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

Защита в операционных системах

рабочая программа дисциплины (модуля)

Закреплена за кафедрой **Информационная безопасность**

Учебный план 10.05.01 _20_00.plx
10.05.01 КОМПЬЮТЕРНАЯ БЕЗОПАСНОСТЬ

Квалификация **специалист по защите информации**

Форма обучения **очная**

Общая трудоемкость **6 ЗЕТ**

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	**7 (4.1)**		**8 (4.2)**		Итого	
Недель	16		16			
Вид занятий	УП	РП	УП	РП	УП	РП
Лекции	24	24	32	32	56	56
Лабораторные	24	24	16	16	40	40
Практические			16	16	16	16
Иная контактная работа	0,25	0,25	0,35	0,35	0,6	0,6
Консультирование перед экзаменом и практикой			2	2	2	2
Итого ауд.	48,25	48,25	66,35	66,35	114,6	114,6
Контактная работа	48,25	48,25	66,35	66,35	114,6	114,6
Сам. работа	51	51	6	6	57	57
Часы на контроль	8,75	8,75	35,65	35,65	44,4	44,4
Итого	108	108	108	108	216	216

г. Рязань

Программу составил(и):
к.т.н., доц., Кузьмин Юрий Михайлович

Рабочая программа дисциплины
Защита в операционных системах
разработана в соответствии с ФГОС ВО:
ФГОС ВО - специалитет по специальности 10.05.01 Компьютерная безопасность (приказ Минобрнауки России от 26.11.2020 г. № 1459)
составлена на основании учебного плана:
10.05.01 КОМПЬЮТЕРНАЯ БЕЗОПАСНОСТЬ
утвержденного учёным советом вуза от 28.01.2022 протокол № 6.

Рабочая программа одобрена на заседании кафедры
Информационная безопасность
Протокол от 29.06.2022 г. № 12
Срок действия программы: 2020-2026 уч.г.
Зав. кафедрой Пржегорлинский Виктор Николаевич

Визирование РПД для исполнения в очередном учебном году

Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в 2023-2024 учебном году на заседании кафедры
Информационная безопасность

Протокол от __ _____ 2023 г. № __

Зав. кафедрой _____

Визирование РПД для исполнения в очередном учебном году

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

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
Информационная безопасность

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
Информационная безопасность

Протокол от __ _____ 2026 г. № __

Зав. кафедрой _____

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)	
1.1	Целью дисциплины «Защита в операционных системах» является получение обучающимися знаний, формирование у них умений и навыков, необходимых при использовании и настройке защищенных операционных систем и систем на их основе для решения задач в профессиональной деятельности.
1.2	Задачами дисциплины являются:
1.3	− получение знаний о защитных механизмах и средствах обеспечения безопасности операционных систем, средствах и методах аутентификации пользователей в защищенных операционных системах, средствах и методах управления доступом в защищенных операционных системах, средствах и методах реализации политики аудита в защищенных операционных системах, средствах и методах управления процессами в защищенных операционных системах, средствах и методах антивирусной защиты в защищенных операционных системах, средствах и методах интеграции защищенных операционных систем в защищенную сеть;
1.4	− приобретение умения применять защитные механизмы и средства обеспечения безопасности защищенных операционных систем; определять и классифицировать угрозы информационной безопасности операционных систем; формулировать, настраивать и реализовывать политику безопасности защищенных операционных систем;
1.5	− приобретение практических навыков применения защитных механизмов и средств обеспечения информационной безопасности защищенных операционных систем, определения и классификации угроз информационной безопасности операционных систем, формулирования требований информационной безопасности к защищенным операционным системам, настройки защищенных операционных систем в соответствии с требованиями политики безопасности, оценки эффективности реализации требований информационной безопасности в защищенных операционных системах и системах на их основе.
2. МЕСТО ДИСЦИПЛИНЫ (МОДУЛЯ) В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ	
Цикл (раздел) ОП:	Б1.О
2.1	**Требования к предварительной подготовке обучающегося:**
2.1.1	Операционные системы
2.1.2	Основы радиотехники
2.2	**Дисциплины (модули) и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:**
2.2.1	Сети и системы передачи информации
2.2.2	Производственная практика
2.2.3	Теория информации
2.2.4	Подготовка к процедуре защиты и процедура защиты выпускной квалификационной работы
2.2.5	Преддипломная практика

