МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Магнитогорский государственный технический университет им. Г.И. Носова»

УТВЕРЖДАЮ
Директор ИЭиАС
_____ В.Р. Храмшин

04.02.2025 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

ПЕНТЕСТ

Направление подготовки (специальность)
22.03.02 Металлургия

Направленность (профиль/специализация) программы
Информационные технологии в современных литейных процессах

Уровень высшего образования - бакалавриат

Форма обучения
очная

Институт/ факультет	Институт энергетики и автоматизированных систем
Кафедра	Информатики и информационной безопасности
Курс	4
Семестр	8

Магнитогорск
2025 год

Рабочая программа составлена на основе ФГОС ВО - бакалавриат по направлению подготовки 22.03.02 Металлургия (приказ Минобрнауки России от 02.06.2020 г. № 702)

Рабочая программа рассмотрена и одобрена на заседании кафедры Информатики и информационной безопасности
03.02.2025 г., протокол № 5

Зав. кафедрой _____ И.И. Баранкова

Рабочая программа одобрена методической комиссией ИЭиАС
04.02.2025 г., протокол № 3

Председатель _____ В.Р. Храмшин

Согласовано:
Зав. кафедрой Литейных процессов и материаловедения

_____ Н.А. Феоктистов

Рабочая программа составлена:
ст. преподаватель кафедры ИиИБ, _____ Ю.А. Мазнина

Рецензент:
Проректор по цифровизации, канд. техн. наук _____ К.А. Рубан

Лист актуализации рабочей программы

Рабочая программа пересмотрена, обсуждена и одобрена для реализации в 2026 - 2027 учебном году на заседании кафедры ПИЛОТЫ

Протокол от __ _____ 20__ г. № __
Зав. кафедрой _____

Рабочая программа пересмотрена, обсуждена и одобрена для реализации в 2027 - 2028 учебном году на заседании кафедры ПИЛОТЫ

Протокол от __ _____ 20__ г. № __
Зав. кафедрой _____

Рабочая программа пересмотрена, обсуждена и одобрена для реализации в 2028 - 2029 учебном году на заседании кафедры ПИЛОТЫ

Протокол от __ _____ 20__ г. № __
Зав. кафедрой _____

Рабочая программа пересмотрена, обсуждена и одобрена для реализации в 2029 - 2030 учебном году на заседании кафедры ПИЛОТЫ

Протокол от __ _____ 20__ г. № __
Зав. кафедрой _____

1 Цели освоения дисциплины (модуля)

Целями освоения дисциплины «Пентест» является формирование у обучающихся понятий о принципах построения и функционирования систем, ПО и сетей передачи информации; составления методик тестирования систем, сетей передачи информации и ПО на проникновение; подбора инструментальных средств тестирования; формирования отчетности об анализе результатов тестирования ПО, систем и сетей передачи информации ;нормативных правовых актах в области защиты информации; руководящих и методических документах уполномоченных федеральных органов исполнительной власти по защите информации и овладение обучающимися необходимым и достаточным уровнем профессиональных компетенций в соответствии с требованиями ФГОС ВО

2 Место дисциплины (модуля) в структуре образовательной программы

Дисциплина Пентест входит в часть учебного плана формируемую участниками образовательных отношений образовательной программы.

Для изучения дисциплины необходимы знания (умения, владения), сформированные в результате изучения дисциплин/ практик:

Цифровая грамотность

Математические основы инженерии

Физика

IT: Интернет вещей

Знания (умения, владения), полученные при изучении данной дисциплины будут необходимы для изучения дисциплин/практик:

Подготовка к сдаче и сдача государственного экзамена

Производственная-преддипломная практика

3 Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля) и планируемые результаты обучения

В результате освоения дисциплины (модуля) «Пентест» обучающийся должен обладать следующими компетенциями:

