МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ "РЯЗАНСКИЙ ГОСУДАРСТВЕННЫЙ РАДИОТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ ИМЕНИ В.Ф. УТКИНА"

СОГЛАСОВАНО
Зав. выпускающей кафедры

УТВЕРЖДАЮ
Проректор по УР

А.В. Корячко

Методы и средства обнаружения вторжений в автоматизированные системы

рабочая программа дисциплины (модуля)

Закреплена за кафедрой **Информационной безопасности**
Учебный план 10.05.03_23_00.plx

Квалификация **специалист по защите информации**
Форма обучения **очная**
Общая трудоемкость **5 ЗЕТ**

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	**10 (5.2)**		Итого	
Недель	16 1/6			
Вид занятий	УП	РП	УП	РП
Лекции	48	48	48	48
Лабораторные	16	16	16	16
Практические	32	32	32	32
Иная контактная работа	0,35	0,35	0,35	0,35
Консультирование перед экзаменом и практикой	2	2	2	2
Итого ауд.	98,35	98,35	98,35	98,35
Контактная работа	98,35	98,35	98,35	98,35
Сам. работа	46	46	46	46
Часы на контроль	35,65	35,65	35,65	35,65
Итого	180	180	180	180

г. Рязань

Программу составил(и):
ст. преп., Павлунин Максим Анатольевич

Рабочая программа дисциплины

Методы и средства обнаружения вторжений в автоматизированные системы

разработана в соответствии с ФГОС ВО:

ФГОС ВО - специалитет по специальности 10.05.03 Информационная безопасность автоматизированных систем (приказ Минобрнауки России от 26.11.2020 г. № 1457)

составлена на основании учебного плана:

10.05.03 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ АВТОМАТИЗИРОВАННЫХ СИСТЕМ

утвержденного учёным советом вуза от 28.04.2023 протокол № 11.

Рабочая программа одобрена на заседании кафедры

Информационной безопасности

Протокол от 29.06.2023 г. № 12
Срок действия программы: 2023-2029 уч.г.
Зав. кафедрой Пржегорлинский Виктор Николаевич

Визирование РПД для исполнения в очередном учебном году

Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в 2024-2025 учебном году на заседании кафедры
Информационной безопасности

Протокол от __ _____ 2024 г. № __

Зав. кафедрой _____

Визирование РПД для исполнения в очередном учебном году

Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в 2025-2026 учебном году на заседании кафедры
Информационной безопасности

Протокол от __ _____ 2025 г. № __

Зав. кафедрой _____

Визирование РПД для исполнения в очередном учебном году

Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в 2026-2027 учебном году на заседании кафедры
Информационной безопасности

Протокол от __ _____ 2026 г. № __

Зав. кафедрой _____

Визирование РПД для исполнения в очередном учебном году

Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в 2027-2028 учебном году на заседании кафедры
Информационной безопасности

Протокол от __ _____ 2027 г. № __

Зав. кафедрой _____

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)	
1.1	Целью освоения Дисциплины является получение обучающимися знаний в области обнаружения действий злоумышленников при их воздействии на вычислительные сети, необходимых для решения задач обеспечения информационной безопасности в профессиональной деятельности.
1.2	Задачами Дисциплины являются:
1.3	- получение теоретических знаний о основных признаках сетевых вторжений и атак;
1.4	- получение теоретических знаний о основных системах защиты информации и ме-ханизмов, применяемых для противодействия реализации атак;
1.5	- получение теоретических знаний о основных тактиках и техниках злоумышленни-ков для реализации атак.
2. МЕСТО ДИСЦИПЛИНЫ (МОДУЛЯ) В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ	
Цикл (раздел) ОП:	Б1.В
2.1	**Требования к предварительной подготовке обучающегося:**
2.1.1	Научно-исследовательская работа
2.1.2	Производственная практика
2.1.3	Модели угроз и нарушителей безопасности информации объектов информатизации
2.2	**Дисциплины (модули) и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:**
2.2.1	Подготовка к процедуре защиты и процедура защиты выпускной квалификационной работы
2.2.2	Преддипломная практика

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)

ПК-4: Способен разрабатывать системы защиты информации автоматизированных, используемых в том числе на объектах критической информационной инфраструктуры, в отношении которых отсутствует необходимость присвоения им категории значимости

ПК-4.1. Тестирует системы защиты информации автоматизированных систем

Знать
- современные информационные технологии (операционные системы, базы данных, вычислительные сети);- способы реализации несанкционированного доступа к информации и специальных программных воздействий на информацию и ее носители в автоматизированных системах;- основные классы и виды уязвимостей программного обеспечения.

