



Федеральное государственное образовательное бюджетное учреждение высшего образования
«ФИНАНСОВЫЙ УНИВЕРСИТЕТ ПРИ ПРАВИТЕЛЬСТВЕ РОССИЙСКОЙ ФЕДЕРАЦИИ»
(Финансовый университет)

Кафедра информационной безопасности
Факультет информационных технологий и анализа больших данных

Документ подписан усиленной неквалифицированной электронной подписью.

Организация: «ФИНАНСОВЫЙ УНИВЕРСИТЕТ ПРИ ПРАВИТЕЛЬСТВЕ
РОССИЙСКОЙ ФЕДЕРАЦИИ»

Сертификат: Ays4QoJhS8CzAkMv9GoEbY3kAHWViZ8C

Утверждено: Проректор по учебной и методической работе, Е.А. Каменева

Дата: 06.05.2026 г.

С.А. Резниченко
Аудит информационной безопасности

Рабочая программа дисциплины
для студентов, обучающихся по направлению подготовки
10.03.01 - Информационная безопасность,
Образовательная программа «Безопасность автоматизированных систем в кредитно-
финансовой сфере»
Профиль:
«Безопасность автоматизированных систем в кредитно-финансовой сфере»

Рекомендовано
Факультет информационных технологий и анализа больших данных
(протокол № 09 от 16.06.2026 г.)

Одобрено
Кафедра информационной безопасности
(протокол № 8 от 09.06.2026 г.)



Содержание

1. Наименование дисциплины	3
2. Перечень планируемых результатов освоения образовательной программы (перечень компетенций) с указанием индикаторов их достижения и планируемых результатов обучения по дисциплине	3
3. Место дисциплины в структуре образовательной программы	6
4. Объем дисциплины (модуля) в зачетных единицах и в академических часах с выделением объема аудиторной (лекции, семинары) и самостоятельной работы обучающихся	6
5. Содержание дисциплины, структурированное по темам (разделам) дисциплины с указанием их объемов (в академических часах) и видов учебных занятий	7
5.1. Содержание дисциплины	7
5.2. Учебно – тематический план	10
5.3. Содержание семинаров, практических занятий	11
6. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине	58
6.1. Перечень вопросов, отводимых на самостоятельное освоение дисциплины, формы внеаудиторной самостоятельной работы	58
6.2. Перечень вопросов, заданий, тем для подготовки к текущему контролю	68
7. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине	69
8. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины	6
9. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины	9
10. Методические указания для обучающихся по освоению дисциплины	93
11. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень необходимого программного обеспечения и информационных справочных систем (при необходимости)	94
12. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине	94



1. Наименование дисциплины

Аудит информационной безопасности

2. Перечень планируемых результатов освоения образовательной программы (перечень компетенций) с указанием индикаторов их достижения и планируемых результатов обучения по дисциплине

Код компетенции	Наименование компетенции	Индикаторы достижения компетенции	Результаты обучения (умения и знания), соотнесенные с индикаторами достижения компетенции
ДПКН-4.3	Способность осуществлять диагностику и мониторинг систем защиты автоматизированных систем	Устанавливает программные, программно—аппаратные, в том числе криптографические и технические средства защиты информации автоматизированных систем	Знать: - классификацию и последствия реализации угроз информационной безопасности (ИБ), основные концепции обеспечения ИБ и теоретические основы диагностики и непрерывного мониторинга систем защиты информации АС; - актуальные нормативные правовые акты и методические акты в сфере диагностики и непрерывного мониторинга систем защиты информации АС; - современные программные, программно-аппаратные, в том числе крипто-графические и технические, средства защиты информации АС; - методики, способы и средства диагностики и непрерывного мониторинга систем защиты информации АС. Уметь: - применять на практике теоретические основы диагностики и непрерывного мониторинга систем защиты информации АС; - устанавливать современные программные, программно-аппаратные, в том числе криптографические и технические, средства защиты информации АС; - применять методики, способы и средства диагностики и непрерывного мониторинга систем защиты информации АС.



Код компетенции	Наименование компетенции	Индикаторы достижения компетенции	Результаты обучения (умения и знания), соотнесенные с индикаторами достижения компетенции
		Тестирует и настраивает программные, программно-аппаратные, в том числе криптографические и технические средства защиты информации автоматизированных систем.	Знать: - теоретические основы тестирования и настройки современных программных, программно-аппаратных, в том числе криптографических и технических, средств защиты информации АС; - современные комплексы тестирования и настройки программных, программно-аппаратных, в том числе криптографических и технических, средств защиты информации АС; - методики и способы тестирования и настройки программных, программно-аппаратных, в том числе криптографических и технических, средств защиты информации АС. Уметь: - применять на практике теоретические основы тестирования и настройки современных программных, программно-аппаратных, в том числе криптографических и технических, средств защиты информации АС; - эксплуатировать современные комплексы тестирования и настройки программных, программно-аппаратных, в том числе криптографических и технических, средств защиты информации АС;
		Контролирует работоспособность программных, программно-аппаратных, в том числе криптографических и технических средств защиты информации автоматизированных систем.	Знать: - теоретические основы контроля работоспособности современных средств защиты информации АС; - актуальные методические документы в сфере контроля работоспособности средств защиты информации АС; - современные программные, программно-аппаратные, в том числе криптографические и технические, средства защиты информации АС; - методики, способы и средства контроля работоспособности средств защиты информации АС.



Код компетенции	Наименование компетенции	Индикаторы достижения компетенции	Результаты обучения (умения и знания), соотнесенные с индикаторами достижения компетенции
			Уметь: - применять методики, способы и средства контроля работоспособности современных программных, программно-аппаратных, в том числе - криптографических и технических, средств защиты информации АС; - принимать соответствующие меры по восстановлению работоспособности контролируемых средств защиты информации АС; - разрабатывать отчётный документ по результатам контроля работоспособности средств защиты информации АС.



3. Место дисциплины в структуре образовательной программы

Дисциплина «Аудит информационной безопасности» относится к «Модулю "Аудит информационной безопасности"».

4. Объем дисциплины (модуля) в зачетных единицах и в академических часах с выделением объема аудиторной (лекции, семинары) и самостоятельной работы обучающихся

Очная форма обучения

Вид учебной работы по дисциплине	Всего (в з/е и часах)	Семестр 6 (в часах)
Общая трудоемкость дисциплины	3/108	108
<i>Контактная работа – Аудиторные занятия</i>	<i>48</i>	<i>48</i>
<i>Лекции</i>	<i>16</i>	<i>16</i>
<i>Семинары, практические занятия</i>	<i>32</i>	<i>32</i>
<i>Самостоятельная работа</i>	<i>60</i>	<i>60</i>
Вид текущего контроля	Контрольная работа	Контрольная работа
Вид промежуточной аттестации	Зачет	Зачет



5. Содержание дисциплины, структурированное по темам (разделам) дисциплины с указанием их объемов (в академических часах) и видов учебных занятий

5.1. Содержание дисциплины

Тема 1. Аудит информационной безопасности. Правовые и методологические основы аудита ИБ. Основные понятия.

Понятия «аудит информационной безопасности» и «критерии аудита информационной безопасности». Нормативно-правовая основа проведения аудита информационной безопасности. Факторы, влияющие на аудит информационной безопасности. Процессы проверки и оценки. Понятия «мониторинг и контроль защитных мер», «самооценка информационной безопасности», «внутренний аудит информационной безопасности» и Понятия «аудит информационной безопасности» и «критерии аудита информационной безопасности». Нормативно-правовая основа проведения аудита информационной безопасности. Факторы, влияющие на аудит информационной безопасности. Процессы проверки и оценки. Понятия «мониторинг и контроль защитных мер», «самооценка информационной безопасности», «внутренний аудит информационной безопасности» и «анализ функционирования». Проверяемые направления деятельности. Требования и действия при проведении аудита информационной безопасности. Принципы проведения аудита информационной безопасности. Методики оценки соответствия информационной безопасности финансовых

Тема 2. Процессы проверки системы обеспечения ИБ

Виды проверок СОИБ. Мониторинг ИБ. Самооценка ИБ. Внутренний аудит ИБ. Цели и задачи внутренних аудитов ИБ. Организационные принципы внутреннего аудита ИБ. Принципы обеспечения эффективности внутреннего аудита ИБ. Подразделение внутреннего аудита, контролирующее вопросы ОИБ в организации. Внешний аудит ИБ. Принципы проведения внешнего аудита ИБ. Управление программой внешнего аудита ИБ. Компетентность аудиторов ИБ. Взаимоотношения представителей аудиторской группы и проверяемых организаций. Анализ СОИБ со стороны высшего руководства организации. Инструментальные средства проверки ИБ.

Тема 3. Внешний аудит информационной безопасности

Понятия «внешний аудит информационной безопасности», «соответствие» и «несоответствие» критериям аудита информационной безопасности. Стороны проведения аудита - «заказчик» и «исполнитель» аудита. Цели, программа и план внешнего аудита информационной безопасности. Последовательность процессов



менеджмента программы внешнего аудита информационной безопасности, основные направления проверки при внешнем аудите информационной безопасности. Внедрение, контроль и анализ программы внешнего аудита информационной безопасности. Этапы проведения внешнего аудита информационной безопасности. Понятие «свидетельство аудита информационной безопасности», источники свидетельств аудита информационной безопасности. Результаты проведения внешнего аудита информационной безопасности и правила их согласования. Контроль за деятельностью аудиторов информационной безопасности. Риски внешнего аудита информационной безопасности. Понятие «компетентность аудитора».

Тема 4. Национальные стандарты управления информационной безопасностью.

Стандарты по обеспечению безопасности информационных технологий в России. Практика оценки соответствия организаций российским стандартам. Отраслевые российские стандарты по обеспечению информационной безопасности. Комплекс документов по стандартизации информационной безопасности Банка России СТО БР ИББС. Обеспечение информационной безопасности критической инфраструктуры. Реализация требований по информационной безопасности на основе приказов и методических материалов ФСТЭК, ФСБ и Банка России. Реализация требований по оценке состояния информационной безопасности финансовых организаций на основе стандартов серии ГОСТ Р 57580.x.

Тема 5. Стандарты по аудиту информационной безопасности.

Стандарты серии ГОСТ Р ИСО/МЭК 27xxx. Стандарт безопасности данных индустрии платежных карт PCI DSS, его назначение, роль и место. Основная цель достижения соответствия требованиям стандарта PCI DSS. Методы проверки соответствия требованиям стандарта PCI DSS. Понятия «торгово-сервисное предприятие», «поставщик услуг» и «квалифицированный аудитор безопасности (QSA)». Разделы требований PCI DSS по обеспечению информационной безопасности. Результаты аудита соответствия информационной инфраструктуры требованиям PCI DSS. Этапы процесса проведения оценки соответствия PCI DSS. СТО БР ИББС 1.0.

Тема 6. Методы тестирования информационной безопасности.

Инструментальные средства тестирования Понятия «обследование», «интервью» и «тестирование». Подготовка и практика интервьюирования. Методы тестирования: тестирование «вслепую», «дважды слепое» тестирование, тестирование методом «серого ящика», тестирование методом «двойного серого ящика», тестированием методом «тандема», реверсивное тестирование. Требования к инструментальным средствам тестирования. Объекты тестирования инструментальных средств. Системы анализа



защищенности, системы сбора и корреляции событий безопасности. Тестирование на проникновение.



5.2. Учебно – тематический план

Очная форма обучения

п/ п	Наименование тем (разделов) дисциплины	Трудоемкость в часах				
		Всего	Контактная работа - Аудиторная работа			Самостоятельная работа
			Общая, в т.ч.:	Лекции	Семинары, практические занятия	
1	Аудит информационной безопасности. Правовые и методологические основы аудита ИБ. Основные понятия.	16	6	2	4	10
2	Процессы проверки системы обеспечения ИБ	16	6	2	4	10
3	Внешний аудит информационной безопасности	16	6	2	4	10
4	Национальные стандарты управления информационной безопасностью.	16	6	2	4	10
5	Стандарты по аудиту информационной безопасности.	22	12	4	8	10
6	Методы тестирования информационной безопасности.	22	12	4	8	10
В целом по дисциплине		108	48	16	32	60



5.3. Содержание семинаров, практических занятий

Наименование тем (разделов) дисциплины	Перечень вопросов для обсуждения на семинарах, практических занятиях	Формы проведения занятий
Аудит информационной безопасности. Правовые и методологические основы аудита ИБ. Основные понятия.	Блок 1. Сущность и место аудита ИБ в системе защиты информации 1. Что вкладывается в понятие «аудит информационной безопасности» и чем он принципиально отличается от смежных процедур (мониторинга, пентеста, аттестации объектов информатизации)? Приведите 2–3 отличия по целям, периодичности и формату результата. 2. Какие ключевые цели преследует аудит ИБ в коммерческой организации и в госоргане? Есть ли разница в приоритетах (например, соответствие регуляторам vs. управление рисками)? 3. Раскройте триаду «конфиденциальность—целостность—доступность» (КЦД) в контексте аудита: как через контрольные процедуры проверяют каждую из составляющих? Приведите по одному примеру контрольного мероприятия для каждой. 4. Что понимается под «независимостью аудитора», и почему это критично для объективности результатов? Какие типичные конфликты интересов возникают на практике (например, если аудит проводит ИТ-отдел)? 5. Как аудит ИБ встраивается в систему управления информационной безопасностью (СУИБ) и в цикл PDCA (Plan-Do-Check-Act)? Покажите на примере одного процесса (например, управление доступом).	1. Семинарские занятия (фокус—осмысление понятий, правовых норм, методологии) Развёрнутая проблемная беседа с опорой на первоисточники. Студенты заранее получают фрагменты нормативных актов (выдержки из 152-ФЗ, приказов ФСТЭК № 17/21, ISO/IEC 27001) и вопросы-ориентиры (например: «Найдите в тексте формулировку, которая может стать критерием аудита; переведите её в проверяемый пункт чек-листа»). На занятии идёт разбор: как из нормы сделать контрольный вопрос, какие свидетельства подойдут, где возможны разночтения. Цель: научиться «переводить» правовые нормы на язык аудита. Роль преподавателя: модерировать, подталкивать к точным формулировкам, не давать расплывчатых ответов. 2. Практические занятия (фокус — навыки настройки, проверки, интерпретации результатов) Кейс-практикум с нормативными актами. Студентам даётся мини-кейс (например: «розничная сеть обрабатывает ПДн; есть веб-сайт, кассы, CRM, удалённые сотрудники»). Задача — составить краткий план аудита: область, критерии (ссылки на 152-ФЗ и приказы ФСТЭК), 8–10 пунктов чек-листа, источники свидетельств. В



Наименование тем (разделов) дисциплины	Перечень вопросов для обсуждения на семинарах, практических занятиях	Формы проведения занятий
	Блок 2. Правовые основы аудита ИБ в РФ 6. Перечислите ключевые нормативные акты, формирующие правовую базу аудита ИБ в России. Соотнесите их с типами проверок: где речь об обязательном подтверждении соответствия, а где — о рекомендациях и лучших практиках. 7. В чём разница между «обязательным» и «добровольным» аудитом ИБ? Приведите по 2 примера ситуаций для каждого типа (например, аттестация ГИС по требованиям ФСТЭК; подготовка к сертификации по ISO/IEC 27001). 8. Какую роль играют приказы ФСТЭК России № 17 и № 21 в аудите? Что именно аудитор будет проверять в рамках этих документов (например, состав мер, уровни защищённости, классы систем)? 9. Каковы правовые последствия для организации при выявлении несоответствий в ходе обязательного аудита (например, по 152-ФЗ или 187-ФЗ)? Рассмотрите варианты от «предупреждения» до «приостановки деятельности». 10. Чем отличаются требования ФСБ и ФСТЭК к защите информации? В каких случаях аудитор ориентируется на документы ФСБ (например, криптография, защищённые каналы), а в каких — на ФСТЭК (классификация систем, базовый набор мер)?	конце — мини-презентация и взаимная рецензия. Цель: отработать планирование и формирование критериев. Инструменты: выдержки из НПА, шаблоны чек-листов.



Наименование тем (разделов) дисциплины	Перечень вопросов для обсуждения на семинарах, практических занятиях	Формы проведения занятий
	11. Как международные стандарты (ISO/IEC 27001, NIST CSF) соотносятся с российским законодательством? Можно ли использовать их как критерии аудита в РФ, и при каких условиях? Блок 3. Методологические основы, виды и этапы аудита 12. Какие существуют виды аудита ИБ (внутренний/ внешний, обязательный/добровольный, экспертно-документальный/технический)? Как выбор вида влияет на методику, сроки и уровень детализации проверки? 13. Опишите типовой жизненный цикл аудита ИБ: от инициации и планирования до формирования отчёта и контроля корректирующих действий. Какие документы создаются на каждом этапе (план аудита, чек-листы, отчёт, план устранения несоответствий)? 14. Что такое «критерии аудита» и как их корректно формировать? Покажите на примере: допустим, аудит защиты персональных данных в розничной сети. Какие источники возьмут за основу (152-ФЗ, приказы ФСТЭК, внутренние регламенты) и как из них вывести проверяемые пункты? 15. Сравните экспертно-документальный и технический аудит: в чём их сильные и слабые стороны? Когда достаточно документального анализа, а когда обязательно	



Наименование тем (разделов) дисциплины	Перечень вопросов для обсуждения на семинарах, практических занятиях	Формы проведения занятий
	нужны инструментальные проверки (сканирование уязвимостей, анализ конфигураций)? 16. Что такое гар-анализ в аудите ИБ? Разберите на практическом примере: как сопоставить текущее состояние (например, «журналы событий не архивируются») с целевым («журналы хранятся 90 дней, есть ротация и защита от несанкционированного изменения») и перевести это в список несоответствий. 17. Как определяют «область аудита» и почему её корректное описание критично? Приведите пример размытой формулировки («проверить безопасность всей ИТ-инфраструктуры») и предложите корректный вариант с границами (подразделения, системы, временные рамки, типы данных). 18. Какие методы сбора свидетельств аудита считаются допустимыми и надёжными? Проанализируйте, насколько весомыми будут разные типы доказательств: запись интервью, скриншот конфигурации, выгрузка логов, результаты сканирования уязвимостей. Блок 4. Основные понятия, терминология и оценка результатов 19. Дайте определения ключевым терминам: «свидетельство аудита», «несоответствие», «контроль безопасности», «риск ИБ». Продемонстрируйте их взаимосвязь на коротком примере (например, «в системе	



Наименование тем (разделов) дисциплины	Перечень вопросов для обсуждения на семинарах, практических занятиях	Формы проведения занятий
	нет двухфакторной аутентификации» → это несоответствие критерию → это контроль безопасности → это повышает риск компрометации учётных записей). 20. Как классифицируют несоответствия в аудите ИБ? Предложите шкалу критичности (например, критическое/значительное/малозначительное) и критерии отнесения (потенциальный ущерб, простота эксплуатации, влияние на КЦД). 21. Что такое «уровень зрелости процессов ИБ» и зачем его оценивают в ходе аудита? Сравните два состояния: «процессы не документированы, действия ситуативные» и «процессы регламентированы, измеряемы, непрерывно улучшаются» — как это повлияет на выводы аудитора? 22. Как из выявленных несоответствий формируют рекомендации? Разберите пример: «пароли пользователей не меняются 1 год» → какие конкретные действия предложить (политика паролей, технические ограничения, обучение), как определить сроки и ответственных? 23. В чём разница между «подтверждением соответствия» и «оценкой эффективности» мер защиты? Покажите на примере антивирусного ПО: формальное наличие лицензии vs. реальная эффективность (актуальность баз, охват устройств, частота обновлений).	



