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

10.02.2023 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

АНАЛИЗ УЯЗВИМОСТЕЙ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Направление подготовки (специальность)
10.05.03 Информационная безопасность автоматизированных систем

Направленность (профиль/специализация) программы
10.05.03 специализация N 8 «Разработка автоматизированных систем в защищенном исполнении»

Уровень высшего образования – специалитет

Форма обучения
очная

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

Магнитогорск
2023 год

Рабочая программа составлена на основе ФГОС ВО – специалитет по специальности 10.05.03 Информационная безопасность автоматизированных систем (приказ Минобрнауки России от 26.11.2020 г. № 1457)

Рабочая программа рассмотрена и одобрена на заседании кафедры Информатики и информационной безопасности
09.02.2023, протокол № 5

Зав. кафедрой _____ И.И. Баранкова

Рабочая программа одобрена методической комиссией ИЭиАС
10.02.2023 г. протокол № 7

Председатель _____ В.Р. Храмшин

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

Рецензент:
Начальник УИТ и АСУ ВТиП, канд. техн. наук _____ К.А. Рубан

Лист актуализации рабочей программы

Рабочая программа пересмотрена, обсуждена и одобрена для реализации в 2024 - 2025 учебном году на заседании кафедры Информатики и информационной безопасности

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

Рабочая программа пересмотрена, обсуждена и одобрена для реализации в 2025 - 2026 учебном году на заседании кафедры Информатики и информационной безопасности

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

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

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

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

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

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

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

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

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

1 Цели освоения дисциплины (модуля)

Общей целью дисциплины «Анализ уязвимостей программного обеспечения» является повышение исходного уровня владения информационными технологиями, достигнутого на предыдущей ступени образования, и овладение студентами необходимым и достаточным уровнем профессиональных компетенций в соответствии с требованиями ФГОС ВО по специальности «Информационная безопасность автоматизированных систем». Специальными целями дисциплины «Анализ уязвимостей программного обеспечения» являются:

- изучение основных видов уязвимостей программного обеспечения;
- изучение контрольно-испытательных и логико-аналитических методов анализа программного обеспечения на наличие уязвимостей;

изучение способов обеспечения надежности программного обеспечения и контроля его технологической безопасности;

- освоение навыков оценки эффективности систем защиты информации автоматизированных систем и технологии разработки систем программно-технической защиты информации автоматизированных систем.

2 Место дисциплины (модуля) в структуре образовательной программы

Дисциплина Анализ уязвимостей программного обеспечения входит в обязательную часть учебного плана образовательной программы.

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

Безопасность сетей ЭВМ

Технология построения защищенных распределенных приложений

Технологии и методы программирования

Организация ЭВМ и вычислительных систем

Языки программирования

Безопасность систем баз данных

Программно-аппаратные средства обеспечения информационной безопасности

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

Методы и стандарты оценки защищенности компьютерных систем

Разработка систем защиты информации автоматизированных систем

Защита программного обеспечения

Защита электронного документооборота

Методы выявления нарушений информационной безопасности

Разработка и эксплуатация автоматизированных систем в защищенном исполнении

Тестирование систем защиты информации автоматизированных систем

Методы проектирования систем защиты распределенных информационных систем

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

В результате освоения дисциплины (модуля) «Анализ уязвимостей программного обеспечения» обучающийся должен обладать следующими компетенциями:

Код индикатора	Индикатор достижения компетенции
ОПК-13 Способен организовывать и проводить диагностику и тестирование систем защиты информации автоматизированных систем, проводить анализ уязвимостей систем защиты информации автоматизированных систем;	

ОПК-13.1	Организовывает тестирование систем защиты информации автоматизированных систем
ОПК-13.2	Проводит диагностику систем защиты информации автоматизированных систем
ОПК-13.3	Анализирует уязвимости автоматизированных систем и их систем защиты

4. Структура, объём и содержание дисциплины (модуля)

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

– контактная работа – 69,8 акад. часов:

– аудиторная – 68 акад. часов;

– внеаудиторная – 1,8 акад. часов;

