МИНОБРНАУКИ РОССИИ

ВЛАДИВОСТОКСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Рабочая программа дисциплины (модуля)

ЗАЩИЩЁННЫЕ ИНФОРМАЦИОННЫЕ СИСТЕМЫ

Направление и направленность (профиль)
11.03.02 Инфокоммуникационные технологии и системы связи. Защищенная инфокоммуникационная инфраструктура

Год набора на ОПОП
2026

Форма обучения
очная

Владивосток 2026

Рабочая программа дисциплины (модуля) «Защищённые информационные системы» составлена в соответствии с требованиями ФГОС ВО по направлению подготовки 11.03.02 Инфокоммуникационные технологии и системы связи (утв. приказом Минобрнауки России от 19.09.2017г. №930) и Порядком организации и осуществления образовательной деятельности по образовательным программам высшего образования – программам бакалавриата, программам специалитета, программам магистратуры (утв. приказом Минобрнауки России от 06.04.2021 г. N245).

Составитель(и):

Етчо С.А.

Шумик Е.Г.

Утверждена на заседании кафедры информационной безопасности от 14.05.2026 , протокол № 8

СОГЛАСОВАНО:

Заведующий кафедрой (разработчика)

Шумик Е.Г.

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ	
Сертификат	eg_1575874368
Номер транзакции	0000000000FE88B6
Владелец	Шумик Е.Г.

1 Цель, планируемые результаты обучения по дисциплине (модулю)

Целью освоения дисциплины является формирование у обучающихся системных знаний и практических навыков в области построения защищенных инфокоммуникационных инфраструктур, обеспечения безопасности сетей передачи данных и оценки эффективности применяемых средств защиты с использованием современных, в том числе отечественных, технологий и программных продуктов

Планируемыми результатами обучения по дисциплине (модулю), являются знания, умения, навыки. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения образовательной программы, представлен в таблице 1.

Таблица 1 – Компетенции, формируемые в результате изучения дисциплины (модуля)

Название ОПОП ВО, сокращенное	Код и формулировка компетенции	Код и формулировка индикатора достижения компетенции	Результаты обучения по дисциплине		
			Код результата	Формулировка результата	
11.03.02 «Инфокоммуникационные технологии и системы связи» (Б-ИК)	ПКВ-3 : Способен решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития информационных технологий, средств технической защиты информации, сетей и систем передачи информации	ПКВ-3.1к : Использует нормативные документы, регламентирующие работу по защите информации, а также положения, инструкции и другие организационно-распорядительные документы для решения поставленных задач	РД1	Знание	основные нормативные правовые акты, ГОСТы и методические документы в области информационной безопасности (ФСТЭК, Роскомнадзор).
		ПКВ-3.2к : Знает современную эталонную модель взаимодействия открытых систем, принципы построения и функционирования систем и сетей передачи информации	РД2	Умение	применять требования нормативной базы для разработки политик безопасности и решения практических задач.
		ПКВ-3.3к : Использует современные информационные технологии и программные средства, в том числе отечественного производства, для решения задач профессиональной деятельности	РД3	Знание	архитектуру модели OSI и TCP/IP, протоколы обмена данными, принципы маршрутизации и адресации в сетях передачи данных
			РД4	Навык	навыками работы с сетевым оборудованием, средствами администрирования, а также

					использованием отечественного ПО (например, операционные системы, средства криптографической защиты) для обеспечения безопасности.
		ПКВ-3.4к : Оценивает эффективность и надежность защиты вычислительных сетей, операционных систем и баз данных	РД5	Умение	проводить анализ защищенности сетевой инфраструктуры, оценивать риски, тестировать систему защиты на проникновение и интерпретировать полученные результаты.

В процессе освоения дисциплины решаются задачи воспитания гармонично развитой, патриотичной и социально ответственной личности на основе традиционных российских духовно-нравственных и культурно-исторических ценностей, представленные в таблице 1.2.

Таблица 1.2 – Целевые ориентиры воспитания

Воспитательные задачи	**Формирование ценностей**	**Целевые ориентиры**
Формирование гражданской позиции и патриотизма		
Воспитание уважения к Конституции и законам Российской Федерации	Гражданственность	Дисциплинированность
Формирование духовно-нравственных ценностей		
Воспитание чувства долга и ответственности перед семьей и обществом	Патриотизм	Доброжелательность и открытость
Формирование научного мировоззрения и культуры мышления		
Формирование осознания ценности научного мировоззрения и критического мышления	Взаимопомощь и взаимоуважение	Гибкость мышления
Формирование коммуникативных навыков и культуры общения		
Воспитание культуры диалога и уважения к мнению других людей	Высокие нравственные идеалы	Индивидуальность

2 Место дисциплины (модуля) в структуре ОПОП

Дисциплина относится к вариативной части учебного плана и опирается на дисциплины "основы информационной безопасности" и является основой для дисциплин "Защита информации с системах беспроводной связи", преддипломной практики

3. Объем дисциплины (модуля)

Объем дисциплины (модуля) в зачетных единицах с указанием количества академических часов, выделенных на контактную работу с обучающимися (по видам учебных занятий) и на самостоятельную работу, приведен в таблице 2.

