

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ОБРАЗОВАНИЯ
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

МЕТОДИЧЕСКИЕ УКАЗАНИЯ
по выполнению практических работ
по дисциплине
«Технологии обеспечения информационной безопасности»
Направление подготовки 10.04.01 Информационная безопасность
направленность (профиль) «Математическое и программное обеспечение защиты
информации»

Ставрополь, 2026 г.

Введение

Настоящие методические указания разработаны в соответствии с рабочей программой дисциплины «Технологии обеспечения информационной безопасности» и предназначены для обучающихся по направлению подготовки 10.04.01 Информационная безопасность, направленность (профиль) «Математическое и программное обеспечение защиты информации».

Учебным планом по дисциплине предусмотрено 108 академических часов (3 зачётные единицы), в том числе 36 часов лекций, 36 часов практических занятий и 36 часов самостоятельной работы. Лабораторные работы учебным планом не предусмотрены. Форма промежуточной аттестации – зачёт с оценкой в 1 семестре.

Дисциплина участвует в формировании компетенций ОПК-1, ОПК-2 и ОПК-5 через индикаторы ИД-1 ОПК-1, ИД-2 ОПК-1, ИД-3 ОПК-1, ИД-1 ОПК-2, ИД-2 ОПК-2, ИД-1 ОПК-5 и ИД-2 ОПК-5. Распределение индикаторов по практическим работам приведено в таблице 1.

Указания состоят из двух частей. Часть 1 содержит методические указания по выполнению шести практических работ, тематика которых полностью соответствует разделам (темам) рабочей программы дисциплины. Каждая работа включает цель, порядок подготовки, теоретическую часть, пошаговый порядок выполнения, формы для оформления результатов, методические рекомендации, требования к отчёту и контрольные вопросы двух уровней сложности. Часть 2 содержит методические указания по организации самостоятельной работы обучающихся с распределением часов, заданиями и вопросами для самопроверки по каждой теме.

Соответствие практических работ темам рабочей программы

Таблица 1 – Соответствие практических работ темам рабочей программы дисциплины

№	Тема (раздел) рабочей программы	Практическая работа	Индикаторы	Ч
1	Введение в технологии обеспечения информационной безопасности. Архитектурные стандарты информационной безопасности	Практическая работа № 1. Архитектурные стандарты информационной безопасности. Экспертный анализ защищённости автоматизированной системы	ИД-1 ОПК-1, ИД-2 ОПК-1	6
2	Требования и рекомендации по защите информации, обрабатываемой средствами вычислительной техники	Практическая работа № 2. Требования и рекомендации по защите информации, обрабатываемой средствами вычислительной техники	ИД-1 ОПК-1, ИД-2 ОПК-1, ИД-3 ОПК-1	6
3	Классификация технических каналов утечки информации. Модель угроз и модель нарушителя	Практическая работа № 3. Классификация технических каналов утечки информации. Разработка модели угроз и модели нарушителя	ИД-2 ОПК-1, ИД-3 ОПК-1	6
4	Стандарты и спецификации информационной безопасности: BS 7799, FIPS 140-2, «Общие критерии»	Практическая работа № 4. Четырёхфазная модель процесса управления информационной безопасностью. Оценка профилей защиты и заданий по безопасности	ИД-3 ОПК-1, ИД-1 ОПК-2	6
5	Эксплуатационное окружение и управление криптографическими ключами. Технические спецификации информационной безопасности	Практическая работа № 5. Эксплуатационное окружение и управление криптографическими ключами. Обеспечение аутентичности	ИД-1 ОПК-2, ИД-2 ОПК-2	6
6	Анализ защищённости информационных систем. Политика безопасности предприятия. Оформление результатов исследований	Практическая работа № 6. Анализ защищённости операционных систем и СУБД. Размещение Web-серверов и выбор поставщика Internet-услуг	ИД-2 ОПК-2, ИД-1 ОПК-5, ИД-2 ОПК-5	6

Итого практических занятий – 36 часов.

Часть 1. Методические указания по выполнению практических работ

Общие требования к выполнению практических работ

Практические занятия проводятся с целью закрепления теоретического материала и приобретения навыков его применения при решении практических задач в области обеспечения информационной безопасности.

Перед началом занятия обучающийся обязан изучить теоретический материал соответствующей лекции, ознакомиться с заданием и подготовить ответы на контрольные вопросы базового уровня. К выполнению работы допускаются обучающиеся, прошедшие входной контроль подготовленности. Обучающийся, не прошедший входной контроль, выполняет работу во время, отведённое для консультаций.

Каждая работа выполняется по индивидуальному варианту, выдаваемому преподавателем. Использование результатов, полученных другими обучающимися, не допускается: при защите работы обучающийся обязан обосновать каждое принятое решение применительно к своему варианту.

По результатам выполнения каждой работы оформляется отчёт. Требования к содержанию отчёта приведены в описании соответствующей работы. Отчёт представляется в печатном или электронном виде не позднее следующего занятия.

Работа считается выполненной после защиты отчёта, в ходе которой обучающийся отвечает на контрольные вопросы базового и повышенного уровня и обосновывает принятые решения. Критерии оценивания приведены в фонде оценочных средств по дисциплине.

Практическая работа № 1. Архитектурные стандарты информационной безопасности. Экспертный анализ защищённости автоматизированной системы

Тема 1. Введение в технологии обеспечения информационной безопасности. Архитектурные стандарты информационной безопасности

Формируемые индикаторы: ИД-1 ОПК-1, ИД-2 ОПК-1. Продолжительность занятия – 6 часов.

В результате выполнения работы обучающийся должен:

- знать состав, назначение и область применения архитектурных стандартов информационной безопасности;
- уметь сопоставлять требования стандартов с фактическим состоянием автоматизированной системы;
- владеть навыками формирования исходных данных для технического задания на систему обеспечения информационной безопасности.

1. Цель занятия

1. Изучить состав и назначение архитектурных стандартов информационной безопасности и их место в системе нормативных документов Российской Федерации.
2. Освоить методику сопоставления сервисов и механизмов безопасности с требованиями стандартов.
3. Отработать навыки экспертного анализа защищённости автоматизированной информационной системы и оформления его результатов.

2. Подготовка к занятию

1. Изучить теоретический материал лекций по теме 1.
2. Ознакомиться с содержанием рекомендаций X.800 и структурой «Оранжевой книги» (TCSEC).
3. Ознакомиться с перечнем действующих нормативных правовых актов в области защиты информации.
4. Подготовить ответы на контрольные вопросы базового уровня.
5. Получить у преподавателя индивидуальный вариант объекта анализа.

3. Теоретическая часть

3.1. Место архитектурных стандартов в системе обеспечения информационной безопасности

Технологии обеспечения информационной безопасности опираются на совокупность нормативных документов разного уровня. Верхний уровень образуют федеральные законы и подзаконные акты, определяющие правовой режим информации. Средний уровень составляют национальные и международные стандарты, задающие требования к процессам и продуктам. Нижний уровень – организационно-распорядительные документы конкретной организации: политика безопасности, регламенты, инструкции.

Архитектурные стандарты занимают промежуточное положение: они не описывают конкретные технические решения, но задают понятийный аппарат, перечень сервисов безопасности и критерии, по которым оценивается защищённость. Именно поэтому обоснование требований к системе обеспечения информационной безопасности начинается с выбора набора стандартов, применимых к объекту защиты.

Практическое значение архитектурных стандартов состоит в том, что они позволяют перейти от неформального описания «система должна быть защищённой» к проверяемому

перечню требований, который может быть включён в техническое задание и впоследствии проверен при приёмке.

3.2. Нормативная база Российской Федерации

Основу правового регулирования составляют следующие документы:

- Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» – вводит понятия информации, информационных технологий, информационной системы, информационно-телекоммуникационной сети, обладателя информации, доступа к информации;
- Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» – определяет понятие персональных данных, состав действий по их обработке, требования к защите информационных систем персональных данных;
- Федеральный закон от 21.07.1993 № 5485-1 «О государственной тайне» – определяет понятие средств защиты информации и порядок работы со сведениями, составляющими государственную тайну;
- приказы и методические документы ФСТЭК России, устанавливающие состав и содержание организационных и технических мер защиты;
- национальные стандарты серии ГОСТ Р, в том числе ГОСТ Р 50922 «Защита информации. Основные термины и определения».

При выполнении работы необходимо для каждого документа определить область его действия применительно к анализируемому объекту: распространяется ли он на объект полностью, частично или не применяется вовсе. Ошибка на этом шаге приводит к формированию избыточных либо, наоборот, недостаточных требований.

3.3. Рекомендации X.800

Рекомендации X.800 Международного союза электросвязи описывают архитектуру безопасности для взаимодействия открытых систем. Документ вводит понятие сервиса безопасности – функции, обеспечивающей защиту одного из свойств информации, и механизма безопасности – способа реализации сервиса.

Таблица 1.1 – Сервисы безопасности согласно рекомендациям X.800

Сервис безопасности	Назначение	Типовые механизмы реализации
Аутентификация партнёров по общению	Подтверждение подлинности взаимодействующих сторон	Пароли, одноразовые пароли, сертификаты, криптографические протоколы
Аутентификация источника данных	Подтверждение подлинности отправителя сообщения	Электронная подпись, имитовставка
Управление доступом	Предотвращение несанкционированного использования ресурсов	Списки контроля доступа, метки безопасности, ролевые модели
Конфиденциальность данных	Защита от раскрытия содержимого	Шифрование, заполнение трафика
Целостность данных	Защита от несанкционированного изменения	Контрольные суммы, имитовставка, электронная подпись
Неотказуемость	Невозможность отрицания факта отправки или получения	Электронная подпись, нотариализация, протоколирование

Рекомендации X.800 распределяют сервисы по уровням эталонной модели взаимодействия открытых систем. Так, аутентификация может быть реализована на сетевом уровне, что важно учитывать при проектировании защищённых сетевых взаимодействий.

3.4. «Оранжевая книга» (TCSEC)

Критерии оценки доверенных компьютерных систем («Оранжевая книга») вводят четыре группы уровней безопасности, обозначаемые буквами от D до A.

Таблица 1.2 – Уровни безопасности согласно «Оранжевой книге»

Уровень	Характеристика	Основное содержание требований
D	Минимальная защита	Системы, не удовлетворяющие требованиям более высоких уровней
C	Произвольное управление доступом	Разграничение доступа по усмотрению владельца ресурса, идентификация и аутентификация, протоколирование (C1, C2)
B	Принудительное управление доступом	Метки безопасности, мандатное разграничение доступа, доверенная вычислительная база, контроль скрытых каналов (B1–B3)
A	Верифицируемая безопасность	Формальная верификация проекта системы и соответствия реализации спецификации

Согласно «Оранжевой книге» политика безопасности включает такие элементы, как метки безопасности, произвольное и принудительное управление доступом. Важно различать элементы политики безопасности и организационные документы, в которых она закрепляется.

3.5. «Общие критерии» (ISO/IEC 15408)

«Общие критерии» реализуют иной подход: вместо фиксированной шкалы уровней вводятся понятия объекта оценки, профиля защиты и задания по безопасности. Требования разделены на функциональные (что система должна делать) и требования доверия (насколько можно верить, что она это делает).

В число классов требований доверия безопасности входят разработка, руководства, поддержка жизненного цикла, тестирование, оценка уязвимостей, а также сертификация. Оценочные уровни доверия (ОУД 1–7) характеризуют глубину и строгость проведённой оценки: чем выше уровень, тем более детальные свидетельства должен предоставить разработчик.

Принципиальное отличие «Общих критериев» от «Оранжевой книги» состоит в гибкости: набор требований формируется под конкретный класс продуктов, а не выбирается из закрытого перечня уровней.