Код индикатора	Индикатор достижения компетенции
ДПК-004-6 Способен анализировать результаты тестирования ПО на соответствие ожидаемым результатам, оформлять и размещать отчет о тестировании в соответствии с жизненным циклом ПО в системе контроля версий	
ДПК-004-6.1	Устанавливает/определяет уровень критичности дефектов ПО
ДПК-004-6.2	Применяет базовые техники проектирования и комбинаторики тестов с учетом типов дефектов ПО, их классификации и статистики возникновения
ДПК-004-6.3	Формирует отчетность об анализе результатов тестирования ПО в соответствии с установленными регламентами

4. Структура, объём и содержание дисциплины (модуля)

Общая трудоемкость дисциплины составляет 3 зачетных единиц 108 акад. часов, в том числе:

– контактная работа – 20,1 акад. часов:

– аудиторная – 20 акад. часов;

– внеаудиторная – 0,1 акад. часов;

– самостоятельная работа – 87,9 акад. часов;

– в форме практической подготовки – 0 акад. час;

Форма аттестации - зачет

Раздел/ тема дисциплины	Семестр	Аудиторная контактная работа (в акад. часах)			Самостоятельная работа студента	Вид самостоятельной работы	Форма текущего контроля успеваемости и промежуточной аттестации	Код компетенции
		Лек.	лаб. зан.	практ. зан.				
1. Методология тестирования на проникновение								
1.1 Международные стандарты и руководства проведения тестирования на проникновение	8			1	6	Самостоятельное изучение учебной и научно литературы, работа с материалами образовательного портала. Подготовка к практическим занятиям.	Тестирование	ДПК-004-6.1, ДПК-004-6.2, ДПК-004-6.3
1.2 Этапы проведения тестирования на проникновение				1	6	Самостоятельное изучение учебной и научно литературы, работа с материалами образовательного портала. Подготовка к практическим занятиям.	Тестирование	ДПК-004-6.1, ДПК-004-6.2, ДПК-004-6.3
Итого по разделу				2	12			
2. Получение цифрового отпечатка целевой машины								
2.1 Получение информации из открытых источников. Использование общих ресурсов	8			1	4	Самостоятельное изучение учебной и научно литературы, работа с материалами	Индивидуальное домашнее задание	ДПК-004-6.1, ДПК-004-6.2, ДПК-004-6.3

						образовательного портала. Подготовка к практическим занятиям. Подготовка ИДЗ		
2.2 Анализ записей DNS и получение сведений о сетевой маршрутизации	8			1	6	Самостоятельное изучение учебной и научно литературы, работа с материалами образовательного портала. Подготовка к практическим занятиям. Подготовка ИДЗ	Индивидуальное домашнее задание	ДПК-004-6.1, ДПК-004-6.2, ДПК-004-6.3
2.3 Автоматизированные инструменты для сбора информации				1	6	Самостоятельное изучение учебной и научно литературы, работа с материалами образовательного портала. Подготовка к практическим занятиям. Подготовка ИДЗ	Индивидуальное домашнее задание	ДПК-004-6.1, ДПК-004-6.2, ДПК-004-6.3
Итого по разделу				3	16			
3. Методы сетевого сканирования								
3.1 Идентификация целевой машины	8			1	4	Самостоятельное изучение учебной и научно литературы, работа с материалами образовательного портала. Подготовка к практическим занятиям. Подготовка ИДЗ	Индивидуальное домашнее задание	ДПК-004-6.1, ДПК-004-6.2, ДПК-004-6.3
3.2 Сканирование TCP/IP и UDP сообщений				1	4	Самостоятельное изучение учебной и научно литературы, работа с материалами образовательного портала. Подготовка к практическим занятиям. Подготовка ИДЗ	Индивидуальное домашнее задание	ДПК-004-6.1, ДПК-004-6.2, ДПК-004-6.3
3.3 Сканирование сетевых				1	4	Самостоятельно	Подготовка	ДПК-004-

