ЮЖНО-УРАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

УТВЕРЖДАЮ:
Заведующий выпускающей кафедрой

Электронный документ, подписанный ПЭП, хранится в системе электронного документооборота Южно-Уральского государственного университета
ЮУрГУ
СВЕДЕНИЯ О ВЛАДЕЛЬЦЕ ПЭП
Кому выдан: Голлай А. В.
Пользователь: gollaiav
Дата подписания: 01.02.2026

А. В. Голлай

РАБОЧАЯ ПРОГРАММА

дисциплины 1.Ф.П0.09 Анализ угроз и уязвимостей ИТ-инфраструктуры
для направления 09.03.01 Информатика и вычислительная техника
уровень Бакалавриат
профиль подготовки ИТ-инженерия
форма обучения очная
кафедра-разработчик Центр подготовки топ-специалистов в сфере ИТ "Цифровой Урал"

Рабочая программа составлена в соответствии с ФГОС ВО по направлению подготовки 09.03.01 Информатика и вычислительная техника, утверждённым приказом Минобрнауки от 19.09.2017 № 929

Зав.кафедрой разработчика, д.техн.н., доц.

Электронный документ, подписанный ПЭП, хранится в системе электронного документооборота Южно-Уральского государственного университета
ЮУрГУ
СВЕДЕНИЯ О ВЛАДЕЛЬЦЕ ПЭП
Кому выдан: Голлай А. В.
Пользователь: gollaiav
Дата подписания: 22.01.2026

А. В. Голлай

Разработчик программы, к.техн.н., доц., заведующий кафедрой

Электронный документ, подписанный ПЭП, хранится в системе электронного документооборота Южно-Уральского государственного университета
ЮУрГУ
СВЕДЕНИЯ О ВЛАДЕЛЬЦЕ ПЭП
Кому выдан: Соколов А. Н.
Пользователь: sokolovan
Дата подписания: 19.01.2026

А. Н. Соколов

Челябинск

1. Цели и задачи дисциплины

Цель дисциплины: формирование у студентов системного понимания угроз и уязвимостей современной ИТ-инфраструктуры, а также развитие практических навыков по обеспечению её безопасности на этапах проектирования, развёртывания и эксплуатации в соответствии с нормативно-правовыми и отраслевыми требованиями информационной безопасности. Задачи дисциплины: 1. Формирование у студентов теоретических знаний: - о типах, источниках и последствиях угроз ИТ-инфраструктуре; - о принципах безопасного проектирования и эксплуатации ИТ-систем; - о нормативно-правовой базе и стандартах в области информационной безопасности. 2. Развитие у студентов умений и навыков в области информационной безопасности, необходимых ИТ-инженеру: - проводить аудит и проверку соответствия конфигураций серверного и сетевого оборудования требованиям ИБ; - настраивать безопасные параметры операционных систем, веб-серверов, СУБД и сетевых компонентов; - использовать инструменты автоматизированного сканирования и мониторинга безопасности (Lynis, OpenSCAP, SIEM и др.). 3. Обеспечение приобретения практических компетенций: - по выявлению и устранению типовых уязвимостей в ИТ-инфраструктуре; - по документированию результатов анализа и подготовке рекомендаций по повышению уровня защищённости; - по применению принципов наименьших привилегий, сегментации, управления патчами и безопасного обновления систем.

Краткое содержание дисциплины

Дисциплина «Анализ угроз и уязвимостей ИТ-инфраструктуры» направлена на формирование у студентов инженерных компетенций в области обеспечения информационной безопасности современных ИТ-систем. В рамках дисциплины изучаются типы угроз и уязвимостей серверного, сетевого и прикладного уровней ИТ-инфраструктуры, рассматриваются нормативно-правовые и отраслевые требования к защите информации. Особое внимание уделяется практическим аспектам: безопасной настройке операционных систем, веб-серверов, СУБД и сетевого оборудования; применению инструментов аудита и мониторинга; проверке соответствия конфигураций требованиям ИБ; документированию и устранению выявленных угроз. Дисциплина ориентирована на подготовку ИТ-инженеров, способных проектировать, развёртывать и эксплуатировать защищённую, отказоустойчивую и соответствующую нормативным требованиям ИТ-инфраструктуру.

