

Министерство образования Ростовской области
государственное бюджетное профессиональное образовательное учреждение
Ростовской области
«Белокалитвинский гуманитарно-индустриальный техникум»

Приложение 3.25
к ОПОП по специальности
09.02.11 Разработка и управление
программным обеспечением

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

ОП.05 «Основы информационной безопасности»

Белая Калитва
2025

Рассмотрена
на заседании цикловой комиссии
специальности 09.02.11 Разработка и
управление программным
обеспечением
Протокол № 4
от «23» декабря 2025г.
Председатель ЦК

 Комиссарова И.В.

УТВЕРЖДАЮ

Заместитель директора по УМР

«24» декабря 2025 г.

 Г. В. Шматко

Рабочая программа учебной дисциплины разработана в соответствии с Федеральным государственным образовательным стандартом среднего профессионального образования по специальности 09.02.11 «Разработка и управление программным обеспечением», утверждённым приказом Министерства просвещения Российской Федерации от 24 февраля 2025 г. № 138; Примерной рабочей программой профессионального модуля по данной специальности, согласованной в установленном порядке (примерная рабочая программа, использованная в качестве основы, утверждена приказом Министерства просвещения Российской Федерации от 13 октября 2025 г. № 01-09-580/2025) и Учебным планом специальности 09.02.11 «Разработка и управление программным обеспечением», утверждённым в Государственном бюджетном профессиональном образовательном учреждении Ростовской области «Белокалитвинский гуманитарно-индустриальный техникум».

Организация разработчик: ГБПОУ РО «БГИТ»

Разработчики:

Комиссарова И.В., преподаватель высшей квалификационной категории

СОДЕРЖАНИЕ

1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ.....	4
2. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ	6
3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ.....	10
4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ.....	14

1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ

1.1. Место дисциплины в структуре основной образовательной программы:

Учебная дисциплина ОП.05 «Основы информационной безопасности» является обязательной частью общепрофессионального цикла дисциплин основной образовательной программы в соответствии с ФГОС по специальности 09.02.11 «Разработка и управление программным обеспечением» и обеспечивает формирование профессиональных и общих компетенций по всем видам деятельности ФГОС по специальности 09.02.11 «Разработка и управление программным обеспечением».

Особое значение дисциплина имеет при формировании и развитии общих и профессиональных компетенций (ОК и ПК):

ОК/ПК	Наименование компетенции
ОК 01	Выбирать способы решения задач профессиональной деятельности применительно к различным контекстам
ОК 02	Использовать современные средства поиска, анализа и интерпретации информации, и информационные технологии для выполнения задач профессиональной деятельности
ОК 03	Планировать и реализовывать собственное профессиональное и личностное развитие, предпринимательскую деятельность в профессиональной сфере, использовать знания по правовой и финансовой грамотности в различных жизненных ситуациях
ОК 04	Эффективно взаимодействовать и работать в коллективе и команде
ОК 05	Осуществлять устную и письменную коммуникацию на государственном языке Российской Федерации с учетом особенностей социального и культурного контекста
ОК 06	Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных российских духовно-нравственных ценностей, в том числе с учетом гармонизации межнациональных и межрелигиозных отношений, применять стандарты антикоррупционного поведения
ОК 07	Содействовать сохранению окружающей среды, ресурсосбережению, применять знания об изменении климата, принципы бережливого производства, эффективно действовать в чрезвычайных ситуациях
ОК 09	Пользоваться профессиональной документацией на государственном и иностранном языках
ПК 1.5	Защищать информацию в базе данных с использованием технологии защиты информации
ПК 2.4	Выполнять тестирование и отладку программного обеспечения
ПК 3.5	Осуществлять аудит безопасности веб-приложения в соответствии с регламентом по безопасности
ПК 4.4	Выполнять тестирование и отладку бизнес-приложений

В рамках освоения рабочей программы осуществляется практическая подготовка обучающихся.