3.6. Методика экспертного анализа защищённости

Экспертный анализ защищённости выполняется в следующей последовательности:

1. Описание объекта анализа: состав технических и программных средств, обрабатываемая информация, границы контролируемой зоны.
2. Выбор набора нормативных документов и стандартов, применимых к объекту.
3. Формирование перечня проверяемых требований на основе выбранных документов.
4. Сопоставление фактического состояния объекта с каждым требованием, фиксация результата в форме «соответствует / соответствует частично / не соответствует».
5. Ранжирование выявленных несоответствий по степени критичности.
6. Формирование предложений по устранению несоответствий и оценка их приоритетности.

Результат анализа оформляется в виде таблицы несоответствий, которая служит исходным материалом для раздела «Требования к системе защиты информации» технического задания.

4. Порядок выполнения работы

1. Ознакомиться с индивидуальным вариантом задания: описанием автоматизированной информационной системы условной организации, составом обрабатываемой информации и границами контролируемой зоны.

2. Составить описание объекта анализа по форме таблицы 1.3, указав технические средства, программные средства, виды обрабатываемой информации и категории пользователей.

3. Сформировать перечень нормативных документов и стандартов, применимых к объекту, с обоснованием области действия каждого документа (форма таблицы 1.4).

4. Провести сопоставление сервисов безопасности по рекомендациям X.800 с механизмами, фактически реализованными в системе. Для каждого сервиса указать: реализован полностью, реализован частично, не реализован (форма таблицы 1.5).

5. Определить уровень безопасности системы по классификации «Оранжевой книги». Обосновать вывод ссылками на конкретные признаки, выявленные при анализе.

6. Сформировать перечень несоответствий, проранжировав их по степени критичности (высокая, средняя, низкая).

7. Сформулировать не менее пяти предложений по повышению защищённости системы и оформить их в виде фрагмента раздела технического задания.

8. Оформить отчёт и защитить работу, ответив на контрольные вопросы преподавателя.

5. Формы для оформления результатов

Таблица 1.3 – Форма описания объекта анализа

Элемент объекта	Характеристика	Обрабатываемая информация

Таблица 1.4 – Форма перечня применимых нормативных документов

Документ	Область действия	Применимость к объекту (обоснование)

Таблица 1.5 – Форма сопоставления сервисов безопасности

Сервис по X.800	Механизм в системе	Степень реализации	Примечание

6. Методические рекомендации по выполнению

При выборе нормативных документов следует избегать двух типичных ошибок. Первая – включение в перечень документов, не относящихся к объекту (например, требований к защите государственной тайны для системы, обрабатывающей только персональные данные). Вторая – пропуск документов, обязательных для данного класса систем.

При определении уровня безопасности по «Оранжевой книге» необходимо опираться на признаки, которые можно проверить: наличие меток безопасности, вид управления доступом, наличие механизмов протоколирования и аудита. Вывод «система соответствует уровню C2» без указания проверенных признаков считается необоснованным.

Предложения по повышению защищённости формулируются в виде требований, а не пожеланий: вместо «улучшить парольную политику» следует писать «установить

минимальную длину пароля не менее 12 символов, срок действия – не более 90 дней, запрет повторного использования последних пяти паролей».

7. Содержание отчёта

Отчёт оформляется в текстовом редакторе на листах формата А4 и содержит:

- титульный лист установленной формы;
- цель работы и индивидуальный вариант задания;
- описание объекта анализа (таблица 1.3);
- перечень применимых нормативных документов (таблица 1.4);
- результаты сопоставления сервисов безопасности (таблица 1.5);
- обоснованный вывод об уровне безопасности системы;
- перечень несоответствий с ранжированием по критичности;
- фрагмент раздела технического задания с предложениями по повышению защищённости;
- выводы по работе;
- список использованных источников.

8. Контрольные вопросы

Базовый уровень:

1. Назначение и состав архитектурных стандартов информационной безопасности.
2. Сервисы безопасности согласно рекомендациям X.800 и механизмы их реализации.
3. Уровни безопасности согласно «Оранжевой книге» и их характеристики.
4. Понятия объекта оценки, профиля защиты и задания по безопасности в «Общих критериях».
5. Основные нормативные правовые акты Российской Федерации в области защиты информации.

Повышенный уровень:

6. Сопоставьте требования «Общих критериев» и «Оранжевой книги»: в чём принципиальное различие подходов к оценке защищённости?
7. Обоснуйте выбор набора стандартов для автоматизированной системы, обрабатывающей персональные данные и коммерческую тайну одновременно.
8. Какие сервисы безопасности по X.800 невозможно реализовать без применения криптографических механизмов? Обоснуйте ответ.
9. Каким образом результаты экспертного анализа защищённости используются при разработке технического задания?

Практическая работа № 2. Требования и рекомендации по защите информации, обрабатываемой средствами вычислительной техники

Тема 2. Требования и рекомендации по защите информации, обрабатываемой средствами вычислительной техники

Формируемые индикаторы: ИД-1 ОПК-1, ИД-2 ОПК-1, ИД-3 ОПК-1. Продолжительность занятия – 6 часов.

В результате выполнения работы обучающийся должен:

- знать состав требований и рекомендаций по технической защите конфиденциальной информации;
- уметь формировать перечень мер защиты информации для объекта информатизации;
- владеть навыками обоснования критериев оценки эффективности системы защиты информации.

1. Цель занятия

1. Изучить требования и рекомендации по технической защите конфиденциальной информации, установленные нормативными документами ФСТЭК России.
2. Освоить порядок определения состава объекта информатизации и перечня защищаемой информации.
3. Отработать навыки формирования перечня мер защиты и обоснования критериев оценки их эффективности.

2. Подготовка к занятию

1. Изучить теоретический материал лекций по теме 2.
2. Ознакомиться с содержанием документа СТР-К.
3. Изучить состав организационных и технических мер защиты информации, установленных приказами ФСТЭК России.
4. Подготовить ответы на контрольные вопросы базового уровня.
5. Получить у преподавателя индивидуальный вариант объекта информатизации.

3. Теоретическая часть

3.1. Назначение и область применения документа СТР-К

Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К) утверждены приказом Гостехкомиссии России от 30.08.2002 № 282. Документ является нормативно-методическим и устанавливает порядок организации работ, требования и рекомендации по обеспечению технической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну, на территории Российской Федерации.

Требования и рекомендации документа распространяются на защиту государственных информационных ресурсов некриптографическими методами (служебная тайна), направленными на предотвращение утечки защищаемой информации по техническим каналам, от несанкционированного доступа к ней и от специальных воздействий на информацию в целях её уничтожения, искажения или блокирования.

Для негосударственных организаций документ носит рекомендательный характер, однако широко применяется как методическая основа при построении систем защиты информации, поскольку содержит проработанную структуру мер и порядок их выбора.

3.2. Объекты защиты на объекте информатизации

Согласно СТР-К объектами защиты являются:

- технические средства и системы, обрабатывающие конфиденциальную информацию: средства вычислительной техники, средства изготовления и размножения документов, иные технические средства обработки речевой, графической, видео- и буквенно-цифровой информации;
- программные средства: операционные системы, системы управления базами данных, другое общесистемное и прикладное программное обеспечение;
- средства защиты информации, используемые для обработки конфиденциальной информации;
- технические средства и системы, не обрабатывающие непосредственно конфиденциальную информацию, но размещённые в помещениях, где она обрабатывается (циркулирует);
- защищаемые помещения.

Разделение объектов защиты на указанные группы принципиально: для каждой группы применяется свой набор мер. Так, для вспомогательных технических средств и систем основную роль играют меры противодействия утечке по техническим каналам, а для программных средств – меры разграничения доступа и контроля целостности.

3.3. Основные принципы и структура защиты информации

Защита информации на объекте информатизации достигается выполнением комплекса организационных мероприятий и применением средств защиты информации от утечки по техническим каналам, от несанкционированного доступа и от программно-технических воздействий с целью нарушения целостности (модификации, уничтожения) и доступности информации в процессе её обработки, передачи и хранения.

Комплекс программно-технических средств и организационных мер по защите информации от несанкционированного доступа реализуется в рамках системы защиты информации от НСД, условно состоящей из четырёх подсистем:

1. подсистема управления доступом;
2. подсистема регистрации и учёта;
3. криптографическая подсистема;
4. подсистема обеспечения целостности.

Такое разбиение удобно использовать как структуру при формировании перечня мер: для каждой подсистемы определяется набор требований, а затем – конкретные механизмы их реализации.

3.4. Классификация мер защиты информации

Таблица 2.1 – Классификация мер защиты информации по областям

Область	Содержание мер	Примеры
Правовые	Закрепление правового режима информации и ответственности	Перечень сведений конфиденциального характера, соглашения о неразглашении, положения трудовых договоров
Организационные	Регламентация деятельности персонала и порядка работ	Политика безопасности, инструкции пользователей и администраторов, порядок допуска, контроль исполнения
Физические	Ограничение физического доступа и защита помещений	Контрольно-пропускной режим, системы охранной сигнализации, экранирование помещений
Аппаратные	Применение технических средств защиты	Аппаратные модули доверенной загрузки, генераторы шума, средства контроля доступа
Программные	Применение программных средств защиты	Средства разграничения доступа, антивирусная защита, средства аудита, средства обнаружения вторжений
Криптографические	Защита конфиденциальности и целостности криптографическими методами	Шифрование данных и каналов связи, электронная подпись, средства управления ключами

При формировании перечня мер необходимо обеспечить их непротиворечивость и полноту: каждая выявленная угроза должна быть перекрыта хотя бы одной мерой, а каждая мера – обоснована наличием соответствующей угрозы или требования нормативного документа.

3.5. Критерии оценки эффективности системы защиты информации

Оценка эффективности системы защиты информации требует заранее определённых критериев. На практике применяют три группы критериев:

- критерии соответствия – доля требований нормативных документов, выполненных полностью, частично и не выполненных;
- критерии результативности – количество и характер выявленных инцидентов, время обнаружения и устранения, доля перекрытых угроз из модели угроз;
- критерии ресурсоёмкости – затраты на создание и эксплуатацию системы защиты, влияние средств защиты на производительность информационной системы.

Критерии должны быть измеримыми и проверяемыми. Формулировка «система защиты должна быть эффективной» критерием не является; формулировка «время обнаружения инцидента не должно превышать 15 минут с момента его возникновения» – является.

4. Порядок выполнения работы

1. Ознакомиться с индивидуальным вариантом задания: описанием объекта информатизации условной организации.

2. Определить состав объекта информатизации: технические средства, программные средства, средства защиты, вспомогательные технические средства и системы, защищаемые помещения (форма таблицы 2.2).

3. Составить перечень видов конфиденциальной информации, обрабатываемой на объекте, с указанием правового основания ограничения доступа и последствий нарушения конфиденциальности.

4. Сформировать перечень мер защиты информации по областям на основе требований СТР-К, оформив результат по форме таблицы 2.3.

5. Распределить сформированные меры по четырём подсистемам системы защиты информации от НСД.

6. Обосновать критерии, по которым будет оцениваться эффективность предложенной системы защиты, с указанием способа измерения каждого критерия (форма таблицы 2.4).

7. Оформить результаты в виде фрагмента раздела технического задания «Требования к системе защиты информации».

8. Оформить отчёт и защитить работу.