Наименование тем (разделов) дисциплины	Перечень вопросов для обсуждения на семинарах, практических занятиях	Формы проведения занятий
	Блок 5. Практические кейсы и разбор ситуаций (для практических занятий) 24. Кейс 1 (документальный аудит). Вам передали проект политики управления доступом. Сформулируйте 5–7 вопросов для интервью с владельцем процесса, чтобы проверить, как политика реализуется на практике (например: «кто утверждает заявки на доступ?», «как быстро отзываются права при увольнении?», «как часто проводится пересмотр прав?»). 25. Кейс 2 (технический аудит). В ходе сканирования сети выявлен открытый порт 3389 (RDP) на внешнем периметре. Какие дополнительные данные нужно собрать, чтобы оценить риск (версия ОС, наличие MFA, геолокация источников подключений)? Как это несоответствие отразить в отчёте? 26. Кейс 3 (аудит в рамках 152-ФЗ). Организация обрабатывает персональные данные. Составьте мини-чек-лист из 8–10 пунктов, по которым аудитор проверит соответствие (например: наличие уведомления в Роскомнадзоре, модель угроз, перечень обрабатываемых данных, меры защиты). 27. Кейс 4 (интерпретация результатов). В отчёте по аудиту указано: «не проводится регулярный анализ журналов безопасности». Обсудите, какие косвенные признаки могут указывать на эту проблему (например, отсутствие отчётов, жалобы пользователей, повторяющиеся инциденты). Как	



Наименование тем (разделов) дисциплины	Перечень вопросов для обсуждения на семинарах, практических занятиях	Формы проведения занятий
	проверить гипотезу, если журналы формально есть, но не анализируются? 28. Кейс 5 (планирование аудита). Сформулируйте план аудита для небольшого филиала банка: определите область, критерии (какие законы/стандарты), методы (интервью + выборочная проверка конфигураций), состав группы, сроки и ключевые риски, которые стоит учесть (например, платёжные транзакции, персональные данные, непрерывность обслуживания).	
Процессы проверки системы обеспечения ИБ	1. Как определить область проверки системы обеспечения ИБ (границы, объекты, временные рамки)? Приведите 2–3 примера корректной и некорректной формулировки области (например, «проверить всю ИБ компании» vs. «аудит процессов управления доступом в CRM за последние 6 месяцев»). 2. Какие источники используют для формирования критериев проверки ИБ? Сопоставьте типы критериев: законодательные (152-ФЗ, 187-ФЗ), отраслевые, международные стандарты (ISO/IEC 27001, NIST), внутренние регламенты. Как из общей нормы («обеспечить защиту ПДн») вывести проверяемый пункт чек-листа? 3. Чем отличается план проверки от программы и чек-листа? Покажите на примере одного процесса	1. Семинар-разбор нормативных требований («от нормы к проверяемому факту»). Студентам заранее выдают выдержки из НПА/стандартов (152-ФЗ, приказы ФСТЭК № 17/21, ISO/IEC 27002, NIST SP 800-53) по 2–3 процессам (журналирование, управление доступом, резервное копирование). На занятии каждая мини-группа берёт один пункт и выполняет цепочку: «норма → критерий аудита → проверяемый факт → тип свидетельства (лог/документ/интервью/конфигурация) → контрольный вопрос для интервью». В конце — сводная таблица на доске. Цель: научиться переводить расплывчатые нормы в конкретные пункты чек-листа. Артефакт: таблица «норма — критерий — свидетельство». 2. Круглый стол «Границы проверки: что входит, что нет».



Наименование тем (разделов) дисциплины	Перечень вопросов для обсуждения на семинарах, практических занятиях	Формы проведения занятий
	(например, управление инцидентами): как цель, область, критерии и методы отражаются в каждом из документов. 4. Как распределить роли и зоны ответственности в группе проверки (руководитель, технические аудиторы, интервьюеры, секретарь)? Какие конфликты интересов типичны (например, аудит ИТ-инфраструктуры силами того же отдела, который её администрирует), и как их исключить? 5. Как учесть риски самой проверки (например, влияние на доступность сервисов при сканировании уязвимостей, утечка чувствительных данных из отчётов)? Назовите 2–3 меры минимизации таких рисков. 6. Какие методы сбора свидетельств считаются надёжными в практике проверок ИБ? Сравните по достоверности: интервью с сотрудниками, анализ конфигураций, выгрузки логов, результаты сканирования уязвимостей, скриншоты, записи совещаний. 7. Как подготовить корректный скрипт интервью для владельца процесса? Разберите на примере: сформулируйте 5–7 уточняющих вопросов к утверждению «у нас настроено резервное копирование» (например: «как часто делается	Обсуждается, как корректно задать область проверки, чтобы избежать «проверим всё сразу». Даются заведомо размытые формулировки («проверить безопасность ИТ»), студенты трансформируют их в чёткие области (объекты, процессы, временные рамки, типы данных, исключения). Разбирают пограничные случаи: облачные сервисы, подрядчики, BYOD, микросервисы. Цель: отработать навык определения области аудита и фиксации исключений. Артефакт: список из 5–7 корректных формулировок областей для разных профилей организаций. 4. Разбор структуры документов проверки. На занятии анализируют обезличенные фрагменты реальных (или учебных) документов: план аудита, чек-лист, отчёт, CAPA (план корректирующих действий). Студенты в малых группах «восстанавливают» недостающие части: к области подбирают критерии, к несоответствию — свидетельства и риск, к рекомендации — метрики успеха. Цель: освоить логику и обязательные элементы документации аудита. Критерии успеха: прослеживаемость «критерий → свидетельство → вывод → рекомендация». 1. Практикум «Составление чек-листа под заданный процесс».



Наименование тем (разделов) дисциплины	Перечень вопросов для обсуждения на семинарах, практических занятиях	Формы проведения занятий
	бэкап?», «где хранятся копии?», «как проверяется их восстанавливаемость?»). 8. Как отличить «наличие процедуры» от «реальной работы процесса»? Приведите по 2 примера свидетельств для каждого случая (например, есть регламент vs. есть регулярные отчёты, журналы, результаты тестов). 9. Какие технические инструменты применяют на разных этапах проверки? Соотнесите задачи и инструменты: инвентаризация активов, сканирование уязвимостей, анализ журналов, проверка конфигураций, тестирование на проникновение. Назовите по 1–2 инструмента для каждой задачи (например, nmap, OpenVAS/Nessus, auditd/Event Viewer, Ansible-проверки). 10. В чём специфика сбора свидетельств в облачной среде (IaaS/PaaS/SaaS)? Какие данные доступны заказчику, а какие — только провайдеру? Как через договор (SLA/DSAR) и артефакты (отчёты SOC 2, аттестаты) подтвердить выполнение требований ИБ? 11. Управление доступом. Какие контрольные точки проверяют при аудите прав доступа? Разберите кейс: «пользователь уволен, но его учётная запись активна 3 недели». Какие свидетельства покажут проблему (журналы кадровых систем, логи	Каждая группа получает один процесс СУИБ (управление инцидентами, управление конфигурациями, журналирование, резервное копирование, управление доступом). Задача — за 30–40 минут подготовить мини-чек-лист из 8–12 пунктов с указанием источника критерия (НПА/стандарт/внутренний регламент) и типа свидетельства. В конце — взаимная рецензия: «можно ли по этому пункту объективно подтвердить соответствие?». Цель: закрепить навык декомпозиции процесса на проверяемые элементы. Инструменты: шаблоны чек-листов, выдержки из ISO/IEC 27002 и приказов ФСТЭК. 2. Тренировка интервью: «Аудитор vs владелец процесса». Работа в парах/тройках: один — аудитор, второй — владелец процесса (например, администратор БД, руководитель ИТ, начальник отдела кадров), третий — наблюдатель/оценщик. Аудитор задаёт вопросы по скрипту (сначала открытые, затем уточняющие), владелец отвечает, опираясь на упрощённую модель организации. Задача аудитора — дойти до конкретных фактов и артефактов, а не общих фраз. Цель: отработать технику интервью, научиться задавать уточняющие вопросы и выявлять «дыры» в процессе. Критерии оценки: переход от «всё работает» к «журналы хранятся 90 дней, есть ротация, доступ только у группы AuditLogs».



Наименование тем (разделов) дисциплины	Перечень вопросов для обсуждения на семинарах, практических занятиях	Формы проведения занятий
	AD/LDAP, отчёты по доступу), и как связать это с риском? 12. Управление инцидентами ИБ. Что проверяют в процессе реагирования: время обнаружения, эскалации, устранения? Как по логам и отчётам подтвердить соответствие целевым показателям (например, MTTR < 4 ч)? Приведите пример ложного срабатывания и способ его верификации. 13. Управление конфигурациями и изменениями. Как убедиться, что изменения в ИТ-инфраструктуре согласованы и протестированы? Какие артефакты служат свидетельствами (RFC, планы отката, журналы изменений, результаты регрессионных проверок)? 14. Журналирование и мониторинг. Какие поля в логах критичны для расследования инцидентов (время, источник, субъект, действие, результат)? Как проверить, что логи не подделываются (целостность, ротация, экспорт, права доступа)? 15. Резервное копирование и непрерывность бизнеса. Как подтвердить, что бэкапы не только создаются, но и восстанавливаются? Назовите метрики и свидетельства (результаты тестовых восстановлений, RPO/RTO, отчёты о проверках). 16. Чем «подтверждение соответствия» отличается от «оценки эффективности» мер ИБ? Разберите на	3. Практикум по оценке зрелости процессов ИБ. Дана 5-уровневая модель зрелости (например, по COBIT или NIST). Студенты оценивают по ней один процесс (управление инцидентами или управление доступом): собирают «признаки» по уровням, определяют текущий уровень, формулируют шаги перехода на следующий. Цель: научиться оценивать зрелость процессов и связывать её с практическими улучшениями. Артефакт: карта зрелости процесса + план перехода на следующий уровень.



Наименование тем (разделов) дисциплины	Перечень вопросов для обсуждения на семинарах, практических занятиях	Формы проведения занятий
	примере антивируса: формальное наличие лицензии vs. реальная защита (актуальность баз, охват устройств, частота обновлений, результаты симуляций атак). 17. Как классифицировать выявленные несоответствия по уровню риска? Предложите шкалу (критический/значительный/малозначительный) и критерии отнесения (ущерб, вероятность, влияние на КЦД). Продемонстрируйте на 2–3 примерах (например, «открытый RDP на периметре» vs. «пароль меняется раз в год»). 18. Как связать несоответствия с бизнес-рисками? Постройте цепочку: уязвимость → угроза → сценарий атаки → потенциальный ущерб → влияние на бизнес-процессы. Возьмите один процесс (например, онлайн-оплата) и покажите, как техническая проблема превращается в операционный риск. 19. Что такое «остаточный риск» и как его документируют в отчёте по проверке? Приведите пример: «невозможно отключить SMBv1 на legacy-оборудовании» → какие компенсирующие меры и обоснования фиксируют? 20. Как оценить зрелость процесса ИБ в ходе проверки? Сравните два состояния: «процесс не документирован, действия ситуативные» и	



Наименование тем (разделов) дисциплины	Перечень вопросов для обсуждения на семинарах, практических занятиях	Формы проведения занятий
	«процесс регламентирован, измеряем, непрерывно улучшается». Какие признаки указывают на переход между уровнями зрелости (по COBIT/NIST)? 21. Из каких разделов состоит отчёт по результатам проверки системы ИБ? Объясните назначение каждого блока: область, критерии, методы, перечень несоответствий, оценка рисков, рекомендации, план корректирующих действий. 22. Как сформулировать несоответствие так, чтобы оно было объективным, проверяемым и однозначным? Разберите плохие и хорошие формулировки (например, «безопасность слабая» vs. «в журналах событий отсутствуют записи об изменениях в AD более 30 дней; источник — выгрузка Security Log, период 01.09–30.09»). 23. Как построить рекомендации, чтобы они были выполнимыми и измеримыми? Покажите структуру: действие → срок → ответственный → критерий успеха. Приведите пример для проблемы «нет регулярного анализа журналов». 24. Что такое «план корректирующих действий» (CAPA) и как его контролируют? Назовите 3–4 метрики, по которым отслеживают исполнение (например, % выполненных пунктов, среднее время закрытия, число просроченных задач).	



Наименование тем (разделов) дисциплины	Перечень вопросов для обсуждения на семинарах, практических занятиях	Формы проведения занятий
	25. Как избежать типичных ошибок в отчётах: субъективные оценки без свидетельств, размытые формулировки, избыток технических деталей без связи с рисками, игнорирование компенсирующих мер? 1. Кейс 1 (планирование). Дана организация: интернет-магазин, обработка ПДн, облачная инфраструктура. Сформулируйте область проверки, выберите 3–4 критерия (с указанием источников: 152-ФЗ + ISO/IEC 27002), составьте мини-чек-лист из 8–10 пунктов для процесса управления доступом. 2. Кейс 2 (сбор свидетельств). В ходе проверки администратор заявляет: «мы регулярно тестируем восстановление из бэкапов». Какие 3–5 артефактов запросите, чтобы подтвердить это? Как интерпретировать отсутствие отчётов о тестах? 3. Кейс 3 (анализ логов). Студентам выдаются фрагменты логов (Windows Event Viewer / Linux auditd). Задача — выявить признаки инцидента (например, массовые неудачные попытки входа, изменение прав доступа) и сформулировать несоответствие с привязкой к критерию. 4. Кейс 4 (приоритизация). Выдан список из 6–8 несоответствий (например, «пароли не	



Наименование тем (разделов) дисциплины	Перечень вопросов для обсуждения на семинарах, практических занятиях	Формы проведения занятий
	меняются», «журналы не экспортируются», «RDP открыт на периметре», «нет обучения ИБ»). Классифицируйте их по критичности и обоснуйте выбор, связав с рисками для бизнеса. 5. Кейс 5 (оформление отчёта). Дан черновик отчёта с субъективными оценками и без свидетельств. Перепишите 2–3 абзаца в формате «факт → критерий → риск → рекомендация», используя только проверяемые данные. 6. Блок 7. Интеграция проверок в систему управления ИБ и непрерывный контроль 7. Как встроить периодические проверки в цикл PDCA (Plan-Do-Check-Act) СУИБ? Покажите на одном процессе (например, управление уязвимостями): какие проверки на этапе Check, какие решения на Act. 8. Чем отличаются плановые, внеплановые и повторные проверки? Назовите по 2–3 триггера для каждого типа (например, плановая — ежегодный аудит; внеплановая — инцидент/изменение инфраструктуры; повторная — контроль исполнения САР). 9. Как автоматизировать сбор свидетельств и мониторинг выполнения рекомендаций? Приведите 3 конкретных примера: что мониторить, каким инструментом, какой порог/алерт (например, Zabbix	



Наименование тем (разделов) дисциплины	Перечень вопросов для обсуждения на семинарах, практических занятиях	Формы проведения занятий
	для доступности сервисов, OpenVAS для уязвимостей, SIEM для аномалий в логах). 10. Какие современные вызовы меняют подходы к проверкам ИБ (DevSecOps, микросервисы, BYOD, ИИ-инструменты)? Как адаптировать классические методы (аудит, пентест) к динамичной среде? 11. Как организовать взаимодействие между службой ИБ, ИТ и бизнесом при проведении проверок? Назовите точки соприкосновения и типичные барьеры (например, ИТ боится «блокировок», бизнес — затрат), предложите 2–3 механизма согласования.	
Внешний аудит информационной безопасности	Блок 1. Сущность, цели и специфика внешнего аудита В чём принципиальные отличия внешнего аудита ИБ от внутреннего (по критериям: независимость, подотчётность, глубина доступа, формат отчётности, последствия выводов)? Приведите по 2–3 примера ситуаций, где внешний аудит обязателен или критически предпочтителен. Какие цели внешнего аудита ИБ типичны для разных заказчиков (банк для ЦБ/платёжной системы, клиника для соответствия 152-ФЗ, промышленное предприятие по КИИ, SaaS-провайдер для SOC 2, компания перед M&A)? Как цель влияет на область, критерии и формат отчёта? Что означает «независимость внешнего аудитора» на практике? Разберите 3–4 кейса, где независимость под	1. Семинар-разбор договора и технического задания на внешний аудит. Студентам заранее дают обезличенный (или учебный) договор/ТЗ на внешний аудит (с разделами: область, критерии, методы, артефакты, ограничения, порядок доступа, NDA). На занятии в малых группах они выделяют ключевые пункты, которые влияют на качество и объективность проверки: как задана область, какие критерии взяты за основу, как прописаны методы сбора свидетельств, где зоны риска (например, «доступ к логам только в рабочее время», «не проверять legacy-системы»). В конце — сводная таблица «пункт договора → риск для объективности аудита → способ минимизации».