Уметь
- разрабатывать концепцию средств и систем информатизации в защищенном исполнении.

Владеть
- навыками формирования требований к средствам и системам информатизации в защищенном исполнении.

ПК-4.3. Разрабатывает эксплуатационную документацию на системы защиты информации автоматизированных систем

Знать
- уязвимости информационных систем;- методы защиты информации от утечки по техническим каналам;- программные (программно-технические) средства защиты автоматизированных систем от несанкционированного доступа к информации и специальных программных воздействий на нее.

Уметь
- проводить анализ угроз безопасности информации на объекте информатизации.

Владеть
- навыками разработки аналитического обоснования необходимости создания системы защиты информации на объекте информатизации (модели угроз безопасности информации).

ПК-5: Способен разрабатывать системы защиты информации автоматизированных систем, используемых в том числе на объектах критической информационной инфраструктуры, в отношении которых отсутствует необходимость присвоения им категории значимости

ПК-5.1. Обосновывает необходимость защиты информации в автоматизированной системе

Знать
- современные информационные технологии и средства защиты информации;- факторы, воздействующие на защищаемую информацию в автоматизированных системах (АС).

Уметь
- определять класс защищенности автоматизируемой системы.

Владеть
- навыками формирования требований к защите информации в АС.

ПК-5.3. Разрабатывает архитектуру системы защиты информации автоматизированной системы

Знать
- факторы, воздействующие на защищаемую информацию в АС;- методы и способы, обследования условий функционирования АС.

Уметь
- определять угрозы безопасности информации в объектах информатизации.

Владеть
- навыками формирования перечня угроз безопасности информации, обрабатываемой в АС.

В результате освоения дисциплины (модуля) обучающийся должен

3.1	**Знать:**
3.1.1	- современные информационные технологии (операционные системы, базы данных, вычислительные сети);
3.1.2	- способы реализации несанкционированного доступа к информации и специальных программных воздействий на информацию и ее носители в автоматизированных системах;
3.1.3	- основные классы и виды уязвимостей программного обеспечения.
3.1.4	- уязвимости информационных систем;
3.1.5	- методы защиты информации от утечки по техническим каналам;
3.1.6	- программные (программно-технические) средства защиты автоматизированных систем от несанкционированного доступа к информации и специальных программных воздействий на нее.
3.1.7	- современные информационные технологии и средства защиты информации;
3.1.8	- факторы, воздействующие на защищаемую информацию в автоматизированных системах (АС).
3.1.9	- факторы, воздействующие на защищаемую информацию в АС;
3.1.10	- методы и способы, обследования условий функционирования АС.
3.1.11	
3.2	**Уметь:**
3.2.1	- разрабатывать концепцию средств и систем информатизации в защищенном исполнении.
3.2.2	- проводить анализ угроз безопасности информации на объекте информатизации.
3.2.3	- определять класс защищенности автоматизируемой системы.
3.2.4	- определять угрозы безопасности информации в объектах информатизации.
3.3	**Владеть:**
3.3.1	- навыками формирования требований к средствам и системам информатизации в защищенном исполнении.
3.3.2	- навыками разработки аналитического обоснования необходимости создания системы защиты информации на объекте информатизации (модели угроз безопасности информации).
3.3.3	- навыками формирования требований к защите информации в АС.
3.3.4	- навыками формирования перечня угроз безопасности информации, обрабатываемой в АС.

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Код занятия	Наименование разделов и тем /вид занятия/	Семестр / Курс	Часов	Компетен-ции	Литература	Форма контроля
	Раздел 1. Введение в дисциплину					
1.1	Введение в дисциплину. /Тема/	10	0			