5. Формы для оформления результатов

Таблица 2.2 – Форма описания состава объекта информатизации

Группа объектов защиты	Состав	Размещение (помещение, зона)

Таблица 2.3 – Форма перечня мер защиты информации

Область мер	Содержание меры	Перекрываемая угроза	Основание (пункт документа)

Таблица 2.4 – Форма перечня критериев оценки эффективности

Критерий	Способ измерения	Целевое значение

6. Методические рекомендации по выполнению

Перечень видов конфиденциальной информации следует составлять не по названиям документов, а по категориям сведений. Например, вместо «договоры» указывается «сведения об условиях сделок, составляющие коммерческую тайну».

Каждая мера защиты должна иметь основание – ссылку на пункт нормативного документа либо на конкретную угрозу из модели угроз. Меры без основания подлежат исключению как избыточные.

При обосновании критериев эффективности полезно проверить каждый критерий вопросом: «каким образом и с какой периодичностью будет измеряться это значение?». Если ответа нет, критерий требует переформулирования.

7. Содержание отчёта

Отчёт оформляется в текстовом редакторе на листах формата А4 и содержит:

- титульный лист;
- цель работы и индивидуальный вариант задания;
- состав объекта информатизации (таблица 2.2);
- перечень видов конфиденциальной информации с правовыми основаниями;
- перечень мер защиты информации по областям (таблица 2.3);
- распределение мер по подсистемам системы защиты информации от НСД;
- перечень критериев оценки эффективности (таблица 2.4);
- фрагмент раздела технического задания;
- выводы по работе;
- список использованных источников.

8. Контрольные вопросы

Базовый уровень:

1. Назначение и область применения документа СТР-К.
2. Объекты защиты на объекте информатизации.
3. Состав подсистем системы защиты информации от несанкционированного доступа.
4. Классификация мер защиты информации по областям.
5. Понятие конфиденциальной информации и правовые основания ограничения доступа.

Повышенный уровень:

6. Предложите критерии оценки эффективности системы защиты информации объекта информатизации и обоснуйте способ измерения каждого из них.
7. Как результаты анализа угроз влияют на состав мер защиты информации?
8. Чем отличается набор мер защиты для средств, обрабатывающих конфиденциальную информацию, от набора мер для вспомогательных технических средств и систем?
9. Каким образом требования СТР-К соотносятся с требованиями к защите информационных систем персональных данных?

Практическая работа № 3. Классификация технических каналов утечки информации. Разработка модели угроз и модели нарушителя

Тема 3. Классификация технических каналов утечки информации. Модель угроз и модель нарушителя

Формируемые индикаторы: ИД-2 ОПК-1, ИД-3 ОПК-1. Продолжительность занятия – 6 часов.

В результате выполнения работы обучающийся должен:

- знать классификацию технических каналов утечки информации и показатели, характеризующие канал;
- уметь разрабатывать модель угроз и модель нарушителя для автоматизированной информационной системы;
- владеть навыками использования банка данных угроз безопасности информации ФСТЭК России.

1. Цель занятия

1. Изучить классификацию технических каналов утечки информации и показатели, позволяющие оценить риск утечки.
2. Освоить порядок построения модели нарушителя и определения его возможностей.
3. Отработать навыки формирования перечня актуальных угроз безопасности информации.

2. Подготовка к занятию

1. Изучить теоретический материал лекций по теме 3.
2. Ознакомиться со структурой банка данных угроз безопасности информации ФСТЭК России.
3. Изучить методический документ ФСТЭК России по оценке угроз безопасности информации.
4. Подготовить ответы на контрольные вопросы базового уровня.
5. Получить у преподавателя индивидуальный вариант автоматизированной системы.

3. Теоретическая часть

3.1. Понятие и показатели технического канала утечки информации

Каждый технический канал утечки информации (ТКУИ) характеризуется показателями, которые позволяют оценить риск утечки: пропускной способностью канала, длиной канала и относительной информативностью.

Пропускная способность канала зависит от ширины полосы пропускания и отношения мощности сигнала к мощности помехи. Различают узкополосные и широкополосные каналы, а также каналы с низкой и высокой энергетикой передаваемого сигнала. Наибольшую пропускную способность имеет оптический канал, наименьшую – акустический. Для примера: полоса телефонного канала составляет около 3,1 кГц, телевизионного – до 8 МГц. Если канал составной (например, акустико-оптический или акустико-радиоэлектронный), его пропускная способность определяется по наименьшему значению среди составляющих.

Длина ТКУИ оценивается расстоянием от источника сигнала до приёмника при условии обеспечения качественного приёма. Она зависит от показателей составных элементов канала, мощности сигнала в среде распространения, технических характеристик приёмной аппаратуры и уровня помех в канале. Чем больше длина ТКУИ, тем более

вероятно успешное действие злоумышленника по перехвату информации, так как возможна организация нескольких несанкционированных точек подключения или перехвата.

Рассмотренные показатели не учитывают ценность передаваемой информации. Вследствие действия помех в несанкционированно организованном канале ценность полученной информации может оказаться существенно ниже исходной. Однако при накоплении информации её ценность может быть восстановлена, при этом играет роль фактор старения информации во времени.

3.2. Классификация технических каналов утечки информации

Таблица 3.1 – Классификация технических каналов утечки информации

Признак классификации	Виды каналов	Характеристика
По физической природе	Акустические, виброакустические, оптические, радиоэлектронные, вещественные	Определяется видом носителя информации и средой распространения сигнала
По времени функционирования	Постоянные, эпизодические, случайные	Наиболее трудно выявляемыми являются случайные каналы
По степени защищённости	Открытые, технически закрытые, шифрованные	Наиболее трудно организуемыми для злоумышленника являются шифрованные каналы
По структуре	Простые, составные (комплексированные)	Пропускная способность составного канала определяется наименьшим значением

Для наиболее полного восстановления информации злоумышленником используется комплексирование каналов: одна и та же информация поступает через разные ТКУИ. Поскольку вероятность одинакового воздействия помех на разные каналы мала, достоверность суммарной информации возрастает. Пример: речь людей в помещении может быть подслушана через дверь, снята с помощью направленного микрофона или извлечена из побочных электромагнитных излучений.

Анализ ТКУИ позволяет сделать следующие выводы: утечка информации возможна по всем техническим каналам; наиболее уязвимым по видовым демаскирующим признакам является оптический канал; основным каналом получения сигнальных демаскирующих признаков является радиоэлектронный; чем больше пропускная способность и длина канала, тем он опаснее для владельца информации.

3.3. Несанкционированный доступ к информации

Согласно ГОСТ Р 50922 несанкционированный доступ (НСД) к информации – доступ к информации, нарушающий правила разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники или автоматизированными системами. Под штатными средствами понимается совокупность программного, микропрограммного и технического обеспечения.

К основным угрозам НСД относятся:

- угрозы проникновения в операционную среду компьютера с использованием штатного программного обеспечения (средств операционной системы или прикладных программ общего применения);
- угрозы создания нештатных режимов работы программных и программно-аппаратных средств за счёт преднамеренных изменений служебных данных, игнорирования предусмотренных ограничений, искажения данных;
- угрозы внедрения вредоносных программ (программно-математического воздействия).

Возможны комбинированные угрозы: например, за счёт внедрения вредоносных программ могут создаваться условия для НСД в операционную среду компьютера.

3.4. Модель нарушителя

Источником угрозы НСД может быть нарушитель, носитель с вредоносной программой или аппаратная закладка. Модель нарушителя – формализованное или неформализованное описание нарушителя. При её разработке определяются: категория лиц, к которой относится нарушитель; мотивы; цели; квалификация и техническая оснащённость; возможные действия; время действия.

Таблица 3.2 – Классификация нарушителей

Признак	Категории
По отношению к АС	Внешние (разведывательные службы государств, криминальные структуры, конкуренты, недобросовестные партнёры, внешние физические лица); внутренние (пользователи АС, персонал АС, сотрудники службы безопасности, руководители различных уровней)
По уровню знаний	Знает функциональные особенности АС и умеет пользоваться штатными средствами; обладает опытом работы с техническими средствами и их обслуживания; обладает высоким уровнем знаний в области программирования и проектирования АС; знает структуру, функции и механизм действия средств защиты
По уровню возможностей	Применяющий только агентурные методы; применяющий пассивные средства перехвата; использующий штатные средства и недостатки систем защиты; применяющий методы и средства активного воздействия
По времени действия	В процессе функционирования АС; в период неактивности компонентов системы; в обоих случаях
По месту действия	Без доступа на контролируемую территорию; с контролируемой территории без доступа в здания; внутри помещений без доступа к техническим средствам; с рабочих мест пользователей; с доступом в зону данных; с доступом в зону управления средствами обеспечения безопасности

Модель нарушителя может иметь разную степень детализации. Содержательная модель отражает систему принятых руководством взглядов на контингент потенциальных нарушителей, причины и мотивацию их действий. Сценарии воздействия определяют типы совершаемых акций с конкретизацией алгоритмов и этапов. Математическая модель представляет собой формализованное описание сценариев в виде логико-алгоритмической последовательности действий и используется для количественных оценок уязвимости объекта.

3.5. Порядок формирования модели угроз

Формирование модели угроз выполняется в следующей последовательности:

1. определение области действия модели: границы информационной системы, состав обрабатываемой информации, режимы обработки;
2. определение негативных последствий, которые могут наступить при реализации угроз;
3. построение модели нарушителя с определением категорий и уровня возможностей;
4. формирование перечня потенциальных угроз с использованием банка данных угроз ФСТЭК России;
5. определение актуальности каждой угрозы исходя из возможностей нарушителя, наличия уязвимостей и возможных последствий;
6. документирование результатов в виде документа «Модель угроз безопасности информации».

4. Порядок выполнения работы

1. Ознакомиться с индивидуальным вариантом задания: описанием автоматизированной информационной системы и условий её эксплуатации.

2. Составить классификационную таблицу технических каналов утечки информации для заданного объекта с указанием типа канала, среды распространения, источника сигнала и возможных средств перехвата (форма таблицы 3.3).

3. Оценить пропускную способность и длину двух-трёх наиболее опасных каналов; обосновать вывод об их относительной опасности.

4. Разработать модель нарушителя: определить категории внешних и внутренних нарушителей, их мотивы, уровень знаний, уровень возможностей, время и место действия (форма таблицы 3.4).

5. Сформировать перечень потенциальных угроз с использованием банка данных угроз безопасности информации ФСТЭК России, указав идентификатор каждой угрозы.

6. Определить актуальность каждой угрозы и обосновать вывод (форма таблицы 3.5).

7. Оформить результаты в виде фрагмента документа «Модель угроз безопасности информации».

8. Оформить отчёт и защитить работу.

5. Формы для оформления результатов

Таблица 3.3 – Форма классификации ТКУИ для объекта

Тип канала	Источник сигнала	Среда распространения	Возможные средства перехвата

Таблица 3.4 – Форма модели нарушителя

Категория нарушителя	Мотивы	Уровень возможностей	Предполагаемые действия

Таблица 3.5 – Форма перечня актуальных угроз

Идентификатор угрозы	Наименование угрозы	Нарушитель	Вывод об актуальности (обоснование)

6. Методические рекомендации по выполнению

При заполнении классификационной таблицы ТКУИ следует идти от источника информации, а не от средств перехвата: сначала определяется, в каком виде существует информация (речь, изображение, электрический сигнал, документ), затем – какие каналы для неё физически возможны.

Типичная ошибка при построении модели нарушителя – сведение её к перечислению должностей. Модель должна отвечать на вопрос, какими возможностями располагает нарушитель каждой категории, а не только кто он.

Угроза признаётся актуальной, если существует нарушитель, обладающий необходимыми возможностями, имеется способ реализации угрозы и её реализация приводит к неприемлемым негативным последствиям. Отсутствие любого из трёх условий делает угрозу неактуальной, что должно быть обосновано в отчёте.