портов целевой машины						е изучение учебной и научно литературы, работа с материалами образовательного портала. Подготовка к практическим занятиям. Подготовка ИДЗ	домашнего задания	6.1, ДПК-004-6.2, ДПК-004-6.3
Итого по разделу				3	12			
4. Сканирование уязвимостей								
4.1 Автоматизированное сканирование уязвимостей	8			2	12	Самостоятельное изучение учебной и научно литературы, работа с материалами образовательного портала. Подготовка к практическим занятиям. Подготовка ИДЗ	Индивидуальное домашнее задание	ДПК-004-6.1, ДПК-004-6.2, ДПК-004-6.3
4.2 Тестирование веб-приложений				4	12	Самостоятельное изучение учебной и научно литературы, работа с материалами образовательного портала. Подготовка к практическим занятиям. Подготовка ИДЗ	Индивидуальное домашнее задание	ДПК-004-6.1, ДПК-004-6.2, ДПК-004-6.3
4.3 Тестирование беспроводных сетей на проникновение				4	12	Самостоятельное изучение учебной и научно литературы, работа с материалами образовательного портала. Подготовка к практическим занятиям.	Тестирование	ДПК-004-6.1, ДПК-004-6.2, ДПК-004-6.3
Итого по разделу				10	36			
5. Отчетная документация о тестировании на проникновение								
5.1 Документация и проверка результатов. Типы отчетов	8			1	6	Самостоятельное изучение учебной и научно литературы,	Индивидуальное домашнее задание	ДПК-004-6.1, ДПК-004-6.2, ДПК-004-6.3

						работа с материалами образовательного портала. Подготовка к практическим занятиям. Подготовка ИДЗ		
5.2 Инструменты для подготовки отчетной документации о тестировании на проникновение	8			1	5,9	Самостоятельное изучение учебной и научно литературы, работа с материалами образовательного портала. Подготовка к практическим занятиям. Подготовка ИДЗ	Индивидуальное домашнее задание	ДПК-004-6.1, ДПК-004-6.2, ДПК-004-6.3
Итого по разделу				2	11,9			
Итого за семестр				20	87,9		зачёт	
Итого по дисциплине				20	87,9		зачет	

5 Образовательные технологии

Для реализации предусмотренных видов учебной работы в качестве образовательных технологий в преподавании дисциплины используются традиционная и модульно-компетентностная технологии.

Реализация компетентностного подхода предусматривает использование в учебном процессе активных и интерактивных форм проведения занятий в сочетании с внеаудиторной работой с целью формирования и развития профессиональных навыков обучающихся.

При проведении учебных занятий преподаватель обеспечивает развитие у обучающихся навыков командной работы, межличностной коммуникации, принятия решений, лидерских качеств посредством проведения интерактивных лекций, групповых дискуссий, ролевых игр, тренингов, анализа ситуаций, учета особенностей профессиональной деятельности выпускников и потребностей работодателей.

Формы учебных занятий с использованием традиционных технологий:

– информационные – для ознакомления с техническими средствами реализации информационных процессов, со стандартами организации сетей, основными приемами защиты информации, и другой справочной информацией;

– семинар – практическое занятие, посвященное освоению конкретных умений и навыков по предложенному алгоритму.

Формы учебных занятий с использованием технологий проблемного обучения:

– практическое занятие в форме практикума – организация учебной работы, направленная на решение комплексной учебно-познавательной задачи, требующей от обучающегося применения как научно-теоретических знаний, так и практических навыков;

– практическое занятие на основе кейс-метода – обучение в контексте моделируемой ситуации, воспроизводящей реальные условия научной, производственной, общественной деятельности; обучающиеся должны проанализировать ситуацию, разобраться в сути проблем, предложить возможные решения и выбрать лучшее из них; кейсы базируются на реальном фактическом материале или же приближены к реальной ситуации;

– подготовка тематических рефератов, содержащих разделы, частично или полностью выносимые на самостоятельное изучение.