Наименование тем (разделов) дисциплины	Перечень вопросов для обсуждения на семинарах, практических занятиях	Формы проведения занятий
	угрозой (например, «аудитор одновременно внедряет СЗИ», «родственные связи», «долгосрочные консалтинговые услуги»), и предложите меры минимизации риска. Как внешний аудит соотносится с другими внешними процедурами (пентест, аттестация, сертификация, due diligence)? Где границы и точки пересечения? Приведите пример, когда смешение процедур ведёт к некорректным ожиданиям заказчика. Какие репутационные и регуляторные последствия могут быть у отчёта внешнего аудита? Разберите на примере: «выявлено критическое несоответствие по журналированию» — как это может повлиять на договор с партнёром, на прохождение сертификации, на позицию в тендере. Блок 2. Договорные рамки, область и критерии внешнего аудита Какие ключевые пункты обязательно должны быть в ТЗ/договоре на внешний аудит ИБ, чтобы обеспечить объективность и исполнимость? Разберите, чем опасна размытая формулировка «проверить безопасность ИТ-инфраструктуры», и покажите, как её трансформировать в корректную область (объекты, процессы, временные рамки, исключения). Как выбрать критерии внешнего аудита под задачу (например, сертификация ISO/IEC 27001 vs. проверка соответствия 152-ФЗ vs. due diligence)? Сопоставьте	Цель: понять, что внешний аудит начинается с договорённостей и формальных границ, а не с «сканирования портов». Артефакт: таблица рисков по договору + список обязательных пунктов ТЗ для внешнего аудита. 2. Дискуссия «Независимость внешнего аудитора: где границы и как их соблюсти». Группа делится на «аудиторскую компанию», «заказчика», «регулятора» и «инвестора». Обсуждаются конфликтные кейсы: «аудитор одновременно внедряет СЗИ в этой компании», «родственник аудитора работает в ИТ-отделе заказчика», «заказчик просит «подправить» уровень критичности уязвимостей». Каждая сторона аргументирует позицию со ссылками на стандарты (ISO 19011, требования СРО/лицензирующих органов), этические кодексы, практику рынка. Цель: закрепить понятие независимости и увидеть типичные угрозы объективности внешнего аудита. Оценка: по качеству аргументации и ссылкам на нормы/лучшие практики. 3. Практикум «Оформление отчёта внешнего аудита для разных стейкхолдеров». Даётся один набор фактов (например, «RDP открыт на периметре», «журналы не экспортируются», «нет регулярного пересмотра прав доступа»). Студенты готовят 2–3 версии отчёта: для совета директоров (кратко, риски/



Наименование тем (разделов) дисциплины	Перечень вопросов для обсуждения на семинарах, практических занятиях	Формы проведения занятий
	источники критериев: законы, приказы регуляторов, международные стандарты, отраслевые требования, SLA/DSAR. Что такое «ограничения внешнего аудита» и как их корректно зафиксировать? Приведите 3–4 типичных ограничения (доступ к логам только в рабочее время, отсутствие прав на пентест, legacy-системы вне области) и объясните, как они влияют на уровень уверенности аудитора и формулировки отчёта. Как формализовать «источники свидетельств» в плане аудита? Соотнесите типы свидетельств (выгрузки логов, отчёты SIEM, результаты сканирования, интервью, документы) с уровнем достоверности и рисками подмены/искажения. Как учесть особенности облачной среды (IaaS/PaaS/SaaS) при определении области и критериев внешнего аудита? Какие доказательства можно запросить у провайдера (SOC 2/3, отчёты о пентестах, сертификаты), а какие нужно собирать самостоятельно? Блок 3. Планирование и управление проектом внешнего аудита Из каких этапов состоит проект внешнего аудита ИБ? Для каждого этапа назовите ключевые артефакты (RFP, КП, план/чек-лист, отчёт, CAPA) и контрольные точки качества (например, согласование области до старта полевых работ).	бизнес-влияние), для ИТ-директора (технические детали, метрики, план действий), для регулятора (ссылки на НПА, соответствие критериям). Цель: научиться адаптировать язык и глубину детализации под аудиторию внешнего аудита. Артефакт: 2–3 фрагмента отчёта под разные аудитории. 4. Кейс-практикум «Приоритизация несоответствий в рамках внешнего аудита». Выдаётся список из 8–10 фактов для условного заказчика (например, клиника, обрабатывающая ПДн). Студенты классифицируют несоответствия по критичности с учётом контекста: отрасль, регулятор, тип данных, зрелость процессов. Для каждого строят цепочку «уязвимость → угроза → сценарий → ущерб → влияние на обязательства по договору/закону». В конце — обсуждение, почему одна и та же проблема (например, слабые пароли) в разных организациях получает разный приоритет. Цель: сформировать навык приоритизации именно в логике внешнего аудита (не «как исправить», а «что критично для подтверждения соответствия и отчётности»). Артефакт: матрица рисков с краткими сценариями и ссылками на критерии.



Наименование тем (разделов) дисциплины	Перечень вопросов для обсуждения на семинарах, практических занятиях	Формы проведения занятий
	Как сформировать команду внешнего аудита под разные профили заказчиков (финсектор, медицина, промышленность)? Какие роли нужны (руководитель проекта, технические аудиторы, интервьюеры, эксперт по НПА), и какие компетенции критичны? Как оценить трудозатраты и риски проекта внешнего аудита? Назовите 3–4 риска (задержка предоставления документов, недоступность ключевых сотрудников, изменение инфраструктуры «на лету») и предложите превентивные меры (резервные окна, альтернативные источники свидетельств, эскалация). Что такое RFP и как по нему оценить качество предложения аудиторской компании? Разберите типовые «красные флаги» в КП (например, «гарантируем отсутствие критических уязвимостей», «проверим всё за 3 дня», «используем только один инструмент»). Как согласовать график внешнего аудита, чтобы минимизировать влияние на бизнес? Приведите примеры компромиссных решений (пассивный сбор вместо активного сканирования в пиковые часы, выборочная проверка вместо сплошной, поэтапный доступ к системам). Блок 4. Сбор свидетельств и проведение полевых работ Какие методы сбора свидетельств считаются надёжными в внешнем аудите? Сравните по достоверности и применимости: интервью, анализ документов, загрузки логов/SIEM, сканирование уязвимостей, выборочные	



Наименование тем (разделов) дисциплины	Перечень вопросов для обсуждения на семинарах, практических занятиях	Формы проведения занятий
	технические проверки. В каких случаях один метод не заменяет другой? Как подготовить и провести интервью с владельцами процессов так, чтобы получить проверяемые факты, а не общие фразы? Разберите на примере: владелец говорит «у нас всё защищено». Сформулируйте 5–7 уточняющих вопросов, которые приведут к артефактам (журналы, отчёты, конфигурации). Как работать с «отсутствием свидетельств» (нет логов, нет регламентов, нет отчётов о тестах)? Какие выводы можно и нельзя делать? Приведите корректные формулировки для отчёта («не подтверждено соответствие по критерию X, источник свидетельств недоступен») vs. некорректные («система не защищена»). Как организовать технический сбор свидетельств в условиях ограничений внешнего аудита (без пентеста, без изменения конфигураций, доступ только к выгрузкам)? Покажите на примере проверки журналирования: какие поля в логах критичны, как подтвердить целостность, как верифицировать охват систем. Как документировать свидетельства, чтобы они были допустимы для третьих лиц (регуляторов, судов, партнёров)? Назовите обязательные элементы: источник, период, метод получения, хэш/контрольная сумма, статус доступа, ограничения выборки. Блок 5. Оценка несоответствий, рисков и приоритизация	



Наименование тем (разделов) дисциплины	Перечень вопросов для обсуждения на семинарах, практических занятиях	Формы проведения занятий
	Чем «несоответствие» в внешнем аудите отличается от «уязвимости» или «инцидента»? Приведите пример: как одна и та же техническая проблема (например, открытый RDP) может быть зафиксирована как несоответствие по процессу управления доступом, как уязвимость в отчёте пентеста и как признак инцидента в SIEM. Как классифицировать несоответствия внешнего аудита по критичности? Предложите шкалу (критический/значительный/малозначительный) и критерии отнесения (ущерб, вероятность, влияние на обязательства). Продемонстрируйте на 2–3 кейсах из разных отраслей. Как построить цепочку «несоответствие → угроза → сценарий → ущерб → влияние на обязательства» для внешнего отчёта? Возьмите один процесс (например, управление учётными записями уволенных сотрудников) и покажите, как технический факт превращается в бизнес-риск и регуляторное несоответствие. Что такое «компенсирующие меры» и как их учитывать при оценке соответствия? Разберите кейс: «нельзя отключить SMBv1 на legacy-оборудовании». Какие компенсирующие меры признаются регуляторами/стандартами, и как их верифицировать? Как учитывать контекст организации при приоритизации несоответствий? Покажите на примерах: «слабые пароли» в интернет-магазине vs. в банке; «нет обучения ИБ» в	



Наименование тем (разделов) дисциплины	Перечень вопросов для обсуждения на семинарах, практических занятиях	Формы проведения занятий
	стартапе vs. в медучреждении. Почему одинаковый факт получает разный уровень риска? Блок 6. Оформление отчёта и коммуникация результатов Из каких обязательных разделов состоит отчёт внешнего аудита ИБ? Объясните назначение каждого блока: область, критерии, методы, ограничения, перечень несоответствий, оценка рисков, рекомендации, оговорки. Почему отсутствие любого из них снижает ценность отчёта для третьих лиц? Как сформулировать вывод внешнего аудита объективно и проверяемо? Сравните плохие и хорошие формулировки (например, «безопасность слабая» vs. «в журналах Security Log отсутствуют записи об изменениях в AD за период 01.09–30.09; источник — выгрузка, охват — контроллеры домена DC1/DC2»). Как адаптировать язык и глубину детализации отчёта под разные аудитории (совет директоров, ИТ-директор, регулятор, инвестор)? Покажите на одном факте (например, «журналы не экспортируются») три версии вывода: бизнес-ориентированную, техническую и нормативно-ориентированную. Что такое САРА (план корректирующих и предупреждающих действий) в контексте внешнего аудита? Как связать рекомендации с метриками успеха и способом верификации? Приведите структуру: действие → срок → ответственный → критерий успеха → способ контроля.	



Наименование тем (разделов) дисциплины	Перечень вопросов для обсуждения на семинарах, практических занятиях	Формы проведения занятий
	Как провести итоговую встречу с заказчиком и согласовать выводы? Разберите типичные возражения («это legacy», «у нас есть компенсирующие меры», «вы не учли контекст») и корректные ответы аудитора, опирающиеся на критерии и свидетельства. Блок 7. Нормативная база, стандарты и подтверждение независимости Какие российские НПА и приказы регуляторов задают требования, проверяемые в ходе внешнего аудита (152-ФЗ, 187-ФЗ, приказы ФСТЭК № 17/21, требования ФСБ)? Соотнесите типичные пункты чек-листа с конкретными нормами. Какие международные стандарты задают методологию внешнего аудита ИБ (ISO 19011, ISO/IEC 27006, ISO/IEC 27007)? Что они требуют в части независимости, планирования, документирования и компетентности аудиторов? Как подтвердить квалификацию и независимость внешней аудиторской организации? Назовите индикаторы: лицензии/аттестаты, членство в СРО, отсутствие конфликта интересов, методология, страхование ответственности, примеры аналогичных проектов. Как в отчёте внешнего аудита отразить ограничения и уровень уверенности? Что значит «reasonable assurance» vs.	



Наименование тем (разделов) дисциплины	Перечень вопросов для обсуждения на семинарах, практических занятиях	Формы проведения занятий
	«absolute assurance», и почему аудитор не может гарантировать отсутствие уязвимостей? Какие этические принципы внешнего аудитора критичны (конфиденциальность, объективность, профессиональная осмотрительность)? Разберите 2–3 кейса нарушения и их последствия для репутации и юридической силы отчёта. Блок 8. Практические кейсы и отработка навыков (для практических занятий) Кейс 1 (ТЗ и область). Дан профиль организации (онлайн-школа, обрабатывающая ПДн). Сформулируйте корректную область внешнего аудита (объекты, процессы, исключения), выберите 4–5 ключевых критериев (с указанием источников) и перечислите ожидаемые свидетельства. Кейс 2 (интервью). Владелец процесса заявляет: «мы регулярно тестируем восстановление из бэкапов». Составьте скрипт из 6–8 уточняющих вопросов и список артефактов, которые подтвердят или опровергнут утверждение. Кейс 3 (анализ логов). Студентам выдаются фрагменты логов (Windows Event Viewer / Linux auditd) с аномалиями. Задача — выделить факт, соотнести с критерием внешнего аудита, сформулировать вывод в стиле отчёта и оценить критичность с учётом контекста. Кейс 4 (приоритизация). Выдан список из 7–9 несоответствий для условного медучреждения.	



Наименование тем (разделов) дисциплины	Перечень вопросов для обсуждения на семинарах, практических занятиях	Формы проведения занятий
	Классифицируйте их по критичности, постройте для 2–3 из них цепочки рисков и предложите компенсирующие меры там, где уместно. Кейс 5 (оформление отчёта). Дан черновик отчёта с субъективными оценками. Перепишите 3–4 абзаца в формате внешнего аудита: «факт → критерий → свидетельство → риск → рекомендация (действие/срок/ответственный/метрика)». Кейс 6 (переговоры). Аудитор зафиксировал критическое несоответствие; заказчик возражает, ссылаясь на legacy и бизнес-приоритеты. Отработайте диалог: аудитор обосновывает вывод через критерии и сценарии рисков, заказчик предлагает компенсирующие меры. Оцените их достаточность.	
Национальные стандарты управления информационной безопасностью.	Блок 1. Понятие и виды критериев аудита ИБ • Что такое «критерий аудита ИБ» и чем он отличается от «нормы закона», «угрозы» и «уязвимости»? Приведите 3–4 примера трансформации общей нормы («обеспечить защиту информации») в проверяемый критерий аудита («в логах фиксируются все изменения прав доступа; период хранения — 90 дней; охват — все контроллеры домена»).	1. Семинар-сопоставление: «Российские требования vs международные стандарты». Студентам заранее выдают по 2–3 пункта из российских документов (например, приказ ФСТЭК №21, 152-ФЗ) и аналогичные по смыслу пункты из международных стандартов (ISO/IEC 27002, COBIT). На занятии мини-группы строят таблицу соответствия: «российский пункт → международный аналог → общий проверяемый факт → различия в акцентах (технические меры vs процессный подход)». В конце — сводная матрица



Наименование тем (разделов) дисциплины	Перечень вопросов для обсуждения на семинарах, практических занятиях	Формы проведения занятий
	• Какие типы критериев используют в аудите ИБ? Сопоставьте: законодательные (обязательные), отраслевые, международные, корпоративные (внутренние регламенты, политики). В каких случаях приоритет отдаётся одному типу над другим? • Как из «мягкой» нормы (рекомендация, лучшая практика) вывести проверяемый критерий? Разберите на примере фразы из стандарта «следует регулярно пересматривать права доступа»: сформулируйте 3–4 конкретных пункта чек-листа и типы свидетельств для каждого. • Что значит «объективность и измеримость критерия аудита»? Сравните формулировки: «администраторы контролируют доступ» vs. «раз в квартал формируется отчёт о правах доступа; отчёт согласовывается у владельца ресурса; несоответствия устраняются в течение 10 рабочих дней». Назовите признаки хорошего критерия. • Как учитывать контекст организации при выборе и интерпретации критериев (размер, отрасль, зрелость процессов, регуляторные обязательства)? Покажите на двух контрастных примерах (стартап vs. банк).	и обсуждение, как эти различия влияют на чек-листы. Цель: научиться «переводить» нормы разных систем в единые проверяемые критерии. Артефакт: таблица сопоставления с выводами о различиях в подходах. 2. Разбор-дискуссия «От расплывчатой нормы к проверяемому критерию». Преподаватель даёт 3–4 размытые формулировки из практики («обеспечить защиту», «вести журналы», «управлять доступом»). Студенты в малых группах трансформируют их в проверяемые критерии по шаблону: «факт → период → охват → тип свидетельства → допустимый результат». Затем группы обмениваются результатами и проводят «перекрёстную рецензию»: что в формулировке остаётся субъективным, чего не хватает для объективной проверки. Цель: отработать навык декомпозиции и измеримости критериев. Критерии успеха: отсутствие оценочных слов («хорошо/плохо»), наличие периода/охвата/источника свидетельств. 3. Тренировка верификации «живых» процессов (имитация сбора свидетельств).



Наименование тем (разделов) дисциплины	Перечень вопросов для обсуждения на семинарах, практических занятиях	Формы проведения занятий
	Блок 2. Национальные стандарты и документы РФ в области управления ИБ: обзор и применение • Назовите ключевые российские документы, задающие критерии аудита ИБ (152-ФЗ, 187-ФЗ, приказы ФСТЭК № 17/21/31, требования ФСБ, ГОСТы). Соотнесите их с объектами проверки: ПДн, КИИ, госинформсистемы, банковские системы. • В чём разница между «обязательными требованиями» (по приказам регуляторов) и «лучшими практиками» (в т.ч. в ГОСТах)? Как аудитор определяет, что именно подлежит обязательной проверке, а что — рекомендательной оценке? • Каковы ключевые положения приказов ФСТЭК № 17, № 21 и № 31? Выделите по 2–3 критерия из каждого, которые чаще всего становятся точками аудита (например, управление доступом, журналирование, резервное копирование, управление обновлениями). • Какую роль играют ГОСТы в аудите ИБ (например, ГОСТ Р ИСО/МЭК 27001-2021, ГОСТ Р 57580.1-2017)? Сравните: когда ГОСТ — это прямой критерий, а когда — методологическая основа для формирования собственных критериев.	В условиях «ограниченного доступа» (только документы/выгрузки/интервью, без прямого доступа к системам) студенты проверяют соответствие по 2–3 критериям (например, «журналы хранятся 90 дней», «права пересматриваются ежеквартально»). Они запрашивают артефакты, анализируют их на полноту/достоверность, фиксируют ограничения. В конце — мини-отчёт: «по критерию X соответствие подтверждено/не подтверждено/не проверяемо; причина; уровень уверенности». Цель: научиться работать с реальными ограничениями внешнего аудита и корректно фиксировать «не проверяемо». Инструменты: учебные регламенты, выгрузки логов/отчётов, скрипты интервью. Результат: мини-отчёт по 2–3 критериям с обоснованием выводов. 6. Кейс-практикум «Работа с компенсирующими мерами и остаточным риском». Выдаётся кейс: «нельзя отключить SMBv1 на legacy-оборудовании» или «журналирование части систем выполняется в нестандартном формате». Студенты формулируют критерий с учётом компенсирующих мер (сегментация, мониторинг, ограничения доступа), определяют, как



Наименование тем (разделов) дисциплины	Перечень вопросов для обсуждения на семинарах, практических занятиях	Формы проведения занятий
	• Что такое ГОСТ Р 57580.1-2017 и как его используют в аудите финансовых организаций? Разберите уровни соответствия (базовый/стандартный/усиленный) и покажите, как уровень влияет на проверяемые пункты (например, по управлению доступом или мониторингу). • Как соотносятся требования к защите ПДн (152-ФЗ + подзаконные акты) с подходами СУИБ? Выделите 3–4 пересекающихся критерия (журналирование, разграничение доступа, резервное копирование) и объясните, как по одному факту (например, отсутствие логов) можно сделать вывод сразу по нескольким нормативным актам. Блок 3. Международные стандарты и их связь с национальными требованиями • Какие международные стандарты задают методологию и критерии аудита ИБ (ISO/IEC 27001, ISO/IEC 27002, ISO 19011, COBIT)? Сопоставьте их назначение: «что защищать» (27001/27002), «как проверять» (19011), «как управлять ИТ-процессами» (COBIT). • Как «перевести» пункты ISO/IEC 27002 в проверяемые критерии для российской организации? Возьмите один пункт (например, «A.9.2.1 User registration») и покажите цепочку: международный пункт → национальный аналог/	верифицировать их наличие, и оценивают остаточный риск. В конце — краткая запись: «критерий → компенсирующие меры → способ проверки → остаточный риск». Цель: научиться включать компенсирующие меры в критерии и корректно оценивать остаточный риск. Артефакт: запись по 1–2 кейсам с оценкой остаточного риска.