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

ОПК-9: Способен решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития методов защиты информации в операционных системах, компьютерных сетях и системах управления базами данных, а также методов и средств защиты информации от утечки по техническим каналам, сетей и систем передачи информации;

ОПК-9.1. Формулирует и настраивает политику безопасности основных операционных систем

Знать
Формулировки и настройки правил политики безопасности операционных систем
Уметь
Формулировать и настраивать правила политики безопасности операционных систем
Владеть
Навыками формулировки и настройки правил политики безопасности операционных систем

ОПК-9.2. Использует защитные механизмы и средства обеспечения безопасности операционных систем для решения задач профессиональной деятельности

Знать
основные защитные механизмы и средства обеспечения безопасности операционных систем для решения задач профессиональной деятельности
Уметь
использовать защитные механизмы и средства обеспечения безопасности операционных систем для решения задач профессиональной деятельности
Владеть
навыками использования защитных механизмов и средств обеспечения безопасности операционных систем для решения задач профессиональной деятельности

ОПК-12: Способен администрировать операционные системы и выполнять работы по восстановлению работоспособности прикладного и системного программного обеспечения;
ОПК-12.2. Использует в работе современные операционные системы и выполняет основные действия по системному администрированию
Знать Требования и правила установки, обслуживания и восстановления работоспособности компонентов общего и специального программного обеспечения **Уметь** Выполнять установку, обслуживание и восстановление работоспособности компонентов общего и специального программного обеспечения **Владеть** Навыками установки, обслуживания и восстановления работоспособности компонентов общего и специального программного обеспечения
ОПК-12.3. Выполняет установку и обслуживание современного общего и специального программного обеспечения по восстановлению работоспособности прикладного и системного программного обеспечения
Знать Характеристики встроенных средств защиты информации операционных систем и прикладных программ, их настраивает **Уметь** Оценивать характеристики встроенных средств защиты информации операционных систем и прикладных программ, использовать и настраивать их **Владеть** Навыками оценки характеристик встроенных средств защиты информации операционных систем и прикладных программ, использоваия и настройки их
ОПК-12.5. Оценивает характеристики основных типов программно- аппаратных средств защиты операционных систем, прикладных программ и данных
Знать **Уметь** **Владеть**

В результате освоения дисциплины (модуля) обучающийся должен

3.1	**Знать:**
3.1.1	Формулировки и настройки правил политики безопасности операционных систем
3.1.2	Основные защитные механизмы и средства обеспечения безопасности операционных систем для решения задач профессиональной деятельности
3.1.3	Требования и правила установки, обслуживания и восстановления работоспособности компонентов общего и специального программного обеспечения
3.1.4	Характеристики встроенных средств защиты информации операционных систем и прикладных программ, их настраивает
3.2	**Уметь:**
3.2.1	Формулировать и настраивать правила политики безопасности операционных систем
3.2.2	Использовать защитные механизмы и средства обеспечения безопасности операционных систем для решения задач профессиональной деятельности
3.2.3	Выполнять установку, обслуживание и восстановление работоспособности компонентов общего и специального программного обеспечения
3.2.4	Оценивать характеристики встроенных средств защиты информации операционных систем и прикладных программ, использовать и настраивать их
3.3	**Владеть:**
3.3.1	Навыками формулировки и настройки правил политики безопасности операционных систем
3.3.2	навыками использования защитных механизмов и средств обеспечения безопасности операционных систем для решения задач профессиональной деятельности
3.3.3	Навыками установки, обслуживания и восстановления работоспособности компонентов общего и специального программного обеспечения
3.3.4	Навыками оценки характеристик встроенных средств защиты информации операционных систем и прикладных программ, использоваия и настройки их

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Код занятия	Наименование разделов и тем /вид занятия/	Семестр / Курс	Часов	Компетен-ции	Литература	Форма контроля

