МИНОБРНАУКИ РОССИИ

ВЛАДИВОСТОКСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Рабочая программа дисциплины (модуля)

МОДЕЛИРОВАНИЕ УГРОЗ И ТЕСТИРОВАНИЕ ЗАЩИЩЕННОСТИ ИНФРАСТРУКТУРЫ

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) «Моделирование угроз и тестирование защищенности инфраструктуры» 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):

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	0000000000FE88D8
Владелец	Шумик Е.Г.

1 Цель, планируемые результаты обучения по дисциплине (модулю)

Цель: Подготовка специалистов, способных выявлять, анализировать и моделировать актуальные угрозы информационной безопасности, а также проводить тестирование защищенности инфраструктуры для оценки эффективности существующих мер защиты .

Задачи:

- Изучить методы построения моделей угроз и нарушителей.
- Освоить методы качественной и количественной оценки рисков.
- Получить навыки тестирования на проникновение сетевого и прикладного уровней.
- Научиться использовать результаты моделирования и тестирования для выработки рекомендаций по усилению защиты.

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-3.2к : Знает современную эталонную модель взаимодействия открытых систем, принципы построения и функционирования систем и сетей передачи информации	РД1	Знание	современную эталонную модель взаимодействия открытых систем (OSI), принципы построения и функционирования систем и сетей передачи информации
		ПКВ-3.4к : Оценивает эффективность и надежность защиты вычислительных сетей, операционных систем и баз данных	РД2	Умение	анализировать конфигурации сетевых устройств, ОС и СУБД на предмет выявления уязвимостей; оценивать корректность применения механизмов аутентификации, разграничения доступа и шифрования
	ПКВ-4 : Способен осуществлять сбор и анализ исходных данных для проектирования,	ПКВ-4.2к : Разрабатывает компоненты комплексных систем защиты информации	РД3	Навык	методами оценки стойкости и надёжности парольных политик, межсетевых

	проектировать и разрабатывать устройства связи и компоненты систем защиты информации	автоматизированных систем			экранов и систем обнаружения вторжений
			РД4	Навык	навыками разработки компонентов СЗИ (политик безопасности, моделей доступа, регламентов) на основе выявленных угроз и уязвимостей; способностью обосновывать выбор и архитектуру технических средств защиты.

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	Осознание ценности профессии
Формирование духовно-нравственных ценностей		
Воспитание чувства долга и ответственности перед семьей и обществом	Высокие нравственные идеалы	Любовь к стране
Формирование научного мировоззрения и культуры мышления		
Развитие познавательного интереса и стремления к знаниям	Взаимопомощь и взаимоуважение	Ответственное отношение к окружающей среде и обществу
Формирование коммуникативных навыков и культуры общения		
Развитие умения эффективно общаться и сотрудничать	Созидательный труд	Чувство коллективизма

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 "Мониторинг событий и управление инцендентами", 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 обучения	Часть УП	Семестр (ОФО) или курс (ЗФО, ОЗФО)	Трудоемкость	Объем контактной работы (час)						СРС	Форма аттестации
				(З.Е.)	Всего	Аудиторная			Внеаудиторная			
						лек.	прак.	лаб.	ПА	КСР		
11.03.02 Инфокоммуникационные технологии и системы связи	ОФО	Б1.В	6	4	55	18	0	36	1	0	89	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 результата обучения	Кол-во часов, отведенное на				Форма текущего контроля
			Лек	Практ	Лаб	СРС	
1	Теоретические основы моделирования угроз	РД1, РД2	6	0	12	30	Лабораторная работа, тест
2	Методы и средства тестирования защищенности	РД1, РД2, РД3, РД4	6	0	12	30	Лабораторная работа, тест
3	Проектирование компонентов СЗИ на основе анализа угроз	РД1, РД3, РД4	6	0	12	30	Лабораторная работа, тест
Итого по таблице			**18**	**0**	**36**	**90**	

4.2 Содержание разделов и тем дисциплины (модуля) для ОФО

Тема 1 Теоретические основы моделирования угроз .