2. Компетенции обучающегося, формируемые в результате освоения дисциплины

Планируемые результаты освоения ОП ВО (компетенции)	Планируемые результаты обучения по дисциплине
ПК-10 Способен выполнять работы по созданию (модификации) и сопровождению информационных ресурсов	Знает: основы информационной безопасности web-ресурсов Умеет: проверять соответствие серверного оборудования требованиям ИР Имеет практический опыт: проверки соответствия web-ресурсов требованиям информационной безопасности

3. Место дисциплины в структуре ОП ВО

Перечень предшествующих дисциплин, видов работ учебного плана	Перечень последующих дисциплин, видов работ
Телекоммуникационные системы и технологии, Разработка Web-приложений, Разработка Web-приложений на Python	Не предусмотрены

Требования к «входным» знаниям, умениям, навыкам студента, необходимым при освоении данной дисциплины и приобретенным в результате освоения предшествующих дисциплин:

Дисциплина	Требования
Разработка Web-приложений на Python	Знает: особенности выбранной среды web-программирования и системы управления базами данных; компоненты программно-технических архитектур ИР, существующие приложения и интерфейсы взаимодействия с ними Умеет: применять выбранные языки web-программирования для написания программного кода ИР; размещать программный код в клиентской и серверной части ИР; оптимизировать программный код ИР с использованием специализированных программных средств. Имеет практический опыт: разработки web-приложений с использованием специализированных программных средств
Телекоммуникационные системы и технологии	Знает: сетевые протоколы и основы web-технологий Умеет: устанавливать программное обеспечение и дополнительные модули, необходимые для корректного функционирования ИР; проверять соответствие серверного оборудования требованиям ИР Имеет практический опыт: установки и настройки программного обеспечения и модулей, проверки соответствия серверного оборудования требованиям информационных ресурсов
Разработка Web-приложений	Знает: принципы функционирования web-технологий (HTTP/HTTPS, REST, SOAP, WebSocket); архитектуру клиент-серверных web-приложений и их компонентов; современные стандарты HTML, CSS, JavaScript и принципы адаптивной и кроссбраузерной верстки; основы backend-разработки (обработка запросов, API, базы данных, ORM, авторизация и аутентификация); современные фреймворки и платформы для разработки web-приложений (например, React и др.), синтаксис выбранного языка web-программирования, особенности программирования на этом языке, стандартные библиотеки языка программирования; особенности выбранной среды web-программирования и системы управления базами

	данных; компоненты программно-технических архитектур ИР, существующие приложения и интерфейсы взаимодействия с ними Умеет: проектировать архитектуру web-приложений с учётом функциональных и нефункциональных требований; разрабатывать фронтенд- и бэкенд-части web-систем с использованием современных инструментов; интегрировать web-приложения с внешними сервисами и базами данных; использовать системы контроля версий (Git); тестировать и отлаживать web-приложения; применять отечественные и открытые программные средства при реализации проектов, применять выбранные языки web-программирования для написания программного кода ИР; размещать программный код в клиентской и серверной части ИР; оптимизировать программный код ИР с использованием специализированных программных средств Имеет практический опыт: навыками командной разработки web-приложений; практикой применения современных технологий и инструментов web-разработки отечественного и зарубежного производства; умением документировать архитектуру и код web-приложений

4. Объём и виды учебной работы

Общая трудоемкость дисциплины составляет 3 з.е., 108 ч., 70,5 ч. контактной работы

Вид учебной работы	Всего часов	Распределение по семестрам в часах
		Номер семестра
		7
Общая трудоёмкость дисциплины	108	108
Аудиторные занятия:	64	64
Лекции (Л)	32	32
Практические занятия, семинары и (или) другие виды аудиторных занятий (ПЗ)	32	32
Лабораторные работы (ЛР)	0	0
Самостоятельная работа (СРС)	37,5	37,5
Подготовка к практическим занятиям: изучение подходов к обеспечению безопасности прикладных ИТ-систем и веб-ресурсов. Подготовка чек-листа соответствия для web-ресурса	7,5	7.5
Подготовка к практическим занятиям: изучение основ обеспечения информационной безопасности - терминов, принципов, базовых моделей защиты	3	3
Подготовка к практическим занятиям: изучение основных угроз и рисков ИТ-инфраструктуры	4	4
Подготовка к практическим занятиям: изучение нормативно-	7,5	7.5

правовых основ и требований к безопасности ПО, методов обеспечения безопасности на этапе разработки и эксплуатации ПО		
Подготовка к практическим занятиям: изучение средств защиты информации и систем управления безопасностью	3	3
Подготовка итогового отчета по результатам практических занятий: аудит безопасности ИТ-инфраструктуры, выбор средств защиты	9,5	9.5
Подготовка к практическим занятиям: изучение систем управления безопасностью	3	3
Консультации и промежуточная аттестация	6,5	6,5
Вид контроля (зачет, диф.зачет, экзамен)	-	диф.зачет