1.2. Цель и планируемые результаты освоения дисциплины:

В рамках программы учебной дисциплины обучающимися осваиваются умения и знания:

Код ПК, ОК	Умения	Знания
ОК 02, ОК 03 ПК 1.5	У1. Анализировать нормативно-правовые акты и стандарты в области ИБ. У2. Классифицировать угрозы и уязвимости информационной безопасности.	31. Законодательство РФ и международные стандарты в области ИБ (ISO 27001, ГОСТ Р ИСО/МЭК 27001). 32. Классификация угроз ИБ (внешние/внутренние), виды вредоносного ПО, методы социальной инженерии.
ПК 2.4, ПК 3.5	У3. Выявлять типовые уязвимости в программном коде (SQLi, XSS, CSRF). У4. Применять инструменты для статического и динамического анализа безопасности кода.	33. Принципы безопасного программирования (OWASP Top 10). 34. Методы и инструменты тестирования на проникновение (пентеста).
ПК 1.5, ОК 09	У5. Настраивать базовые механизмы защиты данных (аутентификация, авторизация, шифрование). У6. Анализировать и выбирать методы криптографической защиты информации.	35. Основные понятия криптографии: симметричное/асимметричное шифрование, хэш-функции, электронная подпись. 36. Методы защиты данных в приложениях и базах данных.
ПК 4.4, ОК 01, ОК 04	У7. Оценивать риски информационной безопасности для ИТ-проекта. У8. Участвовать в моделировании инцидента и составлении отчета.	37. Процесс управления рисками ИБ. 38. Этапы реагирования на инциденты ИБ.

2. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

2.1. Объем учебной дисциплины и виды учебной работы

Вид учебной работы	Объем часов
Объем образовательной программы учебной дисциплины	46
теоретическое обучение	16
практическое обучение	28
практические занятия / в форме практической подготовки	18/10
Промежуточная аттестация – дифференцированный зачет	2

2.2. Тематический план и содержание учебной дисциплины

Наименование разделов и тем	Содержание учебного материала и формы организации деятельности обучающихся	Объем в часах
1	2	3
Раздел 1 Основы информационной безопасности		8
Тема 1.1 Введение в ИБ ОК 02, ОК 03, ПК 1.5	Содержание учебного материала	2
	Понятие информационной безопасности (ИБ). Цели, задачи и принципы ИБ. Роль ИБ в разработке ПО. Основные понятия: активы, угрозы, уязвимости, риски.	2
Тема 1.2 Угрозы ИБ ОК 02, ПК 1.5, ПК 3.5	Содержание учебного материала	4
	Классификация угроз ИБ (внешние, внутренние). Угрозы конфиденциальности, целостности, доступности. Источники угроз: вредоносное ПО, социальная инженерия, хакерские атаки.	2
	В том числе, практических занятий и лабораторных работ	2
	Анализ примеров угроз и инцидентов ИБ.	2
Тема 1.3 Политики и стандарты ИБ ОК 02, ОК 03, ОК 09	Содержание учебного материала	2
	Политики ИБ в организации. Международные и российские стандарты ИБ (ISO 27001, ГОСТ Р ИСО/МЭК 27001). Регламенты и процедуры обеспечения ИБ.	1
	В том числе, практических занятий и лабораторных работ	1
	Разработка фрагмента политики ИБ на основе стандарта.	1
Раздел 2 Криптография и защита данных		12
Тема 2. 1 Основы криптографии ПК 1.5, ОК 09	Содержание учебного материала	4
	Основные понятия криптографии: шифрование, дешифрование, ключи. Симметричное и асимметричное шифрование. Хэш-функции, электронная подпись.	1
	В том числе, практических занятий и лабораторных работ	1
	Использование криптографических инструментов (GPG, OpenSSL). Шифрование и подпись файлов	1
	Из них в форме практической подготовки	2
	Практическое занятие №1 «Работа с криптографическими библиотеками на Python»	2
Тема 2.2 Защита данных в ПО ПК 1.5, ПК 2.4, ПК 3.5	Содержание учебного материала	6
	Методы защиты данных в приложениях. Безопасное хранение паролей и ключей. Защита от SQL-инъекций, XSS, CSRF.	2
	В том числе, практических занятий и лабораторных работ	2

