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)

МЕТОДЫ МОНИТОРИНГА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АС

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, 5
Семестр	8, 9

Магнитогорск
2019 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 2020 - 2021 учебном году на заседании кафедры Информатики и информационной безопасности

Протокол от 01 сентября 2020 г. № 1
Зав. кафедрой _____ И.И. Баранкова

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

1 Цели освоения дисциплины (модуля)

Общей целью дисциплины «Методы мониторинга информационной безопасности автоматизированных систем» является повышение исходного уровня владения ин-формационными технологиями, достигнутого на предыдущей ступени образования, и овладение обучающимися необходимым и достаточным уровнем профессиональных компетенций в соответствии с требованиями ФГОС ВО по специальности «Информационная безопасность автоматизированных систем». Специальными целями дисциплины «Методы мониторинга информационной безопасности автоматизированных систем» являются: изучить архитектуру, функции, методы и алгоритмы, организационную структуру, технологии создания и готовые аппаратно-программные решения систем мониторинга информационной безопасности автоматизированных систем; научится применять в промышленности и сетевых средах системы управления событиями информационной безопасности автоматизированных систем; выполнять аудит информационной безопасности информационных систем.

2 Место дисциплины (модуля) в структуре образовательной программы

Дисциплина Методы мониторинга информационной безопасности АС входит в вариативную часть учебного плана образовательной программы.

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

Информатика

Организация ЭВМ и вычислительных систем

Техническая защита информации

Моделирование систем и процессов защиты информации

Организационное и правовое обеспечение информационной безопасности

Безопасность сетей ЭВМ

Моделирование угроз информационной безопасности

Управление информационной безопасностью

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

Научно-исследовательская работа

Подготовка к защите и защита выпускной квалификационной работы

Подготовка к сдаче и сдача государственного экзамена

Производственная-преддипломная практика

Производственная-практика по получению профессиональных умений и опыта профессиональной деятельности

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

В результате освоения дисциплины (модуля) «Методы мониторинга информационной безопасности АС» обучающийся должен обладать следующими компетенциями:

Структурный элемент компетенции	Планируемые результаты обучения
ПК-15 способностью участвовать в проведении экспериментально-исследовательских работ при сертификации средств защиты информации автоматизированных систем	
Знать	- способы организации автоматизированных систем; - подходы к проведению сертификации средств защиты информационной безопасности;

Уметь	- составлять регламент испытаний средств защиты информации автоматизированных систем;
Владеть	- навыками применения, специализированного ПО для проведения мероприятий при сертификации средств защиты информации автоматизированных систем;
ПК-17 способностью проводить инструментальный мониторинг защищенности информации в автоматизированной системе и выявлять каналы утечки информации	
Знать	- перечень инструментов для проведения мониторинга защищенности информации; - базовый функционал инструментов для проведения мониторинга защищенности информации;
Уметь	- применять технические средства для проведения мониторинга беспроводных сетей; - применять технические средства для проведения мониторинга проводных сетей построенных на основе неуправляемых коммутаторов;
Владеть	- навыками работы с специализированным программным обеспечением для проведения мониторинга защищенности информации в автоматизированной системе;
ПК-24 способностью обеспечить эффективное применение информационно-технологических ресурсов автоматизированной системы с учетом требований информационной безопасности	
Знать	- методы повышения уровня безопасности за счет настройки прав доступа к ресурсам автоматизированной системы;
Уметь	- выполнять работы по оптимизации схем управления автоматизированной системой; - выявлять узлы автоматизированной системы, не обеспечивающие требуемый уровень информационной безопасности;
Владеть	- навыками определения возможных векторов атаки на автоматизированную систему;
ПСК-7.3 способностью проводить аудит защищенности информационно- технологических ресурсов распределенных информационных систем	
Знать	- способы получения информации о внутренней структуре исследуемой распределенной системе; -наиболее распространённые точки для несанкционированного входа в распределенную систему;
Уметь	- проводить анализ уязвимостей распределённой системы; - получать несанкционированный доступ к ресурсам распределенной системы;
Владеть	- навыками противодействия внешним атакам на распределенную информационную сеть;

