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
_____ С.И. Лукьянов

26.02.2020 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 7 "Обеспечение информационной безопасности распределенных информационных систем";

Уровень высшего образования - специалитет

Форма обучения
очная

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

Магнитогорск
2020 год

Рабочая программа составлена на основе ФГОС ВО по специальности 10.05.03 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ АВТОМАТИЗИРОВАННЫХ СИСТЕМ (приказ Минобрнауки России от 01.12.2016 г. № 1509)

Рабочая программа рассмотрена и одобрена на заседании кафедры Информатики и информационной безопасности
18.02.2020, протокол № 6

Зав. кафедрой _____ И.И. Баранкова

Рабочая программа одобрена методической комиссией ИЭиАС
26.02.2020 г. протокол № 5

Председатель _____ С.И. Лукьянов

Рабочая программа составлена:
ст. преподаватель кафедры ИиИБ, канд. техн. наук _____М.В. Коновалов

Рецензент:
Начальник УИТиАСУ , канд. техн. наук _____К.А. Рубан

Лист актуализации рабочей программы

Рабочая программа пересмотрена, обсуждена и одобрена для реализации в 2021 - 2022 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 2022 - 2023 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 2023 - 2024 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 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

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:

- изучить контрольно-испытательные и логико-аналитические методы анализа уязвимости программного обеспечения и способы обеспечения надежности программ для контроля их технологической безопасности;
- освоить способы оценки эффективности систем защиты программного обеспечения и технологии разработки систем программно-технической защиты программного обеспечения.

2 Место дисциплины (модуля) в структуре образовательной программы

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

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

Защита электронного документооборота

Методы мониторинга информационной безопасности АС

Безопасность сетей ЭВМ

Технология построения защищенных распределенных приложений

Технологии и методы программирования

Организация ЭВМ и вычислительных систем

Языки программирования

Безопасность систем баз данных

Тестирование систем защиты информации автоматизированных систем

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

Производственная-практика по получению профессиональных умений и опыта профессиональной деятельности

Подготовка к сдаче и сдача государственного экзамена

Подготовка к защите и защита выпускной квалификационной работы

Производственная-преддипломная практика

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:

Структурный элемент компетенции	Планируемые результаты обучения
ПК-3 способностью проводить анализ защищенности автоматизированных систем	
Знать	- перечень инструментов для проведения анализа уязвимостей программного обеспечения; - базовый функционал инструментов для проведения анализа уязвимостей программного обеспечения;

Уметь	- применять технические средства для проведения анализа уязвимостей программного обеспечения;
Владеть	- навыками работы с специализированным программным обеспечением для проведения анализа уязвимостей программного обеспечения
ПК-6 способностью проводить анализ, предлагать и обосновывать выбор решений по обеспечению эффективного применения автоматизированных систем в сфере профессиональной деятельности	
Знать	Методы, способы, средства, последовательность и содержание этапов разработки программного обеспечения и компонентов безопасности программного обеспечения.
Уметь	- проводить анализ уязвимостей программного обеспечения; - выполнять реверс инжиниринг программного обеспечения;
Владеть	- навыками противодействия атакам на программное обеспечение;
ПК-24 способностью обеспечить эффективное применение информационно-технологических ресурсов автоматизированной системы с учетом требований информационной безопасности	
Знать	- методы повышения уровня безопасности программного обеспечения;
Уметь	- выполнять работы по оптимизации схем управления автоматизированной системой; - выявлять компоненты программного обеспечения, не обеспечивающие требуемый уровень информационной безопасности;
Владеть	- навыками определения возможных векторов атаки на программное обеспечение

4. Структура, объём и содержание дисциплины (модуля)

Общая трудоемкость дисциплины составляет 4 зачетных единиц 144 акад. часов, в том числе:

– контактная работа – 70,8 акад. часов:

– аудиторная – 68 акад. часов;

– внеаудиторная – 2,8 акад. часов

– самостоятельная работа – 73,2 акад. часов;