	Практическое занятие: Анализ уязвимостей в коде. Настройка безопасного доступа к БД.	2
	Из них в форме практической подготовки	2
	Практическое занятие №2 «Аудит кода на уязвимости»	2
Тема 2.3 Аудит безопасности ПК 3.5, ОК 09	Содержание учебного материала	2
	Цели и задачи аудита ИБ. Методики проведения аудита. Инструменты для автоматизированного аудита.	1
	В том числе, практических занятий и лабораторных работ	1
	Практическое занятие: «Составление отчёта по аудиту безопасности.»	1
Раздел 3. Сетевая и веб-безопасность		12
Тема 3.1 Защита сетей ПК 2.4, ПК 4.4	Содержание учебного материала	4
	Основы сетевой безопасности. Межсетевые экраны, IDS/IPS, VPN. Анализ сетевого трафика.	1
	В том числе, практических занятий и лабораторных работ	2
	Практическое занятие: Настройка фаервола и VPN. Анализ пакетов в Wireshark.	2
	Из них в форме практической подготовки	1
	Лабораторная работа № 1 «Настройка правил iptables»	1
Тема 3.2 Безопасность веб-приложений ПК 3.5, ПК 4.4	Содержание учебного материала	6
	OWASP Top 10. Защита от веб-атак (SQLi, XSS, CSRF, инъекции). Безопасная аутентификация и авторизация.	2
	В том числе, практических занятий и лабораторных работ	2
	Практическое занятие: Тестирование веб-приложения на уязвимости.	2
	Из них в форме практической подготовки	2
	Практическое занятие №3 «Использование Burp Suite для тестирования»	2
Тема 3.3 Тестирование на проникновение ПК 2.4, ПК 3.5, ОК 04	Содержание учебного материала	2
	Методология пентеста. Инструменты для тестирования (Kali Linux, Metasploit). Этика и законодательство в области пентеста	1
	В том числе, практических занятий и лабораторных работ	1
	Практическое занятие: Проведение учебного пентеста.	1
Раздел 4. Управление ИБ и инцидентами		12
Тема 4.1 Управление рисками ОК 01, ОК 02, ПК 4.4	Содержание учебного материала	4
	Процесс управления рисками ИБ. Оценка и анализ рисков. Методы снижения рисков.	1
	В том числе, практических занятий и лабораторных работ	2
	Проведение оценки рисков для ИТ-проекта.	2

	Из них в форме практической подготовки	1
	Практическое занятие №4 «Разработка плана управления рисками»	1
Тема 4.2 Реагирование на инциденты ОК 04, ОК 05, ПК 4.4	Содержание учебного материала	6
	Этапы реагирования на инциденты ИБ. Сбор и анализ доказательств. Коммуникация при инцидентах.	2
	В том числе, практических занятий и лабораторных работ	2
	Разбор кейса по реагированию на инцидент. Моделирование инцидента и ответные действия.	2
	Из них в форме практической подготовки	2
	Практическое занятие №6 «Составление отчёта об инциденте»	2
Тема 4.3 ИИ в ИБ ОК 02, ОК 03	Содержание учебного материала	2
	Применение искусственного интеллекта и машинного обучения в ИБ. Анализ аномалий, классификация угроз. Современные тренды и инструменты. Обзор инструментов ИИ для обнаружения угроз.	2
Промежуточная аттестация	<i>Дифференцированный зачет</i>	2
Всего:		46

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ

3.1. Для реализации программы учебной дисциплины предусмотрены следующие специальные помещения:

206 Лаборатория «Программного обеспечения и сопровождения компьютерных систем»

Технические средства обучения:

Автоматизированные рабочие места для обучающихся: процессор QuadCore Intel Core i5, 4GBPC1600(800МГц) DDR3 SDRAM – 8 Гб) в количестве 12 штук.

Автоматизированное рабочее место преподавателя: QuadCore Intel Core i5, 4GBPC1600(800МГц) DDR3 SDRAM – 8 Гб).