Содержание темы: Понятия угрозы, уязвимости, риска. Классификация угроз и нарушителей. Обзор методик ФСТЭК России по моделированию угроз. Модель угроз для АС. Идентификация активов. Анализ структурных и функциональных характеристик системы. Построение модели нарушителя (внешний/внутренний, уровень знаний, оснащённость). Методологии STRIDE и DREAD. Практическое применение для оценки угроз и расчёта критичности рисков. Нормативная база. Обзор требований к защите информации в государственных ИС, КИИ и системах персональных данных. .

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 Методы и средства тестирования защищенности.

Содержание темы: Введение в пентест. Этические и правовые аспекты. Жизненный цикл тестирования (PTES, OWASP). Сбор информации. Технологии OSINT. Пассивный и активный разведка. Сканирование портов, обнаружение служб (Nmap, Masscan). Тестирование сетевого уровня. Анализ уязвимостей протоколов TCP/IP. Атаки на маршрутизацию и коммутацию (ARP-spoofing, VLAN hopping). Тестирование веб-приложений. Основные уязвимости OWASP Top 10: SQL-инъекции, XSS, CSRF. Использование Burp Suite. Анализ защищённости ОС и СУБД. Проверка политик паролей, прав доступа. Поиск типовых ошибок конфигурации (CIS Benchmarks). .

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 Проектирование компонентов СЗИ на основе анализа угроз.

Содержание темы: Выбор средств защиты. Критерии выбора межсетевых экранов, систем обнаружения вторжений (IDS/IPS), антивирусных средств. Разработка политик безопасности. Формирование матриц доступа. Разработка регламентов реагирования на инциденты. Оценка эффективности. Методики оценки эффективности применения СЗИ. Анализ возврата инвестиций (ROI) в безопасность. Документирование. Оформление актов тестирования, отчётов об уязвимостях и частных технических заданий на разработку СЗИ. .

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

Самостоятельная работа студентов (СРС) — это деятельность учащихся, которую они совершают без непосредственной помощи и указаний преподавателя, руководствуясь сформировавшимися ранее представлениями о порядке и правильности выполнения операций. Цель СРС в процессе обучения заключается, как в усвоении знаний, так и в формировании умений и навыков по их использованию в новых условиях на новом учебном материале. Самостоятельная работа призвана обеспечивать возможность осуществления студентами самостоятельной познавательной деятельности в обучении, и является видом учебного труда, способствующего формированию у студентов самостоятельности. В данной учебной программе приведен перечень основных и дополнительных источников, которые предлагается изучить в процессе облучения по дисциплине. Кроме того, для расширения и углубления знаний по данной дисциплине целесообразно использовать: научные публикации в тематических журналах; полнотекстовые базы данных библиотеки; имеющиеся в библиотеках вуза и региона публикаций на электронных и бумажных носителях. Успешное освоение дисциплины предполагает активную работу студентов на всех занятиях аудиторной формы: лекций и практических занятий, выполнение аттестационный мероприятий, эффективную самостоятельную работу. В процессе изучения дисциплины студенту необходимо ориентироваться на самостоятельную проработку лекционного материала, подготовку к практическим занятиям, выполнение

тестов, самостоятельное изучение некоторых разделов курса Для проведения занятий лекционного типа используются учебно-наглядные пособия в форме презентационных материалов, обеспечивающих тематические иллюстрации, соответствующие темам лекций, представленным в пункте 4 настоящей РПД

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. Кунин, Н. Т. Криптографическая защита информации: Практикум : учебное пособие / Н. Т. Кунин. — Москва : РТУ МИРЭА, 2025. — 66 с. — ISBN 978-5-7339-2447-2. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/493382 (дата обращения: 25.05.2026). — Режим доступа: для авториз. пользователей.