Форма аттестации - курсовая работа, 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. 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	ПК-3, ПК-6, ПК-24
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	ПК-3, ПК-6, ПК-24
Итого по разделу		6	6		4			
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		2	Создание тестового ПО, ее конфигурация. Отслеживания действий пользователей в ПО.	Семинарское занятие, устный опрос	ПК-3, ПК-6, ПК-24
2.2 Алгоритмические и программные закладки		3	3		2	Конфигурация прав пользователей в ПО	Семинарское занятие, устный опрос	ПК-3, ПК-6, ПК-24
Итого по разделу		6	6		4			
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	ПК-3, ПК-6, ПК-24
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	ПК-3, ПК-6, ПК-24
Итого по разделу		6	6		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	ПК-3, ПК-6, ПК-24
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	ПК-3, ПК-6, ПК-24
Итого по разделу		6	6		7,2			
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	ПК-3, ПК-6, ПК-24
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	ПК-3, ПК-6, ПК-24
Итого по разделу		6	6		8			
6. Оценка эффективности систем защиты программного обеспечения								
6.1 Критерии оценки: стойкость к исследованию/взлому; отказоустойчивость (надёжность).	8	2	2		3	Анализ HTML кода. Проверка простейших ошибок при конфигурирование страницы авторизации.	Защита проекта, устный опрос	ПК-3, ПК-6, ПК-24
6.2 Критерии оценки: независимость от конкретных реализаций операционных систем; совместимость; неудобства для конечного пользователя программного обеспечения; побочные эффекты; стоимость; доброкачественность		2	2		3	Применение основных типов SQL-инжекции для получения доступа данных авторизации	Защита проекта, устный опрос	ПК-3, ПК-6, ПК-24
Итого по разделу		4	4		6			
7. Аттестация								
7.1 Зачет	8					Подготовка к зачету	Зачет	
7.2 Курсовая работа					40	Выполнение курсовой работы	Защита курсовой работы	ПК-3, ПК-6, ПК-24
Итого по разделу					40			
Итого за семестр		34	34		73,2		зачёт,кр	
Итого по дисциплине		34	34		73,2		курсовая работа, зачет	ПК-3,ПК-6,ПК-24

5 Образовательные технологии

Для реализации предусмотренных видов учебной работы в качестве образовательных технологий в преподавании дисциплины «теория информации» 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

проблемная - 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

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»,

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:

е изд., перераб. и доп. — Москва: Издательство Юрайт, 2020. — 161 с. — (Высшее образование). — ISBN 978-5-534-07248-8. — Текст: электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/422772 (дата обращения: 27.04.2020).

б) Дополнительная литература:

1. Каратунова, Н. Г. Защита информации. Курс лекций [Электронный ресурс] : Учебное пособие / Н. Г. Каратунова. - Краснодар: КСЭИ, 2014. - 188 с. - Режим доступа: http://www.znanium.com.–Заглавие с экрана.

2. 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

*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 Windows 7 Professional(для классов)	Д-1227-18 от 08.10.2018	11.10.2021
MS Office 2007 Professional	№ 135 от 17.09.2007	бессрочно
Atom Editor	свободно распространяемое ПО	бессрочно

NotePad++	свободно распространяемое	бессрочно
MS Visual Studio Code	свободно распространяемое ПО	бессрочно
Adobe Reader	свободно распространяемое	бессрочно
MS Windows 10 Professional (для классов)	Д-1227-18 от 08.10.2018	11.10.2021
Браузер Mozilla Firefox	свободно распространяемое ПО	бессрочно
Браузер Yandex	свободно распространяемое	бессрочно
Git	свободно распространяемое	бессрочно
FAR Manager	свободно распространяемое	бессрочно

Профессиональные базы данных и информационные справочные системы

Название курса	Ссылка
Электронная база периодических изданий East View Information Services, ООО	https://dlib.eastview.com/
Национальная информационно-аналитическая система – Российский индекс научного цитирования (РИНЦ)	URL: https://elibrary.ru/project_risc.asp
Поисковая система Академия Google (Google Scholar)	URL: https://scholar.google.ru/
Информационная система - Единое окно доступа к информационным ресурсам	URL: http://window.edu.ru/
Федеральное государственное бюджетное учреждение «Федеральный институт промышленной собственности»	URL: http://www1.fips.ru/
Российская Государственная библиотека. Каталоги	https://www.rsl.ru/ru/4readers/catalogues/
Электронные ресурсы библиотеки МГТУ им. Г.И. Носова	http://magtu.ru:8085/marcweb2/Default.asp
Федеральный образовательный портал – Экономика. Социология. Менеджмент	http://ecsocman.hse.ru/
Университетская информационная система РОССИЯ	https://uisrussia.msu.ru
Международная наукометрическая реферативная и полнотекстовая база данных научных изданий «Web of science»	http://webofscience.com
Международная реферативная и полнотекстовая справочная база данных	http://scopus.com
Международная база полнотекстовых журналов Springer Journals	http://link.springer.com/
Международная коллекция научных протоколов по различным отраслям знаний	http://www.springerprotocols.com/
Международная база научных материалов в области физических наук и инжиниринга	http://materials.springer.com/
Международная база справочных изданий по всем отраслям знаний SpringerReference	http://www.springer.com/references
Международная реферативная база данных по чистой и прикладной математике	http://zbmath.org/