Наименование тем (разделов) дисциплины	Перечень вопросов для обсуждения на семинарах, практических занятиях	Формы проведения занятий
	требование → проверяемый факт → тип свидетельства. - В чём принципиальные отличия акцентов в международных и российских стандартах? Например, ISO делает упор на риск-ориентированный подход и документирование процессов, а российские приказы — на конкретные технические меры и классы защищённости. Как это влияет на чек-листы и формулировки выводов? - Как использовать COBIT в качестве источника критериев аудита? Соотнесите домены COBIT (APO, BAI, DSS, MEA) с процессами ИБ (управление доступом, управление инцидентами, мониторинг) и предложите по 1–2 проверяемых пункта для каждого. Блок 4. Формирование и декомпозиция критериев на практике - Как из одной общей цели ИБ («обеспечить целостность информации») сформировать набор проверяемых критериев? Постройте цепочку из 4–5 пунктов: цель → процесс → подпроцесс → критерий → тип свидетельства (документ/лог/интервью/конфигурация). - Что такое декомпозиция критерия? Разберите пример: «обеспечить управление учётными записями». Декомпозируйте на 5–7 конкретных	



Наименование тем (разделов) дисциплины	Перечень вопросов для обсуждения на семинарах, практических занятиях	Формы проведения занятий
	пунктов (регистрация, отзыв при увольнении, периодический пересмотр, временные учётные записи, привилегированные учётные записи и т.д.) и укажите для каждого тип свидетельства. • Как избежать «ловушек» при формулировании критериев (слишком широко, слишком узко, субъективно)? Сравните «система защищена» vs. «в течение последних 30 дней не было успешных попыток подбора паролей к привилегированным учётным записям; источник — выгрузка Security Log; охват — контроллеры домена». Назовите 3–4 признака «плохого» критерия. • Как учесть компенсирующие меры при формировании критериев? Покажите на кейсе: «нельзя отключить SMBv1 на legacy-оборудовании». Как изменить критерий, чтобы он учитывал компенсирующие меры (сегментация сети, мониторинг, ограничение доступа), и как верифицировать их наличие? Блок 5. Источники свидетельств и их соответствие критериям • Какие источники свидетельств считаются надёжными в аудите ИБ? Сравните по достоверности: устные заявления, регламенты, журналы событий, результаты сканирования, отчёты SIEM, скриншоты, выгрузки конфигураций.	



Наименование тем (разделов) дисциплины	Перечень вопросов для обсуждения на семинарах, практических занятиях	Формы проведения занятий
	В каких случаях один источник не заменяет другой? • Как выбрать тип свидетельства под конкретный критерий? Составьте мини-таблицу для 4–5 критериев (например, «журналы хранятся 90 дней», «права пересматриваются ежеквартально», «антивирус обновлён») с указанием предпочтительного и альтернативного источника. • Как работать с «отсутствием свидетельств» (нет логов, нет отчётов, нет регламентов)? Какие выводы можно и нельзя делать? Приведите корректные формулировки для отчёта («не подтверждено соответствие по критерию X; причина — отсутствие журналов за период Y») vs. некорректные («система не защищена»). • Как документировать свидетельства, чтобы они были допустимы для регуляторов и третьих лиц? Назовите обязательные элементы: источник, период, метод получения, охват, ограничения выборки, контрольные суммы/хэши (при необходимости). Блок 6. Практическая отработка: перевод норм в критерии и чек-листы (для практических занятий) • Кейс 1 (152-ФЗ). Дан фрагмент закона/приказа (например, требование о регистрации событий безопасности при обработке ПДн). Сформулируйте	



Наименование тем (разделов) дисциплины	Перечень вопросов для обсуждения на семинарах, практических занятиях	Формы проведения занятий
	3–4 проверяемых критерия, перечислите ожидаемые свидетельства и составьте 5–6 вопросов для интервью. • Кейс 2 (Приказ ФСТЭК). Возьмите один пункт из приказа ФСТЭК (например, по управлению обновлениями или журналированию). Переведите его в 4–5 пунктов чек-листа с указанием типа свидетельства и способа верификации. • Кейс 3 (ISO/IEC 27002). Выберите один пункт ISO/IEC 27002 (например, A.12.4.1 «Logging operations») и постройте цепочку: пункт стандарта → национальный аналог → проверяемый факт → артефакт → вопрос для интервью. • Кейс 4 (ГОСТ Р 57580.1). Дан уровень соответствия (стандартный) и процесс (управление доступом). Выделите 3–4 критерия, которые будут проверяться, и укажите, какие метрики/артефакты подтвердят соответствие. • Кейс 5 (декомпозиция). Дана цель «обеспечить непрерывность бизнеса». Декомпозируйте её на 5–7 проверяемых пунктов (резервное копирование, тестовые восстановления, план ОНВД, распределение ролей и т. д.), для каждого укажите критерий и тип свидетельства.	



Наименование тем (разделов) дисциплины	Перечень вопросов для обсуждения на семинарах, практических занятиях	Формы проведения занятий
	Блок 7. Приоритизация критериев и оценка рисков • Как приоритизировать критерии аудита в зависимости от профиля организации? Сравните приоритеты для банка (ПДн, непрерывность, транзакции), медучреждения (ПДн, доступность систем) и промышленного предприятия (КИИ, технологическая безопасность). Назовите по 3–4 ключевых критерия для каждого. • Как связать критерий аудита с риском ИБ? Постройте для одного критерия (например, «отсутствие периодического пересмотра прав доступа») цепочку: уязвимость → угроза → сценарий атаки → потенциальный ущерб → влияние на обязательства (закон/договор/сертификация). • Что такое «остаточный риск» в контексте критериев аудита? Покажите, как компенсирующие меры меняют оценку соответствия по критерию, и как это отразить в отчёте. • Как учитывать зрелость процессов при выборе глубины проверки по критериям? Сравните подход к аудиту в организации с «регламентами на бумаге» и в организации с «измеряемыми и улучшаемыми процессами» (по COBIT/NIST).	



Наименование тем (разделов) дисциплины	Перечень вопросов для обсуждения на семинарах, практических занятиях	Формы проведения занятий
	Блок 8. Документирование критериев и результатов проверки • Из каких элементов состоит корректный пункт чек-листа аудита ИБ? Предложите шаблон: «Критерий → Источник нормы → Проверяемый факт → Тип свидетельства → Метод верификации → Допустимый результат». Заполните его на примере одного процесса (например, управление инцидентами). • Как отразить в отчёте несоответствие по критерию так, чтобы вывод был объективным и проверяемым? Сравните «безопасность низкая» vs. «не подтверждено выполнение критерия X (источник нормы); свидетельства отсутствуют/не соответствуют; период — Y; риск — высокий». • Что такое матрица критериев и зачем она нужна? Постройте упрощённую матрицу для одного процесса (управление доступом): строка — критерий, столбцы — источник нормы, тип свидетельства, критичность, способ верификации. • Как адаптировать набор критериев под разные цели аудита (сертификация, проверка регулятором, due diligence, внутренний контроль)? Покажите различия на одном процессе (журналирование) для двух разных целей.	



Наименование тем (разделов) дисциплины	Перечень вопросов для обсуждения на семинарах, практических занятиях	Формы проведения занятий
	Блок 9. Проблемные зоны и типичные ошибки • Какие типичные ошибки допускают при формировании критериев аудита ИБ? Приведите 5–7 примеров «плохих» формулировок и покажите, как их исправить (например, «всё должно быть защищено» → «в течение 30 дней нет успешных брутфорс-попыток к внешним сервисам; источник — SIEM; охват — периметровые узлы»). • В каких случаях смешение требований разных регуляторов/стандартов приводит к противоречивым критериям? Разберите кейс: требования ФСТЭК к классу защищённости vs. ISO/IEC 27001 к риск-ориентированному подходу. Как найти баланс? • Как избежать «аудита ради бумажек» (когда есть регламенты, но нет реальной работы процессов)? Назовите 3–4 метода верификации «живых» процессов (тестовые восстановления, выборочные проверки конфигураций, анализ журналов, симуляции инцидентов). • Какие этические и правовые аспекты нужно учитывать при выборе и применении критериев аудита? Например, ограничения на сбор данных, работа с чувствительной информацией, корректность ссылок на НПА.	



Наименование тем (разделов) дисциплины	Перечень вопросов для обсуждения на семинарах, практических занятиях	Формы проведения занятий
Стандарты по аудиту информационной безопасности.	Блок 1. Семейство стандартов ISO/IEC 27000 и их назначение В чём разница между ISO/IEC 27001, 27002, 27005, 27007 и ISO 19011? Соотнесите каждый стандарт с его «ролью» (требования, практики, риски, аудит, методология проверок) и приведите по одному примеру, когда аудитор опирается именно на этот документ. Как цикл PDCA (Plan-Do-Check-Act) реализован в ISO/IEC 27001? Разберите на примере одного процесса (например, управление доступом или управление инцидентами), какие пункты стандарта соответствуют каждому этапу цикла. Что такое «применимость» (statement of applicability, SoA) в ISO/IEC 27001 и как она влияет на область аудита? Как аудитор проверяет корректность исключений в SoA (обоснование, документирование, контроль рисков)? Какую роль в аудите ИБ играют метрики (ISO/IEC 27004)? Приведите 3–4 примера метрик для разных процессов (журналирование, управление уязвимостями, обучение пользователей) и объясните, как по ним можно судить об эффективности СУИБ. Почему для проведения аудита недостаточно «просто знать ISO 27002»? Покажите на примере, как ISO 27007 и ISO 19011 задают методы и принципы сбора свидетельств, без которых выводы по 27002 будут субъективными.	1. Семинар-сопоставление «Семейство ISO/IEC 27000: назначение каждого стандарта». Студентам заранее дают список стандартов семейства (ISO/IEC 27000, 27001, 27002, 27004, 27005, 27006, 27007, 19011) и короткие выдержки. На занятии группы распределяют стандарты по ролям («методология», «требования к СУИБ», «практические меры», «оценка и метрики», «риски», «аудит», «аккредитация») и строят мини-схему «кто для кого»: например, «27001 задаёт требования → 27002 даёт практики → 27007 и 19011 задают, как проверять». В конце — общая схема и обсуждение, как это влияет на план аудита. Цель: перестать путать стандарты семейства и научиться подбирать нужный под задачу (сертификация, оценка эффективности, проведение аудита). Артефакт: схема ролей стандартов + список «какой стандарт брать под какую цель аудита». 2. Разбор принципов аудита по ISO 19011. Преподаватель раздаёт короткие кейсы-миниатюры, где нарушены принципы аудита (независимость, объективность, конфиденциальность, риск-ориентированность, должная осмотрительность). Студенты в малых группах определяют, какой принцип затронут, как это искажает результаты и как предотвратить. Затем — сводная таблица «принцип → типичное нарушение → способ минимизации».



Наименование тем (разделов) дисциплины	Перечень вопросов для обсуждения на семинарах, практических занятиях	Формы проведения занятий
	Блок 2. Принципы и методология аудита по международным стандартам Назовите ключевые принципы аудита по ISO 19011 (независимость, объективность, конфиденциальность, должная осмотрительность, риск-ориентированность). Разберите 2–3 кейса, где нарушение одного из принципов искажает результаты (например, «аудитор одновременно внедряет СЗИ», «выводы сделаны по устным заявлениям без артефактов»). Что означает «риск-ориентированный подход» в аудите ИБ? Сравните сценарий аудита для стартапа (низкий уровень риска, фокус на критических активах) и банка (высокий уровень риска, детальная проверка процессов). Как меняются критерии и глубина проверки? Какие методы сбора свидетельств регламентирует ISO 27007? Сопоставьте методы (интервью, анализ документов, наблюдение, выборочная проверка конфигураций/логов) с уровнем достоверности и рисками подмены. Как в рамках стандартов обосновать «ограничения аудита» (например, нет доступа к логам за прошлый год, нет прав на пентест, часть систем — в облаке)? Как зафиксировать это в плане и отчёте, чтобы выводы оставались объективными? Что значит «достаточность свидетельств» по ISO 19011? Разберите кейс: «администраторы утверждают, что права	Цель: закрепить принципы как основу методологии аудита, а не как «красивые слова». Результат: таблица принципов с практическими примерами нарушений и мер. 3. Семинар «Структура и логика ISO/IEC 27001: от контекста до непрерывного улучшения». Группа последовательно разбирает разделы стандарта по циклу PDCA: «Контекст организации» → «Лидерство/ Политика» → «Планирование (риски/цели)» → «Поддержка/Ресурсы» → «Операции» → «Оценка результатов» → «Улучшение». Для каждого блока студенты формулируют 2–3 вопроса аудитора и 1–2 типа свидетельств. В конце — карта аудита по разделам стандарта. Цель: увидеть стандарт как целостную систему, а не набор отдельных мер. Артефакт: карта аудита: раздел стандарта → вопросы → свидетельства. 4. Дискуссия «Риск-ориентированный подход в стандартах: как это меняет аудит». Сравниваются два подхода: «проверка по чек-листу без учёта контекста» vs. «риск-ориентированный аудит» (ISO 27005 + ISO 19011). Даются 2–3 кейса (стартап, банк, промышленное предприятие). Студенты обсуждают, как меняется область, глубина и критерии аудита в зависимости от уровня риска.



Наименование тем (разделов) дисциплины	Перечень вопросов для обсуждения на семинарах, практических занятиях	Формы проведения занятий
	пересматриваются ежеквартально». Какие артефакты и выборки нужны, чтобы подтвердить соответствие? Блок 3. Национальные стандарты и адаптации: связь с ISO Каковы ключевые отличия и точки пересечения ГОСТ Р ИСО/МЭК 27001-2021 и оригинального ISO/IEC 27001? В каких случаях ГОСТ становится обязательным ориентиром, а в каких — методической основой? Какую роль играет ГОСТ Р 57580.1-2017 в аудите финансовых организаций? Выделите 3–4 критерия из этого стандарта, которые часто пересекаются с ISO/IEC 27002 (например, журналирование, управление доступом, мониторинг), и покажите, как они проверяются по-разному (уровень детализации, метрики, охват). Как российские отраслевые/регуляторные требования (приказы ФСТЭК, требования ФСБ, 152-ФЗ, 187-ФЗ) соотносятся с международными стандартами? Постройте цепочку для одного процесса: «требование регулятора → пункт ISO/ГОСТ → проверяемый факт → тип свидетельства». В каких ситуациях аудитор опирается на национальные профили защиты или методические документы регуляторов вместо «чистого» ISO? Приведите 2–3 примера (КИИ, госсинформсистемы, платёжные системы). Как избежать конфликта требований (например, жёсткие технические меры по ФСТЭК vs. гибкость	Цель: понять, что стандарты требуют приоритизации и адаптации под риски, а не «проверить всё подряд». Результат: мини-выводы «для организации с высоким/низким риском фокус аудита смещается на...». 5. Круглый стол «Национальные адаптации и отраслевые профили: ГОСТы и их связь с ISO». Разбираются ГОСТ Р ИСО/МЭК 27001-2021, ГОСТ Р 57580.1-2017 (финсектор), профильные документы по КИИ/госсистемам. Группы определяют: статус (рекомендация/обязательность), ключевые отличия от ISO, как пункты стандарта превращаются в проверяемые факты в российской практике. Цель: научиться «переводить» международные требования в российские критерии и понимать, когда ГОСТ — это норма, а когда — методика. Артефакт: таблица «стандарт/ГОСТ → статус → ключевые критерии → способы верификации». 6. Практикум «Формирование чек-листа на основе ISO/IEC 27007 и ISO 19011». Студенты берут один процесс (например, управление доступом или управление инцидентами) и, опираясь на ISO 27007 (методы сбора свидетельств) и ISO 19011 (принципы), формируют фрагмент чек-листа: «цель проверки → критерий (ссылка на ISO) → метод (интервью/документ/лог/конфигурация) → допустимый результат → риск при несоответствии». Затем группы обмениваются и