5. Содержание дисциплины

№ раздела	Наименование разделов дисциплины	Объем аудиторных занятий по видам в часах			
		Всего	Л	ПЗ	ЛР
1	Основы информационной безопасности ИТ-инфраструктуры	16	8	8	0
2	Инженерная безопасность серверов, СУБД, веб-платформ и сетей	16	8	8	0
3	Инструменты и методы обеспечения соответствия требованиям информационной безопасности	16	8	8	0
4	Современные вызовы и интеграция практик информационной безопасности в ИТ-инфраструктуру	16	8	8	0

5.1. Лекции

№ лекции	№ раздела	Наименование или краткое содержание лекционного занятия	Кол-во часов
1	1	Информационная безопасность в контексте ИТ-инфраструктуры. Роль ИТ-инженера в обеспечении безопасности информации.	2
2	1	Основные угрозы и уязвимости ИТ-инфраструктуры: классификация, источники, последствия.	2
3	1	Нормативно-правовые и отраслевые требования к ИТ-инфраструктуре.	2
4	1	Архитектура современной ИТ-инфраструктуры: серверы, сети, СУБД, веб-платформы, облачные компоненты.	2
5	2	Принципы безопасного проектирования и развертывания ИТ-инфраструктуры.	2
6	2	Безопасность операционных систем Linux и Windows Server. Основные механизмы защиты.	2
7	2	Безопасная конфигурация веб-серверов (Apache, Nginx, IIS) и прикладных серверов.	2
8	2	Управление сетевой безопасностью: межсетевые экраны, VLAN, сегментация, безопасные протоколы.	2
9	3	Безопасность баз данных: настройка, управление доступом, шифрование.	2
10	3	Управление учетными записями, привилегиями и аутентификацией в ИТ-инфраструктуре.	2
11	3	Системы централизованного мониторинга и логирования (SIEM, ELK, журналы ОС и сервисов).	2
12	3	Инструменты аудита и сканирования конфигураций (Lynis, CIS-CAT,	2

		OpenSCAP).	
13	4	Обеспечение безопасного обновления и управления патчами в ИТ-инфраструктуре.	2
14	4	Введение в безопасность облачных ИТ-инфраструктур (IaaS, PaaS): Shared Responsibility Model.	2
15	4	Подходы к проверке соответствия ИТ-инфраструктуры требованиям ИБ (чек-листы, аудит, документирование).	2
16	4	Итоговое обобщение: от проектирования до эксплуатации безопасной ИТ-инфраструктуры.	2

5.2. Практические занятия, семинары

№ занятия	№ раздела	Наименование или краткое содержание практического занятия, семинара	Кол-во часов
1	1	Развертывание лабораторной ИТ-инфраструктуры: веб-сервер, СУБД, клиент (виртуализация/контейнеризация).	2
2	1	Аудит безопасности ОС: проверка конфигурации Linux/Windows с использованием инструмента Lynis и стандартов безопасности CIS Benchmarks.	2
3	1	Настройка сетевой сегментации и базовых правил межсетевого экрана.	2
4	1	Управление учетными данными и привилегиями: принцип наименьших привилегий, настройка команды sudo, групповой политики.	2
5	2	Настройка безопасной конфигурации веб-сервера (Nginx/Apache): отключение ненужных модулей, настройка заголовков, TLS.	2
6	2	Безопасная настройка СУБД (PostgreSQL/MySQL): пользователи, привилегии, шифрование, логирование.	2
7	2	Настройка и проверка TLS-конфигурации.	2
8	2	Настройка централизованного сбора и анализа логов.	2
9	3	Работа с OpenSCAP: сканирование системы на соответствие профилю безопасности.	2
10	3	Автоматизация проверки конфигураций с помощью Ansible или Bash-скриптов.	2
11	3	Аудит обновлений и управление патчами: проверка уязвимых пакетов, планирование обновлений.	2
12	3	Создание и применение чек-листов соответствия для типового веб-ресурса.	2
13	4	Проверка соответствия сервера требованиям ИБ по контрольному списку (чек-листу).	2
14	4	Базовая настройка облачной ИТ-инфраструктуры (AWS EC2 / Yandex.Cloud) с учётом требований ИБ.	2
15	4	Подготовка отчёта по результатам аудита ИТ-инфраструктуры (в т.ч. рекомендации по устранению несоответствий).	2
16	4	Развертывание и аудит безопасной ИТ-инфраструктуры «под ключ».	2