Мультимедийный проектор Epson EB-S400;

Принтер

Программное обеспечение общего и профессионального назначения, включая: Kaspersky Endpoint Security 10, Net Police Pro, Windows 7, Microsoft Office 2010, Microsoft Visio Professional, MS Visual Studio, SublimeText, OpenServer, Android Studio, IntelliJ IDEA,

Оборудование учебного кабинета:

Комплекты специализированной учебной мебели;

Комплект учебно-методической документации;

Доска настенная 1-элементная фломастерная.

207 Лаборатория «Разработки, внедрения и адаптации программного обеспечения отраслевой направленности», кабинет «Архитектуры электронно-вычислительных машин и вычислительных систем», лаборатория «Вычислительной техники, архитектуры персонального компьютера и периферийных устройств», оснащенный оборудованием и техническими средствами обучения:

рабочее место преподавателя: стол одностумбовый, компьютерное кресло;

посадочные места обучающихся:

стол рабочий – 9 шт.; компьютерное кресло – 9 шт.

стол ученический 2-х местный – 4 шт., стул ученический – 8 шт.

оборудование:

компьютер в сборе, в составе: системный блок ProMEGA Game PC 730, монитор BenQ 23 GW2320, клавиатура Keyboard Defender HB-520, мышь Defender Element HB-520, – 10 шт.;

принтер (6374B001) Canon i-SENSYS LBP-6020 – 1 шт.;

сетевое оборудование;

программное обеспечение:

операционная система Microsoft Windows 10, с выходом в сеть «Интернет»;
пакет офисных прикладных программ Microsoft Office;
методические и дидактические материалы, в том числе электронные для проведения учебных занятий.

Лаборатория 208 «Информационных технологий в профессиональной деятельности», лаборатория «Программирования и баз данных» в соответствии с п. 6.1.2.1 ПООП-П по специальности 09.02.11 Разработка и управление программным обеспечением оснащенная необходимым для реализации программы учебной дисциплины оборудованием:

Оборудование учебного кабинета:

Автоматизированные рабочие места на 12-15 обучающихся (процессор 8-Core, оперативная память объемом не менее 32 Гб);

Автоматизированное рабочее место преподавателя (процессор 8- Core, оперативная память объемом не менее 32 Гб);

Проектор и экран;

Маркерная доска;

Программное обеспечение общего и профессионального назначения, в том числе включающее в себя следующее ПО:

Python, EclipseIDEforJavaEEDevelopers, .NETFrameworkJDK 8,
MicrosoftSQLServerExpressEdition, MicrosoftVisioProfessional,
MicrosoftVisualStudio, MySQLInstallerforWindows,
SQLServerManagementStudio, MicrosoftSQLServerJavaConnector,
AndroidStudio, IntelliJIDEA.

Лаборатория 214 «Кабинет информатики и информационных технологий», лаборатория «Программирования и баз данных» оснащенная в соответствии с п. 6.1.1.2 ПОП СПО по специальности 09.02.11 Разработка и управление программным обеспечением необходимым для реализации программы учебной дисциплины оборудованием:

Оборудование учебного кабинета:

Комплекты специализированной учебной мебели;

Комплект учебно-методической документации;

Магнитно-маркерная доска.

Проектор

МФУ

Технические средства обучения:

Автоматизированные рабочие места для 12-15 обучающихся: процессор AMD Ryzen 7 3700X 8-Core Processor 3.6 GHz, оперативная память 64 Gb, SSD 1 Tb, Radeon RX550/550 Series 4 Gb.

Автоматизированное рабочее место преподавателя: процессор Intel(R) Core(TM) i7-10700 2.9 GHz, оперативная память 16 Gb, SSD 500 Gb, Intel(R) UHD Graphics 630 (128 Mb).