Наименование тем (разделов) дисциплины	Перечень вопросов для обсуждения на семинарах, практических занятиях	Формы проведения занятий
	риск-ориентированного подхода ISO)? Какие аргументы и артефакты помогают обосновать выбор критериев в отчёте? Блок 4. Перевод стандартов в проверяемые критерии и чек-листы Как из пункта ISO/IEC 27002 сделать проверяемый критерий аудита? Возьмите один пункт (например, A.9.2.1 «User registration» или A.12.4.1 «Logging operations») и постройте цепочку: «пункт стандарта → проверяемый факт → период → охват → тип свидетельства → допустимый результат». Чем «хороший» критерий аудита отличается от «плохого»? Сравните формулировки: «система защищена» vs. «за последние 30 дней не было успешных попыток подбора паролей к привилегированным учётным записям; источник — выгрузка Security Log; охват — контроллеры домена». Назовите 4–5 признаков корректного критерия. Как декомпозировать процесс ИБ (например, «управление инцидентами») на 6–8 проверяемых пунктов чек-листа с опорой на ISO/IEC 27002 и ISO 27007? Для каждого пункта укажите метод верификации и ожидаемый артефакт. Как учесть компенсирующие меры при формировании критериев? Разберите кейс: «нельзя отключить SMBv1 на legacy-оборудовании». Сформулируйте критерий с учётом компенсирующих мер (сегментация, мониторинг, ограничения доступа) и опишите, как их верифицировать.	проводят «перекрёстную рецензию». Цель: научиться строить чек-лист, который соответствует методологии аудита, а не просто «список вопросов». Инструменты: выдержки из ISO 27007/19011, шаблоны чек-листов. Результат: фрагмент чек-листа из 6–8 пунктов с обоснованием методов. 7. Кейс-практикум «Проведение аудиторской беседы по скрипту ISO». Работа в тройках: «аудитор», «владелец процесса», «наблюдатель». Аудитор использует вопросы, построенные по логике ISO (открытые, уточняющие, направленные на свидетельство). Владелец опирается на упрощённую модель процесса и может давать общие ответы. Наблюдатель оценивает: заданы ли уточняющие вопросы, запрошены ли артефакты, зафиксированы ли противоречия. Цель: отработать технику интервью согласно принципам аудита (объективность, достаточность свидетельств). Критерии успеха: переход от «всё хорошо» к «вот конкретный артефакт/период/охват». Результат: протокол 1 интервью с разбором ошибок и улучшений. 8. Воркшоп «Матрица соответствия: стандарты → критерии → свидетельства». Студенты формируют матрицу для одного процесса (например, управление инцидентами): строки — критерии



Наименование тем (разделов) дисциплины	Перечень вопросов для обсуждения на семинарах, практических занятиях	Формы проведения занятий
	Как связать критерий аудита с риском и последствиями? Постройте для одного критерия (например, «отсутствие периодического пересмотра прав доступа») цепочку: «уязвимость → угроза → сценарий атаки → потенциальный ущерб → влияние на соответствие ISO/НПА». Блок 5. Планирование аудита по стандартам Какие элементы обязательно должны быть в плане аудита по ISO 19011? Составьте мини-шаблон: «область → критерии → методы → ресурсы → график → риски проекта → контрольные точки». Как определить область аудита под разные цели (сертификация ISO 27001, проверка соответствия 152-ФЗ, due diligence перед M&A)? Покажите различия на одном процессе (журналирование событий) для двух разных целей. Как приоритизировать критерии аудита в зависимости от контекста организации? Сравните приоритеты для банка, медучреждения и промышленного предприятия: назовите по 3–4 ключевых критерия для каждого и обоснуйте выбор ссылками на стандарты/НПА. Как спланировать выборку свидетельств (sample size, период, охват) так, чтобы она была репрезентативной? Разберите пример: «проверка журналов безопасности для 500 серверов». Какой объём выборки и критерии отбора допустимы, чтобы вывод был объективным?	(из ISO 27001/27002/19011), столбцы — источник нормы, тип свидетельства, метод верификации, критичность, метрика успеха. Затем обсуждают, как эта матрица превращается в чек-лист и план работ. Цель: систематизировать критерии и увидеть связи между нормами, свидетельствами и методами проверки. Результат: заполненная матрица критериев.



Наименование тем (разделов) дисциплины	Перечень вопросов для обсуждения на семинарах, практических занятиях	Формы проведения занятий
	Как зафиксировать «не проверяемо» в плане и отчёте? Приведите корректные формулировки, которые соответствуют ISO 19011 и не снижают доверие к отчёту. Блок 6. Сбор и оценка свидетельств по стандартам Какие источники свидетельств считаются надёжными в рамках ISO 19011? Сравните по достоверности: устные заявления, регламенты, журналы событий, результаты сканирования, отчёты SIEM, скриншоты, загрузки конфигураций. В каких случаях один источник не заменяет другой? Как работать с «отсутствием свидетельств» (нет логов, нет отчётов, нет регламентов)? Какие выводы можно и нельзя делать? Приведите корректные формулировки для отчёта («не подтверждено соответствие по критерию X; причина — отсутствие журналов за период Y») vs. некорректные («система не защищена»). Как документировать свидетельства, чтобы они были допустимы для регуляторов и третьих лиц? Назовите обязательные элементы: источник, период, метод получения, охват, ограничения выборки, контрольные суммы/хэши (при необходимости). Как оценить «свежесть» и «репрезентативность» свидетельств? Разберите кейс: «предоставлен отчёт о пересмотре прав за текущий квартал, но нет данных за прошлые периоды». Как это влияет на уровень уверенности аудитора?	



Наименование тем (разделов) дисциплины	Перечень вопросов для обсуждения на семинарах, практических занятиях	Формы проведения занятий
	Как верифицировать «живые» процессы, а не «бумажную» безопасность? Назовите 3–4 метода (выборочные проверки конфигураций, анализ журналов, тестовые восстановления, симуляции инцидентов) и соотнесите их с требованиями ISO 27007.	
Методы тестирования информационной безопасности.	Блок 1. Классификация и место методов тестирования в системе ИБ 1. Чем тестирование ИБ отличается от аудита ИБ? Сравните по целям, глубине, методам и формату результатов (например, «аудит проверяет соответствие требованиям», «тестирование проверяет реальную устойчивость к атакам»). 2. Как соотносятся понятия «тестирование на проникновение», «оценка уязвимостей», «анализ конфигурации», «социальный инжиниринг» и «тестирование непрерывности бизнеса»? Постройте матрицу: «метод → цель → глубина → риски для бизнеса → итоговый артефакт». 3. По каким критериям выбирают метод тестирования под задачу (M&A, сертификация, инцидент, запуск новой системы)? Приведите 3–4 сценария и обоснуйте выбор метода для каждого. 4. Как методы тестирования вписываются в цикл PDCA (Plan-Do-Check-Act) и в этапы SDLC? Покажите на примере веб-приложения: какие тесты уместны на этапе проектирования, разработки, приёмки и эксплуатации.	1. Семинар-сопоставление «Карта методов тестирования ИБ». Студентам заранее выдают названия методов (пентест, сканирование уязвимостей, SAST/DAST, социальный инжиниринг, tabletop-учения BC/DR). На занятии мини-группы заполняют матрицу: «метод → цель → глубина → риски для бизнеса → типовой артефакт → релевантные стандарты (NIST SP 800-115, PCI DSS, PTES и т.д.)». В конце — сводная карта и обсуждение, почему «один метод не подходит всем задачам». Цель: перестать смешивать методы и научиться выбирать под задачу. Артефакт: заполненная матрица методов + мини-выводы «когда что применять». 2. Разбор стандартов и «правил игры»: NIST SP 800-115, PTES, OSSTMM. Группы получают по одному стандарту/гайду и готовят 5–7-минутную презентацию: «что регламентирует → какие этапы задаёт → как это влияет на план и отчёт». Затем общий разбор: что общего в этапах разведки/сканирования/эксплуатации/отчётности и где различия в акцентах.



Наименование тем (разделов) дисциплины	Перечень вопросов для обсуждения на семинарах, практических занятиях	Формы проведения занятий
	5. Какова роль тестирования ИБ в риск-ориентированном подходе (ISO 27005)? Постройте цепочку: «актив → угроза → уязвимость → метод тестирования → метрика успеха». Блок 2. Тестирование на проникновение (пентест): подходы, границы, этика 6. В чём разница между подходами «чёрный ящик», «серый ящик» и «белый ящик»? Разберите на кейсе веб-приложения: как меняется план, сроки, стоимость и глубина проверки для каждого подхода. 7. Какие ограничения и «правила игры» обязательно фиксируют в рамках пентеста (scope, stop conditions, часы работ, недопустимые действия)? Приведите 5–7 примеров ограничений и объясните, зачем они нужны. 8. Каковы ключевые этапы пентеста по PTES/OSSTMM/NIST SP 800-115? Сопоставьте этапы (разведка, сканирование, эксплуатация, пост-эксплуатация, отчётность) с артефактами и рисками «перешагивания границ». 9. Как отличить легальный пентест от атаки с точки зрения права и ИБ-процессов? Назовите 3–4 обязательных документа и условия, которые превращают «взлом» в «тестирование». 10. Какие этические и операционные риски несёт пентест? Разберите кейс: «в ходе теста упал критичный сервис». Что должно быть в плане для минимизации ущерба? Блок 3. Оценка уязвимостей и анализ конфигураций	Цель: увидеть, что «пентест по стандарту» — это не «взлом ради демонстрации», а процесс с границами и воспроизводимостью. Результат: сравнительная таблица этапов по стандартам + список «обязательных артефактов» (scope, stop conditions, NDA). 3. Дискуссия «Границы и этика тестирования: где заканчивается тест и начинается атака». Обсуждаются кейсы: «в ходе пентеста упал критичный сервис», «при сканировании с учётными данными администратор случайно удалил лог», «фишинг вызвал панику». Студенты в ролях «юрист», «ИБ-директор», «пентестер», «бизнес-заказчик» аргументируют границы допустимого и формулируют стоп-условия. Цель: понять, что юридическая и операционная безопасность — часть методологии. Артефакт: список из 8–10 обязательных пунктов «правил игры» (договор, scope, часы работ, недопустимые действия, план отката, порядок эскалации). 4. Семинар «Риск-ориентированный выбор методов». Даны 3–4 профиля организаций (интернет-банк, промышленное предприятие, SaaS-провайдер, медучреждение). Группы определяют топ-3 вектора угроз и под них выбирают методы тестирования, обосновывая выбор через вероятность/ущерб. В конце — общая дискуссия: почему для одних критичен пентест, для других



Наименование тем (разделов) дисциплины	Перечень вопросов для обсуждения на семинарах, практических занятиях	Формы проведения занятий
	11. В чём принципиальная разница между «сканированием уязвимостей» и «оценкой уязвимостей»? Сравните по глубине, точности, ложным срабатываниям и требуемым ресурсам. 12. Как работают сканеры уязвимостей (Nessus, OpenVAS, Qualys)? Назовите 3–4 ключевые технологии (баннер-граббинг, проверка версий, активные тесты, учётные данные для аудита) и их влияние на достоверность результатов. 13. Что такое «базовая оценка уязвимости» по CVSS и как её используют при приоритизации? Разберите пример: уязвимость с высоким CVSS, но низким риском для конкретной организации. Почему она может быть не приоритетной? 14. Как анализ конфигураций (compliance scanning) дополняет оценку уязвимостей? Сравните инструменты (OpenSCAP, Ansible Audit, встроенные отчёты SCCM/Intune) по охвату (ОС, СУБД, сетевое оборудование) и формату отчётов. 15. Как избежать «паралича отчётами» (когда сканер выдаёт тысячи уязвимостей)? Назовите 4–5 методов приоритизации (критичность актива, доступность извне, наличие эксплойта, бизнес-влияние) и покажите на мини-кейсе. Блок 4. Динамическое и статическое тестирование ПО (DAST и SAST)	— аудит конфигураций и BC/DR. Цель: уйти от «проверять всё подряд» к приоритизации по рискам. Результат: матрица «профиль → вектор угрозы → метод тестирования → метрика успеха». 5. Круглый стол «SAST/DAST/IAST в SDLC: где и зачем встраивать». Студенты разбирают этапы SDLC (проектирование, разработка, приёмка, эксплуатация) и для каждого определяют уместные методы, инструменты и метрики (порог fail/warn, охват, время). Обсуждают компромиссы: «точность vs скорость», «интеграция vs накладные расходы». Цель: научиться встраивать тестирование ИБ в разработку, а не делать «в конце». Артефакт: мини-схема пайплайна CI/CD с точками SAST/DAST и критериями качества. 6. Семинар «Социальный инжиниринг: безопасность теста важнее результата». Разбираются техники (фишинг, «забытая флешка», вишинг) и этические ограничения. Группы формулируют правила безопасного проведения (предварительное уведомление, исключение публичных наказаний, обучение сразу после теста, анонимность, порядок обратной связи). В конце — проект «уведомления для сотрудников» и «письма-приглашения на обучение».



Наименование тем (разделов) дисциплины	Перечень вопросов для обсуждения на семинарах, практических занятиях	Формы проведения занятий
	16. В чём ключевые отличия SAST и DAST (анализ исходного кода vs анализ работающего приложения)? Сопоставьте по времени внедрения, точности, типам выявляемых уязвимостей, интеграции в CI/CD. 17. Когда оправдано IAST (Interactive Application Security Testing) и RASP (Runtime Application Self-Protection)? Сравните с SAST/DAST по стоимости, накладным расходам и применимости в разных стадиях SDLC. 18. Как интегрировать SAST/DAST в пайплайн разработки? Постройте мини-схему: «коммит → сборка → SAST → тест → DAST → релиз» и укажите, какие метрики (порог fail/warn, время, охват) можно использовать. 19. Какие типы уязвимостей лучше всего выявляет каждый метод (SAST: логические ошибки, небезопасные вызовы; DAST: проблемы аутентификации, инъекции на уровне HTTP)? Приведите по 2–3 примера для каждого. 20. В чём специфика тестирования мобильных приложений? Назовите 3–4 дополнительных вектора (root/jailbreak, межпроцессное взаимодействие, хранение данных) и соответствующие методы проверки. Блок 5. Социальный инжиниринг и проверка осведомлённости пользователей 21. Какие техники социального инжиниринга чаще всего используют в тестах (фишинг, вишинг, претекстинг, «забытая флешка»)? Сопоставьте технику с целью	Цель: показать, что цель теста осведомлённости — не «поймать», а научить. Результат: шаблон уведомления + список метрик эффективности (процент кликов, время реакции, доля сообщений в ИБ). 7. Разбор «паралича отчётами»: как приоритизировать уязвимости. Студентам дают выгрузку сканера (упрощённую) с 15–20 находками. Задача — отфильтровать по контексту: критичность актива, доступность извне, наличие эксплойта, бизнес-влияние. В конце — мини-презентация «топ-5 приоритетных уязвимостей» с обоснованием. Цель: освоить приоритизацию «CVSS + контекст», а не «только CVSS». Артефакт: топ-5 уязвимостей с цепочкой «уязвимость → вектор → потенциальный ущерб → рекомендация». 8. Практикум «Оформление отчёта: от сырых данных к выводам». Студентам дают фрагменты отчётов сканеров, логи, скриншоты. Задача — перевести их в формат «критерий → факт → свидетельство → вывод → риск → рекомендация (действие/срок/ответственный/метрика)». В конце — перекрёстная рецензия: «что субъективно, чего не хватает для объективности». Цель: освоить язык отчётности, соответствующий



Наименование тем (разделов) дисциплины	Перечень вопросов для обсуждения на семинарах, практических занятиях	Формы проведения занятий
	(получение пароля, запуск вредоноса, физический доступ) и признаками успешной атаки. 22. Как безопасно и этично проводить тесты осведомлённости без демотивации сотрудников? Назовите 5–7 правил (предварительное информирование, исключение публичных наказаний, обучение сразу после теста, анонимность, фокус на навыках). 23. Как измерять эффективность программ обучения через тесты осведомлённости? Приведите 3–4 метрики (процент кликов, время реакции, доля тех, кто сообщил в ИБ) и объясните, как их использовать для улучшения программы. 24. Как юридически оформить тесты осведомлённости, чтобы избежать конфликтов? Назовите обязательные элементы (согласие/уведомление, порядок обработки персональных данных, план обратной связи). 25. Разберите кейс «фишинговая рассылка по сотрудникам». Какие критерии успеха/неудачи корректны с точки зрения ИБ и HR? Как формулировать выводы без обвинений? Блок 6. Тестирование инфраструктуры, сетей и оборудования 26. Какие методы используют для тестирования сетевой безопасности (пассивный мониторинг, активное сканирование, анализ правил МЭ, проверка маршрутизации)? Сопоставьте методы с целями (обнаружение «теневых» устройств, проверка сегментации, поиск открытых портов).	стандартам. Результат: 3–4 фрагмента отчёта в корректном формате.



Наименование тем (разделов) дисциплины	Перечень вопросов для обсуждения на семинарах, практических занятиях	Формы проведения занятий
	27. Что проверяют при тестировании сетевого оборудования (маршрутизаторы, коммутаторы, МЭ)? Выделите 3–4 критических направления (учётные записи, логирование, ACL, резервные конфигурации) и способы верификации. 28. Как тестируют сегментацию сети и «привилегированные зоны»? Приведите 2–3 сценария (перекрёстный доступ между VLAN, обход DMZ, горизонтальное перемещение) и методы их проверки. 29. Как проверить устойчивость инфраструктуры к отказам (resilience)? Сопоставьте методы (отключение канала, отказ ЦОД, «шум» в сети) с метриками (RTO/RPO, время переключения, полнота бэкапов). 30. В чём специфика тестирования облачных сред (AWS/Azure/GCP)? Назовите 3–4 уникальных вектора (IAM-политики, публичные бакеты, неправильные группы безопасности) и инструменты (Prowler, ScoutSuite, CloudSploit). Блок 7. Тестирование непрерывности и устойчивости (BC/DR) 31. Чем отличаются «столовая» (tabletop), «симуляция» и «полное переключение» (failover) в тестировании BC/DR? Сопоставьте тип теста с затратами, рисками и глубиной проверки. 32. Какие метрики используют для оценки готовности BC/DR (RTO, RPO, MTTR, процент покрытия критичных	



Наименование тем (разделов) дисциплины	Перечень вопросов для обсуждения на семинарах, практических занятиях	Формы проведения занятий
	сервисов)? Постройте мини-пример расчёта для веб-сервиса. 33. Как включать ИБ-аспекты в тесты BC/DR (целостность бэкапов, защита ключей шифрования, доступность журналов, безопасность резервных площадок)? Назовите 3–4 контрольные точки. 34. Разберите кейс: «после аварии часть бэкапов не восстановилась». Какие методы тестирования могли бы это выявить заранее? Как оформить вывод и рекомендацию?	



6. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине

6.1. Перечень вопросов, отводимых на самостоятельное освоение дисциплины, формы внеаудиторной самостоятельной работы

Наименование тем (разделов) дисциплины	Перечень вопросов, отводимых на самостоятельное освоение	Формы внеаудиторной самостоятельной работы
Аудит информационной безопасности. Правовые и методологические основы аудита ИБ. Основные понятия.	1. Дайте определение аудита информационной безопасности (ИБ). В чем заключается его основная цель и какие задачи он решает? 2. Какие существуют основные виды аудита ИБ (внешний, внутренний, комплексный) и каковы их ключевые различия? 3. Перечислите и охарактеризуйте основные этапы жизненного цикла проведения аудита ИБ. 4. Какова роль международных стандартов (серия ISO/IEC 27000, COBIT, NIST) в методологии аудита ИБ? 5. Какие требования к организации и проведению аудита ИБ устанавливает международный стандарт ISO/IEC 27007? 6. В чем заключается разница между аудитом и аттестацией информационной системы? 7. Какие существуют подходы к оценке рисков в рамках аудита ИБ (качественный, количественный, смешанный) и каковы их преимущества и недостатки? 8. Какова роль и содержание политики информационной безопасности организации в	- работа с учебной, научной и справочной литературой; - подготовка докладов; - подготовка презентаций



Наименование тем (разделов) дисциплины	Перечень вопросов, отводимых на самостоятельное освоение	Формы внеаудиторной самостоятельной работы
	контексте проведения аудита? 9. Что такое критерии аудита, область аудита и как они определяются при планировании проверки? 10. Каковы основные принципы независимости и объективности аудитора ИБ? Почему они критически важны для результата проверки?	
Процессы проверки системы обеспечения ИБ	1. Опишите методологию сбора аудиторских доказательств. Какие методы (интервью, наблюдение, анализ документов, тестирование) используются наиболее часто? 2. Как классифицируются несоответствия (наблюдения), выявляемые в ходе аудита? Приведите примеры. 3. Какова структура типового аудиторского отчета по информационной безопасности? Какие разделы он должен содержать? 4. Каковы правовые основы проведения аудита ИБ в Российской Федерации? Назовите ключевые федеральные законы. 5. Каким образом Федеральный закон № 152-ФЗ «О персональных данных» влияет на требования к проведению аудита ИБ в организациях-операторах ПДн? 6. Каковы обязанности аудитора по соблюдению конфиденциальности информации, полученной в	- работа с учебной, научной и справочной литературой; - подготовка докладов; - подготовка презентаций



Наименование тем (разделов) дисциплины	Перечень вопросов, отводимых на самостоятельное освоение	Формы внеаудиторной самостоятельной работы
	ходе проверки? Как регулируется этот вопрос? 7. Что такое самооценка (самоаудит) информационной безопасности? В каких случаях она применяется и каковы её ограничения? 8. Опишите процесс мониторинга и контроля выполнения рекомендаций, выданных по результатам аудита ИБ. 9. Каковы квалификационные требования к специалистам по аудиту ИБ (образование, опыт работы, наличие сертификатов)? 10. Каким образом результаты аудита ИБ используются для совершенствования системы управления информационной безопасностью (СУИБ) организации?	
Внешний аудит информационной безопасности	1. Что такое внешний аудит информационной безопасности (ИБ) и каковы его ключевые отличия от внутреннего аудита? 2. Какие основные цели и задачи преследует организация, привлекая внешних аудиторов для проверки своей системы ИБ? 3. Перечислите и охарактеризуйте основные этапы проведения внешнего аудита ИБ: от инициации до подготовки итогового отчета. 4. Каковы критерии выбора внешней аудиторской организации? На что следует обращать внимание	- работа с учебной, научной и справочной литературой; - подготовка докладов; - подготовка презентаций



Наименование тем (разделов) дисциплины	Перечень вопросов, отводимых на самостоятельное освоение	Формы внеаудиторной самостоятельной работы
	при заключении договора? 5. Как определяется и согласовывается область (границы) внешнего аудита ИБ? Что такое «существенность» в контексте аудита? 6. Каким образом обеспечивается независимость и объективность внешнего аудитора? Какие существуют механизмы для предотвращения конфликта интересов? 7. Какие международные стандарты и методологии (например, ISO/IEC 27001, SOC 2, PCI DSS) чаще всего используются в качестве основы для внешнего аудита ИБ? 8. Опишите основные методы сбора аудиторских доказательств, применяемые внешними аудиторами: интервью, наблюдение, анализ документации, техническое тестирование. 9. Что такое penetration testing (тестирование на проникновение) и какова его роль в рамках внешнего аудита ИБ? Чем оно отличается от сканирования уязвимостей? 10. Каковы типичные подходы к оценке рисков в ходе внешнего аудита? Как аудитор оценивает вероятность и последствия реализации угроз?	



Наименование тем (разделов) дисциплины	Перечень вопросов, отводимых на самостоятельное освоение	Формы внеаудиторной самостоятельной работы
Национальные стандарты управления информационной безопасностью.	1. Какова структура и содержание итогового аудиторского отчета? Какие разделы он должен включать (например, описание области, методология, выявленные несоответствия, рекомендации)? 2. Как классифицируются и описываются несоответствия (findings) в отчете внешнего аудита? Приведите примеры критических, существенных и незначительных замечаний. 3. Каковы правовые аспекты проведения внешнего аудита ИБ в России, включая вопросы конфиденциальности информации и ответственности сторон? 4. Как оформляется и передается аудиторское заключение? В чем разница между немодифицированным и модифицированным заключением? 5. Каков порядок взаимодействия между проверяемой организацией и внешними аудиторами в процессе проведения проверки? 6. Что такое «период наблюдения» (remediation period) после завершения основного этапа аудита и как он проходит? 7. Каковы квалификационные требования к внешним аудиторам ИБ? Какую роль играют	- работа с учебной, научной и справочной литературой; - подготовка докладов; - подготовка презентаций



Наименование тем (разделов) дисциплины	Перечень вопросов, отводимых на самостоятельное освоение	Формы внеаудиторной самостоятельной работы
	профессиональные сертификации (CISA, CISSP, ISO 27001 Lead Auditor)? 8. Опишите процесс мониторинга выполнения рекомендаций, выданных по результатам внешнего аудита. 9. Как часто рекомендуется проводить внешний аудит ИБ и от каких факторов зависит периодичность проверок? 10. Как результаты внешнего аудита ИБ используются для совершенствования системы управления информационной безопасностью (СУИБ) и повышения доверия со стороны клиентов и партнеров?	
Стандарты по аудиту информационной безопасности.	1. Что такое критерии аудита информационной безопасности (ИБ) и какова их роль в процессе проведения проверки? 2. Как соотносятся между собой критерии аудита, свидетельства аудита и выводы аудита? 3. Перечислите основные типы критериев аудита ИБ (регуляторные, законодательные, договорные, общепринятые практики) и приведите примеры для каждого типа. 4. Что такое «область аудита» и как она влияет на определение применимых критериев? 5. Каковы основные цели и область применения международного стандарта ISO/IEC 27007 «Руководящие	- работа с учебной, научной и справочной литературой; - подготовка докладов; - подготовка презентаций



Наименование тем (разделов) дисциплины	Перечень вопросов, отводимых на самостоятельное освоение	Формы внеаудиторной самостоятельной работы
	указания по аудиту систем менеджмента информационной безопасности»? 6. В чем заключается ключевое различие между стандартом ISO/IEC 27007 (руководство по аудиту СУИБ) и стандартом ISO/IEC 27001 (требования к СУИБ)? 7. Как стандарт ISO/IEC 27007 определяет принципы проведения аудита, такие как независимость, объективность и компетентность? 8. Опишите структуру и основное содержание стандарта ISO 19011 «Руководящие указания по аудиту систем менеджмента». Почему он является основополагающим для аудита ИБ? 9. Что такое отчёты SOC (Service Organization Control) типов SOC 1, SOC 2 и SOC 3? В чём их различия и для каких целей они используются при внешнем аудите? 10. Какие критерии доверия (Trust Services Criteria) лежат в основе отчёта SOC 2? Опишите каждый из них: безопасность, доступность, целостность обработки, конфиденциальность, приватность.	
Методы тестирования информационной безопасности.	1. Что такое тестирование на проникновение (Penetration Testing) и каковы его основные цели в рамках аудита информационной безопасности? 2. В чём заключается разница между сканированием уязвимостей (Vulnerability Scanning) и тестированием на проникновение с точки зрения методологии и глубины анализа?	- работа с учебной, научной и справочной литературой; - подготовка докладов; - подготовка презентаций



Наименование тем (разделов) дисциплины	Перечень вопросов, отводимых на самостоятельное освоение	Формы внеаудиторной самостоятельной работы
	3. Опишите «социотехническое тестирование» (Social Engineering Testing). Какие методы (например, фишинг, претекстинг) используются для проверки «человеческого фактора»? 4. Что такое «тестирование на проникновение методом «белого ящика» (White Box) и в каких случаях его применение наиболее эффективно по сравнению с «чёрным ящиком» (Black Box) и «серым ящиком» (Grey Box)? 5. Какова роль и содержание «отчёта о тестировании на проникновение» (Penetration Test Report)? Какие ключевые разделы он должен включать? 6. Что такое «тестирование безопасности веб-приложений» и какие специализированные методы (например, SQL-инъекция, XSS) применяются для выявления уязвимостей? 7. Опишите метод «тестирования на обход системы защиты» (Bypass Security Controls testing). Приведите примеры техник обхода сетевых экранов или систем обнаружения вторжений. 8. Что такое «тестирование на отказ в обслуживании» (Denial of Service / DoS Testing) и каковы его цели, риски и ограничения при проведении в рамках аудита? 9. Каковы методологические различия между статическим (SAST) и динамическим (DAST) анализом безопасности приложений? В чём их преимущества и недостатки? 10. Какова процедура и цели «тестирования на восстановление» (Recovery Testing) в контексте обеспечения	



Наименование тем (разделов) дисциплины	Перечень вопросов, отводимых на самостоятельное освоение	Формы внеаудиторной самостоятельной работы
	непрерывности бизнеса и послеаварийного восстановления (Disaster Recovery)?	



6.2. Перечень вопросов, заданий, тем для подготовки к текущему контролю

Примерный перечень вопросов для подготовки к контрольной работе:

1. Что является главной целью системы обеспечения ИБ?
2. Назовите основные задачи системы обеспечения ИБ.
3. Какие виды угроз ИБ встречаются наиболее часто? Приведите примеры источников угроз.
4. Опишите основные модули модели угроз ИБ согласно «Методике оценки угроз безопасности информации» ФСТЭК.
5. Назвать основные компоненты модели построения системы ИБ.
6. С какой целью разрабатывается политика ИБ?
7. Из каких разделов состоит политика ИБ?
8. В чем отличие и особенности проведения внешнего и внутреннего аудита?
9. Назовите основные цели проведения аудита ИБ.
10. Какая последовательность действий при проведении аудита ИБ на предприятии?
11. Чем определяются масштабы аудита ИБ?
12. С какой целью проводится анализ рисков?
13. Назовите задачи, решаемые при анализе рисков.
14. Как может быть оценена величина риска?
15. Какие этапы включает сценарий анализа информационных ресурсов?
16. По каким показателям проводится оценивание информационных рисков?
17. Какие практические подходы используются при проведении аудита ИБ?
18. Назовите задачи аудита ИБ на предприятии.
19. Что необходимо сделать при подготовке предприятия к проведению аудита ИБ?
20. Какие документы должны подготовить предприятия для внешнего аудита ИБ?
21. Дайте характеристику четырех этапов планирования аудита.
22. Как организуется работа с руководителями и сотрудниками предприятия до и после проведения аудита ИБ?
23. Охарактеризуйте последовательность (алгоритм) проведения внешнего аудита ИБ компанией.
24. Назовите виды информации (структуру данных), необходимую для проведения аудита.
25. Опишите структуру отчета по результатам аудита ИБ.
26. Какие этапы включает сценарий аудита на соответствие PCI DSS?



27. Какие этапы включает оценка соответствия финансовой организации положениям стандарта ГОСТ Р 57580.1-2017?

28. Какие этапы включает сценарий аудита на соответствие СТО БР ИББС 1.0-2014?

Дополнительная информация

Критерии балльной оценки различных форм текущего контроля успеваемости содержатся в соответствующих методических рекомендациях кафедры.

В течение семестра студент может набрать максимальное количество баллов равное 40. На промежуточную аттестацию (зачет) отводится 60 баллов. Распределение баллов по видам работ, формирующих текущий контроль



7. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине

Перечень компетенций с указанием индикаторов их достижения в процессе освоения образовательной программы содержится в разделе 2. «Перечень планируемых результатов освоения образовательной программы (перечень компетенций) с указанием индикаторов их достижения и планируемых результатов обучения по дисциплине».

Типовые контрольные задания или иные материалы, необходимые для оценки индикаторов достижения компетенций, умений и знаний

Наименование компетенции	Наименование индикаторов достижения компетенции	Результаты обучения (умения и знания), соотнесенные с индикаторами достижения компетенции	Типовые контрольные задания
ДПКН-4.3. Способность осуществлять диагностику и мониторинг систем защиты автоматизированных систем	Устанавливает программные, программно—аппаратные, в том числе криптографические и технические средства защиты информации автоматизированных систем	Знать: - классификацию и последствия реализации угроз информационной безопасности (ИБ), основные концепции обеспечения ИБ и теоретические основы диагностики и непрерывного мониторинга систем защиты информации АС; - актуальные нормативные правовые акты и методические акты в сфере	Задание 1. Диагностика уязвимостей и настройка мониторинга в сегменте АИС Контекст. Вы — специалист по информационной безопасности в компании, эксплуатирующей автоматизированную систему управления технологическими процессами (АСУ ТП). В сегменте сети, где размещены контроллеры и НМИ-станции, за последние 2 недели наблюдались эпизодические задержки отклика и скачки трафика. Есть подозрение на сканирование портов и попытки подбора учётных данных. Задача. Спланируйте и опишите поэтапную диагностику и организацию мониторинга для выявления причины аномалий. Ответ представьте в виде краткого плана-отчёта (5–7 пунктов), где для каждого этапа указано: • цель действия; • используемые инструменты/механизмы (минимум 2 конкретных примера ПО/утилит/функций ОС); • ожидаемый результат/показатель, по которому можно судить об успехе этапа. Что нужно отразить в решении:



Наименование компетенции	Наименование индикаторов достижения компетенции	Результаты обучения (умения и знания), соотнесенные с индикаторами достижения компетенции	Типовые контрольные задания
		диагностики и непрерывного мониторинга систем защиты информации АС; - современные программные, программно-аппаратные, в том числе крипто-графические и технические, средства защиты информации АС; - методики, способы и средства диагностики и непрерывного мониторинга систем защиты информации АС. Уметь: - применять на практике теоретические основы диагностики и непрерывного мониторинга систем защиты информации АС; - установ-	1. Первичный сбор данных о сетевом трафике и активных соединениях 2. Выявление подозрительных узлов и аномалий трафика (например, через анализ NetFlow/sFlow, сравнение с базовым профилем трафика). 3. Проверка наличия уязвимостей на ключевых узлах (например, сканеры уязвимостей типа OpenVAS, Nessus, MaxPatrol 8). 4. Анализ журналов аудита и событий безопасности (например, сбор через SIEM, анализ событий входа/ошибок аутентификации в журналах ОС/контроллеров). 5. Настройка непрерывного мониторинга критических метрик (например, пороги по количеству неудачных попыток входа, по объёму исходящего трафика, по открытию «нехарактерных» портов). 6. Формирование критериев оповещения (какие события считать инцидентом и требуют немедленного реагирования). 7. Предложение по корректирующим действиям на основе результатов диагностики (например, блокировка подозрительных IP, закрытие лишних портов, усиление политик паролей). Критерии оценки: • логическая последовательность этапов и отсутствие «пропусков» в цепочке диагностики; • релевантность выбранных инструментов под задачу АСУ ТП (учёт специфики промышленных протоколов, ограничений по нагрузке на сеть); • чёткие измеримые критерии успеха для каждого этапа; • наличие конкретных метрик и пороговых значений для мониторинга (например: «более 10 неудачных попыток входа за 5 минут — триггер инцидента»).



Наименование компетенции	Наименование индикаторов достижения компетенции	Результаты обучения (умения и знания), соотнесенные с индикаторами достижения компетенции	Типовые контрольные задания
		ливать современные программные, программно-аппаратные, в том числе криптографические и технические, средства защиты информации АС; - применять методики, способы и средства диагностики и непрерывного мониторинга систем защиты информации АС.	Задание 2. Мониторинг и диагностика сбоев в системе разграничения доступа АИС Контекст. В корпоративной автоматизированной системе (на базе Windows Server + Active Directory + СУБД) пользователи начали жаловаться на периодическую потерю доступа к общим ресурсам и «сбрасывание» прав после перезагрузки. В журналах фиксируются события с кодами 4625 (неудачная аутентификация) и 4776 (попытка NTLM-аутентификации), а также рост числа обращений к контроллеру домена. Предполагается, что проблема может быть связана с истечением срока действия сервисных учётных записей, сбоем репликации AD или некорректной работой групповых политик. Задача. Проведите виртуальную диагностику: опишите, какие данные и откуда нужно собрать, как их проанализировать и по каким признакам локализовать причину. Представьте ответ в виде таблицы из 6–8 строк со следующими колонками: • Источник данных / инструмент (например, Event Viewer, PowerShell-скрипт, консоль AD Users and Computers). • Конкретные события/параметры для анализа (например, коды событий, атрибуты учётных записей, тайминги репликации). • Ожидаемые признаки проблемы (что в данных будет указывать на ту или иную причину). • Действие по устранению/подтверждению гипотезы (что сделать, чтобы проверить или исправить). Пример строки таблицы:



Наименование компетенции	Наименование индикаторов достижения компетенции	Результаты обучения (умения и знания), соотнесенные с индикаторами достижения компетенции	Типовые контрольные задания			
			Источник данных / инструмент	Конкретные события/ параметры	Ожидаемые признаки проблемы	Действие по устранению/ подтверждению
			Журнал безопасности Windows (Security Log)	События 4625, 4771, 4768; время и IP источника	Повторяющиеся неудачные попытки входа с одного IP в одно и то же время	Проверить корректность пароля сервисной учётной записи; исключить атаку методом перебора
В решении обязательно рассмотрите минимум три возможные причины: 1. Истечение срока действия пароля сервисной учётной записи. 2. Сбой репликации между контроллерами домена. 3. Конфликт или некорректное применение групповых политик (GPO). Для каждой причины приведите 2–3 конкретных индикатора в данных и одно проверяющее действие. В конце сформулируйте итоговый вывод: как на практике организовать непрерывный мониторинг этих параметров, чтобы выявлять подобные сбои на ранней стадии (2–3 предложения с указанием конкретных механизмов: например, настройка алертов в SIEM по шаблонам событий, регулярные отчёты по статусу репликации AD и т.п.). Критерии оценки: • полнота охвата потенциальных причин и релевантность выбранных источников данных; • точность формулировок индикаторов (не общие фразы, а конкретные значения/ паттерны в логах);						



Наименование компетенции	Наименование индикаторов достижения компетенции	Результаты обучения (умения и знания), соотнесенные с индикаторами достижения компетенции	Типовые контрольные задания
			• практическая реализуемость предлагаемых действий мониторинга; • логичная связь между собранными данными, выявленными признаками и итоговым выводом.
	Тестирует и настраивает программные, программно-аппаратные, в том числе криптографические и технические средства защиты информации автоматизированных систем.	Знать: - теоретические основы тестирования и настройки современных программных, программно-аппаратных, в том числе криптографических и технических, средств защиты информации АС; - современные комплексы тестирования и настройки программных, программно-аппаратных, в том числе криптографических и технических, средств защиты информации АС; - методики и способы тестирования и	Задание 1. Настройка и тестирование межсетевого экрана и системы обнаружения вторжений в сегменте АИС Контекст. Вы — инженер ИБ в организации, где развёрнута автоматизированная система на базе Windows- и Linux-серверов. В сети выделен DMZ-сегмент для веб-сервисов. Поступил запрос на развёртывание защитного контура: нужно настроить межсетевой экран (на примере pfSense/OPNsense или iptables/nftables) и интегрировать систему обнаружения вторжений (Snort/Suricata), чтобы блокировать типовые атаки на веб-сервисы (SQL-инъекции, сканирование портов, попытки эксплуатации уязвимостей CVE). Задача. Выполните поэтапную настройку и тестирование средств защиты. Представьте результат в виде отчёта из 6–7 пунктов, где для каждого этапа есть: • цель действия; • конкретные команды, параметры конфигурации или шаги в GUI (приведите 1–2 примера реальных правил/параметров, например, правило Suricata для детектирования SQL-инъекций или правило iptables для блокировки сканирования портов); • методика тестирования работоспособности настроенного механизма (какой тест запустить, какой трафик сгенерировать, по каким логам/меткам убедиться, что защита сработала); • ожидаемый результат (что должно появиться в логах, как изменится поведение системы, какие события должны быть заблокированы/затестированы).