4. Структура, объём и содержание дисциплины (модуля)

Общая трудоемкость дисциплины составляет 5 зачетных единиц 180 акад. часов, в том числе:

– контактная работа – 89,1 акад. часов:

– аудиторная – 85 акад. часов;

– внеаудиторная – 4,1 акад. часов

– самостоятельная работа – 55,2 акад. часов;

– подготовка к экзамену – 35,7 акад. часа

Форма аттестации - зачет, экзамен

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. Введение в мониторинг АС								
1.1 Архитектура и функции систем мониторинга информационной безопасности.	8	2	2/1,5И	2/1,5И	2,1	Подготовка к практическому занятию; поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями)	семинарское занятие	ПК-15, ПК-17, ПК-24, ПСК-7.3
1.2 Модульный принцип построения системы информационной безопасности.		3	3	3/1,5И	3	Подготовка к практическому занятию; поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями)	Семинарское занятие, устный опрос	ПК-15, ПК-17, ПК-24, ПСК-7.3
Итого по разделу		5	5/1,5И	5/3И	5,1			
2. Мониторинг ИБ АС								

2.1 Идентификация пользователей, трафика, приложений, протоколов и схем использования ресурсов.	8	3	3/1,5И	3/1,5И	3	Создание тестовой АС, ее конфигурация. Отслеживания действий пользователей АС.	Семинарское занятие, устный опрос	ПК-15, ПК-17, ПК-24, ПСК-7.3
2.2 Ограничение доступа и использования ресурсов на уровне пользователя, протокола, сервиса и приложения. Изоляция пользователей, сервисов и приложений		3	3	3/1,5И	4	Конфигурация прав пользователей АС	Семинарское занятие, устный опрос	ПК-15, ПК-17, ПК-24, ПСК-7.3
Итого по разделу		6	6/1,5И	6/3И	7			
3. Средства мониторинга ИБ АС								
3.1 Применение специализированных дистрибутивов Linux для создания АРМ системы мониторинга ИБ АС	8	3	3	3/1,5И	4	Подбор, описание, экспертная оценка сайтов Интернет	устный опрос	ПК-15, ПК-17, ПК-24, ПСК-7.3
3.2 Установка и настройка дистрибутива Kali Linux 2		3	3	3/1,5И	3,95	Установка и настройка дистрибутива Kali Linux 2.	проектные работы	ПК-15, ПК-17, ПК-24, ПСК-7.3
Итого по разделу		6	6	6/3И	7,95			
Итого за семестр		17	17/3И	17/9И	20,05		Зачёт	
4. Аудит проводных сетей								
4.1 Способы организации зеркалирования трафика.	9	2		2/1,5И	5,2	Настройка коммутатора на зеркалирование траффика на заданный узел. Зеркалирование трафика посредством ARP-инъекций	Защита проекта, устный опрос	ПК-15, ПК-17, ПК-24, ПСК-7.3
4.2 Способы обнаружения угроз по сетевой активности		3		3/1,5И	6	Конфигурирован ие патернов активности при помощи средств дистрибутива Kali Linux	Защита проекта, устный опрос	ПК-15, ПК-17, ПК-24, ПСК-7.3
Итого по разделу		5		5/3И	11,2			
5. Аудит беспроводных сетей								
5.1 Получение доступа к беспроводной сети	9	3		3/1,5И	6	Анализ радиочастот для выявления каналов занятых исследуемой бес -проводной сетью. Выполнение атаки на сеть с целью получения хедшейка.	Защита проекта, устный опрос	ПК-15, ПК-17, ПК-24, ПСК-7.3