Таблица 2 – Общая трудоемкость дисциплины

Название ОПОП ВО	Форма обуче-ния	Часть УП	Семестр (ОФО) или курс (ЗФО, ОЗФО)	Трудо-емкость	Объем контактной работы (час)						СРС	Форма аттес-тации
				(З.Е.)	Всего	Аудиторная			Внеауди-торная			
						лек.	прак.	лаб.	ПА	КСР		
11.03.02 Инфокоммуникационные технологии и системы связи	ОФО	Б1.В	6	5	37	0	0	36	1	0	143	Э

4 Структура и содержание дисциплины (модуля)

4.1 Структура дисциплины (модуля) для ОФО

Тематический план, отражающий содержание дисциплины (перечень разделов и тем), структурированное по видам учебных занятий с указанием их объемов в соответствии с учебным планом, приведен в таблице 3.1

Таблица 3.1 – Разделы дисциплины (модуля), виды учебной деятельности и формы текущего контроля для ОФО

№	Название темы	Код ре-зультата обучения	Кол-во часов, отведенное на				Форма текущего контроля
			Лек	Практ	Лаб	СРС	
1	Нормативно-правовая база защиты информации в РФ	РД1, РД2	0	0	6	24	Лабораторная работа, тест
2	Архитектура защищенных инфокоммуникационных сетей	РД3, РД4	0	0	6	24	Лабораторная работа, тест
3	Сетевые средства защиты информации	РД3, РД4	0	0	6	24	Лабораторная работа, тест
4	Защита операционных систем и баз данных	РД4, РД5	0	0	6	24	Лабораторная работа, тест
5	Криптографические методы защиты и отечественное ПО	РД4, РД5	0	0	6	24	Лабораторная работа, тест
6	Оценка эффективности и надежности системы защиты	РД5	0	0	6	24	Лабораторная работа, тест
Итого по таблице			**0**	**0**	**36**	**144**	

4.2 Содержание разделов и тем дисциплины (модуля) для ОФО

Тема 1 Нормативно-правовая база защиты информации в РФ.

Содержание темы: Система законодательства, органы регулирования (ФСТЭК, Роскомнадзор). Классификация угроз, требования к защите государственной тайны и персональных данных. Анализ рисков информационной безопасности.

Формы и методы проведения занятий по теме, применяемые образовательные технологии: лекция, лабораторные занятие.

Виды самостоятельной подготовки студентов по теме: подготовка к лабораторной работе.

Тема 2 Архитектура защищенных инфокоммуникационных сетей.

Содержание темы: Эталонная модель OSI и ее роль в обеспечении безопасности. Уязвимости на каждом уровне. Принципы построения безопасных сетей и систем передачи информации.

Формы и методы проведения занятий по теме, применяемые образовательные технологии: лекция, лабораторные занятие.

Виды самостоятельной подготовки студентов по теме: подготовка к лабораторной работе.

Тема 3 Сетевые средства защиты информации.

Содержание темы: Межсетевые экраны, системы обнаружения вторжений (СОВ), VPN. Настройка, конфигурирование и применение для защиты периметра сети.

Формы и методы проведения занятий по теме, применяемые образовательные технологии: лекция, лабораторные занятие.

Виды самостоятельной подготовки студентов по теме: подготовка к лабораторной работе.

Тема 4 Защита операционных систем и баз данных.

Содержание темы: Принципы безопасной настройки ОС (в т.ч. отечественных). Политики доступа, аудит, методы защиты СУБД от несанкционированного доступа и SQL-инъекций.

Формы и методы проведения занятий по теме, применяемые образовательные технологии: лекция, лабораторные занятие.

Виды самостоятельной подготовки студентов по теме: подготовка к лабораторной работе.

Тема 5 Криптографические методы защиты и отечественное ПО.

Содержание темы: Стандарты шифрования (ГОСТ), электронная подпись. Применение отечественных криптопровайдеров для защиты каналов связи и хранимой информации.

Формы и методы проведения занятий по теме, применяемые образовательные технологии: лекция, лабораторные занятие.

Виды самостоятельной подготовки студентов по теме: подготовка к лабораторной работе.

Тема 6 Оценка эффективности и надежности системы защиты.

Содержание темы: Методики тестирования на проникновение, сканирование уязвимостей. Анализ защищенности сетей, ОС и БД. Интерпретация результатов аудита безопасности.

Формы и методы проведения занятий по теме, применяемые образовательные технологии: лекция, лабораторные занятие.

Виды самостоятельной подготовки студентов по теме: подготовка к лабораторной работе.

5 Методические указания для обучающихся по изучению и реализации дисциплины (модуля)

5.1 Методические рекомендации обучающимся по изучению дисциплины и по обеспечению самостоятельной работы

5.2 Особенности организации обучения для лиц с ограниченными возможностями здоровья и инвалидов

При необходимости обучающимся из числа лиц с ограниченными возможностями здоровья и инвалидов (по заявлению обучающегося) предоставляется учебная информация в доступных формах с учетом их индивидуальных психофизических особенностей:

- для лиц с нарушениями зрения: в печатной форме увеличенным шрифтом; в форме электронного документа; индивидуальные консультации с привлечением тифлосурдопереводчика; индивидуальные задания, консультации и др.
- для лиц с нарушениями слуха: в печатной форме; в форме электронного документа; индивидуальные консультации с привлечением сурдопереводчика; индивидуальные задания, консультации и др.
- для лиц с нарушениями опорно-двигательного аппарата: в печатной форме; в форме электронного документа; индивидуальные задания, консультации и др.

6 Фонд оценочных средств для проведения текущего контроля и промежуточной аттестации обучающихся по дисциплине (модулю)

В соответствии с требованиями ФГОС ВО для аттестации обучающихся на соответствие их персональных достижений планируемым результатам обучения по дисциплине (модулю) созданы фонды оценочных средств. Типовые контрольные задания, методические материалы, определяющие процедуры оценивания знаний, умений и навыков, а также критерии и показатели, необходимые для оценки знаний, умений, навыков и характеризующие этапы формирования компетенций в процессе освоения образовательной программы, представлены в Приложении 1.

7 Учебно-методическое и информационное обеспечение дисциплины (модуля)

7.1 Основная литература

1. Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для вузов / О. В. Казарин, А. С. Забабурин. — Москва : Издательство Юрайт, 2026. — 312 с. — (Высшее образование). — ISBN 978-5-9916-9043-0. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/584673 (дата обращения: 19.05.2026).