– самостоятельная работа – 38,2 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. 1. Контрольно-испытательные и логико-аналитические методы анализа уязвимостей программного обеспечения								
1.1 Языки формальной спецификации программ. Валидация сценариев требований	8	3	3		2	Подготовка к практическому занятию; поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями)	Семинарское занятие	ОПК-13.1, ОПК-13.2, ОПК-13.3
1.2 Методы анализа структур программ. Верификация и валидация программ. Метод верификации композиции правильных компонентов		3	3		2	Подготовка к практическому занятию; поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями)	Семинарское занятие, устный опрос	ОПК-13.1
Итого по разделу		6	6		4			
2. 2. Теоретические и формальные методы доказательства правильности программ и их спецификаций								

2.1 Проблемы анализа уязвимостей программного обеспечения. Основные уязвимости программного обеспечения.	8	3	3/2И		2	Создание тестового ПО, ее конфигурация. Отслеживания действий пользователей в ПО.	Семинарское занятие, устный опрос	ОПК-13.1
2.2 Алгоритмические и программные закладки		3	3/2И		2	Конфигурация прав пользователей в ПО	Семинарское занятие, устный опрос	ОПК-13.1
Итого по разделу		6	6/4И		4			
3. 3. Методы и средства анализа уязвимостей программ								
3.1 Лексический и синтаксический верификационный анализ, семантический анализ программ. Верификация моделей программ методом model checking.	8	3	3		2	Подбор, описание, экспертная оценка сайтов Интернет	устный опрос	ОПК-13.1
3.2 Логика дерева вычислений: формализм для представления свойств живости и безопасности, алгоритмы верификации		3	3		2	Подбор, описание, экспертная оценка сайтов Интернет	проектные работы	ОПК-13.1
Итого по разделу		6	6		4			
4. 4. Способы обеспечения надежности программ для контроля их технологической безопасности								
4.1 Процессы обеспечения функциональной безопасности программных продуктов в стандартах IEC 61508:1-6: 1998-2000, ISO 15408:1999 93, ISO 13335: 1-5: 1998.	8	3	3		3	Настройка коммутатора на зеркалирование траффика на заданный узел. Зеркалирование трафика посредством ARP-инъекций	Защита проекта, устный опрос	ОПК-13.1
4.2 Методы идентификации программ и их характеристик. Способы оценки подобия целевой и исследуемой программ с точки зрения наличия программных дефектов.		3	3		4,2	Конфигурирование паттернов активности при помощи средств дистрибутива Kali Linux	Защита проекта, устный опрос	ОПК-13.1
Итого по разделу		6	6		7,2			
5. 5. Анализ средств и этапы преодоления систем защиты программного обеспечения								

5.1 Методы защиты программ от исследования	8	3	3		4	Анализ радиочастот для выявления каналов занятых исследуемой бес -проводной сетью. Выполнение атаки на сеть с целью получения хедшейка. Подбор хэша.	Защита проекта, устный опрос	ОПК-13.1
5.2 Технологии разработки систем программно-технической защиты программного обеспечения. Этапы проектирования и разработки систем программно-технической защиты программного обеспечения.		3	3		4	Анализ активности на радиочастотах занятых беспроводной сетью	Защита проекта, устный опрос	ОПК-13.1
Итого по разделу		6	6		8			
6. 6. Оценка эффективности систем защиты программного обеспечения								
6.1 Критерии оценки: стойкость к исследованию/взлому; отказоустойчивость (надёжность).	8	2	2		5	Анализ HTML кода. Проверка простейших ошибок при конфигурирован ие страницы авторизации.	Защита проекта, устный опрос	ОПК-13.1
6.2 Критерии оценки: независимость от конкретных реализаций операционных систем; совместимость; неудобства для конечного пользователя программного обеспечения; побочные эффекты; стоимость; доброкачественность		2	2		6	Применение основных типов SQL-инжекции для получения доступа данных авторизации	Защита проекта, устный опрос	ОПК-13.1
Итого по разделу		4	4		11			
7. Аттестация								
7.1 Зачет	8					Подготовка к зачету	Зачет	ОПК-13.1
Итого по разделу								
Итого за семестр		34	34/4И		38,2		зачёт	
Итого по дисциплине		34	34/4И		38,2		зачет	

5 Образовательные технологии

Для реализации предусмотренных видов учебной работы в качестве образовательных технологий в преподавании дисциплины «Базы данных» 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:

– обзорные лекции – для рассмотрения общих вопросов информатики и информационных технологий, для систематизации и закрепления знаний;

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

– лекции-визуализации – для наглядного представления способов решения алгоритмических и функциональных задач, визуализации результатов решения задач;

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

Формы учебных занятий с использованием технологий проблемного обучения:

– проблемная лекция – изложение материала, предполагающее постановку проблемных и дискуссионных вопросов, освещение различных научных подходов, авторские комментарии, связанные с различными моделями интерпретации изучаемого материала (для развития исследовательских навыков и изучения способов решения задач);

– лекции с заранее запланированными ошибками – направленные на поиск обучающимися синтаксических и алгоритмических ошибок при решении алгоритмических и функциональных задач, с последующей диагностикой слушателей и разбором сделанных ошибок;

– 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 (модуля)

а) Основная литература:

1. Внуков, А. А. Защита информации : учебное пособие для вузов / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2023. — 161 с. — (Высшее образование). — ISBN 978-5-534-07248-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/512268 (дата обращения: 02.05.2023).

2. Казарин, О. В. Надежность и безопасность программного обеспечения : учебное пособие для вузов / О. В. Казарин, И. Б. Шубинский. — Москва : Издательство Юрайт, 2023. — 342 с. — (Высшее образование). — ISBN 978-5-534-05142-1. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/515435 (дата обращения: 02.05.2023).

3. Сычев, Ю. Н. Защита информации и информационная безопасность : учебное пособие / Ю.Н. Сычев. — Москва : ИНФРА-М, 2023. — 201 с. — (Высшее образование: Бакалавриат). — DOI 10.12737/1013711. - ISBN 978-5-16-014976-9. - Текст : электронный. - URL: https://znanium.com/catalog/product/1912987 (дата обращения: 02.05.2023).

б) Дополнительная литература:

1. Баранкова И. И. Теория информации. Кодирование [Электронный ресурс] : учебное пособие / И. И. Баранкова, М. В. Коновалов ; МГТУ. - Магнитогорск : МГТУ, 2017. - 1 электрон. опт. диск (CD-ROM). - Режим доступа: https://magtu.informsystema.ru/uploader/fileUpload?name=3313.pdf&show=dcatalogues/1/1137756/3313.pdf&view=true. - Макрообъект. - ISBN 978-5-9967-1073-7

2. Баранова, Е. К. Информационная безопасность и защита информации : учебное пособие / Е.К. Баранова, А.В. Бабаш. — 4-е изд., перераб. и доп. — Москва : РИОР : ИНФРА-М, 2022. — 336 с. — (Высшее образование). — DOI: https://doi.org/10.29039/1761-6. - ISBN 978-5-369-01761-6. - Текст : электронный. - URL: https://znanium.com/catalog/product/1861657 (дата обращения: 02.05.2023).

3. 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, 2023. — 312 с. — (Высшее образование). — ISBN 978-5-9916-9043-0. — Текст : электронный // Образовательная

платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/513300 (дата обращения: 02.05.2023).

2. *РЕЖИМ ПРОСМОТРА МАКРООБЪЕКТОВ
1. Перейти по адресу электронного каталога https://magtu.informsystema.ru .
2. Произвести авторизацию (Логин: Читатель1 Пароль: 111111)
3. Активизировать гиперссылку макрообъекта*.
*При открытии макрообъектов учитывайте настройки антивирусной защиты

в) Методические указания:

Методические указания по выполнению лабораторных работ представлены в приложении 3

г) Программное обеспечение и Интернет-ресурсы:

Программное обеспечение

Наименование ПО	№ договора	Срок действия лицензии
MS Office 2007 Professional	№ 135 от 17.09.2007	бессрочно
Atom Editor	свободно распространяемое ПО	бессрочно
NotePad++	свободно распространяемое ПО	бессрочно
MS Visual Studio Code	свободно распространяемое ПО	бессрочно
Adobe Reader	свободно распространяемое ПО	бессрочно
Браузер Mozilla Firefox	свободно распространяемое ПО	бессрочно
Браузер Yandex	свободно распространяемое ПО	бессрочно
Git	свободно распространяемое ПО	бессрочно
FAR Manager	свободно распространяемое ПО	бессрочно
7Zip	свободно распространяемое ПО	бессрочно
Oracle Virtual Box	свободно распространяемое ПО	бессрочно
JetBrains PyCharm Community Edition	свободно распространяемое ПО	бессрочно
MS Visual Studio 2017 Community Edition	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/
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/dokumenty-filter