Наименование компетенции	Наименование индикаторов достижения компетенции	Результаты обучения (умения и знания), соотнесенные с индикаторами достижения компетенции	Типовые контрольные задания
		настройки программных, программно-аппаратных, в том числе криптографических и технических, средств защиты информации АС. Уметь: - применять на практике теоретические основы тестирования и настройки современных программных, программно-аппаратных, в том числе криптографических и технических, средств защиты информации АС; - эксплуатировать современные комплексы тестирования и настройки программных, про-	Обязательные этапы, которые нужно отразить: 1. Изоляция DMZ и базовые правила фильтрации. Настройте правила, разрешающие только HTTP/HTTPS из внешней сети в DMZ и ограниченные управляющие соединения из доверенной сети. Запретите весь остальной входящий трафик в DMZ. 2. Настройка сигнатурного анализа трафика. Создайте или активируйте сигнатуры IDS/IPS для выявления попыток SQL-инъекций (например, сигнатура на последовательность ' OR 1=1 --) и сканирования портов (например, детектирование серии SYN-пакетов на разные порты за короткое время). 3. Тестирование корректной работы «разрешённого» трафика. Сгенерируйте легитимный HTTP-запрос к веб-серверу и убедитесь, что он проходит без блокировок. 4. Проверка срабатывания защиты на имитации атак. С помощью curl или nmap сгенерируйте тестовые атаки: ◦ сканирование портов (nmap -sS <IP>); ◦ попытку SQL-инъекции через GET-параметр (curl "http://<IP>/search?q=' OR 1=1--"). 5. Анализ результатов. Покажите фрагменты логов IDS/межсетевого экрана, подтверждающие детектирование/блокировку атак, и отсутствие блокировок легитимного трафика. 6. Оценка ложных срабатываний. Опишите, как отличить легитимные всплески трафика от атак (например, всплеск запросов при рекламной кампании vs. DDoS-паттерн), и предложите 1–2 настройки для снижения числа ложных срабатываний (пороговые значения, исключения по IP, временные окна).



Наименование компетенции	Наименование индикаторов достижения компетенции	Результаты обучения (умения и знания), соотнесенные с индикаторами достижения компетенции	Типовые контрольные задания
		граммно-аппаратных, в том числе криптографических и технических, средств защиты информации АС;	7. Документирование правил и критериев срабатывания. Составьте краткую таблицу сигнатур/правил с полями: «Назначение правила», «Сигнатура/условие», «Действие», «Критерий срабатывания», «Ожидаемые логи». Задание 2. Тестирование и настройка криптографических средств защиты в АИС Контекст. В автоматизированной системе требуется обеспечить конфиденциальность и целостность данных при передаче между серверами и клиентами, а также шифрование данных на дисках. В инфраструктуре используются ОС Linux и Windows, есть СУБД PostgreSQL и веб-приложение. Необходимо развернуть и протестировать криптографические механизмы: TLS для веб-трафика, прозрачное шифрование диска (BitLocker/LUKS) и шифрование на уровне БД (pgcrypto). Задача. Проведите настройку и сквозное тестирование криптографических средств. Представьте решение в виде структурированного отчёта по трём направлениям (А–В), где для каждого направления есть: • цель и нормативная ссылка (укажите хотя бы один релевантный документ: например, требования ФСТЭК по защите информации в ГИС, рекомендации по TLS, ГОСТ Р 34.10/34.11 и т.п.); • шаги настройки (конкретные команды/параметры, например, команда <code>cryptsetup luksFormat</code>, параметры <code>ssl = on</code> в <code>postgresql.conf</code>, генерация CSR через OpenSSL); • план тестирования (какие инструменты использовать: <code>openssl s_client</code>, <code>testssl.sh</code>, проверка статуса BitLocker через PowerShell, тесты записи/чтения зашифрованных данных); • критерии успешного прохождения теста (что именно должно быть видно в выводе команд, какие флаги/статусы должны быть активны, какие данные должны оста-



Наименование компетенции	Наименование индикаторов достижения компетенции	Результаты обучения (умения и знания), соотнесенные с индикаторами достижения компетенции	Типовые контрольные задания
			ваться нечитаемыми при попытке доступа без ключа). Направления для реализации: А. Настройка и проверка TLS для веб-приложения. • Сгенерируйте самоподписанный сертификат (или используйте Let's Encrypt) и настройте веб-сервер (Nginx/Apache) на работу по HTTPS с отключением слабых протоколов (SSLv3, TLS 1.0/1.1) и слабых шифронаборов. • Протестируйте конфигурацию утилитой testssl.sh или через онлайн-сервис SSL Labs. • Убедитесь, что при попытке соединения по HTTP происходит редирект на HTTPS. Б. Настройка шифрования диска и проверка его работы. • На Linux-сервере настройте LUKS-шифрование для отдельного раздела (команды cryptsetup luksFormat, luksOpen, создание файловой системы). • На Windows-машине проверьте статус BitLocker для системного диска (через PowerShell: Get-BitLockerVolume). • Проведите тест «холодного старта»: отключите диск/выключите сервер, затем попробуйте получить доступ к данным без ввода пароля/ключа (данные должны быть недоступны). В. Настройка и тестирование шифрования на уровне СУБД. • В PostgreSQL включите расширение pgcrypto и создайте тестовую таблицу с зашифрованным полем (используйте pgp_sym_encrypt с симметричным ключом). • Выполните запись данных, затем проверьте, что в pg_dump или при прямом SELECT без расшифровки данные хранятся в виде шифротекста.



Наименование компетенции	Наименование индикаторов достижения компетенции	Результаты обучения (умения и знания), соотнесенные с индикаторами достижения компетенции	Типовые контрольные задания
			• Реализуйте SELECT с расшифровкой (pgp_sym_decrypt) и убедитесь, что данные корректно восстанавливаются. • Опишите риски хранения симметричных ключей в коде/скриптах и предложите 1–2 меры по их безопасному управлению (например, использование внешнего HSM/Vault, разделение прав доступа). Итоговый раздел отчёта (200–300 слов). Напишите краткий вывод о комплексном уровне защищённости после внедрения: какие угрозы теперь нейтрализованы (перехват трафика, физический доступ к диску, несанкционированное чтение БД), какие остались (например, компрометация ключей, уязвимости приложений), и как организовать периодическое тестирование этих механизмов (например, ежеквартальные пентесты, автоматизированные проверки конфигурации TLS, аудит прав на ключи шифрования).
	Контролирует работоспособность программных, программно-аппаратных, в том числе криптографических и технических средств защиты информации автоматизированных систем.	Знать: - теоретические основы контроля работоспособности современных средств защиты информации АС; - актуальные методические документы в сфере контроля работоспособности средств защиты информации АС; - со-	Задание 1. Контроль работоспособности средств защиты периметра и сетевого мониторинга в АИС Контекст. Вы — инженер по мониторингу ИБ в организации с распределённой автоматизированной системой (филиалы, ЦОД, DMZ). В эксплуатации находятся: межсетевой экран (на базе pfSense/OPNsense или корпоративного NGFW), система обнаружения/предотвращения вторжений (Suricata/Snort), сетевой сенсор NetFlow, а также агент мониторинга (Zabbix/Prometheus). Вчера поступили жалобы на «зависание» отдельных сервисов; есть подозрение на перегрузку средств защиты или сбой в их работе. Задача. Проведите контроль работоспособности ключевых СЗИ и локализируйте возможную причину сбоев. Представьте результат в виде отчёта из 6–7 пунктов, где для каждого эле-



Наименование компетенции	Наименование индикаторов достижения компетенции	Результаты обучения (умения и знания), соотнесенные с индикаторами достижения компетенции	Типовые контрольные задания
		временные программные, программно-аппаратные, в том числе криптографические и технические, средства защиты информации АС; - методики, способы и средства контроля работоспособности средств защиты информации АС. Уметь: - применять методики, способы и средства контроля работоспособности современных программных, программно-аппаратных, в том числе - криптографических и технических, средств защиты информации АС; - принимать соответствующую	мента защиты указано: • контролируемый параметр/метрика работоспособности; • источник данных и инструмент контроля (например, веб-интерфейс NGFW, Zabbix, <code>top/htop</code>, логи Suricata, вывод <code>show cpu history</code> и т. п.); • пороговое значение/критерий нормы и признак отклонения (конкретные цифры или паттерны в логах); • алгоритм действий при выявлении отклонения (что проверить дополнительно, какое событие зарегистрировать, когда требуется эскалация). Обязательные объекты контроля: 1. Межсетевой экран. Проверьте загрузку CPU/памяти, количество активных сессий, скорость обработки пакетов (pps), наличие «дропов» пакетов. Пример метрики: «CPU < 80 %, дропы пакетов = 0 за 5 минут». 2. Система IDS/IPS. Оцените загрузку CPU движка сигнатурного анализа, число пропущенных пакетов (packet drops/missed packets), частоту срабатываний и долю ложных срабатываний. Пример: «missed packets = 0, CPU < 90 %, всплеск срабатываний < 3× от базового уровня». 3. Сетевые интерфейсы и связность. Проверьте ошибки/дропы на интерфейсах, задержки и потери пакетов до ключевых узлов (через <code>ping/mtr</code>), корректность маршрутов. Пример: «потери пакетов < 1 %, ошибки на порту = 0». 4. Механизм журналирования и экспорта событий. Убедитесь, что логи пишутся, нет переполнения дискового пространства, события передаются в SIEM/на сервер логов. Пример: «свободное место на диске > 20 %, очередь отправки логов = 0».



Наименование компетенции	Наименование индикаторов достижения компетенции	Результаты обучения (умения и знания), соотнесенные с индикаторами достижения компетенции	Типовые контрольные задания
		щие меры по восстановлению работоспособности контролируемых средств защиты информации АС; - разрабатывать отчетный документ по результатам контроля работоспособности средств защиты информации АС.	5. Агенты мониторинга и их доступность. Проверьте «живость» агентов, задержку сбора метрик, отсутствие «пропущенных» опросов. Пример: «пинг до агента успешен, интервал опроса не растёт». 6. Криптографические функции (если есть аппаратные ускорители/HSM). Проверьте статус HSM/ускорителя, счётчики ошибок криптоопераций, доступность ключей. Пример: «статус HSM = ОК, ошибки криптоопераций = 0/час». 7. Итоговый вывод и план реагирования. Сформулируйте, по каким признакам можно отличить «нормальный всплеск нагрузки» от сбоя СЗИ (например, рост трафика при рекламной кампании vs. DDoS), и опишите 2–3 шага эскалации (кому и при каких метриках сообщать, когда включать режим «bypass/fail-open»). Задание 2. Контроль работоспособности криптографических средств и механизмов аутентификации в АИС Контекст. В автоматизированной системе развёрнуты следующие криптографические и аутентификационные механизмы: TLS-терминация на балансировщике/веб-сервере, шифрование дисков (BitLocker/LUKS), PKI (внутренний УЦ на Windows/Linux), двухфакторная аутентификация (2FA) через RADIUS/OIDC, а также HSM для хранения ключей подписи. Пользователи сообщают о периодических ошибках «истек сертификат» и «не удаётся войти» при использовании 2FA. Задача. Выполните контроль работоспособности указанных средств защиты и определите причину сбоев. Представьте ответ в виде таблицы из 7–8 строк (по одному механизму или ключевому аспекту) со следующими колонками: • Объект контроля (например, «сертификаты TLS», «служба RADIUS», «ключи подписи в HSM»);



Наименование компетенции	Наименование индикаторов достижения компетенции	Результаты обучения (умения и знания), соотнесенные с индикаторами достижения компетенции	Типовые контрольные задания
			• Контролируемая метрика/параметр (например, «срок действия сертификата», «время ответа RADIUS», «счётчик ошибок криптоопераций»); • Инструмент/источник данных (например, PowerShell Get-ChildItem, OpenSSL x509, логи RADIUS, SNMP OID HSM, мониторинг через Zabbix); • Критерий нормы / пороговое значение (например, «остаток срока действия > 30 дней», «время отклика < 2 с», «ошибки = 0»); • Признак отклонения (что именно в данных указывает на проблему); • Действие по диагностике/подтверждению (какая команда/запрос уточняет причину); • Реакция/эскалация (что сделать немедленно и кому сообщить). Обязательные строки таблицы (минимум): 1. Сертификаты TLS/PKI. Контроль срока действия, цепочки доверия, статуса отзыва (CRL/OCSP). 2. Ключи подписи и шифрования. Проверка доступности ключей, целостности (контрольные суммы/fingerprint), статуса «не отозван». 3. HSM/криптомодуль. Статус устройства, загрузка CPU/очереди, ошибки криптоопераций. 4. Служба аутентификации (RADIUS/AD/OIDC). Время отклика, число ошибок аутентификации, доля отказов. 5. Механизмы 2FA. Частота отказов, таймауты, сообщения об ошибках синхронизации токенов. 6. Шифрование дисков. Статус шифрования, наличие ошибок разблокировки, целостность метаданных LUKS/BitLocker.



Наименование компетенции	Наименование индикаторов достижения компетенции	Результаты обучения (умения и знания), соотнесенные с индикаторами достижения компетенции	Типовые контрольные задания
			7. Журналирование и аудит криптоопераций. Полнота логов, отсутствие переполнения, корректность экспорта в SIEM.



Примеры практико-ориентированных заданий

Задание № 1. Организация сохраняет магнитные носители с резервных копий в кабинете, размещенном непосредственно за помещением центра обработки данных. Консультант рекомендовал организации хранить резервные копии вне здания, в котором размещен центр обработки данных. Что консультант имел в виду, когда давал эту рекомендацию?

- a) Катастрофа, которая может разрушить центр обработки данных также может разрушить резервную копию
- b) В результате ротации резервной копии могут быть потеряны резервные копии, которые были выполнены несколько недель назад
- c) Разрушение основной базы данных может потребовать быстрого восстановления данных с резервной копии
- d) Физические средства защиты центра обработки данных недостаточны

Задание № 2. Какое из нижеприведенных положений наиболее важно с точки зрения управления непрерывностью бизнеса? Обоснуйте ваш выбор.

- a) Резервный центр обработки данных защищен и размещен на необходимом расстоянии от основного центра обработки данных
- b) Планы восстановления периодически проверяются
- c) На резервном центре обработки данных доступно и протестировано аппаратное обеспечение средств резервного сохранения
- d) Сетевые сервисы предоставляются различными провайдерами коммуникационных сервисов

Задание № 3. С какой из нижеперечисленных областей в наибольшей степени связана непрерывность функционирования бизнеса? Обоснуйте ваш выбор.

- a) Бизнес процессы
- b) Функционирование информационно-технологической инфраструктуры
- c) Устойчивость к авариям
- d) Восстановление данных

Задание № 4. Организация использует схему классификации, позволяющую определить критичность системы с точки зрения возможности аварийного восстановления. Основное приложение организации для ведения электронной коммерции классифицировано как «Критическое». Как организация должна классифицировать DNS-сервера организации?

- a) DNS-сервера должны быть классифицированы отдельно в соответствии с их критичностью
- b) DNS-сервера не должны классифицироваться, так как они не содержат пользовательских данных



с) DNS-сервера должны быть классифицированы как не конфиденциальные, так как они не содержат пользовательских данных

д) DNS-сервера должны быть классифицированы как «Критические», так как пользователи с их помощью взаимодействуют с серверами электронной коммерции

Задание № 5. Аудитор выявил имеющую высокий риск уязвимость при тестировании средств защиты. Какие действия он должен предпринять в первую очередь? Обоснуйте ваш выбор.

а) Немедленно выполнить действия по уменьшению риска

б) Включить уязвимость в отчет и пометить тест как не прошедший проверку

с) Немедленно проинформировать представителей организации, аудит которой проводится

д) Немедленно проинформировать группу по аудиту.

Примеры вопросов для подготовки к промежуточной аттестации

Общетеоретические (15 баллов)

1. Цель и задачи обеспечения информационной безопасности информационно-технологической системы в кредитно-финансовой организации, включая цель и задачи аудита информационной безопасности.