7.2 Дополнительная литература

1. Клименко, И. С. Информационная безопасность и защита информации: модели и методы управления : монография / И.С. Клименко. — Москва : ИНФРА-М, 2026. — 180 с. — (Научная мысль). — DOI 10.12737/monography_5d412ff13c0b88.75804464. - ISBN 978-5-16-015149-6. - Текст : электронный. - URL: https://znanium.ru/catalog/product/2238628 (дата обращения: 31.05.2026)
2. СПС Консультант Плюс
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 Office 2013 Suites and Apps KMS

МИНОБРНАУКИ РОССИИ

ВЛАДИВОСТОКСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

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

МОДЕЛИРОВАНИЕ УГРОЗ И ТЕСТИРОВАНИЕ ЗАЩИЩЕННОСТИ ИНФРАСТРУКТУРЫ

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-3.2к : 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
	ПКВ-4 : Способен осуществлять сбор и анализ исходных данных для проектирования, проектировать и разрабатывать устройства связи и компоненты систем защиты информации	ПКВ-4.2к : Разрабатывает компоненты комплексных систем защиты информации автоматизированных систем

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-3.2к : Знает современную эталонную модель взаимодействия открытых систем, принципы построения и функционирования систем и сетей передачи информации	РД 1	Знание	современную эталонную модель взаимодействия открытых систем (OSI), принципы построения и функционирования систем и сетей передачи информации	тест
ПКВ-3.4к : Оценивает эффективность и надежность защиты вычислительных сетей, операционных систем и баз данных	РД 2	Умение	анализировать конфигурации сетевых устройств, ОС и СУБД на предмет выявления уязвимостей; оценивать корректность применения механизмов аутентификации, разграничения доступа и шифрования	лабораторные работы

Компетенция ПКВ-4 «Способен осуществлять сбор и анализ исходных данных для проектирования, проектировать и разрабатывать устройства связи и компоненты систем защиты информации»

Таблица 2.2 – 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-4.2к : Разрабатывает компоненты комплексных систем защиты информации автоматизированных систем	РД3	Навык	методами оценки стойкости и надёжности парольных политик, межсетевых экранов и систем обнаружения вторжений	лабораторные работы
	РД4	Навык	навыками разработки компонентов СЗИ (политик безопасности, моделей доступа, регламентов) на основе выявленных угроз и уязвимостей; способностью обосновывать выбор и архитектуру технических средств защиты.	лабораторные 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 : современную эталонную модель взаимодействия открытых систем (OSI), принципы построения и функционирования систем и сетей передачи информации	1.1. Теоретические основы моделирования угроз	Тест	Экзамен в устной форме
		1.2. Методы и средства тестирования защищенности	Тест	Экзамен в устной форме
		1.3. Проектирование компонентов СЗИ на основе анализа угроз	Тест	Экзамен в устной форме
РД2	Умение : анализировать конфигурации сетевых устройств, ОС и СУБД на предмет выявления уязвимостей; оценивать корректность применения механизмов аутентификации, разграничения доступа и шифрования	1.1. Теоретические основы моделирования угроз	Лабораторная работа	Экзамен в устной форме
		1.2. Методы и средства тестирования защищенности	Лабораторная работа	Экзамен в устной форме
РД3	Навык : методами оценки стойкости и надёжности парольных политик,	1.2. Методы и средства тестирования защищенности	Лабораторная работа	Экзамен в устной форме