Программное обеспечение общего и профессионального назначения, включая: Kaspersky Endpoint Security, Net Police Pro, Windows 10, Microsoft Office 2019, Microsoft Visio Professional, MS Visual Studio, NET Framework JDK, SublimeText, OpenServer, HTML-Академия <https://htmlacademy.ru> [Электронный ресурс], Docker, Git, VS Code, Postman.

3.2. Информационное обеспечение реализации программы

Для реализации программы библиотечный фонд образовательной организации должен иметь печатные и/или электронные образовательные и информационные ресурсы для использования в образовательном процессе.

3.2.1. Печатные издания

Основные

1. Информационная безопасность: учебное пособие/ Т.Л. Партыка, И.И. Попов. – 5-е изд., перераб. и доп. – М.: ФОРУМ, 2012. – 432 с.: ил. – (Профессиональное образование).

3.2.2. Электронные издания (электронные ресурсы)

Основные

1. Литвиненко, В.И. Основы информационной безопасности: Учебное пособие / В.И. Литвиненко, Е.С. Козлов — Москва: КноРус, 2026. — 199 с. — ISBN 978-5-406-15175-4. — URL: <https://book.ru/book/959148>. — Текст: электронный.

2. Прохорский, Г. В., Информатика и информационные технологии в профессиональной деятельности: учебное пособие / Г. В. Прохорский. — Москва: КноРус, 2023. — 271 с. — ISBN 978-5-406-11333-2. — URL: <https://book.ru/book/948626>. — Текст: электронный.

3.2.3. Дополнительные источники

1. Крылов, Г. О., Базовые понятия информационной безопасности: учебное пособие / Г. О. Крылов, С. Л. Ларионова, В. Л. Никитина. — Москва: Русайнс, 2025. — 257 с. — ISBN 978-5-466-09255-4. — URL: <https://book.ru/book/958467>. — Текст: электронный.

2. Дергачев, К. В., Защита информации: лабораторный практикум: учебное пособие / К. В. Дергачев, Д. В. Титарев. — Москва: Русайнс, 2024. — 158 с. — ISBN 978-5-466-05219-0. — URL: <https://book.ru/book/952795>. — Текст: электронный.

3.2.4. Интернет-ресурсы:

1. <https://book.ru/> – электронная библиотека с актуальными изданиями по ИБ.

2. <https://intuit.ru/> – курсы по информационной безопасности

3.2.5. Нормативно-правовая база:

1. ФСТЭК России – официальные документы по защите информации
2. ГОСТы и ISO – стандарты в области ИБ
3. Законодательные акты РФ в сфере информационной безопасности

3.2.6. Практические материалы:

1. Справочно-правовые системы (Консультант Плюс, Гарант)
2. Методические рекомендации по обеспечению ИБ
3. Практические руководства по настройке средств защиты

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

Результаты освоения (объекты оценивания)	Основные показатели оценки результата и их критерии	Формы и методы контроля и оценки результатов обучения
ПК – профессиональные компетенции ОК – общие компетенции З – знания У – умения ПО – практический опыт		
Раздел 1. Основы информационной безопасности		
Тема 1.1. Введение в ИБ		
31, 32, У1, У2, ОК 02, ОК 03, ПК 1.5	<i>Умеет:</i> анализировать простой сценарий работы с информацией и выявлять потенциальные нарушения принципов ИБ (конфиденциальность, целостность, доступность). <i>Знает:</i> базовые принципы, цели, задачи ИБ и основную терминологию. - Полнота определения основных понятий (актив, угроза, уязвимость, риск). - Точность соотнесения примеров нарушения с принципами CIA-триады. - Логичность и обоснованность предложенного анализа сценария.	- Тестирование по основным понятиям ИБ. - Устный опрос по ключевым принципам ИБ. - Решение ситуационных задач на анализ сценариев.
Тема 1.2. Угрозы ИБ		
31, 32, У1, У2, ОК 02, ПК 1.5, ПК 3.5	<i>Умеет:</i> классифицировать известные угрозы по источникам и видам. Анализировать описание инцидента и определять тип угрозы. <i>Знает:</i> классификацию угроз, основные виды вредоносного ПО, методы социальной инженерии. - Правильность классификации угроз (внутренние/внешние, по виду воздействия). - Глубина анализа кейса, выявление цепочки "уязвимость-угроза-реализация риска". - Точность определения методов защиты от выявленных угроз.	- Практическая работа "Анализ кейса реального инцидента ИБ". - Анализ и обсуждение примеров вредоносного ПО и методов социальной инженерии. - Защита отчета по практической работе.