Формы учебных занятий с использованием игровых технологий:

– учебная игра – форма воссоздания предметного и социального содержания будущей профессиональной деятельности специалиста, моделирования таких систем отношений, которые характерны для этой деятельности как целого;

– деловая игра – моделирование различных ситуаций, связанных с выработкой и принятием совместных решений, обсуждением вопросов в режиме «мозгового штурма», реконструкцией функционального взаимодействия в коллективе и т.п.

Технологии проектного обучения:

– творческий проект – учебно-познавательная деятельность обучающихся осуществляется в рамках рамочного задания, подчиняясь логике и интересам участников проекта, жанру конечного результата (газета, фильм, праздник, издание, экскурсия, подготовка заданий конкурсов и т.п.);

– информационный проект – учебно-познавательная деятельность с ярко выраженной эвристической направленностью (поиск, отбор и систематизация информации о каком-то объекте, ознакомление участников проекта с этой информацией, ее анализ и обобщение для презентации более широкой аудитории).

6 Учебно-методическое обеспечение самостоятельной работы обучающихся

Представлено в приложении 1.

7 Оценочные средства для проведения промежуточной аттестации

Представлены в приложении 2.

8 Учебно-методическое и информационное обеспечение дисциплины

а) Основная литература:

1. Внуков, А. А. Защита информации : учебник для вузов / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2025. — 161 с. — (Высшее образование). — ISBN 978-5-534-07248-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/561313 (дата обращения: 09.05.2025).

2. Защита информации : учебное пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. — 3-е изд. — Москва : РИОР : ИНФРА-М, 2024. — 400 с. — (Высшее образование). — DOI: https://doi.org/10.12737/1759-3. - ISBN 978-5-369-01759-3. - Текст : электронный. - URL: https://znanium.ru/catalog/product/2140566 (дата обращения: 09.05.2025). – Режим доступа: по подписке.

3. Противодействие преступлениям, совершаемым в сфере информационных технологий : учебник / под науч. ред. И.А. Калиниченко. — Москва : ИНФРА-М, 2024. — 642 с. — (Высшее образование: Специалитет). —. - ISBN 978-5-16-017838-7. - Текст : электронный. - URL: https://znanium.ru/catalog/product/2121606 (дата обращения: 09.05.2025). – Режим доступа: по подписке.

б) Дополнительная литература:

1. Внуков, А. А. Защита информации в банковских системах : учебник для вузов / А. А. Внуков. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2025. — 246 с. — (Высшее образование). — ISBN 978-5-534-01679-6. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/561314 (дата обращения: 09.05.2025).

2. Неверов, Д. Идём по киберследу : анализ защищенности Active Directory с помощью утилиты BloodHound : практическое руководство / Д. Неверов. - Москва : Альпина ПРО, 2025. - 304 с. - ISBN 978-5-206-00398-7. - Текст : электронный. - URL: https://znanium.ru/catalog/product/2206535 (дата обращения: 09.05.2025). – Режим доступа: по подписке.

3. Баранкова И. И. Определение критически значимых ресурсов объекта защиты при составлении модели угроз информационной безопасности : учебное пособие / И. И. Баранкова, О. В. Пермякова ; МГТУ. - Магнитогорск : МГТУ, 2017. - 1 электрон. опт. диск (CD-ROM). - URL: https://host.megaprolib.net/MP0109/Download/MObject/1858. - ISBN 978-5-9967-1031-7. - Текст : электронный. - дата обращения: 09.05.2025.