7. Содержание отчёта

Отчёт оформляется в текстовом редакторе на листах формата А4 и содержит:

- титульный лист;
- цель работы и индивидуальный вариант задания;
- краткое описание объекта и обрабатываемой информации;
- классификация ТКУИ для объекта (таблица 3.3);

- оценка показателей наиболее опасных каналов с расчётами;
- модель нарушителя (таблица 3.4);
- перечень актуальных угроз с обоснованием (таблица 3.5);
- фрагмент документа «Модель угроз безопасности информации»;
- выводы по работе;
- список использованных источников.

8. Контрольные вопросы

Базовый уровень:

1. Типы технических каналов утечки информации.
 2. Показатели, характеризующие технический канал утечки информации.
 3. Комплексирование технических каналов утечки информации: назначение и последствия.
 4. Основные угрозы несанкционированного доступа к информации.
 5. Категории нарушителей по отношению к автоматизированной системе.
 6. Состав сведений, определяемых при разработке модели нарушителя.
- Повышенный уровень:
7. Опишите порядок полного анализа технических каналов утечки информации на объекте.
 8. Обоснуйте состав исходных данных, необходимых для разработки модели угроз безопасности информации.
 9. Каким образом уровень возможностей нарушителя влияет на вывод об актуальности угрозы?
 10. В каких случаях применяется математическая модель воздействия нарушителей и какие задачи она позволяет решить?

Практическая работа № 4. Четырёхфазная модель процесса управления информационной безопасностью. Оценка профилей защиты и заданий по безопасности

Тема 4. Стандарты и спецификации информационной безопасности: BS 7799, FIPS 140-2, «Общие критерии»

Формируемые индикаторы: ИД-3 ОПК-1, ИД-1 ОПК-2. Продолжительность занятия – 6 часов.

В результате выполнения работы обучающийся должен:

- знать содержание фаз процесса управления информационной безопасностью и структуру профиля защиты;
- уметь анализировать профиль защиты и задание по безопасности, выделяя функциональные требования и требования доверия;
- владеть навыками планирования мероприятий по управлению информационной безопасностью организации.

1. Цель занятия

1. Изучить четырёхфазную модель процесса управления информационной безопасностью, положенную в основу стандарта BS 7799 (ISO/IEC 27001).
2. Освоить содержание фаз планирования, реализации, оценки и корректировки применительно к системе управления информационной безопасностью организации.
3. Отработать навыки анализа профиля защиты и формирования фрагмента задания по безопасности по «Общим критериям».

2. Подготовка к занятию

1. Изучить теоретический материал лекций по теме 4.
2. Ознакомиться со структурой стандарта ISO/IEC 27001 и перечнем регуляторов безопасности.
3. Ознакомиться с примерами профилей защиты, размещёнными на официальном сайте ФСТЭК России.
4. Подготовить ответы на контрольные вопросы базового уровня.
5. Получить у преподавателя индивидуальный вариант организации и профиль защиты для анализа.

3. Теоретическая часть

3.1. Стандарт BS 7799 и система управления информационной безопасностью

Британский стандарт BS 7799 состоит из двух частей. Первая часть представляет собой свод практических правил и содержит перечень регуляторов безопасности, сгруппированных по областям управления. Вторая часть содержит требования к системе управления информационной безопасностью (СУИБ) и служит основой для сертификации. В дальнейшем стандарт получил развитие в семействе ISO/IEC 27000.

Ключевая идея стандарта состоит в том, что информационная безопасность рассматривается не как разовый проект, а как непрерывный управляемый процесс. Собранные вместе и систематизированные положения стандарта, каждое из которых по отдельности может показаться самоочевидным, обладают несомненной практической ценностью именно как система.

Область действия СУИБ определяется заранее. Ею может быть организация целиком либо лишь её часть; большую область целесообразно поделить на подобласти управления. От правильного определения границ зависит корректность последующего анализа рисков.

3.2. Четырёхфазная модель процесса управления

Процесс управления информационной безопасностью описывается четырёхфазной моделью: планирование – реализация – оценка – корректировка. Модель носит циклический характер: завершение фазы корректировки означает переход к новому циклу планирования, что обеспечивает непрерывное совершенствование СУИБ.

Таблица 4.1 – Содержание фаз процесса управления информационной безопасностью

Фаза	Основное содержание	Результат фазы
Планирование	Определение области действия СУИБ, инвентаризация активов, анализ рисков, выбор регуляторов безопасности	План с графиком, приоритетами, детальным рабочим планом и распределением обязанностей
Реализация	Выделение финансовых, материальных, людских и временных ресурсов, внедрение выбранных регуляторов, обучение персонала	Риски введены в рамки, определённые планом
Оценка	Анализ эффективности функционирования СУИБ, внутренний и внешний аудит, выявление проблем и несоответствий	Перечень выявленных проблем и несоответствий
Корректировка	Установление первопричин несоответствий, реактивные и превентивные действия, рассчитанные на средне- и долгосрочную перспективу	Устранение первопричин, исключающее повторное появление проблем

Ключевым элементом фазы планирования является анализ рисков. Его результат – выбор регуляторов безопасности. Обязанность руководства организации на фазе реализации – не только выделить ресурсы, но и объяснить сотрудникам важность проблем информационной безопасности, организовать курсы обучения и повышения квалификации.

Назначение фазы оценки – проанализировать, насколько эффективно функционирует СУИБ. К типовым проблемам, выявляемым на этой фазе, относится неспособность СУИБ обеспечить проведение в жизнь политики безопасности либо обслуживать производственные цели организации. Задача фазы оценки – выявить проблемы; задача фазы корректировки – докопаться до их корней и устранить первопричины несоответствий, чтобы избежать повторного появления.

3.3. Формы оценки и процесс аудита

Применяются следующие формы оценки СУИБ: самооценка подразделений, внутренний аудит, внешний независимый аудит, а также анализ со стороны руководства. Процесс аудита включает планирование (определение области, критериев и программы), подготовку (изучение документации, формирование чек-листов), проведение (сбор свидетельств путём наблюдения, опроса и анализа записей), формирование заключения (регистрация несоответствий с классификацией по значимости) и последующий контроль устранения.

Процесс корректировки строится по принципу анализа первопричин. Для каждого несоответствия определяется непосредственная причина, затем – системная причина, порождающая класс подобных несоответствий. Реактивные действия устраняют последствия, превентивные – исключают повторение.

3.4. «Общие критерии»: профиль защиты и задание по безопасности

Профиль защиты – независимая от реализации совокупность требований безопасности для определённого класса объектов оценки. Задание по безопасности – совокупность требований, относящихся к конкретному объекту оценки, служащая основой для его оценки.

Функциональные требования группируются по классам: аудит безопасности, криптографическая поддержка, защита данных пользователя, идентификация и

аутентификация, управление безопасностью, приватность, защита функций безопасности объекта оценки, использование ресурсов, доступ к объекту оценки, доверенный маршрут и канал.

Таблица 4.2 – Структура профиля защиты

Раздел	Содержание
Введение	Идентификация профиля защиты, аннотация, обзор объекта оценки
Описание объекта оценки	Тип объекта, границы, предполагаемое применение, среда функционирования
Среда безопасности	Предположения, угрозы, политики безопасности организации
Цели безопасности	Цели для объекта оценки и для среды его функционирования
Требования безопасности	Функциональные требования безопасности и требования доверия к безопасности
Обоснование	Демонстрация достаточности и взаимной согласованности целей и требований

В число классов требований доверия безопасности входят разработка, руководства, поддержка жизненного цикла, тестирование, оценка уязвимостей, а также сертификация. Оценочные уровни доверия (ОУД 1–7) представляют собой предопределённые пакеты требований доверия и характеризуют глубину и строгость проведённой оценки.

При анализе профиля защиты необходимо проверить его внутреннюю согласованность: каждой угрозе из раздела среды безопасности должна соответствовать хотя бы одна цель безопасности, а каждой цели – хотя бы одно требование безопасности.

4. Порядок выполнения работы

1. Ознакомиться с индивидуальным вариантом задания: описанием организации и профилем защиты для анализа.
2. Определить область действия СУИБ для заданной организации, обосновав выбор границ.
3. Провести инвентаризацию информационных активов организации с указанием ценности каждого актива (форма таблицы 4.3).
4. Выполнить упрощённый анализ рисков: для каждого актива определить угрозы, вероятность реализации и возможный ущерб; вычислить оценку риска.
5. Выбрать регуляторы безопасности для рисков, признанных неприемлемыми, и составить план фазы реализации с распределением обязанностей и сроков (форма таблицы 4.4).
6. Предложить показатели, по которым на фазе оценки будет проверяться результативность СУИБ, и описать порядок проведения внутреннего аудита.
7. Проанализировать предложенный профиль защиты: выделить угрозы, цели безопасности, функциональные требования и требования доверия; проверить согласованность разделов (форма таблицы 4.5).
8. Сформировать фрагмент задания по безопасности для заданного средства защиты информации.
9. Оформить отчёт и защитить работу.

5. Формы для оформления результатов

Таблица 4.3 – Форма инвентаризации информационных активов

Актив	Владелец	Вид ценности	Оценка ценности

Таблица 4.4 – Форма плана фазы реализации

Регулятор безопасности	Ответственный	Срок	Требуемые ресурсы

Таблица 4.5 – Форма анализа профиля защиты

Угроза	Цель безопасности	Требование безопасности	Класс требования

6. Методические рекомендации по выполнению

При определении области действия СУИБ следует избегать формулировки «организация в целом» для крупных структур: чем шире область, тем труднее выполнить анализ рисков с приемлемой детализацией. Обоснованием выбора границ служит однородность обрабатываемой информации и подчинённость подразделений.

Оценка риска в учебной работе выполняется по упрощённой качественной шкале: вероятность и ущерб оцениваются по трёхбалльной шкале, риск определяется как их произведение. Важно не само численное значение, а обоснование выставленных оценок.

При анализе профиля защиты типичной ошибкой является смешение функциональных требований и требований доверия. Признак различения: функциональные требования описывают поведение объекта оценки, требования доверия – свидетельства, которые предоставляет разработчик.

7. Содержание отчёта

Отчёт оформляется в текстовом редакторе на листах формата А4 и содержит:

- титульный лист;
- цель работы и индивидуальный вариант задания;
- обоснование области действия СУИБ;
- инвентаризация активов (таблица 4.3) и результаты анализа рисков;
- план фазы реализации (таблица 4.4);
- показатели результативности СУИБ и порядок проведения внутреннего аудита;
- результаты анализа профиля защиты (таблица 4.5) с выводом о его согласованности;
- фрагмент задания по безопасности;
- выводы по работе;
- список использованных источников.

8. Контрольные вопросы

Базовый уровень:

1. Фазы модели управления информационной безопасностью и их содержание.
2. Порядок определения области действия системы управления информационной безопасностью.

3. Формы оценки системы управления информационной безопасностью.

4. Структура профиля защиты по «Общим критериям».

5. Классы требований доверия безопасности «Общих критериев».

Повышенный уровень:

6. Опишите процесс аудита системы управления информационной безопасностью.

7. Опишите процесс корректировки и приведите примеры реактивных и превентивных действий.

8. В чём различие между профилем защиты и заданием по безопасности?

9. Каким образом обеспечивается непрерывное совершенствование СУИБ и в чём преимущества циклической модели управления?

Практическая работа № 5. Эксплуатационное окружение и управление криптографическими ключами. Обеспечение аутентичности

Тема 5. Эксплуатационное окружение и управление криптографическими ключами. Технические спецификации информационной безопасности

Формируемые индикаторы: ИД-1 ОПК-2, ИД-2 ОПК-2. Продолжительность занятия – 6 часов.