	Раздел 1. Общие вопросы безопасности ОС					
1.1	Общие вопросы безопасности ОС /Тема/	7	0			
1.2	Угрозы безопасности ОС. Взаимосвязь понятий защищенность, уязвимость, угроза, атака, ущерб. Угрозы безопасности ОС: классификация угроз безопасности, типичные атаки на ОС. Подходы к построению защищенных ОС. Административные меры защиты. Адекватная политика безопасности. Стандарты защищенности и адекватная политика безопасности. Примеры защищенных ОС. Типовая архитектура подсистемы защиты операционной системы. Основные функции подсистемы защиты операционной системы. Разграничение доступа к объектам операционной системы: правила разграничения доступа, разрешительная система доступа. Идентификация, аутентификация и авторизация субъектов доступа: соотношение идентификации, аутентификации и авторизации, способы и виды аутентификации, идентификация и аутентификация с помощью имени и пароля (методы подбора пароля, защита от компрометации пароля). Идентификация и аутентификация с помощью внешних носителей ключевой информации. Идентификация и аутентификация с помощью биометрических характеристик пользователей. Аудит: цели аудита, требования к аудиту, политика аудита. Технология защищенного канала. Межсетевое экранирование. /Лек/	7	4	ОПК-9.2-З ОПК-12.3-З	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2Л3.1 Л3.2 Э1 Э2 Э3 Э4 Э5 Э6	Конспект лекций.
1.3	Изучение конспекта лекций и литературы по вопросам безопасности в ОС /Ср/	7	24	ОПК-9.2-З ОПК-12.3-З	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2Л3.1 Л3.2 Э1 Э2 Э3 Э4 Э5 Э6	Подготовка конспекта по вопросам темы. Краткий опрос по теме на консультации к экзамену (зачету).
	Раздел 2. Защита в ОС Windows					
2.1	Защита в ОС Windows /Тема/	7	0			

2.2	Компоненты подсистемы защиты. Объекты и субъекты доступа в Windows. Разграничение доступа в ОС Windows. Методы доступа к объектам в Windows. Права доступа к объектам в Windows. Привилегии субъектов в Windows. Разрешения NTFS для файлов и папок. Маркер доступа (АС) пользователя. Дескриптор защиты (SD) объекта: структура дескриптора защиты, списки управления доступом (DACL и SACL), маска прав в ACE, флаги в ACE - их назначение, отличие от флагов в SD, использование при наследовании. Идентификатор безопасности (SID) пользователя. Проверка прав доступа субъекта к объекту: общий порядок проверки SRM прав доступа субъектов к объектам, два варианта (функции) проверки прав доступа субъекта к объекту, примеры проверки прав доступа при обращении субъекта к объекту. Назначение атрибутов защиты (DACL) создаваемым (новым) объектам в Windows. Защита от несанкционированных действий администратора. Процессы-серверы в Windows: подходы к выполнению привилегированных действий в Windows (временное получение дополнительных полномочий (полномочий другого пользователя), обращение к услугам процесса-сервера), процесс-серверы в Windows, олицетворение пользователя. Аудит и обнаружение атак в Windows: журнал аудита, политика аудита, типы регистрируемых событий, использование информации из журнала аудита для анализа (анализ попыток регистрации, анализ доступа к объектам, анализ выполняющихся задач (отслеживание процессов). Анализ использования привилегий, анализ событий с учетными записями, анализ изменения политик). Требования к политике аудита. Администраторы и аудиторы (разделение). Внедрение вредоносных программ через реестр и планировщик заданий Windows: структура и расположение реестра, ключи автозагрузки для внедрения потенциально опасных программ (8 случаев). Планировщик заданий в Windows, средства контроля автозагрузки. Политики ИПС, SRP и Applocker: подходы к созданию изолированной программной среды до Windows XP, политика ограниченного использования программ (SRP). Политика Applocker и ее сравнение с SRP. Идентификация, аутентификация и авторизация пользователей в Windows. Механизм идентификации, аутентификации и авторизации в Windows: структура механизма идентификации и аутентификации, виды (типы) входа с помощью Kerberos v.5. Провайдеры сетевой аутентификации в систему, идентификация и аутентификация с помощью msv1_0(NTLM) - верхний, средний и нижний уровни, идентификация и аутентификация, параметры идентификации и аутентификации в Windows, Credential Provider’ы (поставщики учетных данных) в ОС Windows Vista и выше. Особенности защиты в серверных версиях ОС Windows. /Лек/	7	20	ОПК-9.1-З ОПК-9.2-З ОПК-12.2-З ОПК-12.3-З	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2Л3.1 Л3.2 Э1 Э2 Э3 Э4 Э5 Э6	Конспект лекций.