	межсетевых экранов и с истем обнаружения втор жений	1.3. Проектирование ко мпонентов СЗИ на осно ве анализа угроз	Лабораторная рабо та	Экзамен в устной форме
РД4	Навык : навыками разра ботки компонентов СЗИ (политик безопасности, моделей доступа, регла ментов) на основе выявл енных угроз и уязвимос тей; способностью обос новывать выбор и архит ектуру технических сре дств защиты.	1.2. Методы и средства тестирования защищенн ости	Лабораторная рабо та	Экзамен в устной форме
		1.3. Проектирование ко мпонентов СЗИ на осно ве анализа угроз	Лабораторная рабо та	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 р абота	Экзаме н	Ито го
Лекционные занятия	20			20
Практические занятия		60		60
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 балло в по дисципли не	Оценка по промеж уточной аттестаци и	Характеристика качества сформированности компетенции
от 91 до 100	«зачтено» / «отлично»	Студент демонстрирует сформированность дисциплинарных компетенций, обна руживает всестороннее, систематическое и глубокое знание учебного материала , усвоил основную литературу и знаком с дополнительной литературой, рекоме ндованной программой, умеет свободно выполнять практические задания, пред усмотренные программой, свободно оперирует приобретенными знаниями, уме ниями, применяет их в ситуациях повышенной сложности.
от 76 до 90	«зачтено» / «хорошо»	Студент демонстрирует сформированность дисциплинарных компетенций: осно вные знания, умения освоены, но допускаются незначительные ошибки, неточн ости, затруднения при аналитических операциях, переносе знаний и умений на н овые, нестандартные ситуации.
от 61 до 75	«зачтено» / «удовлетворитель но»	Студент демонстрирует сформированность дисциплинарных компетенций: в хо де контрольных мероприятий допускаются значительные ошибки, проявляется о тсутствие отдельных знаний, умений, навыков по некоторым дисциплинарным к омпетенциям, студент испытывает значительные затруднения при оперировани и знаниями и умениями при их переносе на новые ситуации.
от 41 до 60	«не зачтено» / «неудовлетворите льно»	У студента не сформированы дисциплинарные компетенции, проявляется недос таточность знаний, умений, навыков.
от 0 до 40	«не зачтено» / «неудовлетворите льно»	Дисциплинарные компетенции не сформированы. Проявляется полное или прак тически полное отсутствие знаний, умений, навыков.

5 Примерные оценочные средства

5.1 Пример заданий на лабораторную работу

Лабораторная работа №1. Анализ сетевого трафика с использованием российских DPI-систем

Тема: Модель OSI и сетевой уровень угроз

Цель: Изучить принципы перехвата и анализа сетевого трафика на различных уровнях модели OSI с использованием отечественных средств глубокого анализа пакетов.

Задание:

1. Установить Protosphere на стенде с российской ОС (Astra Linux / Ред ОС).
2. Захватить трафик в учебной сети и выделить отдельные сетевые соединения.
3. Провести детальный анализ пакетов на уровнях L2–L4 модели OSI, идентифицировать аномалии (ARP-spoofing, нестандартные TCP-флаги).
4. Составить отчет о выявленных угрозах на каждом уровне модели.

Лабораторная работа №2. Сканирование уязвимостей с использованием XSpider PRO

Тема: Построение модели угроз и оценка рисков

Цель: Освоить методику выявления уязвимостей в инфраструктуре и научиться интерпретировать результаты сканирования для построения модели угроз.

Задание:

1. Развернуть XSpider PRO на стенде и настроить целевые IP-адреса для сканирования (до 500 хостов).
2. Провести сканирование выделенного сегмента учебной сети в режиме «белого ящика».
3. Проанализировать отчет: классифицировать найденные уязвимости по критичности, сопоставить с актуальными угрозами из БДУ ФСТЭК.
4. На основе результатов заполнить реестр угроз для учебной АС.

Результат: Реестр угроз с ранжированием рисков и предложениями по устранению уязвимостей.

Лабораторная работа №3. Сбор информации об инфраструктуре методами OSINT

Тема: OSINT и пассивная разведка инфраструктуры

Цель: Освоить методы сбора информации об инфраструктуре из открытых источников с использованием инструментов, работающих в российской юрисдикции.

Инструменты:

- Российские поисковые системы и сервисы WHOIS (например, сервисы RU-CENTER, nic.ru).
- **RustScan** — высокопроизводительный сканер портов на языке Rust, может использоваться на российских ОС семейства Linux .
- **Nmap** — открытый инструмент, входит в репозитории всех российских Linux-дистрибутивов, санкциям не подвержен.