2. Пушкин, П. Ю. Организационно-правовое обеспечение информационной безопасности : учебно-методическое пособие / П. Ю. Пушкин, Д. А. Головченко, Е. О. Карамышева. — Москва : РТУ МИРЭА, 2023. — 32 с. — ISBN 978-5-7339-1916-4. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/382658 (дата обращения: 25.05.2026). — Режим доступа: для авториз. пользователей.

3. Финогенов, А. А. Введение в криптографию : учебно-методическое пособие / А. А. Финогенов. — Ханты-Мансийск : ЮГУ, 2024. — 52 с. — Текст : электронный // Лань :

электронно-библиотечная система. — URL: https://e.lanbook.com/book/413330 (дата обращения: 25.05.2026). — Режим доступа: для авториз. пользователей.

7.2 Дополнительная литература

1. СПС Консультант Плюс
2. Хорев, П. Б. Программно-аппаратная защита информации : учебное пособие / П.Б. Хорев. — 2-е изд., испр. и доп. — Москва : ФОРУМ : ИНФРА-М, 2026. — 352 с. — (Среднее профессиональное образование). - ISBN 978-5-00091-557-8. - Текст : электронный. - URL: https://znanium.ru/catalog/product/2207457 (дата обращения: 31.05.2026)
3. Шаньгин, В. Ф. Информационная безопасность компьютерных систем и сетей : учебное пособие / В.Ф. Шаньгин. —Москва : ИНФРА-М, 2026. — 416 с. — (Среднее профессиональное образование). - ISBN 978-5-16-021164-0. - Текст : электронный. - URL: https://znanium.ru/catalog/product/2207574 (дата обращения: 31.05.2026)

7.3 Ресурсы информационно-телекоммуникационной сети "Интернет", включая профессиональные базы данных и информационно-справочные системы (при необходимости):

1. Образовательная платформа "ЮРАЙТ"
2. Электронно-библиотечная система "ZNANIUM.COM"
3. Электронно-библиотечная система "ЛАНЬ"
4. Open Academic Journals Index (OAJI). Профессиональная база данных - Режим доступа: http://oaji.net/
5. Президентская библиотека им. Б.Н.Ельцина (база данных различных профессиональных областей) - Режим доступа: https://www.prlib.ru/

8 Материально-техническое обеспечение дисциплины (модуля) и перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), включая перечень программного обеспечения

Основное оборудование:

- Компьютеры
- Проектор

Программное обеспечение:

- Microsoft Windows Professional 7 Russian

МИНОБРНАУКИ РОССИИ

ВЛАДИВОСТОКСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Фонд оценочных средств
для проведения текущего контроля
и промежуточной аттестации по дисциплине (модулю)

ЗАЩИЩЁННЫЕ ИНФОРМАЦИОННЫЕ СИСТЕМЫ

Направление и направленность (профиль)
11.03.02 Инфокоммуникационные технологии и системы связи. Защищенная инфокоммуникационная инфраструктура

Год набора на ОПОП
2026

Форма обучения
очная

Владивосток 2026

1 Перечень формируемых компетенций

Название ОПОП ВО, сокращенное	Код и формулировка компетенции	Код и формулировка индикатора достижения компетенции
11.03.02 «Инфокоммуникационные технологии и системы связи» (Б-ИК)	ПКВ-3 : Способен решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития информационных технологий, средств технической защиты информации, сетей и систем передачи информации	ПКВ-3.1к : Использует нормативные документы, регламентирующие работу по защите информации, а также положения, инструкции и другие организационно-распорядительные документы для решения поставленных задач
		ПКВ-3.2к : Знает современную эталонную модель взаимодействия открытых систем, принципы построения и функционирования систем и сетей передачи информации
		ПКВ-3.3к : Использует современные информационные технологии и программные средства, в том числе отечественного производства, для решения задач профессиональной деятельности
		ПКВ-3.4к : Оценивает эффективность и надежность защиты вычислительных сетей, операционных систем и баз данных

Компетенция считается сформированной на данном этапе в случае, если полученные результаты обучения по дисциплине оценены положительно (диапазон критериев оценивания результатов обучения «зачтено», «удовлетворительно», «хорошо», «отлично»). В случае отсутствия положительной оценки компетенция на данном этапе считается несформированной.

2 Показатели оценивания планируемых результатов обучения

Компетенция ПКВ-3 «Способен решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития информационных технологий, средств технической защиты информации, сетей и систем передачи информации»

Таблица 2.1 – Критерии оценки индикаторов достижения компетенции

Код и формулировка индикатора достижения компетенции	Результаты обучения по дисциплине			Критерии оценивания результатов обучения
	Код рез-та	Тип рез-та	Результат	
ПКВ-3.1к : Использует нормативные документы, регламентирующие работу по защите информации, а также положения, инструкции и другие организационно-распорядительные документы для решения поставленных задач	РД 1	Знание	основные нормативные правовые акты, ГОСТы и методические документы в области информационной безопасности (ФСТЭК, Роскомнадзор).	решение тестовых заданий
ПКВ-3.2к : Знает современную эталонную модель взаимодействия открытых систем, принципы построения и функционирования систем и сетей передачи информации	РД 2	Умение	применять требования нормативной базы для разработки политик безопасности и решения практических задач.	выполнение лабораторной работы

ПКВ-3.3к : Использует современные информационные технологии и программные средства, в том числе отечественного производства, для решения задач профессиональной деятельности	РД 3	Знание	архитектуру модели OSI и TCP/IP, протоколы обмена данными, принципы маршрутизации и адресации в сетях передачи данных	решение тестовых заданий
	РД 4	Навык	навыками работы с сетевым оборудованием, средствами администрирования, а также использованием отечественного ПО (например, операционные системы, средства криптографической защиты) для обеспечения безопасности.	выполнение лабораторной работы
ПКВ-3.4к : Оценивает эффективность и надежность защиты вычислительных сетей, операционных систем и баз данных	РД 5	Умение	проводить анализ защищенности сетевой инфраструктуры, оценивать риски, тестировать систему защиты на проникновение и интерпретировать полученные результаты.	выполнение лабораторной работы

Таблица заполняется в соответствии с разделом 1 Рабочей программы дисциплины (модуля).