2.3	Исследование средств защиты в операционной системе Microsoft Windows NT 4.0 /Лаб/	7	4	ОПК-9.1-У ОПК-9.1-В ОПК-9.2-У ОПК-9.2-В ОПК-12.2-У ОПК-12.2-В ОПК-12.3-У ОПК-12.3-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2Л3.1 Л3.2 Э1 Э2 Э3 Э4 Э5 Э6	Отчет по ЛР Защита ЛР.
2.4	Исследование системы защиты в ОС indows XP /Лаб/	7	4	ОПК-9.1-У ОПК-9.1-В ОПК-9.2-У ОПК-9.2-В ОПК-12.2-У ОПК-12.2-В ОПК-12.3-У ОПК-12.3-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2Л3.1 Л3.2 Э1 Э2 Э3 Э4 Э5 Э6	Отчет по ЛР Защита ЛР.
2.5	Изучение подсистемы защиты ОС Windows (часть 1) /Лаб/	7	4	ОПК-9.1-У ОПК-9.1-В ОПК-9.2-У ОПК-9.2-В ОПК-12.2-У ОПК-12.2-В ОПК-12.3-У ОПК-12.3-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2Л3.1 Л3.2 Э1 Э2 Э3 Э4 Э5 Э6	Отчет по ЛР Защита ЛР.
2.6	Изучение подсистемы защиты ОС Windows (часть 2) /Лаб/	7	4	ОПК-9.1-У ОПК-9.1-В ОПК-9.2-У ОПК-9.2-В ОПК-12.2-У ОПК-12.2-В ОПК-12.3-У ОПК-12.3-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2Л3.1 Л3.2 Э1 Э2 Э3 Э4 Э5 Э6	Отчет по ЛР Защита ЛР.
2.7	Изучение подсистемы защиты ОС Windows Server 2003 (часть 1) /Лаб/	7	4	ОПК-9.1-У ОПК-9.1-В ОПК-9.2-У ОПК-9.2-В ОПК-12.2-У ОПК-12.2-В ОПК-12.3-У ОПК-12.3-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2Л3.1 Л3.2 Э1 Э2 Э3 Э4 Э5 Э6	Отчет по ЛР Защита ЛР.
2.8	Изучение подсистемы защиты ОС Windows Server 2003 (часть 2) /Лаб/	7	4	ОПК-9.1-У ОПК-9.1-В ОПК-9.2-У ОПК-9.2-В ОПК-12.2-У ОПК-12.2-В ОПК-12.3-У ОПК-12.3-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2Л3.1 Л3.2 Э1 Э2 Э3 Э4 Э5 Э6	Отчет по ЛР Защита ЛР.