Тема 1.3. Политики и стандарты ИБ		
31, У1, ОК 02, ОК 03, ОК 09	<i>Умеет:</i> на основе предоставленного шаблона разработать фрагмент политики ИБ (например, политика парольной защиты). <i>Знает:</i> назначение и структуру основных стандартов ИБ (ISO 27001, ГОСТ Р ИСО/МЭК 27001). - Соответствие фрагмента политики структуре и требованиям стандарта ISO 27001 (ГОСТ Р ИСО/МЭК 27001). - Практическая применимость и конкретность сформулированных правил. - Умение работать с профессиональной документацией на русском языке.	- Практическое задание "Разработка фрагмента политики ИБ". - Экспертная оценка разработанного документа. - Проектная работа по анализу требований стандарта.
Раздел 2. Криптография и защита данных		
Тема 2.1. Основы криптографии		
35, 36, У5, У6, ПК 1.5, ОК 09	<i>Умеет:</i> использовать консольные утилиты (GPG, OpenSSL) для шифрования, расшифрования и создания ЭЦП файлов. <i>Знает:</i> основные понятия криптографии, виды шифрования, назначение хэш. - Корректность выполнения команд шифрования и подписи файлов. - Понимание различий между симметричным и асимметричным шифрованием, знание областей применения. - Умение интерпретировать результат работы криптографических инструментов.-функций и ЭЦП.	- Лабораторная работа "Шифрование и электронная подпись файлов с помощью GPG/OpenSSL". - Практическое задание на создание и проверку ключевой пары, хэширование данных. - Контрольный опрос по видам шифрования.
Тема 2.2. Защита данных в ПО		
33, 34, 36, У3, У4, У6, ПК 1.5, ПК 2.4, ПК 3.5	<i>Умеет:</i> выявлять в предложенном фрагменте кода уязвимости типа SQLi, XSS, CSRF. Применять базовые методы защиты. <i>Знает:</i> методы защиты данных в приложениях, способы безопасной работы с БД. - Точность идентификации типа уязвимости (SQLi, XSS, CSRF). - Корректность предложенных методов защиты (использование подготовленных выражений, валидация и санитизация ввода).	- Лабораторная работа "Аудит кода на наличие уязвимостей". - Практическое занятие "Настройка параметров безопасного доступа к БД". - Тестирование с использованием специализированного ПО для статического анализа кода.

	- Понимание принципов безопасного хранения учетных данных.	
Тема 2.3. Аудит безопасности		
33, 34, У3, У4, ПК 3.5, ОК 09	<i>Умеет:</i> составить структурированный отчет по результатам учебного аудита безопасности, включая выводы и рекомендации. <i>Знает:</i> цели, задачи и основные методики проведения аудита ИБ. - Полнота и логичность структуры отчета об аудите. - Конкретность и практическая ценность рекомендаций по устранению уязвимостей. - Грамотное использование профессиональной терминологии в отчете.	- Практическое занятие "Составление отчета по аудиту безопасности". - Защита отчета перед учебной группой. - Экспертная оценка качества отчета.
Раздел 3. Сетевая и веб-безопасность		
Тема 3.1. Защита сетей		
34, У4, ПК 2.4, ПК 4.4	<i>Умеет:</i> настраивать базовые правила фильтрации сетевого трафика. Анализировать сетевой трафик с помощью Wireshark для выявления аномалий. <i>Знает:</i> базовые принципы сетевой безопасности, назначение и типы средств защиты. - Корректность настройки правил фильтрации трафика (разрешение/запрет портов, адресов). - Умение анализировать дампы трафика и идентифицировать подозрительную активность. - Понимание принципов работы VPN, IDS/IPS.	- Лабораторная работа "Настройка правил межсетевого экрана (iptables)". - Практическое занятие "Анализ сетевых пакетов в Wireshark". - Контрольное задание по классификации типов сетевых атак.
Тема 3.2. Безопасность веб-приложений		
33, 34, У3, У4, ПК 3.5, ПК 4.4	<i>Умеет:</i> проводить ручное тестирование веб-приложения на наличие уязвимостей из OWASP Top 10 с использованием инструментов (Burp Suite). <i>Знает:</i> основные уязвимости веб-приложений (OWASP Top 10) и методы защиты от них. - Успешное выявление заданных уязвимостей в тестовом веб-приложении. - Понимание механизма эксплуатации уязвимостей (SQLi, XSS) и способов их предотвращения.	- Практическая работа "Тестирование веб-приложения с использованием Burp Suite". - Экспертное наблюдение за процессом тестирования и анализ отчета. - Тестирование по теме OWASP Top 10.