5.3. Лабораторные работы

Не предусмотрены

5.4. Самостоятельная работа студента

Выполнение СРС			
Подвид СРС	Список литературы (с указанием	Семестр	Кол-

	разделов, глав, страниц) / ссылка на ресурс		во часов
Подготовка к практическим занятиям: изучение подходов к обеспечению безопасности прикладных ИТ-систем и веб-ресурсов. Подготовка чек-листа соответствия для web-ресурса	Нефедов, В. С. Безопасность прикладных информационных технологий и систем : учебное пособие / В. С. Нефедов. — 2-е изд. — Москва : РТУ МИРЭА, 2025. — 113 с. — ISBN 978-5-7339-2570-7. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/504831 (дата обращения: 11.12.2025). — Режим доступа: для авториз. пользователей. Разделы: гл. 2, 3, 6 («Модели угроз для прикладных систем», «Методы защиты веб-приложений», «Подтверждение соответствия».).	7	7,5
Подготовка к практическим занятиям: изучение основ обеспечения информационной безопасности - терминов, принципов, базовых моделей защиты	Прохорова, О. В. Информационная безопасность и защита информации : учебник для вузов / О. В. Прохорова. — 6-е изд., стер. — Санкт-Петербург : Лань, 2025. — 124 с. — ISBN 978-5-507-52899-8. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/462293 (дата обращения: 11.12.2025). — Режим доступа: для авториз. пользователей. Разделы: гл. 1–2 («Основные понятия ИБ», «Модели нарушителя и угроз»).	7	3
Подготовка к практическим занятиям: изучение основных угроз и рисков ИТ-инфраструктуры	Суворов, С. А. Современные угрозы и риски цифровых коммуникаций : учебно-методическое пособие / С. А. Суворов. — Тамбов : ТГУ им. Г.Р.Державина, 2025. — 121 с. — ISBN 978-5-00078-919-3. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/504523 (дата обращения: 11.12.2025). — Режим доступа: для авториз. пользователей. Разделы: введение, гл. 1–2 («Типы угроз», «Анализ рисков»).	7	4
Подготовка к практическим занятиям: изучение нормативно-правовых основ и требований к безопасности ПО, методов обеспечения безопасности на этапе разработки и эксплуатации ПО	Казарин, О. В. Надежность и безопасность программного обеспечения : учебник для вузов / О. В. Казарин, И. Б. Шубинский. — 2-е изд. — Москва : Издательство Юрайт, 2025. — 352 с. — (Высшее образование). — ISBN 978-5-534-19386-2. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/580669 (дата обращения: 11.12.2025). Разделы: гл. 3, 4, 5, 6 («Методы обеспечения надёжности», «Защита ПО от анализа и модификации», «Нормативно-правовое регулирование», «Подтверждение соответствия»).	7	7,5

Подготовка к практическим занятиям: изучение средств защиты информации и систем управления безопасностью	Шипулин, Г. Ф. Мониторинг инцидентов информационной безопасности. Средства защиты информации: межсетевые экраны, системы обнаружения и предотвращения вторжений : учебное пособие / Г. Ф. Шипулин. — Москва : РТУ МИРЭА, 2025. — 151 с. — ISBN 978-5-7339-2689-6. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/508442 (дата обращения: 11.12.2025). — Режим доступа: для авториз. пользователей. Разделы: Гл. 1, 2 («Архитектура средств защиты», «Работа с межсетевыми экранами и IDS»).	7	3
Подготовка итогового отчета по результатам практических занятий: аудит безопасности ИТ-инфраструктуры, выбор средств защиты	Прохорова, О. В. Информационная безопасность и защита информации : учебник для вузов / О. В. Прохорова. — 6-е изд., стер. — Санкт-Петербург : Лань, 2025. — 124 с. — ISBN 978-5-507-52899-8. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/462293 (дата обращения: 11.12.2025). — Режим доступа: для авториз. пользователей. Шипулин, Г. Ф. Мониторинг инцидентов информационной безопасности. Средства защиты информации: межсетевые экраны, системы обнаружения и предотвращения вторжений : учебное пособие / Г. Ф. Шипулин. — Москва : РТУ МИРЭА, 2025. — 151 с. — ISBN 978-5-7339-2689-6. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/508442 (дата обращения: 11.12.2025). — Режим доступа: для авториз. пользователей. Шипулин, Г. Ф. Классификация средств защиты информации. Средства защиты информации: системы управления информацией о безопасности и событиями безопасности, системы предотвращения утечек данных : учебное пособие / Г. Ф. Шипулин. — Москва : РТУ МИРЭА, 2025. — 111 с. — ISBN 978-5-7339-2690-2. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/508443 (дата обращения: 11.12.2025). — Режим доступа: для авториз. пользователей.	7	9,5
Подготовка к практическим занятиям: изучение систем управления безопасностью	Шипулин, Г. Ф. Классификация средств защиты информации. Средства защиты информации: системы управления информацией о безопасности и событиями безопасности, системы	7	3