Международная реферативная и полнотекстовая справочная база данных научных изданий	https://www.nature.com/siteindex
Архив научных журналов «Национальный электронно-информационный	https://archive.neicon.ru/xmlui/
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/normotvorcheskaya/tekhnicheskaya-zashchita-informatsii
Информационная система - Банк данных угроз безопасности информации ФСТЭК России	https://bdu.fstec.ru/
Федеральное агентство по техническому регулированию и метрологии	https://www.rst.gov.ru/portal/gost

9 Материально-техническое обеспечение дисциплины (модуля)

Материально-техническое обеспечение дисциплины включает:
Лекционная аудитории:
Мультимедийные средства хранения, передачи и представления информации.
Компьютерный класс:
Персональные компьютеры с установленным ПО и выходом в интернет.
Аудитории для самостоятельной работы
Персональные компьютеры с установленным ПО и выходом в интернет.

Приложение 1

По дисциплине «Анализ уязвимостей программного обеспечения» предусмотрено выполнение и защита лабораторных работ и внеаудиторная самостоятельная работа обучающихся.

Аудиторная самостоятельная работа обучающихся на лабораторных занятиях осуществляется под контролем преподавателя в виде решения задач и выполнения упражнений, которые определяет преподаватель для обучающихся.

Внеаудиторная самостоятельная работа обучающихся осуществляется в виде изучения литературы по соответствующему разделу с проработкой материала; выполнения домашних заданий, подготовки к аудиторным контрольным работам и выполнения домашних заданий с консультациями преподавателя.

Примерный индивидуальные домашние задания

Модуль 1. Теоретические и формальные методы доказательства правильности программ и их спецификаций

1.Дайте определение формальной спецификации программного обеспечения.
2. Назовите категории классификации спецификаций программного обеспечения.
3. Определите основные понятия формальной спецификации VDM.
4. Определите основные базовые элементы спецификации RAISE.
5. Сравните математические понятия методов VDM и RAISE.
6. Определите цель и структуру концепторного языка.
7. Назовите формальные методы доказательства правильности программного обеспечения и приведите их короткую аннотацию.
8. Определите понятия пред- и постусловий, аксиом и утверждений программного обеспечения.
9. Опишите, как проходит процесс доказательства правильности программного обеспечения, заданной спецификацией.
10. В чем проблемы проведения доказательства правильности программного обеспечения с помощью формальных методов?
11. Приведите отличие техники формального доказательства правильности программного обеспечения от символьного выполнения программ?

Модуль 2 Контрольно-испытательные и логико-аналитические методы анализа уязвимости программного обеспечения.

1. Дайте определение верификации и валидации программного обеспечения.
2. В чем суть композиции верифицированных программ?
3. Расскажите о международном проекте по верификации программного обеспечения.
4. Перечислите контрольно-испытательные и логико-аналитические методы анализа безопасности программного обеспечения.
5. Какие бывают проблемы анализа безопасности программного обеспечения?
6. Назовите основные угрозы безопасности программного обеспечения.
7. Что такое алгоритмические и программные закладки программного обеспечения?

Модуль 3. Методы и средства анализа уязвимости программ

1. Приведите классификацию методов и средств анализа безопасности программ.
2. Как используют лексический, синтаксический и семантический верификационный анализ для анализа безопасности программного обеспечения?
3. Как делается верификация моделей программ методом model checking?
4. Опишите логику дерева вычислений: формализм для представления свойств живости и безопасности, алгоритмы верификации.

5. Опишите технологии создания алгоритмически безопасных процедур.
6. Какие бывают методы создания самотестирующихся и самокорректирующихся программ?
7. Опишите создание безопасного программного обеспечения на базе методов теории конфиденциальных вычислений.