5.2 Способы противодействия атакам на беспроводную сеть		3		3	6	Анализ активности на радиочастотах занятых беспроводной сетью	Защита проекта, устный опрос	ПК-15, ПК-17, ПК-24, ПСК-7.3
Итого по разделу		6		6/1,5И	12			
6. Аудит Web-ресурсов								
6.1 Аудит средств авторизации	9	3		3/1,5И	6	Анализ HTML кода. Проверка простейших ошибок при конфигурирован ии страницы авторизации	Защита проекта, устный опрос	ПК-15, ПК-17, ПК-24, ПСК-7.3
6.2 Защита от SQL инъекций		3		3	5,95	Применение основных типов SQL-инжекции для получения доступа данных авторизации	Защита проекта, устный опрос	
Итого по разделу		6		6/1,5И	11,95			
7. Экзамен								
7.1 Экзамен	9					Подготовка к экзамену	Экзамен	
7.2 ВКРН						Подготовка вопросов	устный опрос	
Итого по разделу								
Итого за семестр		17		17/6И	35,15		экзамен	
Итого по дисциплине		34	17/3И	34/15И	55,2		зачет, экзамен	ПК-15,ПК-17,ПК-24,ПСК-7.3

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 ре-шений, 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», 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, 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).

2. Душкин, А. В. Методологические основы построения защищенных автоматизированных систем: Монография / Душкин А.В. - Воронеж:Научная книга, 2016. - 76 с. ISBN 978-5-4446-0902-6. - Текст : электронный. - URL: https://new.znanium.com/catalog/product/923295 (дата обращения: 27.04.2020)

б) Дополнительная литература:

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

2. Барнс, К. Защита от хакеров беспроводных сетей [Электронный ресурс] / К. Барнс, Т. Боутс, Д. Лойд, Э. Уле. — Электрон. дан. — Москва : ДМК Пресс, 2005. — 480 с. — Режим доступа: https://e.lanbook.com/book/1119. — Загл. с экрана.

3. Ковалев, Д. В. Информационная безопасность: Учебное пособие / Ковалев Д.В., Богданова Е.А. - Ростов-на-Дону:Южный федеральный университет, 2016. - 74 с.: ISBN 978-5-9275-2364-1. - Текст : электронный. - URL: https://new.znanium.com/catalog/product/997105 (дата обращения: 27.04.2019)

4. Баранкова И. И. Теория информации. Кодирование [Электронный ресурс] : учеб-ное 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..

в) Методические указания:

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
MS Office Project Prof 2013(для классов)	Д-1227-18 от 08.10.2018	11.10.2021
NotePad++	свободно распространяемое ПО	бессрочно
7Zip	свободно распространяемое ПО	бессрочно
LibreOffice	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
FAR manager	свободно распространяемое ПО	бессрочно

Профессиональные базы данных и информационные справочные системы

Название курса	Ссылка
Поисковая система Академия Google (Google Scholar)	URL: https://scholar.google.ru/
Национальная информационно-аналитическая система – Российский индекс научного цитирования (РИНЦ)	URL: https://elibrary.ru/project_
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/
Федеральная служба по техническому и экспортному контролю	URL: http://www.fstec.ru/
Федеральное агентство по техническому регулированию и метрологии	URL: 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.
Аудитории для самостоятельной работы
Персональные компьютеры с установленным ПО.

ПРИЛОЖЕНИЕ 1

По дисциплине «Методы мониторинга информационной безопасности автоматизированных систем» предусмотрена аудиторная и внеаудиторная самостоятельная работа обучающихся.

Аудиторная самостоятельная работа обучающихся предполагает решение контрольных задач на практических занятиях.

Аудиторная самостоятельная работа обучающихся на практических 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 1-6

Из имеющихся сетевых устройств сконфигурировать локальную сеть с заданными параметрами безопасности.

Ранжировать права доступа пользователей сети

Выполнить настройку АРМ для проведения мониторинга сетевой активности

При помощи Wireshark выполнить запись дампов пакетов данных полученных при зеркалировании трафика.

Выполнить сканирование радиочастот стандарта 802.11

Определить исследуемую сеть и выполнить ее анализ.

При помощи утилиты nmap выполнить сканирование заданного узла.