Архив научных журналов «Национальный электронно-информационный	https://archive.neicon.ru/xmlui/
Международная реферативная и полнотекстовая справочная база данных научных изданий «Springer	https://www.nature.com/siteindex
Международная база полнотекстовых журналов Springer Journals	http://link.springer.com/
Университетская информационная система РОССИЯ	https://uisrussia.msu.ru
Федеральный образовательный портал – Экономика. Социология.	http://ecsocman.hse.ru/
Электронные ресурсы библиотеки МГТУ им. Г.И. Носова	https://magtu.informsystema.ru/Marc.html?locale=ru
Российская Государственная библиотека. Каталоги	https://www.rsl.ru/ru/4readers/catalogues/
Федеральное государственное бюджетное учреждение «Федеральный институт	URL: http://www1.fips.ru/
Информационная система - Единое окно доступа к информационным	URL: http://window.edu.ru/
Поисковая система Академия Google (Google Scholar)	URL: https://scholar.google.ru/
Национальная информационно-аналитическая система – Российский индекс	URL: https://elibrary.ru/project_risc.asp
Электронная база периодических изданий East View Information	https://dlib.eastview.com/

9 Материально-техническое обеспечение дисциплины (модуля)

Материально-техническое обеспечение дисциплины включает:

Материально-техническое обеспечение дисциплины включает:

Лекционные аудитории:

- 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.

Помещения для самостоятельной работы обучающихся:

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

Лекционные аудитории: ауд. 2124, ауд. 2122, 2113, 226, 238, 365, 388, 433 и др. (мультимедийные аудитории).

Учебные аудитории для проведения практических занятий, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации: ауд. 245, 247, 249, 279, 372, 394 и др. (компьютерные классы)

Аудитории для самостоятельной работы: ауд. 132а, компьютерные классы, читальные залы библиотеки.

Приложение 1

Учебно-методическое обеспечение самостоятельной работы обучающихся

Аудиторная самостоятельная работа обучающихся на лабораторных 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*.

1. Контрольные вопросы и задания для проведения текущего контроля

1. Понятие уязвимости в информационной системе.
2. Причины появления уязвимостей в информационной системе.
3. Источники появления уязвимостей в информационной системе.
4. Уязвимости в программных средствах, конфигурационные уязвимости, уязвимости в бизнес-процессах.
5. Классификация уязвимостей в программном обеспечении.
6. Общепринятые системы классификации и оценки уязвимостей информационных систем.
7. Понятие и принцип взлома программного обеспечения. Виды взлома программного обеспечения.
8. Типовые примеры эксплуатации уязвимостей и слабостей системы.
9. Подходы к поиску уязвимостей в программном обеспечении.
10. Общий подход к устранению уязвимостей в информационной системе.
11. Протоколирование уязвимостей.
12. Политика разглашения информации об уязвимостях.
13. Основные методы и подходы при проведении аудита информационной системы и приложений.
14. Основные уязвимости и понятия, которые встречаются при реализации web-приложений.
15. Внедрение кода на клиенте. OWASP-Top 10.
16. Внедрение кода на клиенте: обход аутентификации и CSRF-атаки.
17. Инструментарий для анализа уязвимостей Web-приложений.
18. Внедрение кода на сервере. Инъекции команд. SQL-инъекции. XML-инъекции и другие типы инъекций.
19. Уязвимости, связанные с манипуляциями программной памятью.
20. Организация памяти в современном программном обеспечении. Переполнение буфера на стеке. Уязвимости в динамической памяти. Уязвимости форматной строки. Инструментарий для поиска уязвимостей.
21. Ошибки, связанные с целочисленным переполнением. Арифметические операции в современных языках программирования. Уязвимости, возникающие из-за целочисленного переполнения.
22. Уязвимости, связанные с форматированными строками.
23. Уязвимости, связанные с некорректной обработкой исключений.
24. Слабости в реализации криптографических модулей информационных систем.
25. Уязвимости, связанные с некорректной конфигурацией информационной системы.
26. Понятие эксплойта.
27. Средства защиты от эксплойтов.
28. Особенности тестирования безопасности программного обеспечения.

29. Статический анализ исходного кода программного обеспечения.
30. Динамический анализ исходного кода программного обеспечения.
31. Средства для статического и динамического анализа исходного кода приложений. Декомпиляция приложений.
32. Принципы работы и область применения сканеров безопасности (уязвимостей).
33. Сертификационные испытания программных средств.
34. Аттестация программного обеспечения на отсутствие недекларированных возможностей.