3 Перечень оценочных средств

Таблица 3 – Перечень оценочных средств по дисциплине (модулю)

Контролируемые планируемые результаты обучения		Контролируемые темы дисциплины	Наименование оценочного средства и представление его в ФОС	
			Текущий контроль	Промежуточная аттестация
Очная форма обучения				
РД1	Знание : основные нормативные правовые акты, ГОСТы и методические документы в области информационной безопасности (ФСТЭК, Роскомнадзор).	1.1. Нормативно-правовая база защиты информации в РФ	Лабораторная работа	Экзамен в устной форме
			Тест	Экзамен в устной форме
РД2	Умение : применять требования нормативной базы для разработки политик безопасности и решения практических задач.	1.1. Нормативно-правовая база защиты информации в РФ	Лабораторная работа	Экзамен в устной форме
РД3	Знание : архитектуру модели OSI и TCP/IP, протоколы обмена данными, принципы маршрутизации и адресации в сетях передачи данных	1.2. Архитектура защищенных инфокоммуникационных сетей	Тест	Экзамен в устной форме
		1.3. Сетевые средства защиты информации	Тест	Экзамен в устной форме
РД4	Навык : навыками работы с сетевым оборудованием, средствами администрирования, а также использованием отечестве	1.2. Архитектура защищенных инфокоммуникационных сетей	Лабораторная работа	Экзамен в устной форме
		1.3. Сетевые средства защиты информации	Лабораторная работа	Экзамен в устной форме

	нного ПО (например, операционные системы, средства криптографической защиты) для обеспечения безопасности.	1.4. Защита операционных систем и баз данных	Лабораторная работа	Экзамен в устной форме
		1.5. Криптографические методы защиты и отечественное ПО	Лабораторная работа	Экзамен в устной форме
РД5	Умение : проводить анализ защищенности сетевой инфраструктуры, оценивать риски, тестировать систему защиты на проникновение и интерпретировать полученные результаты.	1.4. Защита операционных систем и баз данных	Лабораторная работа	Экзамен в устной форме
		1.5. Криптографические методы защиты и отечественное ПО	Лабораторная работа	Экзамен в устной форме
		1.6. Оценка эффективности и надежности системы защиты	Лабораторная работа	Экзамен в устной форме

4 Описание процедуры оценивания

Качество сформированности компетенций на данном этапе оценивается по результатам текущих и промежуточных аттестаций при помощи количественной оценки, выраженной в баллах. Максимальная сумма баллов по дисциплине (модулю) равна 100 баллам.

Вид учебной деятельности	Оценочное средство			
	Тест 1-5	Практическая работа	Экзамен	Итого
Лабораторные занятия	20	60		80
Промежуточная аттестация			20	20
Итого	20	60	20	100

Сумма баллов, набранных студентом по всем видам учебной деятельности в рамках дисциплины, переводится в оценку в соответствии с таблицей.

Сумма баллов по дисциплине	Оценка по промежуточной аттестации	Характеристика качества сформированности компетенции
от 91 до 100	«зачтено» / «отлично»	Студент демонстрирует сформированность дисциплинарных компетенций, обнаруживает всестороннее, систематическое и глубокое знание учебного материала, усвоил основную литературу и знаком с дополнительной литературой, рекомендованной программой, умеет свободно выполнять практические задания, предусмотренные программой, свободно оперирует приобретенными знаниями, умениями, применяет их в ситуациях повышенной сложности.
от 76 до 90	«зачтено» / «хорошо»	Студент демонстрирует сформированность дисциплинарных компетенций: основные знания, умения освоены, но допускаются незначительные ошибки, неточности, затруднения при аналитических операциях, переносе знаний и умений на новые, нестандартные ситуации.
от 61 до 75	«зачтено» / «удовлетворительно»	Студент демонстрирует сформированность дисциплинарных компетенций: в ходе контрольных мероприятий допускаются значительные ошибки, проявляется отсутствие отдельных знаний, умений, навыков по некоторым дисциплинарным компетенциям, студент испытывает значительные затруднения при оперировании знаниями и умениями при их переносе на новые ситуации.
от 41 до 60	«не зачтено» / «неудовлетворительно»	У студента не сформированы дисциплинарные компетенции, проявляется недостаточность знаний, умений, навыков.
от 0 до 40	«не зачтено» / «неудовлетворительно»	Дисциплинарные компетенции не сформированы. Проявляется полное или практически полное отсутствие знаний, умений, навыков.

5 Примерные оценочные средства

5.1 Пример заданий на лабораторную работу

Лабораторная работа №1

Тема: «Анализ нормативно-правовой базы и разработка организационно-распорядительных документов по защите информации»

Формируемые индикаторы:

- ПКВ-3.1к — использует нормативные документы, регламентирующие работу по защите информации, а также положения, инструкции и другие организационно-распорядительные документы для решения поставленных задач.
- ПКВ-3.2к — знает современную эталонную модель взаимодействия открытых систем, принципы построения и функционирования систем и сетей передачи информации.

Цель работы: Научиться применять требования нормативных актов РФ для создания базовых документов по защите инфокоммуникационной инфраструктуры.