В результате выполнения работы обучающийся должен:

- знать структуру требований стандарта FIPS 140-2 и этапы жизненного цикла криптографического ключа;
- уметь обосновывать выбор механизма аутентификации и уровня безопасности криптографического модуля;
- владеть навыками анализа технических спецификаций информационной безопасности.

1. Цель занятия

1. Изучить требования федерального стандарта FIPS 140-2 к криптографическому модулю, его эксплуатационному окружению и управлению криптографическими ключами.
2. Освоить содержание технических спецификаций информационной безопасности Internet-сообщества.
3. Отработать навыки анализа механизмов обеспечения аутентичности и защищённой передачи данных.

2. Подготовка к занятию

1. Изучить теоретический материал лекций по теме 5.
2. Ознакомиться со структурой стандарта FIPS 140-2 и перечнем групп требований.
3. Ознакомиться с назначением протоколов семейства IPsec и интерфейса GSS-API.
4. Подготовить ответы на контрольные вопросы базового уровня.
5. Получить у преподавателя индивидуальный вариант условий эксплуатации криптографического модуля.

3. Теоретическая часть

3.1. Криптографический модуль и структура требований FIPS 140-2

В федеральном стандарте США FIPS 140-2 «Требования безопасности для криптографических модулей» под криптографическим модулем понимается набор аппаратных и (или) программных, в том числе встроенных, компонентов, реализующих утверждённые функции безопасности – включая криптографические алгоритмы, генерацию и распределение криптографических ключей, аутентификацию – и заключённых в пределах явно определённого непрерывного периметра.

Требования стандарта разделены на одиннадцать групп:

1. спецификация криптографического модуля;
2. порты и интерфейсы модуля;
3. роли, сервисы и аутентификация;
4. конечно-автоматная модель;
5. физическая безопасность;
6. эксплуатационное окружение;
7. управление криптографическими ключами;
8. электромагнитная совместимость;
9. самотестирование;

10. доверие проектированию;

11. сдерживание прочих атак.

Спецификация модуля включает определение криптографического периметра, реализуемых функций и режимов, описание модуля, его аппаратных и программных компонентов, а также документированную политику безопасности. Среди портов и интерфейсов должны быть выделены обязательные и дополнительные; следует специфицировать все интерфейсы, а также все маршруты входных и выходных данных. Порты для незащищённых параметров, критичных для безопасности, требуют отдельного рассмотрения.

3.2. Уровни безопасности криптографического модуля

Таблица 5.1 – Уровни безопасности по FIPS 140-2

Уровень	Аутентификация и доступ	Дополнительные требования
Первый	Аутентификация может не требоваться	Базовые требования к спецификации, интерфейсам и самотестированию
Второй	Ролевая аутентификация	Замки на съёмных оболочках и дверцах, защитные покрытия и пломбы, сохраняющие свидетельства вторжений; использование ОС, сертифицированных на соответствие профилям защиты «Общих критериев» с ОУД не ниже второго; произвольное управление доступом с определением ролей; протоколирование действий крипто-офицера
Третий	Персональная аутентификация с проверкой допустимости принятия определённых ролей	Отделение портов и интерфейсов для нешифрованного ввода/вывода ключей и критичных данных; средства оперативного выявления и реагирования на попытки вторжений; использование доверенного маршрута
Четвёртый	Персональная аутентификация	Операционная система с повышенным оценочным уровнем доверия; защита от воздействий окружающей среды; максимальные требования к физической безопасности

3.3. Требования к эксплуатационному окружению

Эксплуатационное окружение – совокупность программных и аппаратных средств, в среде которых функционирует криптографический модуль. Требования к нему состоят в следующем:

- доступ процессов, внешних по отношению к модулю, к данным, критичным для безопасности, запрещается;
- некриптографические процессы не должны прерывать работу криптографического модуля;
- программное обеспечение модуля следует защитить от несанкционированного раскрытия и модификации;
- целостность программного обеспечения модуля контролируется утверждёнными средствами.

Для второго уровня безопасности требуется использование операционных систем, сертифицированных на соответствие определённым профилям защиты на основе «Общих критериев» с оценочным уровнем доверия не ниже второго. Для защиты критичных данных должно применяться произвольное управление доступом с определением соответствующих ролей, необходимо протоколирование действий крипто-офицера. Характерная черта третьего уровня безопасности – использование доверенного маршрута.

3.4. Управление криптографическими ключами

Управление криптографическими ключами охватывает полный жизненный цикл ключа. Нарушение защиты на любом этапе обесценивает стойкость применяемых алгоритмов.

Таблица 5.2 – Этапы жизненного цикла криптографического ключа

Этап	Содержание	Основные меры защиты
Генерация	Выработка ключа с требуемыми характеристиками	Применение аттестованного генератора случайных чисел, контроль качества ключевого материала
Распределение	Доставка ключа участникам взаимодействия	Использование защищённого канала, схем распределения с открытым ключом, разделения секрета
Хранение	Размещение ключа на носителе	Шифрование ключа на ключе более высокого уровня, аппаратные носители, контроль доступа
Использование	Применение ключа в криптографических операциях	Ограничение области применения, контроль числа операций, запрет вывода ключа за периметр модуля
Смена	Плановая или внеплановая замена ключа	Регламент периодичности смены, порядок действий при компрометации
Архивирование	Хранение выведенных из обращения ключей	Раздельное хранение, ограничение доступа, учёт
Уничтожение	Гарантированное удаление ключевого материала	Затирание областей памяти, документирование факта уничтожения

3.5. Технические спецификации Internet-сообщества

Технические спецификации информационной безопасности разрабатываются в рамках деятельности Internet-сообщества и публикуются в виде документов RFC. Наибольшее практическое значение имеют спецификации семейства IPsec и обобщённый прикладной программный интерфейс службы безопасности.

IPsec обеспечивает защиту на сетевом уровне и включает протокол аутентифицирующего заголовка (AH), протокол инкапсулирующей защиты содержимого (ESP) и протокол согласования параметров и управления ключами (IKE). Различают транспортный и туннельный режимы: первый защищает содержимое пакета, второй инкапсулирует пакет целиком, что и позволяет строить виртуальные частные сети сетевого уровня. Все обсуждаемые сетевые услуги выигрывают от организации надёжной защиты на сетевом уровне средствами IPsec.

Обобщённый прикладной программный интерфейс службы безопасности (GSS-API) предназначен для отделения приложений от конкретных механизмов безопасности. Приложение обращается к стандартизованному набору функций – формированию контекста безопасности, защите передаваемых сообщений, проверке их подлинности, – а конкретный механизм (например, Kerberos) выбирается на этапе развёртывания. Это обеспечивает переносимость приложений между различными средами.

3.6. Обеспечение аутентичности

Идентификация – присвоение субъекту идентификатора и сравнение предъявленного идентификатора с перечнем присвоенных. Аутентификация – проверка принадлежности субъекту предъявленного идентификатора, подтверждение его подлинности. Согласно рекомендациям X.800 аутентификация может быть реализована на сетевом уровне.

Парольная аутентификация остаётся наиболее распространённой, но обладает известными недостатками: пароль может быть перехвачен при передаче, подобран, разглашён. Требования к паролю включают достаточную длину, использование символов разных категорий, отсутствие явной связи с владельцем, ограничение срока действия.

Система одноразовых паролей S/KEY устраняет угрозу перехвата. Её работа основана на многократном применении односторонней функции к секретному значению: сервер хранит результат n -кратного применения функции, а пользователь предъявляет результат $(n-1)$ -кратного применения. Сервер применяет функцию к предъявленному значению и сравнивает результат с хранимым. Перехваченный пароль бесполезен, так как при следующей аутентификации требуется другое значение. Ограничением схемы является конечное число паролей в серии и необходимость её периодической переинициализации.

4. Порядок выполнения работы

1. Ознакомиться с индивидуальным вариантом задания: описанием условий эксплуатации криптографического модуля.
2. Составить перечень требований FIPS 140-2 к эксплуатационному окружению криптографического модуля с разбивкой по уровням безопасности (форма таблицы 5.3).
3. Обосновать выбор уровня безопасности криптографического модуля для заданных условий эксплуатации.
4. Описать жизненный цикл криптографического ключа для заданной системы и указать меры защиты на каждом этапе (форма таблицы 5.4).
5. Разработать регламент смены ключей, включающий периодичность плановой смены и порядок действий при компрометации.
6. Проанализировать схему аутентификации по системе одноразовых паролей S/KEY: описать порядок формирования и проверки пароля, указать сильные и слабые стороны.
7. Описать состав протоколов IPsec и порядок установления защищённого соединения при построении VPN сетевого уровня; изобразить схему прохождения пакета в туннельном режиме.
8. Сформулировать обоснованный выбор механизма аутентификации для заданных условий и оформить обоснование (форма таблицы 5.5).
9. Оформить отчёт и защитить работу.

5. Формы для оформления результатов

Таблица 5.3 – Форма перечня требований к эксплуатационному окружению

Уровень безопасности	Требование	Способ выполнения в заданных условиях

Таблица 5.4 – Форма описания жизненного цикла ключа

Этап	Выполняемые действия	Ответственный	Меры защиты

Таблица 5.5 – Форма обоснования выбора механизма аутентификации

Механизм	Достоинства	Недостатки	Вывод о применимости

6. Методические рекомендации по выполнению

Выбор уровня безопасности криптографического модуля обосновывается не «чем выше, тем лучше», а соотношением ценности защищаемой информации, возможностей нарушителя и стоимости реализации. В отчёте должны быть указаны признаки условий эксплуатации, определившие выбор.

При описании жизненного цикла ключа необходимо указывать ответственного за каждый этап. Отсутствие персональной ответственности за уничтожение ключевого материала является типичным несоответствием, выявляемым при аудите.

При сравнении механизмов аутентификации следует опираться на конкретные угрозы: перехват при передаче, подбор, повторное использование, компрометация базы аутентификационных данных. Общие рассуждения о «надёжности» без привязки к угрозам не принимаются.

7. Содержание отчёта

Отчёт оформляется в текстовом редакторе на листах формата А4 и содержит:

- титульный лист;
- цель работы и индивидуальный вариант задания;
- перечень требований к эксплуатационному окружению (таблица 5.3);
- обоснование выбора уровня безопасности криптографического модуля;
- описание жизненного цикла криптографического ключа (таблица 5.4) и регламент смены ключей;
- описание и схема работы системы S/KEY с анализом сильных и слабых сторон;
- описание состава IPsec и схема прохождения пакета в туннельном режиме;
- обоснование выбора механизма аутентификации (таблица 5.5);
- выводы по работе;
- список использованных источников.

8. Контрольные вопросы

Базовый уровень:

1. Понятие криптографического модуля и криптографического периметра.
2. Группы требований безопасности стандарта FIPS 140-2.
3. Требования к эксплуатационному окружению криптографического модуля.
4. Этапы жизненного цикла криптографического ключа.
5. Назначение и состав протоколов семейства IPsec.
6. Идентификация и аутентификация: определения и различия.

Повышенный уровень:

7. Обоснуйте выбор уровня безопасности криптографического модуля для информационной системы, обрабатывающей персональные данные.
8. Сравните парольную аутентификацию и систему S/KEY по устойчивости к перехвату аутентификационных данных.
9. В чём состоит назначение обобщённого прикладного программного интерфейса службы безопасности и какие задачи он решает?
10. Каким образом транспортный и туннельный режимы IPsec различаются по составу защищаемых данных и области применения?