Модуль 4. Способы обеспечения надежности программ для контроля их технологической безопасности.

1. Как делается защита программ и забывающее моделирование на RAM-машинах?
2. Какие вы знаете способы обеспечения надежности программ для контроля их технологической безопасности?
3. Перечислите процессы обеспечения функциональной безопасности программных продуктов в международных стандартах IEC и ISO.
4. Назовите методы идентификации программ и их характеристик.
5. Какие вы знаете способы оценки подобия целевой и исследуемой программ с точки зрения наличия программных дефектов?

Модуль 5. Анализ средств и этапы преодоления систем защиты программного обеспечения.

1. Охарактеризуйте анализ средств и этапы преодоления систем защиты программного обеспечения.
2. Перечислите и опишите методы защиты программ от исследования.
3. Опишите технологии разработки систем программно-технической защиты программного обеспечения.
4. Назовите этапы проектирования и разработки систем программно-технической защиты программного обеспечения.
5. Как делается оценка эффективности систем защиты программного обеспечения?
6. Какие вы знаете критерии оценки стойкости к исследованию или взлому программного обеспечения?

Модуль 6. Оценка эффективности систем защиты программного обеспечения.

1. Укажите критерии устойчивости программного обеспечения к исследованию и взлома.
2. Укажите критерии отказоустойчивости и надежности программного обеспечения
3. Укажите критерии оценки независимости программного обеспечения от конкретных реализаций операционных систем.
4. Укажите критерии оценки совместимости программного обеспечения.
5. Укажите критерии оценки графического интерфейса пользователя программного обеспечения.
6. Укажите критерии оценки побочных эффектов программного обеспечения.
7. Укажите критерии оценки стоимости программного обеспечения.

Приложение 2

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

Структурный элемент компетенции	Планируемые результаты обучения	Оценочные средства
ПК-3: способностью проводить анализ защищенности автоматизированных систем		
Знать	- перечень инструментов для проведения анализа уязвимостей программного обеспечения; - базовый функционал инструментов для проведения анализа уязвимостей программного обеспечения;	1. В чем проблемы проведения доказательства правильности программного обеспечения с помощью формальных методов? 2. Приведите отличие техники формального доказательства правильности программного обеспечения от символьного выполнения программ? 3. Дайте определение верификации и валидации программного обеспечения. 4. В чем суть композиции верифицированных программ? 5. Расскажите о международном проекте по верификации программного обеспечения. 6. Перечислите контрольно-испытательные и логико-аналитические методы анализа безопасности программного обеспечения. 7. Какие бывают проблемы анализа безопасности программного обеспечения? 8. Назовите основные угрозы безопасности программного обеспечения. 9. Что такое алгоритмические и программные закладки программного обеспечения? 10. Приведите классификацию методов и средств анализа безопасности программ.
Уметь	- применять технические средства для проведения анализа уязвимостей программного обеспечения	Определить протокол, используемый для авторизации участников сети. Выполнить атаку Pixie Dust. Определить причины по которым атака прошла успешно. Предложить меры по увеличению защищенности программного обеспечения.
Владеть	- навыками работы с специализированным программным обеспечением для проведения анализа безопасности программного обеспечения	Провести комплексный тест выбранного экземпляра ПО при помощи инструментов дистрибутива Kali Linux 2.

ПК-6: способностью проводить анализ, предлагать и обосновывать выбор решений по обеспечению эффективного применения автоматизированных систем в сфере профессиональной деятельности		
Знать	- Методы, способы, средства, последовательность и содержание этапов разработки программного обеспечения и компонентов безопасности программного обеспечения;	1.Как делается верификация моделей программ методом model checking? 2. Опишите логику дерева вычислений: формализм для представления свойств живости и безопасности, алгоритмы верификации. 3. Опишите технологии создания алгоритмически безопасных процедур. 4. Какие бывают методы создания самотестирующихся и самокорректирующихся программ? 5. Опишите создание безопасного программного обеспечения на базе методов теории конфиденциальных вычислений. 6. Как делается защита программ и забывающее моделирование на RAM-машинах? 7. Какие вы знаете способы обеспечения надежности программ для контроля их технологической безопасности? 8. Перечислите процессы обеспечения функциональной безопасности программных продуктов в международных стандартах IEC и ISO. 9. Назовите методы идентификации программ и их характеристик.
Уметь	- проводить анализ уязвимостей программного обеспечения; - выполнять реверс инжиниринг программного обеспечения;	Выполнить анализ экземпляра ПО на наличие следующих уязвимостей: Уязвимость к включению файлов, возможность SQL-инъекции, Возможность переполнения буфера, подверженность состоянию гонки. При помощи встроенных утилит Linux выполнить реверс-инжиниринг предложенного экземпляра ПО
Владеть	- навыками противодействия атакам на программное обеспечение;	Разработать модуль контроля целостности исполняемого файла ПО. Реализовать защиту от XSS
ПК-24. Способностью обеспечить эффективное применение информационно-технологических ресурсов автоматизированной системы с учетом требований информационной безопасности		