	предотвращения утечек данных : учебное пособие / Г. Ф. Шипулин. — Москва : РТУ МИРЭА, 2025. — 111 с. — ISBN 978-5-7339-2690-2. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/508443 (дата обращения: 11.12.2025). — Режим доступа: для авториз. пользователей. Разделы: Гл. 2, 3 («Системы управления событиями безопасности (SIEM)», «Средства предотвращения утечек данных (DLP)»).		

6. Фонд оценочных средств для проведения текущего контроля успеваемости, промежуточной аттестации

Контроль качества освоения образовательной программы осуществляется в соответствии с Положением о балльно-рейтинговой системе оценивания результатов учебной деятельности обучающихся.

6.1. Контрольные мероприятия (КМ)

№ КМ	Се-местр	Вид контроля	Название контрольного мероприятия	Вес	Макс. балл	Порядок начисления баллов	Учи-тыва-ется в ПА
1	7	Текущий контроль	Тестирование по тематике раздела 1	1	10	Студенту предлагается ответить на 10 тестовых вопросов, выбранных случайным образом. За каждый правильный ответ начисляется 1 балл.	дифференцированный зачет
2	7	Текущий контроль	Сдача отчета по практическим занятиям раздела 1	2	5	5 баллов выставляется, если: Все практические задания раздела выполнены полностью и корректно. Продемонстрировано глубокое понимание инженерных принципов ИБ. Все команды, конфигурации, скриншоты работоспособны и соответствуют цели. Отчёт структурирован, содержит все обязательные элементы (цель, ход	дифференцированный зачет

						работы, выводы). Использована рекомендованная литература (при необходимости). Нет фактических, технических или логических ошибок. 4 балла выставляется, если: Выполнены все задания, но с незначительными недочётами (например, одна ошибка в конфигурации, нет одного скриншота). Понимание темы достаточное, но не глубокое. Отчёт в целом соответствует требованиям, но возможны мелкие нарушения структуры или оформления. Имеются незначительные неточности в терминологии или рекомендациях. 3 балла выставляется, если: Выполнена основная часть заданий, но пропущены или ошибочны 1–2 пункта. Понимание ограничено: ответы шаблонные, без анализа. Отчёт не полностью структурирован (например, отсутствуют выводы или методология). Есть технические ошибки, но не критичные. Использование литературы поверхностное или отсутствует. 2 балла выставляется, если: Выполнено менее 50% заданий. Серьёзные	

						технические ошибки (некорректные команды, нерабочие конфигурации). Отчёт фактически отсутствует или сформирован формально (копипаст, без личного вклада). Нет соответствия целям практического занятия. Отсутствуют доказательства выполнения (нет скриншотов, логов, выводов). 1 балла выставляется, если: Отчёт не представлен. Представлен файл-заглушка (пустой, не по теме, чужая работа без ссылок). Полное непонимание задачи и методологии. Конфигурации или команды противоречат принципам ИБ (например, рекомендуется оставить root-доступ открытым).	
3	7	Текущий контроль	Тестирование по тематике раздела 2	1	10	Студенту предлагается ответить на 10 тестовых вопросов, выбранных случайным образом. За каждый правильный ответ начисляется 1 балл.	дифференцированный зачет
4	7	Текущий контроль	Сдача отчета по практическим занятиям раздела 2	2	5	5 баллов выставляется, если: Все практические задания раздела выполнены полностью и корректно. Продемонстрировано глубокое понимание инженерных принципов ИБ. Все команды, конфигурации, скриншоты работоспособны и	дифференцированный зачет