в) Методические указания:

г) Программное обеспечение и Интернет-ресурсы:

Программное обеспечение

Наименование ПО	№ договора	Срок действия лицензии
MS Office 2007 Professional	№ 135 от 17.09.2007	бессрочно
7Zip	свободно распространяемое ПО	бессрочно
Anaconda Python	свободно распространяемое ПО	бессрочно
NotePad++	свободно распространяемое ПО	бессрочно
LibreOffice	свободно распространяемое ПО	бессрочно
MS Visual Studio Code	свободно распространяемое ПО	бессрочно
JetBrains PyCharm Community Edition	свободно распространяемое ПО	бессрочно
Браузер Mozilla Firefox	свободно распространяемое ПО	бессрочно
Браузер Yandex	свободно распространяемое ПО	бессрочно
PostgreSQL	свободно распространяемое ПО	бессрочно
FAR Manager	свободно распространяемое ПО	бессрочно
Linux Calculate	свободно распространяемое ПО	бессрочно
PuTTY	свободно распространяемое ПО	бессрочно

Профессиональные базы данных и информационные справочные системы

Название курса	Ссылка
Информационная система - Банк данных угроз безопасности информации ФСТЭК России	https://bdu.fstec.ru/?ysclid=lujkqy7cnw630508962

Информационная система - Нормативные правовые акты, организационно-распорядительные документы, нормативные и методические документы и подготовленные проекты документов по технической защите информации ФСТЭК России	https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty-tzi?ysclid=lujknksfy724757053
Международная реферативная и полнотекстовая справочная база данных научных изданий «Springer Nature»	https://www.nature.com/siteindex
Федеральный образовательный портал – Экономика. Социология. Менеджмент	http://ecsocman.hse.ru/
Электронные ресурсы библиотеки МГТУ им. Г.И. Носова	https://host.megaprolib.net/MP0109/Web
Российская Государственная библиотека. Каталоги	https://www.rsl.ru/ru/4readers/catalogues/
Федеральное государственное бюджетное учреждение «Федеральный институт промышленной собственности»	URL: http://www1.fips.ru/
Национальная информационно-аналитическая система – Российский индекс научного цитирования (РИНЦ)	URL: https://elibrary.ru/project_risc.asp
Электронная база периодических изданий East View Information Services, ООО «ИВИС»	https://dlib.eastview.com/

9 Материально-техническое обеспечение дисциплины (модуля)

Материально-техническое обеспечение дисциплины включает:

Лаборатория программно-аппаратных средств обеспечения информационной безопасности:

– компьютер Destene Volution i560 на базе Windows Server 2008 R2(Standart) MSDN;

– ПЭВМ на базе Windows 7 – 12 шт.;

– мультимедийные средства хранения, передачи и представления информации.

Учебные аудитории для проведения практических занятий, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации:

– персональные компьютеры с ПО, выходом в Интернет и с доступом в электронную информационно-образовательную среду университета;

– мультимедийные средства хранения, передачи и представления информации;

– комплекс тестовых заданий для проведения промежуточных и рубежных контролей.

Помещения для самостоятельной работы обучающихся:

– персональные компьютеры с ПО, выходом в Интернет и с доступом в электронную информационно-образовательную среду университета.

Помещения для хранения и профилактического обслуживания учебного оборудования:

– шкафы для хранения учебно-методической документации, учебного оборудования и учебно-наглядных пособий.

Помещения для самостоятельной работы обучающихся:

– персональные компьютеры с ПО, выходом в Интернет и с доступом в электронную информационно-образовательную среду университета.

Помещения для хранения и профилактического обслуживания учебного оборудования:

шкафы для хранения учебно-методической документации, учебного оборудования и учебно-наглядных пособий.

Приложение 1

Учебно-методическое обеспечение самостоятельной работы обучающихся

Аудиторная самостоятельная работа обучающихся на практических занятиях осуществляется под контролем преподавателя в виде решения задач и выполнения упражнений, которые определяет преподаватель для обучающегося с использованием методов IT.

Внеаудиторная самостоятельная работа обучающихся осуществляется в виде чтения литературы по соответствующему разделу с проработкой материала и выполнения домашних заданий с консультациями преподавателя, а так же с применением кейс-технологий.