1.2	Цель изучения, задачи и место дисциплины в структуре основной профессиональной образовательной программы подготовки специалиста по защите информации. Планируемые результаты обучения по дисциплине. Виды и объёмы учебной работы и содержание дисциплины. /Лек/	10	2	ПК-4.1-З ПК-4.1-У ПК-4.1-В ПК-5.1-З ПК-5.1-У ПК-5.1-В ПК-5.3-З ПК-5.3-У ПК-5.3-В ПК-4.3-З ПК-4.3-У ПК-4.3-В	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Э1 Э2	Конспект лекций.
1.3	Изучение конспекта лекций. /Ср/	10	1	ПК-4.1-З ПК-4.1-У ПК-4.1-В ПК-5.1-З ПК-5.1-У ПК-5.1-В ПК-5.3-З ПК-5.3-У ПК-5.3-В ПК-4.3-З ПК-4.3-У ПК-4.3-В	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3	подготовка конспекта по вопросам темы. Краткий опрос по теме на консультации к экзамену.
	Раздел 2. Основы компьютерных сетей					
2.1	Основы компьютерных сетей /Тема/	10	0			
2.2	Введение в основы компьютерных сетей. Основные протоколы прикладного уровня стека TCP/IP. Основные протоколы транспортного, сетевого и канального уровня стека TCP/IP. Сетевое оборудование, принци1пы работы. Vlan и Vpn, принципы построения сетей. Передача пакетов на сетевом и канальном уровнях. /Лек/	10	5	ПК-4.1-З ПК-4.1-У ПК-4.1-В ПК-5.1-З ПК-5.1-У ПК-5.1-В ПК-5.3-З ПК-5.3-У ПК-5.3-В ПК-4.3-З ПК-4.3-У ПК-4.3-В	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Э1 Э2	Конспект лекций.
2.3	Разработка схемы сети защищаемой инфраструктуры /Пр/	10	4	ПК-4.1-З ПК-4.1-У ПК-4.1-В ПК-5.1-У ПК-5.1-В ПК-5.3-З ПК-5.3-У ПК-5.3-В ПК-4.3-З ПК-4.3-У ПК-4.3-В ПК-5.1-З	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Э1 Э2	Устный опрос по теме.Решение задач.Проверка домашнего задания.
2.4	Изучение конспекта лекцийПодготовка к практическому занятиюПодготовка к экзамену /Ср/	10	3	ПК-4.1-З ПК-4.1-У ПК-4.1-В ПК-5.1-У ПК-5.1-В ПК-5.3-З ПК-5.3-У ПК-5.3-В ПК-4.3-З ПК-4.3-У ПК-4.3-В ПК-5.1-З	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Э1 Э2	подготовка конспекта по вопросам темы. Краткий опрос по теме на консультации к экзамену.
	Раздел 3. Мониторинг событий информационной безопасности					

3.1	Мониторинг событий информационной безопасности /Тема/	10	0			
3.2	Виды систем защиты информации. Принципы работы и использования систем защиты информации: Host IDS, Network IDS/IPS, Antivirus, Data Loss Prevention, Web Application Firewall, Proxy, Firewall, Vulnerability Scanner, Sandbox, SIEM. Принципы вы-явления атак на основе модели Cyber-Kill Chain. События ИБ и их анализ для выявления атак. Инциденты ИБ. Способы реагирования на инциденты ИБ. /Лек/	10	5	ПК-4.1-З ПК-4.1-У ПК-4.1-В ПК-5.1-У ПК-5.1-В ПК-5.3-З ПК-5.3-У ПК-5.3-В ПК-4.3-З ПК-4.3-У ПК-4.3-В ПК-5.1-З	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Э1 Э2	Конспект лекций.
3.3	Расстановка систем защиты информации для обеспечения ИБ в защищаемой инфраструктуре /Пр/	10	4	ПК-4.1-З ПК-4.1-У ПК-4.1-В ПК-5.1-З ПК-5.1-У ПК-5.1-В ПК-5.3-З ПК-5.3-У ПК-5.3-В ПК-4.3-З ПК-4.3-У ПК-4.3-В	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Э1 Э2	Устный опрос по теме.Решение задач.Проверка домашнего задания.
3.4	Изучение конспекта лекцийПодготовка к практическому занятиюПодготовка к экзамену /Ср/	10	5	ПК-4.1-З ПК-4.1-У ПК-4.1-В ПК-5.1-З ПК-5.1-У ПК-5.1-В ПК-5.3-У ПК-5.3-В ПК-4.3-З ПК-4.3-У ПК-4.3-В ПК-5.3-З	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Э1 Э2	подготовка конспекта по вопросам темы. Краткий опрос по теме на консультации к экзамену.
	Раздел 4. Технические средства обнаружения вторжений					
4.1	Технические средства обнаружения вторжений /Тема/	10	0			
4.2	Архитектура и общее описание стека технологий ELK. Изучение агентов для сбора информации с ОС Windows, Linux. Логирование ОС Windows, политики аудита.Изучение возможностей Sysmon. Изучение возможностей системы Network IDS Suricata. Принципы работы с консолью Kibana для поиска и анализа событий ИБ. Разра-ботка запросов на языке Query DSL. Изучение принципов разработки панелей визуализа-ции событий. Изучение общих принципов разворачивания инструментов для мониторинга и диагностики неисправностей. /Лек/	10	4	ПК-4.1-З ПК-4.1-У ПК-4.1-В ПК-5.1-З ПК-5.1-У ПК-5.1-В ПК-5.3-З ПК-5.3-У ПК-5.3-В ПК-4.3-З ПК-4.3-У ПК-4.3-В	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Э1 Э2	Конспект лекций.