						соответствуют цели. Отчёт структурирован, содержит все обязательные элементы (цель, ход работы, выводы). Использована рекомендованная литература (при необходимости). Нет фактических, технических или логических ошибок. 4 балла выставляется, если: Выполнены все задания, но с незначительными недочётами (например, одна ошибка в конфигурации, нет одного скриншота). Понимание темы достаточное, но не глубокое. Отчёт в целом соответствует требованиям, но возможны мелкие нарушения структуры или оформления. Имеются незначительные неточности в терминологии или рекомендациях. 3 балла выставляется, если: Выполнена основная часть заданий, но пропущены или ошибочны 1–2 пункта. Понимание ограничено: ответы шаблонные, без анализа. Отчёт не полностью структурирован (например, отсутствуют выводы или методология). Есть технические ошибки, но не критичные. Использование литературы	

						поверхностное или отсутствует. 2 балла выставляется, если: Выполнено менее 50% заданий. Серьёзные технические ошибки (некорректные команды, нерабочие конфигурации). Отчёт фактически отсутствует или сформирован формально (копипаст, без личного вклада). Нет соответствия целям практического занятия. Отсутствуют доказательства выполнения (нет скриншотов, логов, выводов). 1 балла выставляется, если: Отчёт не представлен. Представлен файл-заглушка (пустой, не по теме, чужая работа без ссылок). Полное непонимание задачи и методологии. Конфигурации или команды противоречат принципам ИБ (например, рекомендуется оставить root-доступ открытым).	
5	7	Текущий контроль	Тестирование по тематике раздела 3	1	10	Студенту предлагается ответить на 10 тестовых вопросов, выбранных случайным образом. За каждый правильный ответ начисляется 1 балл.	дифференцированный зачет
6	7	Текущий контроль	Сдача отчета по практическим занятиям раздела 3	2	5	5 баллов выставляется, если: Все практические задания раздела выполнены полностью и корректно. Продемонстрировано глубокое понимание	дифференцированный зачет

						инженерных принципов ИБ. Все команды, конфигурации, скриншоты работоспособны и соответствуют цели. Отчёт структурирован, содержит все обязательные элементы (цель, ход работы, выводы). Использована рекомендованная литература (при необходимости). Нет фактических, технических или логических ошибок. 4 балла выставляется, если: Выполнены все задания, но с незначительными недочётами (например, одна ошибка в конфигурации, нет одного скриншота). Понимание темы достаточное, но не глубокое. Отчёт в целом соответствует требованиям, но возможны мелкие нарушения структуры или оформления. Имеются незначительные неточности в терминологии или рекомендациях. 3 балла выставляется, если: Выполнена основная часть заданий, но пропущены или ошибочны 1–2 пункта. Понимание ограничено: ответы шаблонные, без анализа. Отчёт не полностью структурирован (например, отсутствуют выводы	

						или методология). Есть технические ошибки, но не критичные. Использование литературы поверхностное или отсутствует. 2 балла выставляется, если: Выполнено менее 50% заданий. Серьёзные технические ошибки (некорректные команды, нерабочие конфигурации). Отчёт фактически отсутствует или сформирован формально (копипаст, без личного вклада). Нет соответствия целям практического занятия. Отсутствуют доказательства выполнения (нет скриншотов, логов, выводов). 1 балла выставляется, если: Отчёт не представлен. Представлен файл-заглушка (пустой, не по теме, чужая работа без ссылок). Полное непонимание задачи и методологии. Конфигурации или команды противоречат принципам ИБ (например, рекомендуется оставить root-доступ открытым).	
7	7	Текущий контроль	Тестирование по тематике раздела 4	1	10	Студенту предлагается ответить на 10 тестовых вопросов, выбранных случайным образом. За каждый правильный ответ начисляется 1 балл.	дифференцированный зачет
8	7	Текущий контроль	Сдача отчета по практическим занятиям раздела 4	2	5	5 баллов выставляется, если: Все практические	дифференцированный зачет

						задания раздела выполнены полностью и корректно. Продемонстрировано глубокое понимание инженерных принципов ИБ. Все команды, конфигурации, скриншоты работоспособны и соответствуют цели. Отчёт структурирован, содержит все обязательные элементы (цель, ход работы, выводы). Использована рекомендованная литература (при необходимости). Нет фактических, технических или логических ошибок. 4 балла выставляется, если: Выполнены все задания, но с незначительными недочётами (например, одна ошибка в конфигурации, нет одного скриншота). Понимание темы достаточное, но не глубокое. Отчёт в целом соответствует требованиям, но возможны мелкие нарушения структуры или оформления. Имеются незначительные неточности в терминологии или рекомендациях. 3 балла выставляется, если: Выполнена основная часть заданий, но пропущены или ошибочны 1–2 пункта. Понимание ограничено: ответы	