Задание

1. **Изучите нормативные документы** из локальной базы, предоставленной преподавателем:
   - Приказ ФСТЭК России от 05.02.2021 № 31 «Об утверждении Требований к защите информации…»;
   - Методику оценки угроз безопасности информации (утв. ФСТЭК 05.02.2021);
   - ГОСТ Р 56545-2015 «Защита информации. Уязвимости информационных систем. Правила описания уязвимостей».
2. **Выберите объект защиты** из предложенного списка (по указанию преподавателя):
   - Учебная сеть университетского кампуса;
   - Сеть небольшого интернет-провайдера;
   - Отдел информационных технологий предприятия;
   - Локальная сеть государственного учреждения.
3. **Составьте Частную модель угроз** для выбранного объекта в табличной форме:

№	Источник угрозы	Тип угрозы	Объект воздействия	Возможный ущерб	Мера противодействия
1	Внешний злоумышленник	DDoS-атака на маршрутизатор	Сетевой периметр	Нарушение доступности услуг	Использование МЭ с защитой от DDoS
2	Инсайдер (сотрудник)	Несанкционированный доступ к БД клиентов	Сервер БД	Утечка персональных данных	Разграничение доступа, аудит
...	...	...	...	...	...

Примечание: модель должна содержать не менее 8 угроз, охватывающих разные уровни модели OSI.

1. **Разработайте фрагмент «Политики безопасности»** для выбранного объекта, включающий:
   - Правила управления сетевым доступом (кто, куда, при каких условиях);
   - Требования к регистрации событий безопасности (аудит);
   - Порядок реагирования на инциденты (начальные действия).
2. **Оформите отчёт** в виде внутреннего организационно-распорядительного документа организации (шрифт Times New Roman 14, межстрочный интервал 1,5, объём 5–7 страниц).

Лабораторная работа №2
Тема: «Анализ уязвимостей сетевых протоколов на основе модели OSI/TCP/IP»
Формируемые индикаторы:

- ПКВ-3.2к — знает современную эталонную модель взаимодействия открытых систем, принципы построения и функционирования систем и сетей передачи информации.
- ПКВ-3.4к — оценивает эффективность и надежность защиты вычислительных сетей, операционных систем и баз данных.

Цель работы: Научиться выявлять типовые уязвимости на разных уровнях модели OSI и предлагать меры защиты с использованием штатных средств ОС.

Задание

1. **Настройте захват трафика** на виртуальной машине с РЕД ОС с использованием штатного сниффера tcpdump:
   - Захватите 100 пакетов на интерфейсе eth0: sudo tcpdump -i eth0 -c 100 -w capture.pcap.
   - Просмотрите содержимое: tcpdump -r capture.pcap -vv.
2. **Выполните следующие действия и запишите трафик для каждого:**
   - ping на IP-адрес локального шлюза (или другого узла в лабораторной сети);
   - подключение к локальному HTTP-серверу (развёрнутому в лабораторной сети);
   - подключение к локальному FTP-серверу (если доступен);
   - DNS-запрос к локальному DNS-серверу (если доступен).
3. **Для каждого захваченного сеанса определите:**
   - используемые протоколы (MAC, IP, TCP/UDP, HTTP, FTP, DNS);
   - какая информация передаётся в открытом виде;
   - какие атаки возможны на каждом уровне модели OSI.
4. **Составьте таблицу уязвимостей** с рекомендациями по защите:

Уровень OSI	Протокол	Тип уязвимости	Способ противодействия (отечественное средство)
Канальный	ARP	Подмена ARP-таблиц	Статические ARP-записи, сегментация VLAN
Сетевой	IP	IP-спуфинг	Входная фильтрация на МЭ
Транспортный	TCP	SYN-flood	Настройка параметров стека TCP + МЭ
Прикладной	HTTP	Перехват данных	Использование HTTPS, СКЗИ
...	...	...	...

1. **Оформите отчёт** — включите скриншоты захвата, анализ каждого протокола и таблицу уязвимостей.

Лабораторная работа №3
Тема: «Установка и настройка отечественной ОС с элементами защиты»
Формируемые индикаторы:

- ПКВ-3.3к — использует современные информационные технологии и программные средства, в том числе отечественного производства, для решения задач профессиональной деятельности.
- ПКВ-3.4к — оценивает эффективность и надежность защиты операционных систем.

Цель работы: Получить практические навыки установки, первичной настройки и аудита безопасности ОС семейства Linux отечественного производства.

Задание

1. **Установите РЕД ОС** (или Astra Linux Special Edition) на виртуальную машину:
   - Используйте гипервизор, предоставленный в лаборатории (РЕД Виртуализация, zVirt или VirtualBox из локального репозитория).
   - Параметры ВМ: ОЗУ — 2 ГБ, HDD — 20 ГБ, сеть — NAT + мост.
2. **Создайте учётные записи:**
   - admin — с полными правами (группа wheel);
   - operator — с ограниченными правами (только для выполнения заданных команд);
   - guest — только для просмотра системных логов.
3. **Настройте парольную политику:**
   - Минимальная длина пароля — 12 символов;
   - Срок действия пароля — 90 дней;
   - Блокировка учётной записи после 3 неудачных попыток входа.
4. **Включите системный аудит (**auditd**)** для отслеживания:
   - Неудачных попыток входа;
   - Изменений файлов /etc/passwd и /etc/shadow;
   - Изменений конфигурации сетевых интерфейсов.
5. **Проведите оценку защищённости** с использованием oscap:
   - Выполните сканирование по профилю безопасности (например, CIS или профиль ФСТЭК).
   - Сгенерируйте отчёт в формате HTML.
   - Исправьте не менее 3 критических замечаний и зафиксируйте изменения.
6. **Оформите отчёт** — приложите скриншоты процесса установки, настроек PAM, конфигурации auditd, результатов oscap и список внесённых изменений.

Лабораторная работа №4
Тема: «Настройка межсетевого экрана в отечественной ОС»
Формируемые индикаторы:

- ПКВ-3.3к — использует современные информационные технологии и программные средства, в том числе отечественного производства.
- ПКВ-3.4к — оценивает эффективность и надежность защиты вычислительных сетей.

Цель работы: Освоить базовое конфигурирование межсетевого экрана на российской ОС.