Лабораторная работа №4. Оценка надежности межсетевого экранирования

Тема: Активное сканирование и оценка надежности сетевых экранов

Цель: Проверить эффективность правил межсетевого экранирования и выявить возможные пути обхода.

Задание:

1. Настроить учебный межсетевой экран с набором правил фильтрации.
2. Используя RedCheck, провести сканирование на предмет обхода правил Firewall (TCP SYN-, XMAS-, FIN-сканирование).
3. Провести аудит конфигурации сетевых устройств с помощью MaxPatrol VM.
4. Идентифицировать правила, которые можно обойти, и разработать корректные списки ACL.

Результат: Разработанные правила фильтрации трафика (ACL) для закрытия выявленных векторов обхода.

Лабораторная работа №5. Анализ защищенности ОС и СУБД

Тема: Тестирование защищенности операционных систем и баз данных

Цель: Провести комплексную оценку надежности конфигурации ОС и СУБД с использованием российских средств аудита.

Задание:

1. Настроить тестовый стенд с сервером под управлением российской ОС (Astra Linux / Ред ОС) и СУБД (Postgres Pro).
2. Провести сканирование с использованием Сканер-ВС в режиме аудита конфигурации.
3. Выполнить проверку парольной политики и прав доступа к файлам БД.
4. Сравнить результаты с требованиями CIS Benchmarks и рекомендациями ФСТЭК.

Результат: Шаблон политики паролей и прав доступа для ОС и СУБД.

Лабораторная работа №6. Тестирование веб-приложений и разработка рекомендаций по WAF

Тема: Веб-безопасность и эксплуатация OWASP Top 10

Цель: Выявить уязвимости веб-приложений и разработать компонент системы защиты прикладного уровня.

Задание:

1. Развернуть учебное веб-приложение с преднамеренными уязвимостями (аналог DVWA на отечественном ПО).
2. Используя Int3rceptor, перехватить и проанализировать HTTP-запросы к приложению.
3. С помощью VulnScout Platform провести автоматизированное тестирование на SQL-инъекции и XSS.
4. По результатам тестирования разработать рекомендации по экранированию входных данных и настройке WAF.

Краткие методические указания

На выполнение одной лабораторной работы отводится не менее одного двухчасового занятия. 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. В соответствии с моделью OSI, на каком уровне работает межсетевой экран (Firewall) при фильтрации пакетов?

- А) Физический уровень
- Б) Канальный уровень
- В) Сетевой уровень (L3) и Транспортный уровень (L4)
- Г) Прикладной уровень

2. Какие угрозы в соответствии с методикой ФСТЭК России относятся к угрозам, приводящим к нарушению доступности информации?

- А) Внедрение вредоносного кода
- Б) Отказ в обслуживании (DoS-атака)
- В) Перехват данных
- Г) Модификация базы данных

3. Какой документ регламентирует порядок оценки угроз безопасности информации в России?

- А) ISO/IEC 27001
- Б) Методика оценки угроз безопасности информации (утв. ФСТЭК России 05.02.2021)
- В) GDPR
- Г) OWASP Testing Guide

4. Что такое SQL-инъекция?

- А) Техника внедрения вредоносного JavaScript-кода в веб-страницу
- Б) Атака на протокол ARP для подмены MAC-адресов
- В) Техника эксплуатации веб-приложений путем внедрения SQL-кода через невалидированный ввод
- Г) Метод перехвата сессионных cookies

5. Какое из перечисленных средств является российским сканером уязвимостей, сертифицированным ФСТЭК России?

- А) Nessus
- Б) OpenVAS
- В) XSpider PRO
- Г) Nmap

6. Согласно методике ФСТЭК России, угроза считается актуальной, если...

- А) Она описана в международной базе CVE
- Б) Существуют условия для ее реализации и реализация угрозы приводит к негативным последствиям для системы
- В) О ней сообщили в СМИ
- Г) Ее можно обнаружить с помощью сканера уязвимостей

7. Какой тип атаки используется для подмены MAC-адреса в сети с целью перехвата трафика?