Практическая работа № 6. Анализ защищённости операционных систем и СУБД. Размещение Web-серверов и выбор поставщика Internet-услуг

Тема 6. Анализ защищённости информационных систем. Политика безопасности предприятия. Оформление результатов исследований

Формируемые индикаторы: ИД-2 ОПК-2, ИД-1 ОПК-5, ИД-2 ОПК-5. Продолжительность занятия – 6 часов.

В результате выполнения работы обучающийся должен:

- знать методику анализа защищённости операционных систем и систем управления базами данных;
- уметь формировать требования к поставщику Internet-услуг и разрабатывать положения политики безопасности предприятия;
- владеть навыками оформления результатов проведённого исследования в виде научно-технического отчёта.

1. Цель занятия

1. Отработать навыки анализа защищённости операционных систем и систем управления базами данных.
2. Изучить требования к размещению Web-серверов и порядок формирования требований к поставщику Internet-услуг.
3. Освоить общие принципы выработки официальной политики предприятия в области информационной безопасности.
4. Отработать навыки применения методов научных исследований и оформления их результатов в виде научно-технического отчёта.

2. Подготовка к занятию

1. Изучить теоретический материал лекций по теме 6.
2. Ознакомиться с документом «Дополнение к Руководству по информационной безопасности предприятия: как выбирать поставщика Internet-услуг».
3. Ознакомиться с требованиями к структуре и оформлению научно-технических отчётов.
4. Подготовить ответы на контрольные вопросы базового уровня.
5. Получить у преподавателя индивидуальный вариант анализируемой системы и вариант размещения Web-сервера.

3. Теоретическая часть

3.1. Методика анализа защищённости операционной системы

Анализ защищённости операционной системы выполняется по следующим направлениям:

1. учётные записи: перечень локальных и доменных учётных записей, наличие неиспользуемых и встроенных записей, распределение привилегий;
2. политика паролей: минимальная длина, требования к сложности, срок действия, история паролей, порядок блокировки при неудачных попытках;
3. управление доступом: права на объекты файловой системы и реестра, применение принципа минимума привилегий;
4. протоколирование и аудит: состав регистрируемых событий, объём и срок хранения журналов, порядок их анализа;
5. установленное программное обеспечение: состав, актуальность версий, наличие неиспользуемых компонентов и служб;
6. обновления безопасности: своевременность установки, порядок контроля;

7. сетевые параметры: перечень открытых портов, настройки межсетевого экрана, параметры удалённого доступа.

По каждому направлению фиксируется фактическое состояние, сопоставляется с требуемым и определяется несоответствие с оценкой критичности.

3.2. Методика анализа защищённости системы управления базами данных

Для СУБД дополнительно к перечисленным направлениям проверяются: разграничение доступа к объектам базы данных (таблицам, представлениям, процедурам); наличие учётных записей с избыточными привилегиями; применение ролевой модели; шифрование данных при хранении и передаче; настройки аудита операций с данными; порядок и периодичность резервного копирования, а также проверка восстановимости резервных копий.

Отдельного внимания требует защита от внедрения кода через приложения, обращающиеся к базе данных: применение параметризованных запросов, ограничение прав учётной записи приложения, контроль обработки ошибок, не допускающий раскрытия структуры базы данных.

3.3. Требования к поставщику Internet-услуг

Поставщику Internet-услуг следует иметь ясные правила и процедуры, касающиеся передачи информации о нарушении безопасности своим потребителям, другим поставщикам, группам реагирования, правоохранительным органам, средствам массовой информации и общественности, а также средства для организации защищённого канала передачи такой информации.

Рекомендуется иметь специальные почтовые ящики: SECURITY – для сообщений о нарушениях безопасности, ABUSE – для сообщений о ненадлежащем поведении, NOC – для сообщений о проблемах в сетевой инфраструктуре. При нарушении, затрагивающем инфраструктуру поставщика, потребителям немедленно сообщается: кто координирует реакцию на нарушение, какая уязвимость использована атакующим, как нарушение сказалось на предоставляемых услугах, что делается для реагирования, могут ли быть скомпрометированы данные потребителей.

Поставщики ответственны за такое управление сетевой инфраструктурой, чтобы обеспечивалась разумная устойчивость к появлению известных слабостей в защите, а атакующие не могли легко организовать плацдарм для последующих атак. Основные направления:

- маршрутизаторы: ограничение доступа только уполномоченным администраторам, аутентификация соседей в рамках протокола BGP, защита маршрутной информации от изменения без надёжной аутентификации;
- фильтрация: во всех граничных маршрутизаторах, к которым подключены потребители, применяется входная и выходная фильтрация для защиты от подделки исходных адресов;
- управление сетью: применение SNMP преимущественно как средства получения информации; сведения, передаваемые в центр управления сетью, считаются конфиденциальными;
- физическая безопасность: особое внимание при совместном размещении оборудования нескольких организаций с разной политикой безопасности; запрет подключения компьютеров к транзитным сегментам и подсоединения к сети неиспользуемых физических интерфейсов;
- почтовые серверы: отдельные агенты приёма/отправки и обработки; ограничение удалённого запуска очередей; представление сообщений через порт MAIL SUBMIT (587) с аутентификацией расширением AUTH вместо порта 25; выявление исключительных ситуаций и генерация докладов;

– DNS-серверы: контроль доступности, синхронизация часов по протоколу NTP с аутентификацией, применение DNSSEC.

3.4. Размещение Web-серверов

Таблица 6.1 – Варианты размещения Web-серверов

Вариант	Содержание	Ключевые вопросы к поставщику
Colocation	Оборудование потребителя размещается на площадке поставщика	Физическая безопасность площадки, порядок доступа персонала, разграничение зон ответственности, электропитание и охлаждение
Dedicated Server	Потребителю предоставляется выделенный сервер поставщика	Порядок администрирования, разграничение прав, установка обновлений, резервное копирование, порядок реагирования на инциденты
Cloud Hosting	Ресурсы предоставляются в виде виртуальной инфраструктуры	Изоляция виртуальных машин, местонахождение центров обработки данных, порядок удаления данных, доступность и уровень обслуживания

При размещении Web-сервера следует руководствоваться такими положениями: контроль DocumentRoot с тщательной проверкой всего, что располагается ниже этого каталога, и желательным применением системного вызова chroot; контроль UserDir с запретом доступа к информации пользователей и выполнения командных процедур от их имени; разбиение на виртуальные серверы так, чтобы данные и программы одного домена были недоступны другому; лимитирование потребления астрономического и процессорного времени и дискового пространства; применение абсолютных маршрутных имён; управление доступом на основе надёжной аутентификации – сертификатов или одноразовых паролей.

При размещении приложений электронной коммерции транзакции нельзя хранить на сервере в открытом виде; допускается применение криптографии с открытыми ключами, так что расшифровать транзакции сможет только потребитель. Передача транзакций производится по доверенному каналу; следует аккуратно производить ротацию транзакционных файлов, чтобы каждая транзакция выполнялась ровно один раз. Загрузку информационного наполнения на сервер следует производить по защищённому каналу.

3.5. Политика безопасности предприятия

Политика поставщика Internet-услуг по отношению к защите персональных данных, обеспечению аутентичности, подотчётности, наложению защитных заплат, поддержке доступности, реагированию на доклады о нарушениях представляет интерес для потребителей и подлежит публикации в общедоступном месте, например на Web-сервере поставщика.

Официальная политика безопасности предприятия строится по аналогичным принципам. Политика верхнего уровня формулирует цели: решение сформировать или пересмотреть комплексную программу безопасности, обеспечение базы для соблюдения законов и правил, распределение ответственности. Политики среднего и нижнего уровней конкретизируют правила по отдельным направлениям и системам.

Каждое положение политики должно быть проверяемым и обеспеченным механизмом контроля исполнения. Положения, исполнение которых невозможно проконтролировать, снижают доверие ко всему документу.

3.6. Оформление результатов исследования

Результаты проведённого анализа оформляются в виде научно-технического отчёта. Структура отчёта: титульный лист; содержание; перечень сокращений и обозначений; введение с обоснованием актуальности и постановкой задачи; основная часть, включающая

описание методики, исходных данных и полученных результатов; заключение с выводами; список использованных источников; приложения.

При изложении результатов следует разделять фактические данные, полученные в ходе анализа, и собственные выводы. Каждый вывод должен опираться на конкретный результат, приведённый в основной части. Список источников оформляется по ГОСТ Р 7.0.100-2018.

Обзор источников по теме исследования строится не как последовательный пересказ работ, а как сопоставление подходов с выделением их достоинств, ограничений и нерешённых вопросов, что и позволяет обосновать постановку собственной задачи.

4. Порядок выполнения работы

1. Ознакомиться с индивидуальным вариантом задания: описанием анализируемой системы и вариантом размещения Web-сервера.

2. Провести анализ защищённости заданной операционной системы по направлениям, перечисленным в теоретической части; зафиксировать фактическое состояние и выявленные несоответствия (форма таблицы 6.2).

3. Провести анализ защищённости заданной СУБД: проверить учётные записи, привилегии, применение ролевой модели, настройки протоколирования и порядок резервного копирования.

4. Проранжировать выявленные несоответствия по критичности и предложить меры по их устранению.

5. Составить перечень вопросов к поставщику Internet-услуг для назначенного варианта размещения Web-сервера (форма таблицы 6.3).

6. Разработать фрагмент официальной политики безопасности предприятия по одному из направлений: защита персональных данных, реагирование на инциденты, управление обновлениями, управление доступом.

7. Оформить результаты работы в виде научно-технического отчёта в соответствии с требованиями, приведёнными в п. 3.6.

8. Подготовить краткое сообщение по результатам исследования (5–7 минут) и представить его на защите работы.

5. Формы для оформления результатов

Таблица 6.2 – Форма результатов анализа защищённости

Направление проверки	Фактическое состояние	Требуемое состояние	Несоответствие и его критичность

Таблица 6.3 – Форма перечня вопросов к поставщику Internet-услуг

Направление	Вопрос	Обоснование значимости

6. Методические рекомендации по выполнению

Анализ защищённости должен опираться на проверяемые факты. Формулировка «политика паролей настроена неудовлетворительно» заменяется на «минимальная длина пароля установлена равной 6 символам при требуемых 12; история паролей не ведётся».

Критичность несоответствия определяется не сложностью его устранения, а возможными последствиями его использования нарушителем. Несоответствие, позволяющее получить привилегии администратора, критично независимо от того, что устраняется оно изменением одного параметра.

При подготовке научно-технического отчёта следует отделять описание методики от результатов. Читатель отчёта должен иметь возможность воспроизвести анализ по

приведённому описанию и получить сопоставимые результаты – это основной признак корректно оформленного исследования.

7. Содержание отчёта

Отчёт оформляется в текстовом редакторе на листах формата А4 и содержит:

- титульный лист;
- содержание;
- введение с постановкой задачи исследования;
- описание методики анализа защищённости;
- результаты анализа операционной системы и СУБД (таблица 6.2);
- ранжированный перечень несоответствий и предложения по их устранению;
- перечень вопросов к поставщику Internet-услуг (таблица 6.3);
- фрагмент политики безопасности предприятия;
- заключение с выводами по результатам исследования;
- список использованных источников, оформленный по ГОСТ Р 7.0.100-2018.

8. Контрольные вопросы

Базовый уровень:

1. Направления анализа защищённости операционной системы.
2. Особенности анализа защищённости системы управления базами данных.
3. Варианты размещения Web-серверов и их характеристика.
4. Специальные почтовые ящики поставщика Internet-услуг и их назначение.
5. Состав официальной политики безопасности предприятия.
6. Структура научно-технического отчёта о результатах исследования.