Задание

1. **Настройте nftables** на виртуальной машине с РЕД ОС в соответствии со следующей политикой:
   - Политика по умолчанию для INPUT — DROP, для OUTPUT — ACCEPT, для FORWARD — DROP;
   - Разрешить локальный интерфейс lo и все установленные соединения (ct state established,related);
   - Разрешить SSH-доступ только с IP-адреса, указанного преподавателем;
   - Разрешить HTTP (порт 80) и DNS (порт 53) для всех;
   - Настроить маскарадинг (SNAT) для интерфейса eth0.
2. **Проверьте работоспособность:**
   - Подключение по SSH с разрешённого IP (должно быть разрешено);
   - Подключение по SSH с любого другого IP (должно быть заблокировано);

- Доступ к веб-страницам (если сеть позволяет).

3. **Сохраните конфигурацию** в /etc/nftables.conf и настройте автозапуск.
4. **Настройте систему обнаружения вторжений** (IDS) на основе штатного аудита РЕД ОС или отечественного продукта (при наличии):
   - Настройте мониторинг неудачных попыток подключения к SSH.
   - Протестируйте — выполните несколько неудачных попыток входа и проверьте, что они зафиксированы в логах.
5. **Оформите отчёт** — приложите содержимое конфигурационных файлов и результаты проверки.

Лабораторная работа №5
Тема: «Организация защищённого канала с использованием отечественного СКЗИ»
Формируемые индикаторы:

- ПКВ-3.3к — использует современные информационные технологии и программные средства, в том числе отечественного производства.
- ПКВ-3.4к — оценивает эффективность и надежность защиты каналов связи.

Цель работы: Создать защищённый туннель с использованием российского сертифицированного СКЗИ.

Задание

1. **Установите ViPNet Coordinator HW** (или CryptoPro VPN) на две виртуальные машины (сервер и клиент). Если коммерческое ПО недоступно — используйте OpenVPN с плагином ГОСТ (предоставляется преподавателем).
2. **Настройте туннель между двумя ВМ:**
   - Используйте алгоритмы шифрования по ГОСТ 28147-89 (или ГОСТ Р 34.12-2015);
   - Настройте взаимную аутентификацию через сертификаты (для ViPNet — встроенные средства; для OpenVPN — через сертификаты с поддержкой ГОСТ).
3. **Проверьте работоспособность:**
   - Выполните ping между ВМ через туннель (должен проходить);
   - Захватите трафик на внешнем интерфейсе с помощью tcpdump — убедитесь, что данные зашифрованы;
   - Запустите iperf3 (если установлен локально) для оценки пропускной способности туннеля и сравните с незашифрованным каналом.
4. **Проанализируйте** преимущества сертифицированного СКЗИ перед зарубежными аналогами с точки зрения законодательства РФ.
5. **Оформите отчёт** — включите конфигурационные файлы, скриншоты захвата трафика и результаты замеров.

Лабораторная работа №6
Тема: «Оценка защищённости инфокоммуникационной инфраструктуры»
Формируемые индикаторы:

- ПКВ-3.4к — оценивает эффективность и надежность защиты вычислительных сетей, операционных систем и баз данных.
- ПКВ-3.1к — использует нормативные документы для решения поставленных задач.

Цель работы: Провести ограниченный анализ защищённости учебной сети и подготовить рекомендации по устранению уязвимостей.

Задание

1. **Создайте тестовый стенд** из двух виртуальных машин:
   - ВМ-сервер: РЕД ОС + Apache HTTP Server + PostgreSQL (Postgres Pro);
   - ВМ-клиент: РЕД ОС с набором инструментов для анализа (nmap, Nikto — из локального репозитория).
2. **Выполните сбор информации о целевой системе:**
   - nmap -sV -p- 192.168.x.x — сканирование портов и определение служб;
   - nmap --script http-enum 192.168.x.x — перебор скрытых директорий веб-сервера.
3. **Выполните проверку на наличие простейших уязвимостей:**
   - Проверка наличия стандартных уязвимых скриптов на веб-сервере;
   - Проверка наличия открытых портов с слабой аутентификацией (например, Telnet).
4. **Составьте отчёт о защищённости** в соответствии с ГОСТ Р 56545-2015:
   - Введение (цель, методы, объект);
   - Описание методологии (какие инструменты и почему использованы);
   - Таблица найденных уязвимостей с уровнем критичности (CRITICAL, HIGH, MEDIUM, LOW);
   - Рекомендации по устранению каждой уязвимости с указанием конкретных настроек или нормативных требований;
   - Заключение.
5. **Подготовьте краткую презентацию (5 минут)** для защиты отчёта.

Краткие методические указания

На выполнение одной лабораторной работы отводится не менее трех занятий. После выполнения каждой практической работы студент должен представить отчет о ее выполнении, а также, по указаниям преподавателя, выполнить дополнительные задания по теме

Шкала оценки

Оценка	Баллы	Описание
5	8-10	Оценка «отлично» выставляется, если студент выполнил задание, правильно применил методы.
4	5-7	Оценка «хорошо» выставляется, если студент выполнил задание, правильно применил методы, но совершил логические ошибки.
3	2-4	Оценка «удовлетворительно» выставляется, если студент выполнил задание, но применил методы не все необходимые методы для его выполнения.
2	0-1	Оценка «неудовлетворительно» выставляется в случае, если студент не выполнил задание и/ или неверно применил методы необходимые его выполнения.

5.2 Примеры тестовых заданий

1. Какой документ является основным при определении требований к защите информации в государственных информационных системах?

а) ГОСТ Р 56545-2015
б) Приказ ФСТЭК России от 05.02.2021 № 31
в) Методика оценки угроз безопасности информации
г) ВСЕ перечисленные документы применяются в совокупности

2. Что такое Частная модель угроз?

а) Перечень всех возможных угроз для любого объекта информатизации
б) Перечень угроз, актуальных для конкретного объекта информатизации, с оценкой реализуемости и опасности

в) Модель, описывающая только внешние угрозы
г) Модель, описывающая только внутренние угрозы

3. Какой орган власти в РФ осуществляет регулирование в области защиты государственной тайны и сертификации СКЗИ?