	- Качество отчета, включающего описание шагов, доказательства и рекомендации.	
Тема 3.3. Тестирование на проникновение		
34, У4, ПК 2.4, ПК 3.5, ОК 04	<i>Умеет:</i> следовать методологии учебного пентеста. Использовать базовые инструменты (nmap, Metasploit) в учебной среде. <i>Знает:</i> основные этапы и методологии пентеста, этические и правовые аспекты. - Последовательное выполнение этапов пентеста в контролируемой среде. - Применение этических принципов и правовых норм при тестировании. - Эффективная работа в команде при моделировании инцидента (для групповых заданий).	- Практическое занятие "Проведение учебного пентеста" на стенде с уязвимыми виртуальными машинами. - Анализ отчета, содержащего описание обнаруженных уязвимостей и проведенных атак. - Наблюдение за взаимодействием в команде.
Раздел 4. Управление ИБ и инцидентами		
Тема 4.1. Управление рисками		
37, У7, ОК 01, ОК 02, ПК 4.4	<i>Умеет:</i> проводить качественную оценку рисков ИБ для упрощенного ИТ-проекта. <i>Знает:</i> основные этапы процесса управления рисками ИБ. - Полнота идентификации рисков для заданного сценария. - Обоснованность присвоения уровней вероятности и воздействия. - Практическая целесообразность предложенных мер по снижению рисков.	- Практическое задание "Оценка рисков ИБ для учебного ИТ-проекта". - Разработка плана управления рисками (в виде таблицы или матрицы). - Защита проекта управления рисками.
Тема 4.2. Реагирование на инциденты		
38, У8, ОК 04, ОК 05, ПК 4.4	<i>Умеет:</i> воспроизводить основные этапы реагирования на инцидент ИБ на учебном кейсе. Составлять отчет об инциденте. <i>Знает:</i> этапы жизненного цикла инцидента ИБ. - Правильная последовательность действий при реагировании на инцидент. - Полнота и структурированность отчета об инциденте. - Качество коммуникации при презентации отчета (ясность, логичность, ответы на вопросы).	- Практическое занятие "Моделирование инцидента ИБ и составление отчета". - Разбор учебного кейса по реагированию на инциденты. - Оценка навыков устной презентации отчета.
Тема 4.3. ИИ в ИБ		
31, 32, 34, ОК 02, ОК 03	<i>Умеет:</i> приводить примеры применения технологий ИИ/МО для решения конкретных задач ИБ.	- Подготовка и защита краткого аналитического обзора

	<i>Знает:</i> возможности и современные тренды применения ИИ и машинного обучения в сфере ИБ. - Точность примеров применения ИИ/МО для задач ИБ (обнаружение аномалий, классификация угроз, анализ вредоносного кода). - Понимание современных трендов и ограничений использования ИИ в ИБ. - Навыки поиска и анализа актуальной информации по теме.	"Применение ИИ в современных системах защиты". - Дискуссия на занятии по теме. - Экспертная оценка представленного обзора.
--	---	--