Приложение 2

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

Структурный элемент компетенции	Планируемые результаты обучения	Оценочные средства
ПК-15. Способностью участвовать в проведении экспериментально-исследовательских работ при сертификации средств защиты информации автоматизированных систем		
Знать	- способы организации автоматизированных систем; - подходы к проведению сертификации средств защиты информационной безопасности;	1. Децентрализованные автоматизированные системы. 2. Гомогенные и гетерогенные автоматизированные системы. 3. Система сертификации ФСТЭК России. 4. Порядок проведения сертификации средства защиты информации 5. Сертификационные испытания средства защиты информации
Уметь	- составлять регламент испытаний средств защиты информации автоматизированных систем	По заявленным характеристикам определить является ли средство подлежащим сертификации и определить перечень требуемых испытаний.
Владеть	- навыками применения специализированного ПО для проведения мероприятий при сертификации средств защиты информации автоматизированных систем;	При помощи утилиты aircrack-ng выполнить анализ радиочастот в диапазоне 2.4 гГц. Определить количество беспроводных сетей и количество участников этих сетей. При помощи Metasploit провести аудит безопасности страница авторизации роутера.
ПК-17. Способностью проводить инструментальный мониторинг защищенности информации в автоматизированной системе и выявлять каналы утечки информации		
Знать	- перечень инструментов для проведения мониторинга защищенности информации;	1. Режимы сканирования сетей. 2. Способы определения операционной системы на исследуемом узле. 3. Инструменты для проведения MITM атаки 4. Инструменты для проведения bruteforce.
Уметь	- применять технические средства для проведения мониторинга беспроводных сетей; - применять технические средства для проведения мониторинга проводных сетей построенных на основе неуправляемых коммутаторов;	Определить протокол, используемый для авторизации участников сети. Выполнить атаку Pixie Dust. Определить причины по которым атака прошла успешно. Предложить меры по увеличению защищенности устройства. Выполнить атаку на роутер с авторизацией по протоколу WPA2. Определить причины по которым атака прошла успешно. Предложить меры по увеличению защищенности устройства.

Владеть	- навыками работы с специализированным программным обеспечением для проведения мониторинга защищенности информации в автоматизированной системе;	Провести комплексный тест выбранного узла при помощи инструментов дистрибутива Kali Linux 2.
ПК-24. Способностью обеспечить эффективное применение информационно-технологических ресурсов автоматизированной системы с учетом требований информационной безопасности		
Знать	- методы повышения уровня безопасности за счет настройки прав доступа к ресурсам автоматизированной системы;	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 узлы автоматизированной системы, не обеспечивающие требуемый уровень информационной безопасности;	1. На виртуальной машине по управление ОС Linux настроить iptable. 2. Настроить шаблон по которому весь трафик с заданного IP проходящий через порт 23 будет записан в файл. 3. При помощи утилиты Metasploit выполнить анализ узлов сети.
Владеть	- навыками определения возможных векторов атаки на автоматизированную систему;	Проанализировать конфигурацию узла автоматизированной системы и определить какие параметры конфигурации узла снижают его защищенность.
ПСК-7.3. Способностью проводить аудит защищенности информационно-технологических ресурсов распределенных информационных систем		

Знать	- способы получения информации о внутренней структуре исследуемой распределенной системе; -наиболее распространённые точки для несанкционированного входа в распределенную систему;	1. Получение информации о базе данных. 2. Применение функции include для проведения аудита защищённости. 3. Защита от SQL-инъекций. 4. Области применения XSS. 5. Слепая SQL-инъекция. 6. Получение доступа к таблице user SQL базы данных.
Уметь	- проводить анализ уязвимостей распределённой системы; -получать несанкционированный доступ к ресурсам распределенной системы;	При помощи утилиты Nmap провести тест заданного узла. Определить операционную систему сервера. Используемые протоколы и порты. Используя данные DNS определить связанные ресурсы. Провести их тест.
Владеть	- навыками противодействия внешним атакам на распределенную информационную сеть;	На Web сервере сконфигурировать авторизацию таким образом, чтобы сделать применение утилиты Hydra неэффективной. Разработать скрипт выполняющий проверку входной переменной для SQL – запроса. Если содержание переменной не корректно вывести соответствующее предупреждение.