а) ФСТЭК России
б) Роскомнадзор
в) ФСБ России
г) Министерство цифрового развития

4. Какой раздел обязательно должен присутствовать в Политике безопасности организации?

а) Финансовые показатели деятельности
б) Правила управления доступом к информационным ресурсам
в) Описание бизнес-процессов
г) Структура штатного расписания

5. На каком уровне модели OSI работает протокол IP?

а) Физический
б) Канальный
в) Сетевой
г) Транспортный

6. Какой протокол используется для преобразования доменных имён в IP-адреса?

а) ARP
б) DNS
в) DHCP
г) ICMP

7. Какая из перечисленных атак характерна для канального уровня модели OSI?

а) SYN-flood
б) ARP-spoofing
в) SQL-инъекция
г) IP-спуфинг

8. Какой протокол обеспечивает установку соединения с гарантированной доставкой данных?

а) UDP
б) TCP
в) ICMP
г) IGMP

9. Какая отечественная операционная система включена в реестр российского ПО и используется для защиты объектов КИИ?

а) Windows Server
б) macOS Server
в) РЕД ОС
г) Ubuntu Server

10. Каким инструментом в РЕД ОС выполняется настройка сетевого экрана?

а) iptables
б) nftables
в) ipfw
г) pf

11. Какой механизм в Linux позволяет ограничивать ресурсы (например, количество процессов) для пользователей и групп?

а) cgroups
б) systemd

в) SELinux
г) PAM

12. Какой модуль PAM отвечает за блокировку учётной записи после нескольких неудачных попыток входа?

а) pam_unix
б) pam_tally2
в) pam_limits
г) pam_env

13. Какое программное обеспечение относится к средствам криптографической защиты информации (СКЗИ), сертифицированным в РФ?

а) OpenSSL
б) CryptoPro
в) GnuPG
г) OpenVPN

14. Какой тип межсетевого экрана анализирует содержимое пакетов и принимает решения на основе правил, заданных администратором?

а) Прокси-сервер
б) Фильтрующий маршрутизатор
в) Межсетевой экран с инспекцией состояния (stateful)
г) Шлюз прикладного уровня

15. В nftables какие правила применяются к пакетам, входящим на интерфейс?

а) Цепочка INPUT
б) Цепочка OUTPUT
в) Цепочка FORWARD
г) Цепочка PREROUTING

16. Какое правило в nftables позволяет разрешить все установленные соединения?

а) ct state new accept
б) ct state related accept
в) ct state established accept
г) ct state established,related accept

17. Что такое система обнаружения вторжений (IDS)?

а) Система, которая блокирует все входящие соединения
б) Система, которая анализирует трафик или логи для выявления аномалий и атак
в) Система, которая шифрует весь сетевой трафик
г) Система, которая управляет доступом к файлам

18. Какой из перечисленных инструментов предназначен для сканирования сети и определения открытых портов?

а) Wireshark
б) nmap
в) hydra
г) sqlmap

19. Какой алгоритм шифрования является национальным стандартом РФ?

а) AES
б) DES
в) ГОСТ 28147-89
г) RSA

20. Что такое тест на проникновение (пентест)?

а) Оценка соответствия системы требованиям нормативных документов
б) Моделирование действий злоумышленника для выявления уязвимостей в системе
в) Установка дополнительных средств защиты
г) Аудит конфигурации системы

Краткие методические указания

Тестовые задания состоят из вопроса и нескольких вариантов ответа. Решение представляет собой указание номера вопроса и букву, которой обозначен правильный, по мнению студента, вариант ответа. В течение семестра проводится 6 тестов по 6 темам на лекционных занятиях, в каждом тесте 16 вопросов.

Шкала оценки

Оценка	Баллы	Описание
5	5	Студент допустил не более 2х ошибок
4	4	Студент совершил от 3 до 6 ошибок в ответах на тест
3	2-3	Студент совершил от 7 до 10 ошибок в ответах на тест
2	0-1	Студент совершил 11 и более ошибок в ответах на тест

5.3 Вопросы к экзамену

Вопрос 1.
Нормативно-правовое регулирование защиты информации в Российской Федерации.
Перечислите основные органы государственной власти, осуществляющие регулирование в области информационной безопасности (ФСТЭК, ФСБ, Роскомнадзор). Опишите их полномочия и сферы ответственности. Какие нормативные документы являются ключевыми при разработке системы защиты инфокоммуникационной инфраструктуры?

Вопрос 2.
Эталонная модель взаимодействия открытых систем (OSI): назначение, уровни, протоколы.
Дайте характеристику семи уровням модели OSI. Для каждого уровня укажите: основную функцию, примеры протоколов, типовые угрозы безопасности. Чем модель OSI отличается от стека протоколов TCP/IP?

Вопрос 3.
Классификация угроз информационной безопасности в инфокоммуникационных системах.
По каким признакам классифицируются угрозы? Приведите примеры угроз по источникам (внешние/внутренние), по характеру воздействия (активные/пассивные), по цели (нарушение конфиденциальности, целостности, доступности). Что такое модель угроз и для чего она разрабатывается?

Вопрос 4.
Организационно-распорядительные документы в области защиты информации.
Что такое Политика безопасности? Какие разделы она должна содержать? Какие ещё организационно-распорядительные документы разрабатываются в организации (инструкции, регламенты, положения)? Приведите пример структуры Политики безопасности для оператора связи.

Вопрос 5.
Архитектура защищённых инфокоммуникационных сетей.
Какие принципы закладываются при проектировании защищённой сети? Опишите понятия «периметр безопасности», «зоны доверия», «демилитаризованная зона (DMZ)». Как эти принципы соотносятся с уровнями модели OSI?