2.9	Изучение конспекта лекций и литературы по защите информации в ОС Windows. /Ср/	7	24	ОПК-9.1-З ОПК-9.2-З ОПК-12.2-З ОПК-12.3-З	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2Л3.1 Л3.2 Э1 Э2 Э3 Э4 Э5 Э6	Подготовка конспекта по вопросам темы. Краткий опрос по теме на консультации к экзамену (зачету).
2.10	Подготовка к лабораторным работам. /Ср/	7	3	ОПК-9.2-З ОПК-12.2-З ОПК-12.3-З	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2Л3.1 Л3.2 Э1 Э2 Э3 Э4 Э5 Э6	Подготовка конспекта по вопросам темы. Краткий опрос по теме на консультации к экзамену (зачету).
2.11	Сдача зачета /ИКР/	7	0,25		Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2Л3.1 Л3.2 Э1 Э2 Э3 Э4 Э5 Э6	Ответы на Контрольные вопросы Результаты решения задач. Ответы на дополнительные вопросы. Результаты тестирования.
2.12	Подготовка к зачету /Зачёт/	7	8,75	ОПК-9.1-З ОПК-9.1-У ОПК-9.1-В ОПК-9.2-З ОПК-9.2-У ОПК-9.2-В ОПК-12.2-З ОПК-12.2-У ОПК-12.2-В ОПК-12.3-З ОПК-12.3-У ОПК-12.3-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2Л3.1 Л3.2 Э1 Э2 Э3 Э4 Э5 Э6	Задачи к зачету. Билеты к зачету. Тесты к зачету.
	Раздел 3. Защита в ОС Unix (Linux)					
3.1	/Тема/	8	0			

3.2	Компоненты подсистемы защиты в Unix (Linux). Объекты и субъекты доступа в в Unix (Linux). Разграничение доступа в Unix (Linux). Встроенные средства шифрования Unix (Linux). Аудит и обнаружение атак в ОС Unix (Linux). Идентификация, аутентификация и авторизация пользователей в ОС Unix (Linux). Процессы-серверы в ОС Unix (Linux). Внедрение вредоносных программ в ОС Unix (Linux). Особенности защиты в серверных версиях ОС Unix (Linux). Компоненты подсистемы защиты в Unix (Linux). Объекты и субъекты доступа в в Unix (Linux). Разграничение доступа в Unix (Linux). Встроенные средства шифрования Unix (Linux). Аудит и обнаружение атак в ОС Unix (Linux). Идентификация, аутентификация и авторизация пользователей в ОС Unix (Linux). Процессы-серверы в ОС Unix (Linux). Внедрение вредоносных программ в ОС Unix (Linux). Особенности защиты в серверных версиях ОС Unix (Linux). /Лек/	8	24	ОПК-9.1-З ОПК-9.2-З ОПК-12.2-З ОПК-12.3-З	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2Л3.1 Л3.2 Э1 Э2 Э3 Э4 Э5 Э6	Конспект лекций.
3.3	Подготовка к лабораторным работам /Ср/	8	2	ОПК-9.1-З ОПК-9.2-З ОПК-12.2-З ОПК-12.3-З	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2Л3.1 Л3.2 Э1 Э2 Э3 Э4 Э5 Э6	Подготовка конспекта по вопросам темы. Краткий опрос по теме на консультации к экзамену (зачету).
3.4	Структура подсистемы защиты информации в ОС Linux /Пр/	8	2	ОПК-9.1-З ОПК-9.1-У ОПК-9.2-З ОПК-9.2-У ОПК-12.2-З ОПК-12.2-У ОПК-12.3-З ОПК-12.3-У	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2Л3.1 Л3.2 Э1 Э2 Э3 Э4 Э5 Э6	Устный опрос по теме. Решение задач. Проверка домашнего задания.
3.5	Разграничение доступа в ОС Linux ч.1 /Пр/	8	2	ОПК-9.1-З ОПК-9.1-У ОПК-9.2-З ОПК-9.2-У ОПК-12.2-З ОПК-12.2-У ОПК-12.3-З ОПК-12.3-У	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2Л3.1 Л3.2 Э1 Э2 Э3 Э4 Э5 Э6	Устный опрос по теме. Решение задач. Проверка домашнего задания.
3.6	Разграничение доступа в ОС Linux ч.2 /Пр/	8	2	ОПК-9.1-З ОПК-9.1-У ОПК-9.2-З ОПК-9.2-У ОПК-12.2-З ОПК-12.2-У ОПК-12.3-З ОПК-12.3-У	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2Л3.1 Л3.2 Э1 Э2 Э3 Э4 Э5 Э6	Устный опрос по теме. Решение задач. Проверка домашнего задания.