Знать	- методы повышения уровня безопасности программного обеспечения;	1. Управление учетными записями пользователей. 2. Мониторинг процессов и приложений 3. Аудит событий в локальной системе 4. Объекты групповой политики (GPO). Создание. Редактирование. Хранение. 5. Сетевая информационная система NIS (NIS+) и ее конфигурирование. 6. Доступ к удаленным компьютерам 7. Виртуальные частные сети 8. Выбор режима проверки подлинности. 9. Авторизация пользователей. 10. Системные процедуры администрирования учетных записей Windows. 11. Системные процедуры администрирования учетных записей SQL Server.
Уметь	- выполнять работы по оптимизации схем управления автоматизированной системой; - выявлять компоненты программного обеспечения, не обеспечивающие требуемый уровень информационной безопасности;	При помощи утилиты htop определить PID процессов, созданных экземпляром исследуемого ПО. Определить иерархию процессов. Определит права с которыми запущены процессы. Соотнести задачи процессов и предоставленные им права. Ограничить права процессов при помощи средств ОС.
Владеть	- навыками определения возможных векторов атаки на программное обеспечение;	Проанализировать конфигурацию программного обеспечения и определить какие параметры конфигурации снижают защищенность ПО.

Примерный перечень тем курсовых работ:

1. Дизасемблировать EXE-файл и выполнить анализ его внутренней структуры.
2. Разработать комплект тестов для выявления уязвимостей ПО «NotePad++»
3. Разработать комплект тестов для выявления уязвимостей ПО «PaintNET»
4. Разработать комплект тестов для выявления уязвимостей ПО «Tree»
5. Разработать комплект тестов для выявления уязвимостей ПО «Download+»

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

Промежуточная аттестация по дисциплине включает теоретические вопросы, позволяющие оценить уровень усвоения обучающимися знаний, и практические задания, выявляющие степень сформированности умений и владений, проводится в форме зачета и экзамена.

Критерии оценки для получения зачета

«зачтено» – обучающийся показывает средний уровень сформированности компетенций.

«не зачтено» – результат обучения не достигнут, обучающийся не может показать знания на уровне воспроизведения и объяснения информации, не может показать

интеллектуальные навыки решения простых задач, не может показать знания на уровне воспроизведения и объяснения информации.

Показатели и критерии оценивания курсовой работы:

– на оценку «отлично» (5 баллов) – работа выполнена в соответствии с заданием, обучающийся показывает высокий уровень знаний не только на уровне воспроизведения и объяснения информации, но и интеллектуальные навыки решения проблем и задач, нахождения уникальных ответов к проблемам, оценки и вынесения критических суждений;

– на оценку «хорошо» (4 балла) – работа выполнена в соответствии с заданием, обучающийся показывает знания не только на уровне воспроизведения и объяснения информации, но и интеллектуальные навыки решения проблем и задач, нахождения уникальных ответов к проблемам;

– на оценку «удовлетворительно» (3 балла) – работа выполнена в соответствии с заданием, обучающийся показывает знания на уровне воспроизведения и объяснения информации, интеллектуальные навыки решения простых задач;

– на оценку «неудовлетворительно» (2 балла) – задание преподавателя выполнено частично, в процессе защиты работы обучающийся допускает существенные ошибки, не может показать интеллектуальные навыки решения поставленной задачи.

– на оценку «неудовлетворительно» (1 балл) – задание преподавателя выполнено частично, обучающийся не может воспроизвести и объяснить содержание, не может показать интеллектуальные навыки решения поставленной задачи.

Приложение 3

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ВЫПОЛНЕНИЮ ЛАБОРАТОРНЫХ РАБОТ

Рекомендации направлены на оказание методической помощи студентам при выполнении лабораторных занятий.