Вопрос 6.
Уязвимости сетевых протоколов: причины возникновения и методы защиты.
Опишите типовые уязвимости для протоколов: ARP, IP, TCP, HTTP. Какие атаки возможны на каждом уровне модели OSI? Какие меры защиты применяются на сетевом и прикладном уровнях?

Вопрос 7.
Международные и российские стандарты в области информационной безопасности.
Охарактеризуйте стандарты серии ISO/IEC 27000, ГОСТ Р ИСО/МЭК 15408, ГОСТ Р 56545-2015. Для каких целей они применяются? Какие российские стандарты обязательны для выполнения требований ФСТЭК?

Вопрос 8.
Принципы построения систем и сетей передачи информации.
Опишите основные топологии сетей (звезда, кольцо, шина, mesh). Какие требования к надёжности и безопасности предъявляются к сетям передачи данных? Как выбор топологии влияет на защищённость инфраструктуры?

Вопрос 9.
Отечественные операционные системы: архитектура, механизмы защиты, применение.
Опишите архитектуру РЕД ОС и Astra Linux. Какие механизмы мандатного управления доступом (для Astra Linux) и дискреционного управления доступом используются? В чём преимущества использования российских ОС для объектов КИИ?

Вопрос 10.
Настройка парольной политики и управление учётными записями в Linux.
Опишите механизмы PAM (Pluggable Authentication Modules) и их роль в аутентификации. Как настроить срок действия пароля, минимальную длину и сложность? Как реализовать блокировку учётной записи после нескольких неудачных попыток входа?

Вопрос 11.
Системный аудит в ОС Linux: назначение, настройка, анализ.
Что такое auditd? Опишите правила аудита, форматы логов. Какие события рекомендуется отслеживать на защищённом сервере? Приведите примеры правил для отслеживания изменений конфигурационных файлов и неудачных попыток входа.

Вопрос 12.
Межсетевые экраны: классификация, функции, принципы работы.
Опишите типы межсетевых экранов (пакетный фильтр, stateful-МЭ, прокси-сервер, UTM). В чём отличие iptables от nftables? Приведите примеры правил для блокировки определённых протоколов и адресов.

Вопрос 13.
Системы обнаружения вторжений (IDS) и системы предотвращения вторжений (IPS).
В чём отличие IDS от IPS? Опишите принципы работы сигнатурного и поведенческого анализа. Какие российские продукты в этой области вам известны? Приведите примеры событий, которые должны фиксироваться IDS.

Вопрос 14.
Криптографическая защита информации (СКЗИ): законодательство, алгоритмы, применение.
Какие нормативные документы регулируют использование СКЗИ в РФ? Опишите основные алгоритмы шифрования по ГОСТ (ГОСТ 28147-89, ГОСТ Р 34.12-2015). Где применяется СКЗИ в инфокоммуникационных системах? Приведите примеры отечественных криптопровайдеров.

Вопрос 15.
Защищённые виртуальные частные сети (VPN): протоколы, архитектура, отечественные решения.
Опишите принципы работы VPN (туннелирование, шифрование, аутентификация). Какие протоколы используются? Какие российские VPN-решения (ViPNet, S-Terra, CryptoPro VPN) вам известны? В чём их преимущества перед зарубежными аналогами?

Вопрос 16.
Оценка защищённости операционной системы: методы и инструменты.
Опишите методику аудита безопасности ОС. Какие инструменты используются (например, oscap, lynis)? Что такое профили безопасности (CIS, ФСТЭК)? Как интерпретировать результаты аудита и исправлять найденные уязвимости?

Вопрос 17.
Оценка эффективности межсетевого экрана: методика и критерии.
Как проверить корректность работы правил межсетевого экрана? Какие тесты проводятся

для оценки эффективности (сканирование портов, тестирование прохождения пакетов)? Как оценить производительность МЭ (пропускная способность, задержки)?

Вопрос 18. Тестирование на проникновение (пентест): цели, этапы, этические ограничения. Опишите этапы проведения пентеста (сбор информации, сканирование, эксплуатация уязвимостей, анализ). Какие нормативные документы регламентируют проведение пентеста в РФ? Какие ограничения накладываются на проведение пентеста на объектах КИИ?

Вопрос 19. Анализ уязвимостей веб-приложений и СУБД: методы обнаружения. Какие уязвимости характерны для веб-приложений (OWASP Top 10)? Опишите методы обнаружения SQL-инъекций и XSS. Какие инструменты используются для сканирования уязвимостей веб-приложений? Приведите примеры защиты СУБД от несанкционированного доступа.

Вопрос 20. Комплексная оценка защищённости инфокоммуникационной инфраструктуры. Опишите методику комплексной оценки защищённости, включающую анализ сетевой безопасности, защищённости ОС и БД, оценки политик безопасности и организационных мер. Как готовится итоговый отчёт о защищённости? Какую структуру должен иметь отчёт в соответствии с ГОСТ Р 56545-2015?

Краткие методические указания

Для подготовки к экзамену студенту необходимо изучить материал в рамках лабораторных работ, а так же материал представленный в дополнительных источниках.

Шкала оценки

Оценка	Баллы	Описание
5	14-20	Оценка «отлично» выставляется студенту, если он глубоко и прочно усвоил программный материал исчерпывающе, последовательно, четко и логически стройно его излагает, умеет тесно увязывать теорию с практикой.
4	8-12	Оценка «хорошо» выставляется студенту, если он твердо знает материал, грамотно и по существу излагает его, не допуская существенных неточностей в ответе на вопрос, правильно применяет теоретические положения при решении практических вопросов и задач.
3	2-6	Оценка «удовлетворительно» выставляется студенту, если он имеет знания только основного материала, но не усвоил его деталей, допускает неточности, недостаточно правильные формулировки.
2	0-2	Оценка «неудовлетворительно» выставляется студенту, который не знает значительной части программного материала, допускает существенные ошибки.