- А) SQL-инъекция
- Б) ARP-spoofing
- В) XSS
- Г) CSRF

8. Какая из перечисленных уязвимостей относится к OWASP Top 10?

- А) Неправильная настройка межсетевого экрана
- Б) Межсайтовый скриптинг (XSS)
- В) Отсутствие антивируса
- Г) Использование устаревшего оборудования

9. Какой инструмент из перечисленных является российским HTTP/HTTPS-прокси для тестирования веб-приложений (аналог Burp Suite)?

- А) Int3rceptor
- Б) Metasploit
- В) ZAP
- Г) Wireshark

10. Что понимается под «моделью нарушителя» в информационной безопасности?

- А) Перечень всех возможных уязвимостей системы
- Б) Описание потенциального злоумышленника, включая его возможности, цели и уровень доступа
- В) Архитектура системы защиты
- Г) План тестирования на проникновение

11. Для чего предназначена российская система «Сканер-ВС»?

- А) Для управления проектами
- Б) Для комплексного тестирования защищенности и поиска уязвимостей
- В) Для криптографической защиты данных
- Г) Для мониторинга работоспособности серверов

12. Какой метод защиты наиболее эффективен против SQL-инъекций?

- А) Блокировка IP-адреса
- Б) Использование параметризованных запросов (Prepared Statements)
- В) Установка антивируса
- Г) Использование SSL-сертификата

13. Что такое OSINT в контексте тестирования защищенности?

- А) Сканирование портов
- Б) Сбор информации об инфраструктуре из открытых источников
- В) Анализ исходного кода
- Г) Тестирование на проникновение

14. Какой метод тестирования имитирует атаку внешнего злоумышленника, не имеющего внутренних данных о системе?

- А) Тестирование «белого ящика»
- Б) Тестирование «черного ящика»
- В) Тестирование «серого ящика»
- Г) Аудит исходного кода

15. Какой уровень модели OSI отвечает за сквозную передачу данных между конечными узлами и управление сессией?

- А) Физический уровень
- Б) Транспортный уровень
- В) Сеансовый уровень
- Г) Прикладной уровень

16. Какая база данных уязвимостей ведется ФСТЭК России и используется для оценки защищенности отечественного ПО?

- А) CVE
- Б) БДУ ФСТЭК (Банк данных угроз)
- В) NVD
- Г) OWASP

17. Что такое Cross-Site Scripting (XSS)?

- А) Атака на серверную часть приложения
- Б) Внедрение вредоносного скрипта в веб-страницу, выполняемого в браузере пользователя
- В) Атака на сетевой протокол
- Г) Метод подбора паролей

18. Какой сервис, разработанный компанией «Инферит», предназначен для композиционного анализа ПО и поиска уязвимостей в зависимостях?

- А) XSpider
- Б) MaxPatrol
- В) СКАТмен
- Г) RedCheck

19. С какой целью в рамках Bug Bounty привлекаются внешние исследователи для тестирования системы?

- А) Для снижения затрат на разработку
- Б) Для выявления уязвимостей, которые могут быть пропущены при внутренних проверках
- В) Для рекламы продукта
- Г) Для сертификации системы

20. Какой из методов защиты наиболее эффективен для предотвращения XSS-атак при выводе пользовательского контекста?

- А) Экранирование (escaping) специальных символов HTML
- Б) Установка брандмауэра
- В) Использование SSL/TLS
- Г) Регулярное обновление ОС

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.

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. Модель OSI и анализ сетевых угроз

Опишите структуру эталонной модели взаимодействия открытых систем (OSI). Для каждого уровня (L2–L7) приведите примеры типовых угроз и укажите, на каких уровнях осуществляется фильтрация трафика межсетевым экраном. Объясните, как знание модели OSI помогает в построении модели угроз для автоматизированной системы.