Лабораторное занятие – это занятие, проводимое под руководством преподавателя в учебной аудитории (компьютерном классе университета или учебной специализированной лаборатории университета), направленное на углубление научно-теоретических знаний и получение лабораторных навыков решения типовых и прикладных задач.

Целью лабораторных занятий является формирование и отработка лабораторных умений и навыков, необходимых в последующей деятельности обучающихся.

Основными задачами лабораторных занятий являются:

- углубление уровня освоения общекультурных и профессиональных компетенций;
- обобщение, систематизация, углубление, закрепление полученных лабораторных знаний по конкретным темам дисциплин различных циклов;
- приобретение студентами умений и навыков использования современных теоретических знаний в решении конкретных прикладных задач;
- развитие профессионального мышления, профессиональной и познавательной мотивации.

Перечень тем лабораторных работ определяется рабочей программой дисциплины. План лабораторных занятий отвечает общей направленности лекционного курса и соотнесен с ним в последовательности тем.

Структура лабораторного занятия включает следующие компоненты: вступительная часть; ответы на вопросы обучающихся; практическая часть; заключительное слово преподавателя. Во вступительной части объявляется тема текущей лабораторной работы, ставится ее цели и задачи, проводиться инструктаж по технике безопасности выполнения работы, проверяется исходный уровень готовности студентов к лабораторной работе (выполнение тестов, контрольные вопросы и т.п.), выдается порядок и условия выполнения лабораторной работы.

На лабораторном занятии преподаватель может использовать разнообразные образовательные технологии (методы IT, работа в команде, case-study, проблемное обучение, учебные дискуссии и т.п.) по своему выбору для достижения качественного уровня обучения.

Правила по технике безопасности для обучающихся при проведении лабораторных работ

Общие правила:

1. Лабораторные работы проводятся под наблюдением преподавателя. К выполнению лабораторных работ студенты допускаются только после прослушивания инструктажа по технике безопасности, правилам поведения, противопожарным мерам в компьютерном классе и специализированных лабораториях.

2. Обучаемый должен строго выполнять правила техники безопасности и санитарно-гигиенические нормы при работе в компьютерных классах и специализированных лабораториях университета.

Порядок выполнения лабораторных работ

При подготовке к выполнению лабораторных работ студент должен повторить теоретический материал, необходимый для выполнения заданий по текущей теме.

Лабораторная работа выполняется каждым студентом самостоятельно, согласно индивидуальному заданию.

Студенты, пропустившие занятия, выполняют лабораторные работы во внеурочное время.

После выполнения каждой лабораторной работы студент демонстрирует результат выполнения преподавателю в виде отчета по лабораторной работе и отвечает на вопросы. Преподаватель оценивает работу в соответствии с заданными критериями оценки лабораторных работ.

Правила оформления результатов и оценивания лабораторной работы

Результаты выполненной лабораторной работы оформляются в соответствии с требованиями к выполнению конкретной работы.

Практическая работа считается выполненной, если студент набрал балл, который составляет половину максимального количества баллов.

Для оценивания работы прилагаются следующие критерии.

Оценка «отлично» – работа выполнена в полном объеме и без замечаний.

Оценка «хорошо» – работа выполнена правильно с учетом 2-3 несущественных ошибок, исправленных самостоятельно по требованию преподавателя.

Оценка «удовлетворительно» – работа выполнена правильно не менее чем на половину или допущена существенная ошибка.

Оценка «неудовлетворительно» – допущены две (и более) существенные ошибки в ходе работы, которые студент не может исправить даже по требованию преподавателя, или работа не выполнена.

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ВЫПОЛНЕНИЮ ВНЕАУДИТОРНЫХ САМОСТОЯТЕЛЬНЫХ РАБОТ

Общие положения

Настоящие методические указания предназначены для организации внеаудиторной самостоятельной работы студентов и оказания помощи в самостоятельном изучении теоретического и реализации компетенций обучаемых.

Данные методические указания не являются учебным пособием, поэтому перед началом выполнения самостоятельного задания следует изучить соответствующие разделы лекционных занятий, материалов образовательного портала, разделов основной и дополнительной литературы, представленных в пункте 8. «Учебно-методическое и информационное обеспечение дисциплины (модуля)» данной РПД.