4.3	Знакомство со стендом для мониторинга событий ИБ /Пр/	10	5	ПК-4.1-З ПК-4.1-У ПК-4.1-В ПК-5.1-З ПК-5.1-У ПК-5.1-В ПК-5.3-З ПК-5.3-У ПК-5.3-В ПК-4.3-З ПК-4.3-У ПК-4.3-В	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Э1 Э2	Устный опрос по теме.Решение задач.Проверка домашнего задания.
4.4	Изучение конспекта лекцийПодготовка к практическому занятиюПодготовка к экзамену /Ср/	10	4	ПК-4.1-З ПК-4.1-У ПК-4.1-В ПК-5.1-З ПК-5.1-У ПК-5.1-В ПК-5.3-З ПК-5.3-У ПК-5.3-В ПК-4.3-З ПК-4.3-У ПК-4.3-В	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Э1 Э2	подготовка конспекта по вопросам темы. Краткий опрос по теме на консультации к экзамену.
	Раздел 5. Стадия атаки «Разведка»					
5.1	Стадия атаки «Разведка» /Тема/	10	0			
5.2	Изучение тактик и техник злоумышленника на стадии «Разведка». Изучение воз-можностей инструмента Nmap. Изучение техник и инструментов энумерации информа-ции. Изучение техник и инструментов, используемых при Brute-force атаках. /Лек/	10	3	ПК-4.1-З ПК-4.1-У ПК-4.1-В ПК-5.1-З ПК-5.1-У ПК-5.1-В ПК-5.3-З ПК-5.3-У ПК-5.3-В ПК-4.3-З ПК-4.3-У ПК-4.3-В	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Э1 Э2	конспект лекций
5.3	Методы выявления атак на стадии «Разведка». /Пр/	10	5	ПК-4.1-З ПК-4.1-У ПК-4.1-В ПК-5.1-З ПК-5.1-У ПК-5.1-В ПК-5.3-З ПК-5.3-У ПК-5.3-В ПК-4.3-З ПК-4.3-У ПК-4.3-В	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Э1 Э2	Устный опрос по теме.Решение задач.Проверка домашнего задания.
5.4	Изучение конспекта лекций.Подготовка к практическому занятиюПодготовка к экзамену /Ср/	10	4	ПК-4.1-З ПК-4.1-У ПК-4.1-В ПК-5.1-З ПК-5.1-У ПК-5.1-В ПК-5.3-З ПК-5.3-У ПК-5.3-В ПК-4.3-З ПК-4.3-У ПК-4.3-В	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Э1 Э2	подготовка конспекта по вопросам темы. Краткий опрос по теме на консультации к экзамену.
	Раздел 6. Стадия атаки «Доставка»					