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.

Экзамен по данной дисциплине проводится в компьютерном классе по экзаменационным билетам, каждый из которых включает 1 теоретический вопрос и 2 практических задания.

Показатели и критерии оценивания экзамена:

– на оценку «отлично» (5 баллов) – обучающийся демонстрирует высокий уровень сформированности компетенций, всестороннее, систематическое и глубокое знание учебного материала, свободно выполняет практические задания, свободно оперирует знаниями, умениями, применяет их в ситуациях повышенной сложности.

– на оценку «хорошо» (4 балла) – обучающийся демонстрирует средний уровень сформированности компетенций: основные знания, умения освоены, но допускаются незначительные ошибки, неточности, затруднения при аналитических операциях, переносе знаний и умений на новые, нестандартные ситуации.

– на оценку «удовлетворительно» (3 балла) – обучающийся демонстрирует пороговый уровень сформированности компетенций: в ходе контрольных мероприятий допускаются ошибки, проявляется отсутствие отдельных знаний, умений, навыков,

обучающийся испытывает значительные затруднения при оперировании знаниями и умениями при их переносе на новые ситуации.

– на оценку «неудовлетворительно» (2 балла) – обучающийся демонстрирует знания не более 20% теоретического материала, допускает существенные ошибки, не может показать интеллектуальные навыки решения простых задач.

– на оценку «неудовлетворительно» (1 балл) – обучающийся не может показать знания на уровне воспроизведения и объяснения информации, не может показать интеллектуальные навыки решения простых задач.

ПРИЛОЖЕНИЕ 3

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ВЫПОЛНЕНИЮ ПРАКТИЧЕСКИХ РАБОТ

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

Практическое 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 практических навыков решения типовых и прикладных задач.

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

Основными задачами практических занятий являются:

углубление уровня освоения общекультурных и профессиональных компетенций;

обобщение, систематизация, углубление, закрепление полученных практических знаний по конкретным темам дисциплин различных циклов;

приобретение студентами умений и навыков использования современных теоретических знаний в решении конкретных практических задач;

развитие профессионального мышления, профессиональной и познавательной мотивации.

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

Структура практического занятия включает следующие компоненты: вступительная часть; ответы на вопросы обучающихся; практическая часть; заключительное слово преподавателя. Во вступительной части объявляется тема текущего практического занятия, ставится его цели и задачи, проверяется исходный уровень готовности студентов к практическому занятию (выполнение тестов, контрольные вопросы и т.п.)

На практическом 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 практических работ

Общие правила:

1. Практические работы проводятся под наблюдением преподавателя. К выполнению практических 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 практических работ

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

Практическая работа выполняется каждым студентом самостоятельно, согласно индивидуальному заданию.

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

После выполнения каждой практической работы студент демонстрирует результат выполнения преподавателю, отвечает на вопросы. Преподаватель оценивает работу в соответствии с заданными критериями оценки практических работ.

Правила оформления результатов и оценивания практической работы

Результаты выполненной практической 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 прилагается 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:

внимательно изучить соответствующие теоретические разделы дисциплины, пользуясь материалами (лекционными, презентационными, аудио-визуальными):

предоставляемыми преподавателем на лекционных занятиях;

предоставляемыми преподавателем в рамках электронных образовательных курсов;

содержащимися в учебниках и учебных пособиях ЭБС (электронно-библиотечных систем), электронных каталогов университета и интернет-ресурсов.

Подробно разобрать типовые примеры решения задач, рассмотренные в рамках аудиторной контактной работы с преподавателем.

Применить полученные теоретические знания и практические навыки к решению индивидуальных заданий, к прохождению компьютерных тестирований.

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.