а) Контрольные вопросы и задания для проведения текущего контроля

1. Что такое пентест (тестирование на проникновение)? Каковы его цели и задачи? Чем отличается пентест от оценки уязвимостей?
2. Какие основные этапы включает в себя процесс пентеста?
3. Какие существуют типы пентеста? В чем их различия?
4. Какие существуют правовые и этические аспекты проведения пентестов? Какие основные нормативные документы и стандарты регулируют проведение пентестов?
5. Каковы основные квалификационные требования к пентестеру?
6. Какие основные инструменты и программное обеспечение используются при проведении пентестов?
7. Что такое уровень критичности дефекта? Как классифицируются уязвимости по степени опасности (критичности)? Приведите примеры дефектов разного уровня критичности.
8. Какие факторы влияют на определение уровня критичности дефекта?
9. Какие существуют шкалы для определения уровня критичности дефектов? Приведите примеры оценки дефектов разного уровня критичности по этим шкалам.
10. Какие инструменты и техники можно использовать для автоматизации определения уровня критичности дефектов?
11. Какие типы уязвимостей наиболее часто встречаются в современных веб-приложениях?
12. Что такое проектирование тестов? Каковы его цели?
13. Какие существуют базовые техники проектирования тестов?
14. Что такое комбинаторное тестирование? Для чего оно используется?
15. Какие существуют методы комбинаторного тестирования? Как выбрать наиболее подходящую технику проектирования тестов для конкретной ситуации?
16. Как использовать статистику возникновения дефектов для оптимизации процесса тестирования?
17. Что такое отчет о пентесте? Какова цель анализа результатов тестирования на соответствие ожидаемым результатам? Как оценить эффективность проведенного пентеста на основе анализа результатов?
18. Какие метрики можно использовать для оценки результатов пентеста?
19. Какие основные разделы должен содержать отчет об анализе результатов тестирования? Как оформить отчет о пентесте, чтобы он был понятен как техническим специалистам, так и руководству? Как обеспечить соответствие отчета установленным регламентам и требованиям заказчика?
20. Какие инструменты можно использовать для автоматизации формирования отчетов о пентесте?
21. Какие выводы можно сделать на основе анализа результатов пентеста для улучшения безопасности организации?
22. Как использовать результаты пентеста для обучения и повышения осведомленности сотрудников в области информационной безопасности?

23. Как документировать процесс воспроизведения найденной уязвимости?

24. Как использовать информацию об известных эксплойтах для подтверждения и демонстрации воздействия найденных уязвимостей?

25. Как определить, какие уязвимости представляют наибольшую угрозу для организации? Какие критерии используются для определения приоритетности исправления найденных уязвимостей?

26. Как обеспечить конфиденциальность информации, содержащейся в отчете о пентесте?

27. Какова роль системы контроля версий в процессе пентеста? Как правильно размещать отчет о тестировании в системе контроля версий?

б) Примеры индивидуальных домашних заданий

Тема	Задание
Тема 2.1	Используя открытый источник поиска архивов сайтов произвести поиск заданного хоста. Используя открытые источники,найти информацию о регистрации домена
Тема 2.2	Выполнить поиск A, AAAA и MX записей домена по заданному адресу домена. Используя ICMP-запрос, получить информацию о маршрутизации до целевого домена. Структурировать полученные данные и сформировать отчет.
Тема 2.3	Используя автоматизированный инструмент сбора информации, выполнить поиск документов формата pdf и docx на целевом домене. Сформировать HTML-отчет по результатам поиска.
Тема 3.1	По заданному диапазону IPv4 адресов определить задействованные адреса. Указать размер пакета 1024 байта и проверить время ответа эксплуатируемых адресов. Сформировать по полученным данным отчет.
Тема 3.2	Используя программе-анализатор трафика для компьютерных сетей WhireShark, провести анализ трафика. Определить сетевые адреса, с которыми взаимодействует целевая машина. По полученному трафику определить тип сообщений и структуру пакетов.
Тема 3.3	Выполнить сканирование портов целевой машины, используя разные режимы сканирования. Определить открытые порты целевой машины. Получить информацию об ОС целевой машины.
Тема 4.1	Используя функции автоматизированного сканирования, выполнить поиск уязвимостей целевой виртуальной машины на базе ОС Linux. Сформировать отчет по полученным данным.
Тема 4.2	Произвести сканирование открытых портов целевой виртуальной машины. Пройти на http и ftp целевой машины. Выполнить анализ доступа к данных на ftp целевой машины. Получить доступ к личному кабинету веб-приложения целевой машины.
Тема 5.1	Провести анализ отчета о тестировании на проникновение. По структуре документа определить тип отчета и полноту предоставленных данных. Сформировать рекомендации по устранению уязвимостей.
Тема 5.2	По результатам тестирования на проникновение сформировать отчет для руководителей организации и технический отчет, используя автоматизированные средства предоставления отчетов.