Цели и задачи самостоятельной работы

Цель самостоятельной работы – содействие оптимальному усвоению учебного материала обучающимися, развитие их познавательной активности, готовности и потребности в самообразовании.

Задачи самостоятельной работы:

- повышение исходного уровня владения информационными технологиями;
- углубление и систематизация знаний;

- постановка и решение стандартных задач профессиональной деятельности;
- развитие работы с различной по объему и виду информацией, учебной и научной литературой;
- практическое применение знаний, умений;
- самостоятельно использование стандартных программных средств сбора, обработки, хранения и защиты информации
- развитие навыков организации самостоятельного учебного труда и контроля за его эффективностью.

Виды внеаудиторной самостоятельной работы и формы контроля и время на выполнение каждого вида самостоятельной работы указаны в пункте 4. «Структура и содержание дисциплины» данной РПД.

Порядок выполнения

При выполнении текущей внеаудиторной самостоятельной работы обучающемуся следует придерживаться следующего порядка действий:

1) внимательно изучить соответствующие теоретические разделы дисциплины, пользуясь материалами (лекционными, презентационными, аудио-визуальными):
   a) предоставляемыми преподавателем на лекционных занятиях;
   b) предоставляемыми преподавателем в рамках электронных образовательных курсов;
   c) содержащимися в учебниках и учебных пособиях ЭБС (электронно-библиотечных систем), электронных каталогов университета и интернет-ресурсов.
2) Подробно разобрать типовые примеры решения задач, рассмотренные в рамках аудиторной контактной работы с преподавателем.
3) Применить полученные теоретические знания и практические навыки к решению индивидуальных заданий, к прохождению компьютерных тестирований.
4) При необходимости, сформировать перечень вопросов, вызвавших затруднения в процессе самостоятельной работы. Обсудить возникшие вопросы со студентами группы, в рамках командно-проектной работы, и с преподавателем, в рамках консультационной помощи, реализованной либо в контактной форме, либо средствами информационно-образовательной среды ВУЗа.

Критерии оценки внеаудиторных самостоятельных работ

Качество выполнения внеаудиторной самостоятельной работы обучающихся оценивается посредством текущего контроля самостоятельной работы обучающихся с использованием балльно-рейтинговой системы.

В качестве форм текущего контроля по дисциплине используются: индивидуальные задания, аудиторные контрольные работы, компьютерное тестирование.

Максимальное количество баллов обучающийся получает, если:

- выполняет индивидуальные задания в соответствии со всеми заявленными требованиями;
- дает правильные формулировки, точные определения, понятия терминов;
- может обосновать рациональность решения текущей задачи.;
- обстоятельно с достаточной полнотой излагает соответствующую теоретический раздел;
- правильно отвечает на дополнительные вопросы преподавателя, имеющие целью выяснить степень понимания им данного материала.

50~85% от максимального количества баллов обучающийся получает, если:

- неполно (не менее 70% от полного), но правильно выполнено задание;
- при изложении были допущены 1-2 несущественные ошибки, которые он исправляет после замечания преподавателя;
- дает правильные формулировки, точные определения, понятия терминов;

- может обосновать свой ответ, привести необходимые примеры;
- правильно отвечает на дополнительные вопросы преподавателя, имеющие целью выяснить степень понимания им данного материала.

36~50% от максимального количества баллов обучающийся получает, если:

- неполно (не менее 50% от полного), но правильно изложено задание;
- при изложении была допущена 1 существенная ошибка;
- знает и понимает основные положения данной темы, но допускает неточности в формулировке понятий;
- излагает выполнение задания недостаточно логично и последовательно;
- затрудняется при ответах на вопросы преподавателя.

35% и менее от максимального количества баллов обучающийся получает, если:

- неполно (менее 50% от полного) изложено задание;
- при изложении были допущены существенные ошибки. В "0" баллов преподаватель вправе оценить выполненное обучающимся задание, если оно не удовлетворяет требованиям, установленным преподавателем к данному виду работы или не было представлено для проверки.

Сумма полученных баллов по всем видам заданий внеаудиторной самостоятельной работы составляет рейтинговый показатель обучающегося. Рейтинговый показатель обучающегося влияет на выставление итоговой оценки по результатам изучения дисциплины.

Показатели и критерии оценивания полученных знаний представлены в пункте 7.б) «Оценочные средства для проведения промежуточной аттестации» данной РПД.