6.1	Стадия атаки «Доставка» /Тема/	10	0			
6.2	Способы доставки ВПО. Виды исполняемых файлов. Каналы доставки ВПО. /Лек/	10	5	ПК-4.1-З ПК-4.1-У ПК-4.1-В ПК-5.1-З ПК-5.1-У ПК-5.1-В ПК-5.3-З ПК-5.3-У ПК-5.3-В ПК-4.3-З ПК-4.3-У ПК-4.3-В	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Э1 Э2	Конспект лекций.
6.3	Методы выявления атак на стадии «Доставка» /Пр/	10	4	ПК-4.1-З ПК-4.1-У ПК-4.1-В ПК-5.1-З ПК-5.1-У ПК-5.1-В ПК-5.3-З ПК-5.3-У ПК-5.3-В ПК-4.3-З ПК-4.3-У ПК-4.3-В	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Э1 Э2	Устный опрос по теме.Решение задач.Проверка домашнего задания.
6.4	Изучение конспекта лекцийПодготовка к практическому занятиюПодготовка к экзамену /Ср/	10	6	ПК-4.1-З ПК-4.1-У ПК-4.1-В ПК-5.1-З ПК-5.1-У ПК-5.1-В ПК-5.3-З ПК-5.3-У ПК-5.3-В ПК-4.3-З ПК-4.3-У ПК-4.3-В	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Э1 Э2	подготовка конспекта по вопросам темы. Краткий опрос по теме на консультации к экзамену.
	Раздел 7. Стадия атаки «Эксплуатация»					
7.1	Стадия атаки «Эксплуатация» /Тема/	10	0			
7.2	Виды эксплойтов. Тактики и техники злоумышленников при эксплуатации уязвимостей. Изучение Metasploit Framework, MSFvenom, MSF Multi handler. Способы формирования полезной нагрузки. Принципы взаимодействия злоумышленников с скомпрометированными системами. /Лек/	10	5	ПК-4.1-З ПК-4.1-У ПК-4.1-В ПК-5.1-З ПК-5.1-У ПК-5.1-В ПК-5.3-З ПК-5.3-У ПК-5.3-В ПК-4.3-З ПК-4.3-У ПК-4.3-В	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Э1 Э2	Конспект лекций.
7.3	Методы выявления атак на стадии «Эксплуатация». /Пр/	10	5	ПК-4.1-З ПК-4.1-У ПК-4.1-В ПК-5.1-З ПК-5.1-У ПК-5.3-З ПК-5.3-В ПК-4.3-З ПК-4.3-У ПК-4.3-В ПК-5.1-В ПК-5.3-У	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Э1 Э2	Устный опрос по теме.Решение задач.Проверка домашнего задания.

7.4	Изучение конспекта лекцийПодготовка к практическому занятиюПодготовка к экзамену /Ср/	10	3	ПК-4.1-З ПК-4.1-У ПК-4.1-В ПК-5.1-З ПК-5.1-У ПК-5.3-З ПК-5.3-В ПК-4.3-З ПК-4.3-У ПК-4.3-В ПК-5.1-В ПК-5.3-У	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Э1 Э2	подготовка конспекта по вопросам темы. Краткий опрос по теме на консультации к экзамену.
	Раздел 8. Методы автоматизации выявления инцидентов ИБ					
8.1	Методы автоматизации выявления инцидентов ИБ /Тема/	10	0			
8.2	Изучение принципов автоматизации выявления инцидентов ИБ, применяемых в SIEM системах. Разработка правил автоматизированного выявления на примере подсис-темы «Сигнал». /Лек/	10	5	ПК-4.1-З ПК-4.1-У ПК-4.1-В ПК-5.1-З ПК-5.1-У ПК-5.1-В ПК-5.3-З ПК-5.3-У ПК-5.3-В ПК-4.3-З ПК-4.3-У ПК-4.3-В	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Э1 Э2	Конспект лекций.
8.3	Разработка правил автоматизиро-ванного выявления инцидентов ИБ /Пр/	10	5	ПК-4.1-З ПК-4.1-У ПК-4.1-В ПК-5.1-З ПК-5.1-У ПК-5.1-В ПК-5.3-З ПК-5.3-У ПК-5.3-В ПК-4.3-З ПК-4.3-У ПК-4.3-В	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Э1 Э2	Устный опрос по теме.Решение задач.Проверка домашнего задания.
8.4	Изучение конспекта лекцийПодготовка к практическому занятиюПодготовка к экзамену /Ср/	10	6	ПК-4.1-З ПК-4.1-У ПК-4.1-В ПК-5.1-З ПК-5.1-У ПК-5.1-В ПК-5.3-З ПК-5.3-У ПК-5.3-В ПК-4.3-З ПК-4.3-У ПК-4.3-В	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Э1 Э2	подготовка конспекта по вопросам темы. Краткий опрос по теме на консультации к экзамену.
	Раздел 9. Стадии атаки «Заражение, Закрепление, Уничтожение следов»					
9.1	Стадии атаки «Заражение, Закрепление, Уничтожение следов» /Тема/	10	0			