Приложение 2

Оценочные средства для проведения промежуточной аттестации

а) Планируемые результаты обучения и оценочные средства для проведения промежуточной аттестации

Код индикатора	Индикатор достижения компетенции	Оценочные средства
ДПК-004-6: Способен анализировать результаты тестирования ПО на соответствие ожидаемым результатам, оформлять и размещать отчет о тестировании в соответствии с жизненным циклом ПО в системе контроля версий – ДПК-004-6.1: Устанавливает/определяет уровень критичности дефектов ПО – ДПК-004-6.2: Применяет базовые техники проектирования и комбинаторики тестов с учетом типов дефектов ПО, их классификации и статистики возникновения – ДПК-004-6.3: Формирует отчетность об анализе результатов тестирования ПО в соответствии с установленными регламентами		
ДПК-004-6.1	Устанавливает/ определяет уровень критичности дефектов ПО	Теоретические вопросы к зачету: 1. Что такое пентест (тестирование на проникновение)? Каковы его цели и задачи? Чем отличается пентест от оценки уязвимостей? 2. Какие основные этапы включает в себя процесс пентеста? 3. Какие существуют типы пентеста? В чем их различия? 4. Какие существуют правовые и этические аспекты проведения пентестов? Какие основные нормативные документы и стандарты регулируют проведение пентестов? 5. Каковы основные квалификационные требования к пентестеру? 6. Какие основные инструменты и программное обеспечение используются при проведении пентестов? 7. Что такое уровень критичности дефекта? Как классифицируются уязвимости по степени опасности (критичности)? Приведите примеры дефектов разного уровня критичности. 8. Какие факторы влияют на определение уровня критичности дефекта? 9. Какие существуют шкалы для определения уровня критичности дефектов? Приведите примеры оценки дефектов разного уровня критичности по этим шкалам. 10. Какие инструменты и техники можно использовать для автоматизации определения уровня критичности дефектов? Примеры практических заданий для зачета: 1. Используя Burp Suite и другие инструменты, найдите и проэксплуатируйте уязвимость SQL-инъекции в заданном веб-приложении. Оцените уровень критичности уязвимости, предложите рекомендации по устранению уязвимости в отчете.