2. Примеры тем лабораторных работ:

1. Уязвимости, связанные с манипуляциями программной памяти.
2. Анализ программного обеспечения на предмет наличия наиболее известных уязвимостей методом экспериментов с «черным ящиком».
3. Сбор информации об уязвимостях программного обеспечения с помощью специального инструментария. Анализ собранной информации. Формирование сводной заявки на устранение уязвимости для исполнителя.

Приложение 2

Оценочные средства для проведения промежуточной аттестации

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

Структурный элемент компетенции	Планируемые результаты обучения	Оценочные средства
ОПК-13: Способен организовывать и проводить диагностику и тестирование систем защиты информации автоматизированных систем, проводить анализ уязвимостей систем защиты информации автоматизированных систем		
ОПК-13.1	Организовывает тестирование систем защиты информации автоматизированных систем	35. Понятие уязвимости в информационной системе. 36. Причины появления уязвимостей в информационной системе. 37. Источники появления уязвимостей в информационной системе. 38. Уязвимости в программных средствах, конфигурационные уязвимости, уязвимости в бизнес-процессах. 39. Классификация уязвимостей в программном обеспечении. 40. Общепринятые системы классификации и оценки уязвимостей информационных систем. 41. Понятие и принцип взлома программного обеспечения. Виды взлома программного обеспечения. 42. Типовые примеры эксплуатации уязвимостей и слабостей системы. 43. Подходы к поиску уязвимостей в программном обеспечении. 44. Особенности тестирования безопасности программного обеспечения. 45. Общий подход к устранению уязвимостей в информационной системе. 46. Протоколирование уязвимостей. 47. Политика разглашения информации об уязвимостях.
ОПК-13.2	Проводит диагностику систем защиты информации автоматизированных систем	1. Основные методы и подходы при проведении аудита информационной системы и приложений. 2. Основные уязвимости и понятия, которые встречаются при реализации web-приложений. 3. Внедрение кода на клиенте. OWASP-Top 10. 4. Внедрение кода на клиенте: обход аутентификации и CSRF-атаки. 5. Инструментарий для анализа уязвимостей Web-приложений. 6. Внедрение кода на сервере. Инъекции команд. SQL-инъекции. XML-инъекции и другие типы инъекций. 7. Уязвимости, связанные с манипуляциями программной памятью. 8. Организация памяти в современном программном обеспечении. Переполнение буфера на стеке. Уязвимости в динамической памяти. Уязвимости форматной строки. Инструментарий для поиска уязвимостей. 9. Ошибки, связанные с целочисленным переполнением. Арифметические операции в современных языках программирования. Уязвимости, возникающие из-за целочисленного переполнения. 10. Уязвимости, связанные с форматированными строками. 11. Уязвимости, связанные с некорректной обработкой исключений. 12. Слабости в реализации криптографических модулей информационных систем. 13. Уязвимости, связанные с некорректной конфигурацией информационной системы. 14. Понятие эксплойта. 15. Средства защиты от эксплойтов.

Структурный элемент компетенции	Планируемые результаты обучения	Оценочные средства
ОПК-13.3	Анализирует уязвимости автоматизированных систем и их систем защиты	1. Статический анализ исходного кода программного обеспечения. 2. Динамический анализ исходного кода программного обеспечения. 3. Средства для статического и динамического анализа исходного кода приложений. Декомпиляция приложений. 4. Принципы работы и область применения сканеров безопасности (уязвимостей). 5. Сертификационные испытания программных средств. 6. Аттестация программного обеспечения на отсутствие недекларированных возможностей.

б) Порядок проведения промежуточной аттестации, показатели и критерии оценивания:

Промежуточная аттестация по дисциплине «Анализ уязвимостей программного обеспечения» включает компьютерное тестирование, позволяющее оценить уровень усвоения обучающимися знаний, и практическое задание, выявляющие степень сформированности умений и владений; проводится в форме зачета.

Показатели и критерии оценивания зачета:

– на оценку «зачтено» – обучающийся должен набрать не менее 50% баллов при прохождении компьютерного тестирования, показав знание теоретического материала на уровне воспроизведения и объяснения информации, а также выполнить лабораторную работу, продемонстрировав умения и навыки решения стандартных задач.

– на оценку «не зачтено» – обучающийся не демонстрирует знание теоретического материала на уровне воспроизведения и объяснения информации, набрав на компьютерном тестировании менее 50% баллов, а также не может выполнить лабораторную работу и не может показать интеллектуальные навыки решения простых задач.