						шаблонные, без анализа. Отчёт не полностью структурирован (например, отсутствуют выводы или методология). Есть технические ошибки, но не критичные. Использование литературы поверхностное или отсутствует. 2 балла выставляется, если: Выполнено менее 50% заданий. Серьёзные технические ошибки (некорректные команды, нерабочие конфигурации). Отчёт фактически отсутствует или сформирован формально (копипаст, без личного вклада). Нет соответствия целям практического занятия. Отсутствуют доказательства выполнения (нет скриншотов, логов, выводов). 1 балла выставляется, если: Отчёт не представлен. Представлен файл-заглушка (пустой, не по теме, чужая работа без ссылок). Полное непонимание задачи и методологии. Конфигурации или команды противоречат принципам ИБ (например, рекомендуется оставить root-доступ открытым).	
9	7	Проме-жуточная аттестация	Сдача дифференцированного зачета	-	5	Студент по итогам изучения дисциплины сдает дифференцированный зачет,	дифференцированный зачет

						предполагающий устный ответ на 3 вопроса из разных разделов курса. 5 баллов выставляется, если: По всем трём вопросам даны полные, глубокие, логически стройные ответы. Чётко использованы профессиональные термины, приведены примеры из практики ИТ-инженера. Демонстрируется системное понимание взаимосвязей между угрозами, уязвимостями, архитектурой и средствами защиты. Допускается не более одной незначительной неточности. 4 балла выставляется, если: Ответы по всем вопросам в целом полные, но недостаточно глубокие или частично обобщённые. Используется корректная терминология, но примеры отсутствуют или слабо связаны с темой. Есть небольшие пробелы в раскрытии отдельных аспектов (например, не указаны нормативные требования или пропущен этап аудита). 3 балла выставляется, если: Ответы фрагментарные: по 1–2 вопросам даны неполные или поверхностные пояснения. Наблюдаются ошибки	

						в терминах, неточности в определениях (например, путаница между угрозой и уязвимостью). Отсутствует логическая связь между компонентами ИТ-инфраструктуры и мерами защиты. Ответы демонстрируют базовое, но недостаточное владение компетенциями ИТ-инженера. 2 балла выставляется, если: Ответы содержательно слабые: по большинству вопросов — общие фразы без сути. Грубые ошибки в понятиях. Отсутствует понимание роли ИТ-инженера в обеспечении ИБ. Не раскрыта суть ни одного вопроса. 1 балл выставляется, если: Студент не смог ответить ни на один вопрос. Ответы полностью неверны или отсутствуют. Проявлено полное непонимание дисциплины и её целей.	

6.2. Процедура проведения, критерии оценивания

Вид промежуточной аттестации	Процедура проведения	Критерии оценивания
дифференцированный зачет	При оценивании результатов учебной деятельности обучающегося по дисциплине используется балльно-рейтинговая система оценивания результатов учебной деятельности обучающихся. Оценка за дисциплину формируется на основе полученных оценок за контрольно-рейтинговые мероприятия текущего контроля. Отлично: Величина рейтинга обучающегося по дисциплине 85…100 %. Хорошо: Величина рейтинга	В соответствии с пп. 2.5, 2.6 Положения

	обучающегося по дисциплине 75…84 %.Удовлетворительно: Величина рейтинга обучающегося по дисциплине 60…74 %. Неудовлетворительно: Величина рейтинга обучающегося по дисциплине 0…59 %. Если студент не согласен с оценкой, полученной по результатам текущего контроля, студент проходит мероприятие промежуточной аттестации в виде сдачи дифференцированного зачета по билетам, включающим 3 вопроса из разных разделов курса. На подготовку к ответу студенту дается 45 минут. По результатам дифференцированного зачета студент получает от 1 до 5 баллов. В случае прохождения дифференцированного зачета оценка за дисциплину рассчитывается на основе полученных оценок за контрольно-рейтинговые мероприятия текущего контроля и промежуточной аттестации. Фиксация результатов учебной деятельности по дисциплине проводится в день проведения дифференцированного зачета при личном присутствии студента.	

6.3. Паспорт фонда оценочных средств

Компетенции	Результаты обучения	№ КМ								
		1	2	3	4	5	6	7	8	9
ПК-10	Знает: основы информационной безопасности web-ресурсов	+	+	+	+					+
ПК-10	Умеет: проверять соответствие серверного оборудования требованиям ИР					+	+			+
ПК-10	Имеет практический опыт: проверки соответствия web-ресурсов требованиям информационной безопасности							+	+	+

Типовые контрольные задания по каждому мероприятию находятся в приложениях.