Код индикатора	Индикатор достижения компетенции	Оценочные средства
		2. Найдите и проэксплуатируйте уязвимость XSS в веб-приложении. Продемонстрируйте возможность выполнения произвольного JavaScript-кода в браузере пользователя. Оцените уровень критичности уязвимости, предложите рекомендации по устранению уязвимостей в отчете. 3. Проанализируйте систему аутентификации и авторизации веб-приложения. Найдите и проэксплуатируйте слабые места. Оцените уровень критичности найденных уязвимостей, предложите рекомендации по устранению уязвимости в отчете. Оцените уровень критичности найденных уязвимостей, предложите рекомендации по устранению уязвимостей в отчете. 4. Используя инструменты анализа веб-сервера, проведите анализ конфигурации веб-сервера. Определите известные уязвимости и небезопасные настройки. Оцените уровень критичности найденных уязвимостей, предложите рекомендации по устранению уязвимостей в отчете.
ДПК-004-6.2	Применяет базовые техники проектирования и комбинаторики тестов с учетом типов дефектов ПО, их классификации и статистики возникновения	Теоретические вопросы к зачету: 1. Что такое проектирование тестов? Каковы его цели? 2. Какие существуют базовые техники проектирования тестов? 3. Что такое комбинаторное тестирование? Для чего оно используется? 4. Какие существуют методы комбинаторного тестирования? Как выбрать наиболее подходящую технику проектирования тестов для конкретной ситуации? 5. Как использовать статистику возникновения дефектов для оптимизации процесса тестирования? Примеры практических заданий для зачета: 1. Для заданного модуля или функциональности веб-приложения разработайте набор тестовых сценариев, используя технику «Таблица решений». Проведите тестирование и сформируйте отчет о его результатах. 2. Для заданного модуля или функциональности веб-приложения, имеющего несколько параметров, примените технику попарного тестирования. Сгенерируйте минимальный набор тестовых сценариев, обеспечивающих покрытие всех пар значений параметров. Проведите тестирование и сформируйте отчет о его результатах.
ДПК-004-6.3	Формирует отчетность об анализе результатов тестирования	Теоретические вопросы к зачету: 28. Что такое отчет о пентесте? Какова цель анализа результатов тестирования на соответствие ожидаемым результатам? Как оценить эффективность проведенного пентеста на основе анализа результатов?

Код индикатора	Индикатор достижения компетенции	Оценочные средства
	ПО в соответствии с установленным и регламентами	29. Какие метрики можно использовать для оценки результатов пентеста? 30. Какие основные разделы должен содержать отчет об анализе результатов тестирования? Как оформить отчет о пентесте, чтобы он был понятен как техническим специалистам, так и руководству? Как обеспечить соответствие отчета установленным регламентам и требованиям заказчика? 31. Какие инструменты можно использовать для автоматизации формирования отчетов о пентесте? 32. Какие выводы можно сделать на основе анализа результатов пентеста для улучшения безопасности организации? 33. Как использовать результаты пентеста для обучения и повышения осведомленности сотрудников в области информационной безопасности? 34. Как документировать процесс воспроизведения найденной уязвимости? 35. Как использовать информацию об известных эксплойтах для подтверждения и демонстрации воздействия найденных уязвимостей? 36. Как определить, какие уязвимости представляют наибольшую угрозу для организации? Какие критерии используются для определения приоритетности исправления найденных уязвимостей? 37. Как обеспечить конфиденциальность информации, содержащейся в отчете о пентесте? 38. Какова роль системы контроля версий в процессе пентеста? Как правильно размещать отчет о тестировании в системе контроля версий? Примеры практических заданий для зачета: 1. Реализуйте bruteforce атаку на форму логина веб-приложения. Оцените эффективность различных методов защиты от bruteforce атак. Сформируйте отчет о результатах пентеста, дайте рекомендации по усилению защиты от bruteforce в отчете. 2. Найдите и проэксплуатируйте уязвимость CSRF в веб-приложении. Продемонстрируйте возможность выполнения действий от имени пользователя без его ведома. Оцените уровень критичности найденной уязвимости. Сформируйте отчет о найденной уязвимости, дайте рекомендации по устранению найденной уязвимости в отчете. 3. Проанализируйте статистику уязвимостей в заданном веб-приложении. Определите наиболее часто встречающиеся типы уязвимостей и их причины. Сформируйте отчет. Предложите меры по улучшению безопасности заданного веб-приложения, обоснуйте их использование.

б) Порядок проведения промежуточной аттестации, показатели и критерии оценивания

Показатели и критерии оценивания зачета:

− «зачтено» – обучающийся должен показать пороговый уровень знаний на уровне воспроизведения и объяснения информации, навыки решения типовых задач;

− «не зачтено» – обучающийся демонстрирует знания не более 20% теоретического материала, допускает существенные ошибки, не может показать интеллектуальные навыки решения простых задач.