Вопрос 2. Методология построения модели угроз по требованиям ФСТЭК России

Изложите последовательность действий при построении модели угроз безопасности информации в соответствии с Методикой ФСТЭК России (утв. 05.02.2021). Дайте определение актуальной угрозы. Опишите, как определяются условия реализации угрозы и как формируется перечень актуальных угроз для конкретной автоматизированной системы.

Вопрос 3. Моделирование нарушителя и оценка рисков

Опишите классификацию нарушителей в соответствии с российскими нормативными документами. Какие характеристики нарушителя (уровень знаний, оснащенность, мотивация) учитываются при построении модели угроз? Объясните, как качественная оценка рисков (например, матрица вероятности и ущерба) влияет на выбор мер защиты. Приведите пример заполнения матрицы рисков для учебной системы.

Вопрос 4. Тестирование на проникновение: этапы, виды и правовые аспекты

Дайте определение тестирования на проникновение (пентест). Опишите основные этапы жизненного цикла пентеста (сбор информации, сканирование, эксплуатация уязвимостей, закрепление, отчетность). В чем разница между тестированием «черного», «белого» и «серого» ящика? Какие нормативные и правовые ограничения существуют в России для проведения пентеста?

Вопрос 5. Сбор информации об инфраструктуре: OSINT и активное сканирование

Опишите методы пассивного (OSINT) и активного сбора информации об инфраструктуре. Какие открытые источники используются для получения данных о доменах, IP-адресах и сетевых службах? Объясните, как сканирование портов (TCP SYN, FIN, XMAS) помогает определить состояние сетевых сервисов. Какие меры защиты позволяют снизить информационную освещенность периметра?

Вопрос 6. Анализ защищенности операционных систем и СУБД

Какие параметры конфигурации операционной системы (Windows/Linux) и СУБД наиболее критичны с точки зрения безопасности? Опишите методику проверки парольной политики, прав доступа к файлам и регламентным задачам. Какие стандарты безопасности (например, CIS Benchmarks) и российские нормативные документы используются для оценки надежности ОС и СУБД? Приведите примеры типовых ошибок конфигурации, выявляемых российскими сканерами.

Вопрос 7. Уязвимости веб-приложений (OWASP Top 10)

Опишите механизмы возникновения SQL-инъекций и межсайтового скриптинга (XSS). В чем разница между хранимой и отраженной XSS? Какие методы защиты наиболее эффективны против этих уязвимостей? Объясните, как работают параметризованные запросы (Prepared Statements) и почему они предотвращают SQL-инъекции. Назовите российские инструменты для тестирования веб-приложений.

Вопрос 8. Разработка компонентов СЗИ на основе модели угроз

Опишите, как результаты моделирования угроз и тестирования защищенности используются для разработки компонентов комплексной системы защиты информации (СЗИ). Какие компоненты СЗИ могут быть разработаны на этапе проектирования: политики безопасности, правила фильтрации трафика, регламенты реагирования на инциденты? Приведите примеры обоснования выбора средств защиты на основе анализа рисков.

Вопрос 9. Российские средства тестирования защищенности

Назовите и охарактеризуйте основные российские сканеры уязвимостей и средства тестирования (XSpider PRO, «Сканер-ВС», MaxPatrol VM, RedCheck, Int3rceptor). Каковы их ключевые возможности и различия? Опишите, какие базы данных уязвимостей (БДУ ФСТЭК, CVE, OWASP) используются в этих продуктах. Обоснуйте необходимость применения сертифицированных средств в государственных информационных системах и объектах КИИ.

Вопрос 10. Комплексная оценка защищенности инфраструктуры

Опишите процесс комплексной оценки защищенности инфраструктуры: от моделирования угроз до выработки рекомендаций по усилению защиты. Как взаимосвязаны этапы тестирования на проникновение, сканирования уязвимостей и аудита конфигураций? Предложите алгоритм действий для учебной автоматизированной системы (несколько серверов, веб-приложение, СУБД), включающий использование российских средств и нормативных документов.

Краткие методические указания

Для подготовки к экзамену студенту необходимо изучить лекционный материал, 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.