Повышенный уровень:

7. Обоснуйте выбор варианта размещения Web-сервера для организации, обрабатывающей персональные данные.
8. Сформулируйте требования к структуре и содержанию научно-технического отчёта о результатах анализа защищённости.
9. Каким образом обеспечивается проверяемость положений политики безопасности предприятия?
10. Чем обзор источников по теме исследования отличается от последовательного изложения содержания прочитанных работ?

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ОБРАЗОВАНИЯ
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

МЕТОДИЧЕСКИЕ УКАЗАНИЯ
по организации самостоятельной работы обучающихся
по дисциплине
«Технологии обеспечения информационной безопасности»
Направление подготовки 10.04.01 Информационная безопасность
направленность (профиль) «Математическое и программное обеспечение защиты
информации»

Ставрополь, 2026 г.

1. Цель и задачи самостоятельной работы

Цель самостоятельной работы – закрепление и углубление знаний, полученных на лекционных и практических занятиях, формирование навыков самостоятельного освоения нормативных документов, стандартов и специальной литературы в области обеспечения информационной безопасности, а также развитие умений применять методы научных исследований и оформлять их результаты.

Задачи самостоятельной работы:

1. Проработка лекционного материала и рекомендованных источников по каждой теме дисциплины.
2. Подготовка к практическим занятиям, входному контролю и защите отчётов.
3. Самостоятельное изучение нормативных документов ФСТЭК России, национальных и международных стандартов информационной безопасности.
4. Выполнение индивидуальных заданий по построению модели угроз, анализу профиля защиты и анализу защищённости информационных систем.
5. Подготовка докладов, научно-технических обзоров и презентаций по результатам самостоятельного изучения материала.
6. Подготовка к промежуточной аттестации.

2. Распределение часов самостоятельной работы по темам дисциплины

Таблица 2 – Распределение часов самостоятельной работы

№	Тема дисциплины	Основное содержание самостоятельной работы	Часов	Форма контроля
1	Введение в технологии обеспечения информационной безопасности. Архитектурные стандарты информационной безопасности	Проработка лекционного материала; ведение глоссария дисциплины; изучение рекомендаций Х.800 и «Оранжевой книги»; подготовка к практической работе № 1.	6	Собеседование
2	Требования и рекомендации по защите информации, обрабатываемой средствами вычислительной техники	Изучение документа СТР-К и приказов ФСТЭК России; составление сравнительной таблицы мер защиты по областям; подготовка к практической работе № 2.	6	Собеседование
3	Классификация технических каналов утечки информации. Модель угроз и модель нарушителя	Работа с банком данных угроз ФСТЭК России; построение фрагмента модели угроз по индивидуальному варианту; подготовка доклада и презентации.	6	Доклад
4	Стандарты и спецификации информационной безопасности: BS 7799, FIPS 140-2, «Общие критерии»	Изучение ISO/IEC 27001 и «Общих критериев»; разбор профиля защиты; подготовка тезисов к круглому столу.	6	Круглый стол
5	Эксплуатационное окружение и управление криптографическими ключами. Технические спецификации информационной безопасности	Изучение структуры FIPS 140-2; проработка спецификаций IPsec и GSS-API; составление схемы жизненного цикла криптографического ключа.	6	Собеседование
6	Анализ защищённости информационных систем. Политика безопасности предприятия. Оформление результатов исследований	Изучение методик анализа защищённости ОС и СУБД; подготовка научно-технического обзора; подготовка доклада и презентации.	6	Доклад

Итого самостоятельной работы – 36 часов.

3. Задания для самостоятельной работы по темам дисциплины

Тема 1. Введение в технологии обеспечения информационной безопасности. Архитектурные стандарты информационной безопасности

Объём самостоятельной работы – 6 часов. Форма контроля – собеседование.

Задания для самостоятельной работы

1. Проработать конспект лекций по теме, выделив определения основных понятий: информация, информационные технологии, информационная система, информационно-телекоммуникационная сеть, обладатель информации, доступ к информации, конфиденциальная информация.
2. Начать ведение глоссария дисциплины; внести в него не менее 20 терминов с указанием нормативного документа, в котором приведено определение.
3. Изучить структуру рекомендаций X.800: составить схему соответствия сервисов безопасности уровням эталонной модели взаимодействия открытых систем.
4. Изучить структуру «Оранжевой книги»: составить сравнительную таблицу уровней безопасности С и В с указанием отличительных признаков.
5. Подготовиться к практической работе № 1: изучить перечень нормативных правовых актов, применимых к автоматизированным системам различного назначения.

Вопросы для самопроверки

1. Каким образом соотносятся понятия «информационная система» и «информационно-телекоммуникационная сеть»?
2. Какие сервисы безопасности по X.800 обеспечивают защиту целостности, а какие – конфиденциальности?
3. В чём состоит различие между произвольным и принудительным управлением доступом?
4. Почему архитектурные стандарты не содержат описания конкретных технических решений?

Тема 2. Требования и рекомендации по защите информации, обрабатываемой средствами вычислительной техники

Объём самостоятельной работы – 6 часов. Форма контроля – собеседование.

Задания для самостоятельной работы

1. Изучить документ СТР-К: составить конспект с выделением области применения, объектов защиты и порядка организации работ.
2. Составить сравнительную таблицу мер защиты информации по областям (правовые, организационные, физические, аппаратные, программные, криптографические) с примерами по каждой области.
3. Изучить состав подсистем системы защиты информации от несанкционированного доступа; для каждой подсистемы привести не менее трёх реализующих механизмов.
4. Изучить приказы ФСТЭК России, устанавливающие состав мер защиты информации; выписать меры, относящиеся к подсистеме управления доступом.
5. Подготовиться к практической работе № 2: подобрать описание объекта информатизации по индивидуальному варианту.

Вопросы для самопроверки

1. На какие организации распространяются требования документа СТР-К, а для каких он носит рекомендательный характер?

2. Почему вспомогательные технические средства и системы отнесены к объектам защиты?
3. Какие меры защиты относятся к подсистеме обеспечения целостности?
4. Что должно служить основанием для включения меры защиты в перечень?

Тема 3. Классификация технических каналов утечки информации. Модель угроз и модель нарушителя

Объём самостоятельной работы – 6 часов. Форма контроля – доклад.

Задания для самостоятельной работы

1. Изучить классификацию технических каналов утечки информации; составить схему, отражающую признаки классификации и виды каналов.
2. Освоить работу с банком данных угроз безопасности информации ФСТЭК России: выполнить поиск угроз по заданному типу объекта воздействия, изучить структуру описания угрозы.
3. Выполнить индивидуальное задание: построить фрагмент модели угроз для информационной системы по варианту, включив не менее десяти угроз с обоснованием актуальности.
4. Изучить методический документ ФСТЭК России по оценке угроз безопасности информации; выписать порядок определения актуальности угрозы.
5. Подготовить доклад по одной из тем, приведённых в п. 4.3 настоящих указаний, и презентацию к нему.

Вопросы для самопроверки

1. От каких параметров зависит пропускная способность технического канала утечки информации?
2. Каким образом определяется пропускная способность составного канала?
3. В чём состоит смысл комплексирования технических каналов утечки информации для злоумышленника?
4. При каких условиях угроза признаётся актуальной?
5. Чем содержательная модель нарушителя отличается от математической?

Тема 4. Стандарты и спецификации информационной безопасности: BS 7799, FIPS 140-2, «Общие критерии»

Объём самостоятельной работы – 6 часов. Форма контроля – круглый стол.

Задания для самостоятельной работы

1. Изучить структуру стандарта ISO/IEC 27001 и перечень регуляторов безопасности; выписать регуляторы, относящиеся к управлению доступом и к управлению инцидентами.
2. Составить схему четырёхфазной модели процесса управления информационной безопасностью с указанием входов, выходов и участников каждой фазы.
3. Выполнить индивидуальное задание: самостоятельно разобрать профиль защиты, назначенный преподавателем, и составить таблицу соответствия угроз, целей и требований безопасности.
4. Изучить структуру «Общих критериев»: выписать классы функциональных требований и классы требований доверия.
5. Подготовить тезисы объёмом до одной страницы к круглому столу по одному из вопросов, приведённых в п. 4.5, с указанием не менее трёх источников.

Вопросы для самопроверки

1. Что является результатом фазы планирования и почему план должен включать распределение обязанностей?
2. Какие проблемы выявляются на фазе оценки?
3. В чём различие между реактивными и превентивными действиями на фазе корректировки?
4. Какие требования «Общих критериев» описывают поведение объекта оценки, а какие – свидетельства разработчика?
5. Что означает оценочный уровень доверия и как он влияет на объём предоставляемых свидетельств?

Тема 5. Эксплуатационное окружение и управление криптографическими ключами. Технические спецификации информационной безопасности

Объём самостоятельной работы – 6 часов. Форма контроля – собеседование.

Задания для самостоятельной работы

1. Изучить структуру стандарта FIPS 140-2: составить таблицу из одиннадцати групп требований с кратким описанием содержания каждой группы.
2. Составить схему жизненного цикла криптографического ключа с указанием мер защиты и ответственных на каждом этапе.
3. Изучить назначение и состав протоколов семейства IPsec; составить сравнительную таблицу транспортного и туннельного режимов.
4. Изучить назначение обобщённого прикладного программного интерфейса службы безопасности; описать последовательность вызовов при установлении контекста безопасности.
5. Разобрать схему работы системы одноразовых паролей S/KEY: описать порядок инициализации серии и порядок проверки предъявленного пароля.

Вопросы для самопроверки

1. Что понимается под криптографическим периметром модуля?
2. Какие требования предъявляются к эксплуатационному окружению на втором уровне безопасности?
3. Почему перехват одноразового пароля системы S/KEY не позволяет нарушителю пройти следующую аутентификацию?
4. Какие протоколы входят в семейство IPsec и какие задачи решает каждый из них?
5. Каким образом GSS-API обеспечивает переносимость приложений между средами с разными механизмами безопасности?

Тема 6. Анализ защищённости информационных систем. Политика безопасности предприятия. Оформление результатов исследований

Объём самостоятельной работы – 6 часов. Форма контроля – доклад.

Задания для самостоятельной работы

1. Изучить методики анализа защищённости операционных систем и систем управления базами данных; составить чек-лист проверки по направлениям.
2. Изучить документ «Дополнение к Руководству по информационной безопасности предприятия: как выбирать поставщика Internet-услуг»; выписать рекомендации, относящиеся к маршрутизаторам, почтовым и DNS-серверам.
3. Выполнить индивидуальное задание: провести анализ защищённости заданной информационной системы и оформить результаты в виде научно-технического обзора объёмом 8–12 страниц.

4. Изучить требования ГОСТ Р 7.0.100-2018 к библиографическому описанию; оформить список источников к обзору.

5. Подготовить доклад по результатам выполненного исследования и презентацию объёмом 8–12 слайдов.

Вопросы для самопроверки

1. Какие направления включает анализ защищённости операционной системы?
2. Чем определяется критичность выявленного несоответствия?
3. Какие вопросы к поставщику Internet-услуг являются ключевыми при варианте размещения Colocation?
4. Какими свойствами должно обладать положение политики безопасности, чтобы его исполнение можно было проконтролировать?
5. Чем обзор источников отличается от последовательного изложения содержания прочитанных работ?

4. Виды самостоятельной работы и порядок её выполнения

4.1. Проработка лекционного материала и работа с литературой

Проработка лекционного материала выполняется в течение недели после проведения лекции, пока материал сохраняется в оперативной памяти. Рекомендуется вести конспект в форме структурированных тезисов с выделением определений, классификаций и нормативных требований.

При конспектировании целесообразно применять следующий приём: страница делится на две части, в широкой части записывается содержание, в узкой – ключевые слова, вопросы и ссылки на нормативные документы. Такая структура существенно ускоряет последующее повторение материала при подготовке к промежуточной аттестации.