2. Аудит подсистемы обеспечения доступности в защищённой информационно-технологической системе кредитно-финансовой организации.

3. Аудит подсистемы обеспечения целостности в защищённой информационно-технологической системе кредитно-финансовой организации.

4. Аудит подсистемы обеспечения конфиденциальности в защищённой информационно-технологической системе кредитно-финансовой организации.

5. Аудит подсистемы обеспечения идентифицируемости в информационно-технологической системе кредитно-финансовой организации.

6. Аудит подсистемы обеспечения гарантированности в защищённой информационно-технологической системы кредитно-финансовой организации.

7. Цель, задачи и содержание Федерального закона от 26.07.2017 N 187-ФЗ "О безопасности критической информационной инфраструктуры Российской Федерации". Аудит ИБ на соответствие требованиям Федерального закона от 26.07.2017 N 187-ФЗ.

8. Структура служб (подразделений) аудита информационной безопасности в информационно-технологической системе кредитно-финансовой организации.

9. Сущность принципов достаточной глубины контроля и разграничения потоков информации как основных принципов защиты информации от



несанкционированного доступа?

10. Понятие, классификация аудита информационной безопасности. Основные нормативно-правовые акты аудита информационной безопасности.

11. Функция, способы и средства аудита информационной безопасности в информационно-технологической системе кредитно-финансовой организации.

12. Аудит ИБ на соответствие Положению Банка России № 683-П для финансовых организаций. Обязательные для кредитных организаций требования по обеспечению информационной безопасности

13. Сущность, содержание нормативно правовых актов проведения аудита информационной безопасности ЦБ России.

14. Факторы, влияющие на аудит информационной безопасности.

15. Предмет, содержание, задачи дисциплины «Аудит информационной безопасности». Основные понятия, общеметодологические принципы аудита информационной безопасности.

16. Теоретические основы обеспечения неотказуемости. Этапы и участники процесса обеспечения неотказуемости. Обеспечение неотказуемости и аудит информационной безопасности.

17. Виды проверок СИБ. Мониторинг ИБ. Самооценка ИБ. Методика проведения аудита информационной безопасности

18. Общие критерии безопасности ИТ: модель безопасности, задания по безопасности, профили защиты. Аудит на соответствие ГОСТ Р ИСО/МЭК 15408-1-2012.

19. Парадигма функциональных требований по безопасности, и проведение аудита по функциональным компонентам безопасности согласно ГОСТ Р ИСО/МЭК 15408-2-2013.

20. Компоненты доверия безопасности. Аудит по требованиям доверия безопасности согласно ГОСТ Р ИСО/МЭК 15408-3-2013.

21. Менеджмент программы аудита информационной безопасности по стандарту ГОСТ Р ИСО/МЭК 27007-2014.

22. Результаты проведения внешнего аудита информационной безопасности и правила их согласования. Контроль за деятельностью аудиторов информационной безопасности.

23. Инфраструктуры открытых ключей (назначение и состав) и их использование в процедурах и процессах аудита информационной безопасности в кредитно-финансовой организации.

24. Криптографические методы защиты данных в процедурах и процессах аудита информационной безопасности в кредитно-финансовой организации.

25. Предмет, содержание, задачи дисциплины «Аудит информационной безопасности». Основные понятия, общеметодологические принципы аудита



информационной безопасности.

Теоретико-прикладные (20 баллов)

1. Основные направления и принципы организации системы обеспечения информационной безопасности в кредитно-финансовой организации, которые анализируются при проведении аудита информационной безопасности.
2. Организация системы обеспечения информационной безопасности в кредитно-финансовой компании, которая анализируется при проведении аудита информационной безопасности.
3. Аудит функционирования системы обеспечения информационной безопасности (целевые функции) кредитно-финансовой организации.
4. Документы, определяющие функционирование системы обеспечения информационной безопасности в кредитно-финансовой организации, и которые анализируются при проведении аудита информационной безопасности.
5. Аудит подсистемы аутентификации в защищённой информационно-технологической системе кредитно-финансовой организации.
6. Аудит подсистемы управления доступом в защищённой информационно-технологической системе кредитно-финансовой организации.
7. Аудит подсистемы обеспечения неотказуемости в защищённой информационно-технологической системе кредитно-финансовой организации.
8. Аудит подсистемы обеспечения конфиденциальности в защищённой информационно-технологической системе кредитно-финансовой организации.
9. Аудит подсистемы обеспечения целостности в защищённой информационно-технологической системе кредитно-финансовой организации.
10. Подсистема аудита информационной безопасности кредитно-финансовой организации.
11. Аудит подсистемы оповещения о нарушениях безопасности в защищённой информационно-технологической системе кредитно-финансовой организации.
12. Аудит подсистемы обеспечения криптографическими ключами в защищённой информационно-технологической системе кредитно-финансовой организации.
13. Аудит внутренней инфраструктуры открытых ключей в защищённой информационно-технологической системе кредитно-финансовой организации.
14. Аудит применения асимметричных криптографических систем (электронной подписи) в финансово-экономической сфере.
15. Данные, необходимые для обеспечения и проведения аудита информационной безопасности.



16. Внутренний аудит ИБ. Цели и задачи внутренних аудитов ИБ. Организационные принципы внутреннего аудита ИБ.

17. Аудит политики обеспечения информационной безопасности.

18. Аудит используемых вспомогательных и функциональных средств обеспечения информационной безопасности.

19. Доверенная третья сторона в системах аутентификации и обеспечения неотказуемости (определение и функции). Аудит привлекаемой доверенной третьей стороны.

20. Виды проверок СУИБ. Принципы обеспечения эффективности внутреннего аудита ИБ.

21. Задачи аудита менеджмента непрерывности бизнеса, определение эффективности плана менеджмента непрерывностью бизнеса.

22. Международные и российские организации по стандартизации в области информационной безопасности.

23. Методы и методики проверки соответствия требованиям на основе критериев аудита ИБ для банковской сферы. Основные нормативно-правовые акты.

24. Внешний аудит ИБ. Риски внешнего аудита информационной безопасности. Понятие «соответствие» и «несоответствие» критериям аудита информационной безопасности.

25. Внешний аудит ИБ. Контроль за деятельностью аудиторов информационной безопасности. Понятие «компетентность аудитора».

Практико-ориентированные (25 баллов)

Вычислить итоговые показатели на основе методики оценки соответствия информационной безопасности организаций требованиям СТО БР ИББС-1.0-2014.

Исходные данные: Значение групповых показателей, корректирующих коэффициентов даны в таблице.

Исходные данные:										
№ билета	EV1	EV2	EV3	k ¹ _{БИТП}	k ¹ _{БИТП}	k ¹ _{ООПД}	k ¹ _{ОЗПД} 1	k ¹ _{ОЗПД} 2	k2	k3
1	0,75	0,95	0,85	0,85	0,7	0,85	0,7	0,85	1	0,85
2	0,75	0,95	0,95	0,7	0,85	0,7	0,85	1	0,85	0,85
3	0,55	0,95	0,9	0,85	0,7	0,85	0,7	0,85	1	0,85
4	0,75	0,95	0,85	0,7	0,85	0,7	0,85	1	0,85	0,85
5	0,85	0,95	0,8	0,85	0,7	0,85	0,7	0,85	1	0,85
6	0,75	0,75	0,85	0,7	0,85	0,7	0,85	1	0,85	0,85
7	0,75	0,95	0,75	0,85	0,85	0,85	0,85	0,85	0,85	0,85
8	0,85	0,9	0,7	0,85	0,7	0,85	0,7	0,85	1	0,85
9	0,75	0,85	0,65	0,7	0,85	0,7	0,85	1	0,85	0,85
10	0,85	0,8	0,6	0,85	0,7	0,85	0,7	0,85	1	0,85
11	0,75	0,85	0,65	0,7	0,85	0,7	0,85	1	0,85	0,85



12	0,85	0,75	0,55	0,85	0,7	0,85	0,7	0,85	1	0,85
13	0,75	0,8	0,5	0,7	0,85	0,7	0,85	1	0,85	0,85
14	0,95	0,65	0,85	0,85	0,7	0,85	0,7	0,85	1	0,85
15	0,9	0,6	0,85	0,7	0,85	0,7	0,85	1	0,85	0,85
16	0,85	0,65	0,85	0,85	0,7	0,85	0,7	0,85	1	0,85
17	0,8	0,55	0,85	0,7	0,85	0,7	0,85	1	0,85	0,85
18	0,85	0,5	0,85	0,85	0,7	0,85	0,7	0,85	1	0,85
19	0,5	0,95	0,85	0,7	0,85	0,7	0,85	1	0,85	0,85
20	0,7	0,8	0,85	0,85	0,7	0,85	0,7	0,85	1	0,85
21	0,65	0,85	0,85	0,7	0,85	0,7	0,85	1	0,85	0,85
22	0,6	0,75	0,85	0,85	0,7	0,85	0,7	0,85	1	0,85
23	0,65	0,7	0,85	0,7	0,85	0,7	0,85	1	0,85	0,85
24	0,95	0,65	0,85	0,85	0,7	0,85	0,7	0,85	1	0,85
25	0,75	0,6	0,85	0,85	0,85	0,7	0,85	0,7	0,85	1
Найти:										
	EV_{М6}	EV_{М7}	EV_{М8}	EV_{БИП}	EV_{БИП}	EV_{ООПД}	EV¹_{ОЗПД}	EV²_{ОЗПД}	EV_{М9}	R
1-25	X	X	X	X	X	X	X	X	X	X



Найти: на основе исходных данных определить все остальные показатели, обозначенные X, сделать вывод о соответствии требованиям и при необходимости предложить мероприятия по повышению групповых показателей.



8. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины

Основная литература:

1. Козьминых, С.И. Аудит информационной безопасности : Учебное пособие / С.И. Козьминых, С.А. Борисов Электрон. дан. Москва : КноРус, 2026 328 с. Режим доступа: book.ru Internet access <https://book.ru/book/961209> ISBN 978-5-406-15552-3. [БИК ID: RU\bookru\bibl\961209]

Дополнительная литература:

1. Баранова, Елена Константиновна Информационная безопасность и защита информации : Учебное пособие / Национальный исследовательский университет "Высшая школа экономики" 5, перераб. и доп. Москва : Издательский Центр РИОР, 2026 384 с. (Высшее образование) ВО - Бакалавриат <https://znanium.ru/catalog/document?id=477891> ISBN 978-5-369-02005-0 ISBN 978-5-16-114639-2 (электр. издание) ISBN 978-5-16-021869-4 (ISBN соиздателя) . [БИК ID: RU\infra-m\znanium\bibl\2233509]
2. Киреева, Н. В. Аудит информационной безопасности [Электронный ресурс] : методические указания к практическим занятиям / Киреева Н. В.,Поздняк И. С.,Караулова О. А. Самара : ПГУТИ, 2019 21 с. Книга из коллекции ПГУТИ - Информатика <https://e.lanbook.com/book/223223>. [БИК ID: RU-LAN-BOOK-223223]

Нормативные правовые акты:

Федеральные законы

- Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации». Определяет базовые понятия, принципы правового регулирования отношений в сфере информации, классификацию информации по категориям доступа, порядок её предоставления или распространения, а также общие условия защиты информации.
- Федеральный закон от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры». Регулирует защиту объектов критической информационной инфраструктуры (КИИ), устанавливает обязанности субъектов КИИ, включая использование доверенных программно-аппаратных комплексов и отечественного ПО.
- Федеральный закон от 6 апреля 2011 г. №63-ФЗ «Об электронной подписи». Определяет правовой режим технологического обеспечения защиты информации в системе базовых законов информационного законодательства.

Указы Президента РФ



- Указ Президента РФ от 5 декабря 2016 г. №646 «Об утверждении Доктрины информационной безопасности Российской Федерации». Определяет стратегические цели и задачи в области информационной безопасности, включая защиту критической информационной инфраструктуры.

- Указ Президента РФ от 22 мая 2015 г. № 260 «О некоторых вопросах информационной безопасности Российской Федерации».

Постановления Правительства РФ

- Постановление Правительства РФ от 6 июля 2015 г. № 675 «О порядке осуществления контроля за соблюдением требований, предусмотренных частью 2.1 статьи 13 и частью 6 статьи 14 Федерального закона „Об информации, информационных технологиях и о защите информации“». Устанавливает правила контроля за размещением технических средств информационных систем и соблюдением требований к их созданию, развитию, эксплуатации и выводу из эксплуатации.

- Постановление Правительства РФ от 8 февраля 2018 г. № 127 «Об утверждении правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений». Определяет порядок категорирования объектов КИИ.

- Постановление Правительства РФ от 17 февраля 2018 г. № 162 «Об утверждении Правил осуществления государственного контроля в области обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации». Устанавливает порядок государственного контроля за безопасностью объектов КИИ.

Приказы регуляторов

- Приказ ФСТЭК России от 11 апреля 2025 г. № 117 «Об утверждении Требований о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений». Вводит требования к защите информации в ГИС и других информационных системах госорганов, ГУП и госучреждений, включая процессный подход, непрерывный мониторинг и управление привилегированным доступом.

- Приказ ФСБ России от 10 июля 2014 г. №378 «Об утверждении Составы и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации». Определяет меры по защите персональных данных с применением криптографии.

- Приказ ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну,



содержащейся в государственных информационных системах». Устанавливает требования к защите информации в государственных информационных системах.

Другие нормативные акты

- Стандарт внешнего государственного аудита (контроля) СГА 305 «Аудит федеральных информационных систем и проектов» (утверждён постановлением Коллегии Счётной палаты РФ от 23 декабря 2016 г. № 11ПК, в редакции от 28 декабря 2018 г. № 19ПК). Содержит перечень законодательных и иных нормативных правовых актов, используемых при аудите информационных систем и проектов.

- ГОСТы в области информационной безопасности, например, ГОСТ Р 59709–2022 «Защита информации. Управление компьютерными инцидентами. Общие положения», ГОСТ Р 59710–2022 «Защита информации. Управление компьютерными инцидентами. Организация деятельности по управлению компьютерными инцидентами».

9. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

1. <https://www.planetaexcel.ru/>
2. Электронная библиотека Финансового университета (ЭБ) <http://elib.fa.ru/> (<http://library.fa.ru/files/elibfa.pdf>)
3. Электронно-библиотечная система BOOK.RU <http://www.book.ru>
4. Электронно-библиотечная система "Университетская библиотека ОНЛАЙН" <http://biblioclub.ru/>
5. Электронно-библиотечная система Znanium <http://www.znanium.com>
6. Электронно-библиотечная система издательства "Лань" <https://e.lanbook.com/>
7. Образовательная платформа "ЮРАЙТ" <https://urait.ru/>
8. Научная электронная библиотека eLibrary.ru <http://elibrary.ru>
9. Информационно-образовательный портал Финуниверситета: <https://org.fa.ru>
10. • Электронная библиотека Финансового университета (ЭБ) <http://elib.fa.ru/>
11. • Электронно-библиотечная система BOOK.RU <http://www.book.ru>
12. • Электронно-библиотечная система «Университетская библиотека ОНЛАЙН» <http://biblioclub.ru/>
13. • Электронно-библиотечная система издательства «ЮРАЙТ» <https://urait.ru/>
14. • Электронно-библиотечная система издательства Проспект <http://ebs.prospekt.org/books>
15. • Научная электронная библиотека eLibrary.ru <http://elibrary.ru>
16. • Национальная электронная библиотека <http://нэб.рф/>
17. • Электронные продукты издательства Elsevier <http://www.sciencedirect.com>
18. 4. Официальный сайт Федеральной службы государственной статистики. URL: <http://www.gks.ru> (Росстат)



19. Банк АО «Альфа-Банк» [официальный сайт]. – Текст : электронный. - URL:
<https://alfabank.ru/>.
20. Интернет-репозиторий образовательных ресурсов – URL:
<http://repository.vzfei.ru>
21. Электронно-библиотечная система (ЭБС) ООО «Издательский Дом ИНФРА-М»



10. Методические указания для обучающихся по освоению дисциплины

Самостоятельная работа студентов реализуется в соответствии с приказом Финансового университета от 11.05.2021 № 1040/о «Об утверждении Методических рекомендаций по планированию и организации внеаудиторной самостоятельной работы студентов по образовательным программам бакалавриата и магистратуры в Финансовом университете». Промежуточная аттестация проводится в соответствии с приказом Финансового университета от 01.10.2024 № 2187/о «Об утверждении Положения о проведении текущего контроля успеваемости и промежуточной аттестации студентов, обучающихся по образовательным программам высшего образования в Финансовом университете». Кафедрой могут разрабатываться дополнительные методические рекомендации для отдельных форм проведения аудиторных занятий и самостоятельной работы студентов.



11. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень необходимого программного обеспечения и информационных справочных систем

Комплект лицензионного программного обеспечения:

1. Windows
2. Операционная система
3. Пакет офисных программ
4. Astra Linux

Современные профессиональные базы данных и информационные справочные системы

1. Информационно-правовая система «Гарант»
2. Информационно-правовая система «Консультант Плюс»

Сертифицированные программные и аппаратные средства защиты информации

1. не предусмотрены

12. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

1. Учебная аудитория для проведения учебных занятий, предусмотренных программой, в том числе групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, оснащенная оборудованием и техническими средствами обучения: мебель аудиторная (столы, стулья, доска аудиторная), набор демонстрационного оборудования (проектор, экран)
2. **Компьютерный класс** для проведения учебных занятий, предусмотренных программой, в том числе групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, оснащенный оборудованием и техническими средствами обучения: мебель аудиторная (столы, стулья, доска аудиторная), персональные компьютеры, набор демонстрационного оборудования (проектор, экран)
3. Лаборатория для проведения учебных занятий, предусмотренных программой, в том числе групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, оснащенная оборудованием и техническими средствами обучения: мебель аудиторная (столы, стулья, доска аудиторная), лабораторное оборудование, расходные материалы, набор демонстрационного оборудования (проектор, экран)



4. Программное обеспечение с возможностью лицензирования или свободно распространяемое (Open Source). Все перечисленные инструменты являются бесплатными.
5. Доступ к сети Интернет для использования онлайн-ресурсов, репозитория, документации.
6. Библиотека, читальный зал
7. Помещение для самостоятельной работы обучающихся оснащенное компьютерной техникой с возможностью подключения к сети "Интернет" и обеспечением доступа к электронной информационно-образовательной среде Университета.