7. Учебно-методическое и информационное обеспечение дисциплины

Печатная учебно-методическая документация

а) основная литература:

Не предусмотрена

б) дополнительная литература:

Не предусмотрена

в) отечественные и зарубежные журналы по дисциплине, имеющиеся в библиотеке:

Не предусмотрены

г) методические указания для студентов по освоению дисциплины:

1. Методические указания к практическим занятиям по дисциплине «Анализ угроз и уязвимостей ИТ-инфраструктуры» (профиль подготовки: ИТ-инженерия)

из них: учебно-методическое обеспечение самостоятельной работы студента:

Электронная учебно-методическая документация

№	Вид литературы	Наименование ресурса в электронной форме	Библиографическое описание
1	Основная литература	Образовательная платформа Юрайт	Казарин, О. В. Надежность и безопасность программного обеспечения : учебник для вузов / О. В. Казарин, И. Б. Шубинский. — 2-е изд. — Москва : Издательство Юрайт, 2025. — 352 с. — (Высшее образование). — ISBN 978-5-534-19386-2. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/580669 (дата обращения: 11.12.2025).
2	Дополнительная литература	ЭБС издательства Лань	Нефедов, В. С. Безопасность прикладных информационных технологий и систем : учебное пособие / В. С. Нефедов. — 2-е изд. — Москва : РТУ МИРЭА, 2025. — 113 с. — ISBN 978-5-7339-2570-7. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/504831 (дата обращения: 11.12.2025). — Режим доступа: для авториз. пользователей.
3	Основная литература	ЭБС издательства Лань	Прохорова, О. В. Информационная безопасность и защита информации : учебник для вузов / О. В. Прохорова. — 6-е изд., стер. — Санкт-Петербург : Лань, 2025. — 124 с. — ISBN 978-5-507-52899-8. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/462293 (дата обращения: 11.12.2025). — Режим доступа: для авториз. пользователей.
4	Дополнительная литература	ЭБС издательства Лань	Шипулин, Г. Ф. Мониторинг инцидентов информационной безопасности. Средства защиты информации: межсетевые экраны, системы обнаружения и предотвращения вторжений : учебное пособие / Г. Ф. Шипулин. — Москва : РТУ МИРЭА, 2025. — 151 с. — ISBN 978-5-7339-2689-6. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/508442 (дата обращения: 11.12.2025). — Режим доступа: для авториз. пользователей.
5	Дополнительная литература	ЭБС издательства Лань	Шипулин, Г. Ф. Классификация средств защиты информации. Средства защиты информации: системы управления информацией о безопасности и событиями безопасности, системы предотвращения утечек данных : учебное пособие / Г. Ф. Шипулин. — Москва : РТУ МИРЭА, 2025. — 111 с. — ISBN 978-5-7339-2690-2. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/508443 (дата обращения: 11.12.2025). — Режим доступа: для авториз. пользователей.
6	Основная литература	ЭБС издательства Лань	Суворов, С. А. Современные угрозы и риски цифровых коммуникаций : учебно-методическое пособие / С. А. Суворов. — Тамбов : ТГУ им. Г.Р.Державина, 2025. — 121 с. — ISBN 978-5-00078-919-3. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/504523 (дата обращения: 11.12.2025). — Режим доступа: для авториз. пользователей.

Перечень используемого программного обеспечения:

1. The Wireshark developer community, http://www.wireshark.org-Wireshark (бессрочно)
2. -Oracle VM VirtualBox(бессрочно)
3. Docker-Docker(бессрочно)

Перечень используемых профессиональных баз данных и информационных справочных систем:

Нет

8. Материально-техническое обеспечение дисциплины

Вид занятий	№ ауд.	Основное оборудование, стенды, макеты, компьютерная техника, предустановленное программное обеспечение, используемое для различных видов занятий
Практические занятия и семинары	626 (3)	Комплект компьютерного оборудования; Локальная вычислительная сеть; Коммутатор, Программное обеспечение: ОС Windows XP , MS Office 2007, Matlab, WinRar, Mozila Firefox, Консультант+; Локальные СЗИ: Secret Net 6.5 (автономный вариант), Страж 3.0; Межсетевые экраны: ViPNet Custom 3.1, User Gate 5.2
Лекции	615 (3)	Комплект компьютерного оборудования, LCD Проектор, Экран проекционный, настенные стенды по защите информации (5 шт.), программное обеспечение: ОС Windows XP , MS Office 2007, Matlab, WinRar, Mozila Firefox, Консультант+