Термины, вводимые в ходе лекций, заносятся в глоссарий, который ведётся на протяжении всего курса. Для каждого термина указывается определение и источник – нормативный документ или стандарт. Глоссарий предъявляется при промежуточной аттестации.

При работе с нормативными документами (СТР-К, приказы ФСТЭК России, ГОСТ Р, ISO/IEC 27001, ISO/IEC 15408, FIPS 140-2) необходимо фиксировать: область применения документа, объекты защиты, состав требований и порядок их применения. Читать нормативный документ целиком последовательно нецелесообразно; следует начинать с раздела области применения и определений, затем переходить к разделам, относящимся к решаемой задаче. Результатом работы является структурированный конспект или сравнительная таблица.

4.2. Подготовка к практическим занятиям

Подготовка включает изучение теоретической части соответствующей практической работы, разбор порядка выполнения и подготовку ответов на контрольные вопросы базового уровня. Заранее подбираются исходные данные по индивидуальному варианту, согласованному с преподавателем.

Рекомендуется до занятия заполнить те графы форм, которые не требуют работы с программными средствами: перечни нормативных документов, описания объектов, классификационные признаки. Это позволяет использовать аудиторное время для содержательной части работы.

4.3. Подготовка доклада

Доклад готовится по теме, согласованной с преподавателем, и сопровождается презентацией объёмом 8–12 слайдов. Продолжительность выступления – 7–10 минут, после чего следуют вопросы аудитории.

Структура доклада: актуальность рассматриваемого вопроса; постановка задачи; обзор существующих подходов с указанием их достоинств и ограничений; результаты собственного анализа; выводы; список использованных источников (не менее пяти, из них не менее двух – за последние пять лет).

Рекомендуемые темы докладов:

1. Экспертные информационные системы в комплексном анализе информационной безопасности автоматизированных систем.
2. Сравнительный анализ отечественной и зарубежной нормативной базы в области защиты информации.
3. Технические каналы утечки информации в системах видеоконференцсвязи.
4. Побочные электромагнитные излучения и наводки как канал утечки информации: современные средства противодействия.
5. Модель нарушителя для информационных систем персональных данных: практика применения методических документов ФСТЭК России.
6. Банк данных угроз безопасности информации ФСТЭК России: структура, порядок применения, ограничения.
7. Развитие семейства стандартов ISO/IEC 27000 и его применение в российской практике.
8. Оценочные уровни доверия «Общих критериев»: содержание и практика применения.
9. Управление криптографическими ключами в распределённых информационных системах.
10. Виртуальные частные сети сетевого уровня: сравнительный анализ реализаций.
11. Многофакторная аутентификация: механизмы, области применения, ограничения.
12. Системы обнаружения и предотвращения вторжений: классификация и сравнительный анализ.
13. Анализ защищённости систем управления базами данных: методики и инструментальные средства.
14. Безопасность облачных сервисов: разграничение ответственности поставщика и потребителя.
15. Политика информационной безопасности предприятия: структура, порядок разработки и внедрения.
16. Методы научных исследований в области обеспечения информационной безопасности.

Обучающийся вправе предложить собственную тему доклада, согласовав её с преподавателем не позднее чем за две недели до выступления.

4.4. Выполнение индивидуальных заданий

Индивидуальные задания выдаются по темам 3, 4 и 6 и предполагают самостоятельное построение фрагмента модели угроз, разбор профиля защиты и проведение анализа защищённости заданной информационной системы.

Результат оформляется в виде расчётно-пояснительной записки объёмом 5–8 страниц, включающей постановку задачи, исходные данные, ход выполнения, результаты в форме таблиц и выводы. Записка представляется не позднее чем через две недели после выдачи задания.

4.5. Подготовка к круглому столу

К круглому столу по теме 4 обучающийся готовит аргументированную позицию по одному из следующих вопросов:

1. Применимость модели непрерывного совершенствования системы управления информационной безопасностью в организациях различного масштаба.

2. Соотношение отечественной и зарубежной нормативной базы: возможен ли единый подход к оценке защищённости?

3. Целесообразность сертификации средств защиты информации по «Общим критериям»: аргументы за и против.

4. Формальные требования нормативных документов и реальная защищённость: где проходит граница между соответствием и безопасностью?

5. Роль человеческого фактора в обеспечении информационной безопасности: технические меры против организационных.

Требуется подготовить тезисы объёмом до одной страницы, содержащие формулировку позиции, два-три аргумента в её поддержку и указание не менее трёх источников. Оценивается не совпадение позиции с мнением преподавателя, а обоснованность аргументации и способность отвечать на возражения.

4.6. Подготовка научно-технического обзора

Научно-технический обзор готовится по теме 6 и обеспечивает формирование индикаторов ИД-1 ОПК-5 и ИД-2 ОПК-5. Объём обзора – 8–12 страниц.

Структура обзора: титульный лист; содержание; введение с обоснованием актуальности и постановкой задачи; основная часть, содержащая описание применённых методов исследования, изложение и сопоставление существующих подходов, результаты собственного анализа; заключение с выводами; список источников, оформленный по ГОСТ Р 7.0.100-2018.

Обзор строится не как последовательный пересказ прочитанных работ, а как сопоставление подходов по единому набору признаков с выделением достоинств, ограничений и нерешённых вопросов. Именно выявленные нерешённые вопросы позволяют обосновать постановку собственной задачи исследования.

При изложении результатов следует разделять фактические данные и собственные выводы. Каждый вывод должен опираться на конкретный результат, приведённый в основной части. Заимствование текста без ссылки на источник не допускается.

4.7. Подготовка презентации

Презентация к докладу или обзору строится по правилу: один слайд – одна мысль. Рекомендуемая структура: титульный слайд; актуальность; постановка задачи; 3–5 содержательных слайдов; выводы; список источников.

Текст на слайде оформляется тезисно, размер шрифта – не менее 20 пунктов. Таблицы и схемы предпочтительнее сплошного текста. Слайд, содержащий более семи строк текста, подлежит переработке.

5. Формы контроля самостоятельной работы

Текущий контроль самостоятельной работы осуществляется в формах собеседования, доклада и круглого стола в соответствии с рабочей программой дисциплины. Результаты выполнения индивидуальных заданий учитываются при защите отчётов по практическим работам.

Таблица 3 – Формы контроля и оцениваемые результаты

Форма контроля	Что оценивается	Индикаторы
Собеседование	Знание понятийного аппарата, состава нормативных требований и содержания стандартов; способность обосновать выбор мер защиты	ИД-1 ОПК-1, ИД-2 ОПК-1, ИД-3 ОПК-1, ИД-1 ОПК-2
Доклад	Способность самостоятельно проработать тему, сопоставить подходы, изложить и защитить результаты	ИД-2 ОПК-1, ИД-2 ОПК-2, ИД-1 ОПК-5, ИД-2 ОПК-5

Форма контроля	Что оценивается	Индикаторы
Круглый стол	Способность формулировать и аргументировать позицию, отвечать на возражения, опираться на источники	ИД-3 ОПК-1, ИД-1 ОПК-2
Защита отчёта по практической работе	Полнота и корректность выполнения задания, обоснованность принятых решений	Согласно таблице 1
Научно-технический обзор	Применение методов научных исследований, корректность оформления результатов	ИД-1 ОПК-5, ИД-2 ОПК-5

При оценивании учитываются: полнота и корректность раскрытия вопроса, обоснованность выводов, самостоятельность выполнения работы, корректность ссылок на нормативные документы и источники, соблюдение требований к оформлению. Подробные критерии оценивания приведены в фонде оценочных средств по дисциплине.

6. График выполнения самостоятельной работы

Таблица 4 – График выполнения самостоятельной работы

Неделя	Вид самостоятельной работы	Часов	Форма отчётности	Срок представления
1–3	Проработка темы 1, ведение глоссария, подготовка к практической работе № 1	6	Собеседование	3-я неделя
4–6	Изучение СТР-К, составление сравнительной таблицы мер защиты	6	Собеседование	6-я неделя
7–9	Индивидуальное задание: фрагмент модели угроз; подготовка доклада	6	Доклад, записка	9-я неделя
10–12	Разбор профиля защиты; подготовка тезисов к круглому столу	6	Круглый стол, записка	12-я неделя
13–15	Проработка FIPS 140-2, IPsec, GSS-API; схема жизненного цикла ключа	6	Собеседование	15-я неделя
16–18	Анализ защищённости ОС и СУБД; научно-технический обзор и презентация	6	Доклад, обзор	18-я неделя

7. Подготовка к промежуточной аттестации

Промежуточная аттестация проводится в форме зачёта с оценкой. К аттестации допускаются обучающиеся, выполнившие и защитившие все шесть практических работ, представившие индивидуальные задания и прошедшие все формы текущего контроля.

Подготовка к аттестации строится на основе перечня заданий, приведённого в фонде оценочных средств по дисциплине. Рекомендуется следующий порядок: повторение глоссария; проработка конспектов лекций по каждой теме; повторение отчётов по практическим работам с восстановлением обоснования принятых решений; ответы на контрольные вопросы повышенного уровня.

Особое внимание следует уделить вопросам, требующим не воспроизведения, а обоснования: выбор набора стандартов, обоснование актуальности угрозы, обоснование уровня безопасности криптографического модуля, обоснование выбора механизма аутентификации.

Список литературы, рекомендуемый к использованию

Основная литература

1. Корецкий, В. П. Информационная безопасность и защита информации : учебное пособие / В. П. Корецкий. – Москва : РТУ МИРЭА, 2025. – 479 с. – ISBN 978-5-7339-2775-6. – URL: <https://e.lanbook.com/book/515271>
2. Технологии обеспечения безопасности информационных систем : учебное пособие / А. Л. Марухленко, Л. О. Марухленко, М. А. Ефремов [и др.]. – Москва ; Берлин : Директ-Медиа, 2021. – 210 с.

Дополнительная литература

1. Авдошин, С. М. Технологии и продукты Microsoft в обеспечении информационной безопасности / С. М. Авдошин, А. А. Савельева, В. А. Сердюк. – Москва : Интернет-Университет Информационных Технологий, 2010. – 384 с.
2. Галатенко, В. А. Стандарты информационной безопасности : курс лекций / В. А. Галатенко ; под ред. В. Б. Бетелина. – 2-е изд. – Москва : Интернет-Университет Информационных Технологий, 2006. – 264 с.
3. Зайцев, А. П. Технические средства и методы защиты информации : учеб. пособие для студентов вузов / А. П. Зайцев, А. А. Шелупанов, Р. В. Мещеряков [и др.] ; под ред. А. П. Зайцева и А. А. Шелупанова. – Изд. 4-е, испр. и доп. – Москва : Горячая линия-Телеком, 2009.
4. Кондаков, В. В. Информационная безопасность систем физической защиты, учёта и контроля ядерных материалов : учебное пособие / В. В. Кондаков, А. А. Краснобородько. – Москва : МИФИ, 2008. – 48 с.

Нормативные документы и интернет-ресурсы

1. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
2. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных».
3. Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К), утв. приказом Гостехкомиссии России от 30.08.2002 № 282.
4. ГОСТ Р 7.0.100-2018. Библиографическая запись. Библиографическое описание. Общие требования и правила составления.
5. Официальный сайт ФСТЭК России. – URL: <https://fstec.ru>
6. Банк данных угроз безопасности информации ФСТЭК России. – URL: <https://bdu.fstec.ru>
7. Федеральное агентство по техническому регулированию и метрологии (Росстандарт). – URL: <https://www.rst.gov.ru>