболь»	0,390	0,345	0,044	0,304		
«Аккорд-АМДЗ»	0,458	0,221	0,120	0,304		
«Криптон – замок»	0,112	0,209	0,590	0,086		
«Максим-М1»	0,039	0,224	0,247	0,304		

Затем перемножаем коэффициент значимости на коэффициенты каждого СДЗ, получается значение в скобках – таблица 4.9.

Таблица 4.9

	Поддерживаемые файловые системы	Срок действия сертификата	Функциональный набор СДЗ	Требования к СДЗ ФСТЭК	**Общий коэф.**	
Значимость критерия	0,055	0,243	0,530	0,172		
«Соболь»	0,390 (0,021)	0,345 (0,08)	0,044 (0,232)	0,304 (0,052)	0,385	
«Аккорд-АМДЗ»	0,458 (0,025)	0,221 (0,05)	0,120 (0,06)	0,304 (0,052)	0,187	
«Криптон –замок»	0,112 (0,006)	0,209 (0,05)	0,590 (0,31)	0,086 (0,014)	0,38	
«Максим-М1»	0,039 (0,002)	0,224 (0,05)	0,247 (0,13)	0,304 (0,052)	0,234	

Далее полученные коэффициенты суммируем по строке. Затем переходим к стоимости СДЗ – таблица 4.10.

Таблица 4.10

	Цена	**Коэф.**
«Соболь»	10290 р.	0,223
«Аккорд-АМДЗ»	10800 р.	0,234
«Криптон – замок»	8350 р.	0,181
«Максим-М1»	16597 р.	0,360
	46039	

Далее данные сводим в одну таблицу и делим общий коэффициент СДЗ на коэффициент стоимости СДЗ – таблица 4.11.

Таблица 4.11

	Общий коэф. СДЗ	**Коэф. – стоимость СДЗ**	
«Соболь»	0,385	0,223	1,721
«Аккорд-АМДЗ»	0,187	0,234	0,79
«Криптон – замок»	0,38	0,181	2,09
«Максим-М1»	0,234	0,360	0,65

Соответственно по выбранным количественным и качественным критериям СДЗ «Криптон-замок» занимает первое место с самым высоким

коэффициентом, которое будет предлагаться для покупки и установки на рабочие станции и сервера корпоративной сети авиапредприятия.

Таким образом, для решения задачи выбора средств защиты информации, их покупки и установки на рабочие станции и сервера корпоративной сети авиапредприятия, целесообразно применить комплексную методику, основанную на методе анализа иерархий.

3. Порядок выполнения работы.

а) Изучаете необходимые теоретические сведения и уясняете их.

б) Получаете индивидуальное задание на выполнение лабораторной работы

в) Выполнение работы:

выбираете шесть критериев оценки средств защиты информации, из которых два качественные;

вычисляете коэффициенты для количественных критериев;

вычисляете коэффициенты для качественных критериев;

рассчитываете критерии по важности;

определяете коэффициенты средств защиты информации по стоимости;

сводите полученные данные в одну таблицу рассчитанные показатели и определяете оптимальное средство защиты информации.

г) составляете отчет.

4. Содержание отчета

1. Титульный лист.
2. Таблицы по качественным и количественным критериям, их описание для выбора средств защиты информации.
3. Вывод

5. Литература

1. Саати, Т. Принятие решений. Метод анализа иерархий / Т. Саати. – М.: Радио и связь, 1993.

2. Петриченко, Г.С. Оценка эффективности программного обеспечения / Г.С. Петриченко, В.Г. Петриченко // Научные ведомости Белгородского государственного университета. Серия: Экономика, Информатика. - 2016. - № 9 (230). - вып. 38. С. 108- 112.

3. Петриченко, Г.С. Построение программы поиска неисправностей в электронных блоках средств вычислительной техники с применением метода анализа иерархий / Г.С. Петриченко, Н.Ю. Нарыжная, М.Ю. Срур // Политематический сетевой электронный научный журнал Кубанского государственного аграрного университета. - 2011. - № 69. - С. 13-22.

4. Материалы лекций