9.2	Описание тактик и техник злоумышленников на стадиях «Заражение, Закрепление, Уничтожение следов». Изучение основных методов и инструментов пост-эксплуатации в ОС Windows. Принципы обхода UAC и повышения привилегий. Принципы миграции полезной нагрузки в процессы ОС Windows. Способы закрепления злоумышленников на скомпрометированной системе. Изучение принципов Pivoting. Способы создания нелеги-тимных пользователей в ОС. Способы уничтожения следов злоумышленником. /Лек/	10	7	ПК-4.1-З ПК-4.1-У ПК-4.1-В ПК-5.1-З ПК-5.1-У ПК-5.1-В ПК-5.3-З ПК-5.3-У ПК-5.3-В ПК-4.3-З ПК-4.3-У ПК-4.3-В	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Э1 Э2	Конспект лекций.
9.3	Методы выявления атак на стадиях «Заражение, Закрепление, Уничтожение следов» /Лаб/	10	8	ПК-4.1-З ПК-4.1-У ПК-4.1-В ПК-5.1-З ПК-5.1-У ПК-5.1-В ПК-5.3-З ПК-5.3-У ПК-4.3-З ПК-4.3-У ПК-4.3-В ПК-5.3-В	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Э1 Э2	Отчет по ЛР, Защита ЛР.
9.4	Изучение конспекта лекцийПодготовка к практическому занятиюПодготовка к экзамену /Ср/	10	6	ПК-4.1-З ПК-4.1-У ПК-4.1-В ПК-5.1-З ПК-5.1-У ПК-5.1-В ПК-5.3-З ПК-5.3-У ПК-4.3-З ПК-4.3-У ПК-4.3-В ПК-5.3-В	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Э1 Э2	подготовка конспекта по вопросам темы. Краткий опрос по теме на консультации к экзамену
	Раздел 10. Техники кражи учетных данных пользователей в ОС Windows					
10.1	Техники кражи учетных данных пользователей в ОС Windows /Тема/	10	0			
10.2	Общие принципы хранения учетных данных в ОС Windows. Изучение принципов аутентификации по протоколам NTLM, Kerberos. Изучение техник и инструментов зло-умышленников для извлечения учетных данных пользователей. /Лек/	10	7	ПК-4.1-З ПК-4.1-У ПК-4.1-В ПК-5.1-З ПК-5.1-У ПК-5.1-В ПК-5.3-З ПК-5.3-У ПК-5.3-В ПК-4.3-З ПК-4.3-У ПК-4.3-В		Конспект лекций.
10.3	Методы выявления техник кражи учетных данных пользователей /Лаб/	10	8	ПК-4.1-З ПК-4.1-У ПК-4.1-В ПК-5.1-З ПК-5.1-У ПК-5.1-В ПК-5.3-З ПК-5.3-У ПК-5.3-В ПК-4.3-З ПК-4.3-У ПК-4.3-В		Отчет по ЛР, Защита ЛР.

10.4	Изучение конспекта лекцийПодготовка к практическому занятиюПодготовка к экзамену /Ср/	10	8	ПК-4.1-З ПК-4.1-У ПК-4.1-В ПК-5.1-З ПК-5.1-У ПК-5.1-В ПК-5.3-З ПК-5.3-У ПК-5.3-В ПК-4.3-З ПК-4.3-У ПК-4.3-В		подготовка конспекта по вопросам темы. Краткий опрос по теме на консультации к экзамену
	Раздел 11. Контроль, подготовка к экзамену					
11.1	Контроль, подготовка к экзамену /Тема/	10	0			
11.2	Подготовка к экзамену /Экзамен/	10	35,65	ПК-4.1-З ПК-4.1-У ПК-4.1-В ПК-5.1-З ПК-5.1-У ПК-5.1-В ПК-5.3-З ПК-5.3-У ПК-5.3-В ПК-4.3-З ПК-4.3-У ПК-4.3-В	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Э1 Э2	Изучение вопросов.
	Раздел 12. Иная контактная работа					
12.1	Иная контактная работа /Тема/	10	0			
12.2	Прием экзамена /ИКР/	10	0,35	ПК-4.1-З ПК-4.1-У ПК-4.1-В ПК-5.1-З ПК-5.1-У ПК-5.1-В ПК-5.3-З ПК-5.3-У ПК-5.3-В ПК-4.3-З ПК-4.3-У ПК-4.3-В	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Э1 Э2	Ответы на Контрольные вопросыОтветы на дополнительные вопросы.
	Раздел 13. Консультации					
13.1	Консультации /Тема/	10	0			
13.2	Консультирование перед экзаменом и практикой /Кнс/	10	2	ПК-4.1-З ПК-4.1-У ПК-4.1-В ПК-5.1-З ПК-5.1-У ПК-5.1-В ПК-5.3-З ПК-5.3-У ПК-5.3-В ПК-4.3-З ПК-4.3-У ПК-4.3-В	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Э1 Э2	Вопросы к экзамену.Решение типовых задач.Ответы на вопросы.

5. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

Оценочные материалы приведены в приложении к рабочей программе дисциплины "Методы и средства обнаружения вторжений в автоматизированные системы" (см. документ "ОМ)

6. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

6.1. Рекомендуемая литература

6.1.1. Основная литература

№	Авторы, составители	Заглавие	Издательство, год	Количество/ название ЭБС
Л1.1	Котельников Е. В.	Введение во внутреннее устройство Windows : учебное пособие	Москва, Саратов: Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020, 260 с.	978-5-4497-0315-6, http://www.iprbookshop.ru/89432.html
Л1.2	Котельников Е. В.	Введение во внутреннее устройство Windows	Москва: ИНТУИТ, 2016, 260 с.	, https://e.lanbook.com/book/100722
Л1.3	Котельников, Е. В.	Введение во внутреннее устройство Windows : учебное пособие	Москва, Саратов: Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020, 260 с.	978-5-4497-0315-6, https://www.iprbookshop.ru/89432.html

6.1.2. Дополнительная литература

№	Авторы, составители	Заглавие	Издательство, год	Количество/ название ЭБС
Л2.1	Федин Ф. О., Офицеров В. П., Федин Ф. Ф.	Информационная безопасность : учебное пособие	Москва: Московский городской педагогический университет, 2011, 260 с.	2227-8397, http://www.iprbookshop.ru/26486.html
Л2.2	Бабин С.А.	Лаборатория хакера	Санкт-Петербург: БХВ-Петербург, 2016, 240с.	978-5-9775-3535-9, 20
Л2.3	Минзов А. С., Бобылева С. В., Осипов П. А., Попов А. А.	Информационная безопасность и защита информации : практикум	Дубна: Государственный университет «Дубна», 2020, 85 с.	978-5-89847-608-3, https://e.lanbook.com/book/154490

6.2. Перечень ресурсов информационно-телекоммуникационной сети "Интернет"

Э1	MITRE ATT&CK
Э2	Elasticsearch

6.3 Перечень программного обеспечения и информационных справочных систем

6.3.1 Перечень лицензионного и свободно распространяемого программного обеспечения, в том числе отечественного производства

Наименование	Описание

Adobe Acrobat Reader	Свободное ПО
VirtualBox	Свободное ПО
6.3.2 Перечень информационных справочных систем	
7. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)	
1	268 учебно-административный корпус. компьютерный класс для проведения учебных занятий Специализированная мебель (20 компьютерных столов), 20 персональных компьютеров. Возможность подключения к сети Интернет и обеспечением доступа в электронную информационно-образовательную среду РГРТУ.
2	270 учебно-административный корпус. учебная аудитория для проведения учебных занятий. Специализированная мебель (42 посадочных места), магнитно-маркерная доска. Мультимедиа проектор, 1 экран. Рабочее место (2 стола), 1 персональный компьютер, 1 ноутбук.
8. МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)	
Методическое обеспечение дисциплины приведено в приложении к рабочей программе дисциплины (см. документ "Методы и средства обнаружения вторжений в автоматизированные системы")	

Оператор ЭДО ООО "Компания "Тензор"

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ

ПОДПИСАНО ЗАВЕДУЮЩИМ КАФЕДРЫ	**ФГБОУ ВО "РГРТУ", РГРТУ,** Пржегорлинский Виктор Николаевич, Преподаватель	**29.09.23** 17:20 (MSK)	Простая подпись
ПОДПИСАНО ЗАВЕДУЮЩИМ ВЫПУСКАЮЩЕЙ КАФЕДРЫ	**ФГБОУ ВО "РГРТУ", РГРТУ,** Пржегорлинский Виктор Николаевич, Преподаватель	**29.09.23** 17:20 (MSK)	Простая подпись
ПОДПИСАНО ПРОРЕКТОРОМ ПО УР	**ФГБОУ ВО "РГРТУ", РГРТУ,** Корячко Алексей Вячеславович, Проректор по учебной работе	**29.09.23** 17:21 (MSK)	Простая подпись