3.7	Разграничение доступа в ОС Linux ч.3 /Пр/	8	2	ОПК-9.1-З ОПК-9.1-У ОПК-9.2-З ОПК-9.2-У ОПК-12.2-З ОПК-12.2-У ОПК-12.3-З ОПК-12.3-У	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2Л3.1 Л3.2 Э1 Э2 Э3 Э4 Э5 Э6	Устный опрос по теме. Решение задач. Проверка домашнего задания.
3.8	Аудит в Linux /Пр/	8	2	ОПК-9.1-У ОПК-9.2-З ОПК-9.2-У ОПК-12.2-З ОПК-12.2-У ОПК-12.3-З ОПК-12.3-У	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2Л3.1 Л3.2 Э1 Э2 Э3 Э4 Э5 Э6	Устный опрос по теме. Решение задач. Проверка домашнего задания.
3.9	Встроенные средства шифрования в Linux /Пр/	8	2	ОПК-9.1-З ОПК-9.1-У ОПК-9.2-З ОПК-12.2-З ОПК-12.2-У ОПК-12.3-З ОПК-12.3-У	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2Л3.1 Л3.2 Э1 Э2 Э3 Э4 Э5 Э6	Устный опрос по теме. Решение задач. Проверка домашнего задания.
3.10	Встроенные средства защиты информации в Asntra Linux ч.1 /Пр/	8	2	ОПК-9.1-З ОПК-9.1-У ОПК-9.2-З ОПК-9.2-У ОПК-12.2-З ОПК-12.2-У ОПК-12.3-З ОПК-12.3-У	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2Л3.1 Л3.2 Э1 Э2 Э3 Э4 Э5 Э6	Устный опрос по теме. Решение задач. Проверка домашнего задания.
3.11	Встроенные средства защиты информации в Asntra Linux ч.2 /Пр/	8	2	ОПК-9.1-З ОПК-9.1-У ОПК-9.2-З ОПК-9.2-У ОПК-12.2-З ОПК-12.2-У ОПК-12.3-З ОПК-12.3-У	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2Л3.1 Л3.2 Э1 Э2 Э3 Э4 Э5 Э6	Устный опрос по теме. Решение задач. Проверка домашнего задания.
3.12	Изучение подсистемы защиты в ОС Linux Часть 1. Права доступа в Linux /Лаб/	8	4	ОПК-9.1-З ОПК-9.1-У ОПК-9.1-В ОПК-9.2-З ОПК-9.2-У ОПК-9.2-В ОПК-12.2-З ОПК-12.2-У ОПК-12.2-В ОПК-12.3-З ОПК-12.3-У ОПК-12.3-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2Л3.1 Л3.2 Э1 Э2 Э3 Э4 Э5 Э6	Отчет по ЛР Защита ЛР.

3.13	Изучение подсистемы защиты в ОС Linux Часть 2. Аудит в Linux /Лаб/	8	4	ОПК-9.1-З ОПК-9.1-У ОПК-9.1-В ОПК-9.2-З ОПК-9.2-У ОПК-9.2-В ОПК-12.2-З ОПК-12.2-У ОПК-12.2-В ОПК-12.3-З ОПК-12.3-У ОПК-12.3-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2Л3.1 Л3.2 Э1 Э2 Э3 Э4 Э5 Э6	Отчет по ЛР Защита ЛР.
3.14	Изучение подсистемы защиты в ОС Linux Часть 3. Встроенные средства шифрования в Linux /Лаб/	8	4	ОПК-9.1-З ОПК-9.1-У ОПК-9.1-В ОПК-9.2-З ОПК-9.2-У ОПК-9.2-В ОПК-12.2-З ОПК-12.2-У ОПК-12.2-В ОПК-12.3-З ОПК-12.3-У ОПК-12.3-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2Л3.1 Л3.2 Э1 Э2 Э3 Э4 Э5 Э6	Отчет по ЛР Защита ЛР.
3.15	Изучение подсистемы защиты в ОС Linux Часть 4. Встроенные средства защиты информации в Astra Linux /Лаб/	8	4	ОПК-9.1-З ОПК-9.1-У ОПК-9.1-В ОПК-9.2-З ОПК-9.2-У ОПК-9.2-В ОПК-12.2-З ОПК-12.2-У ОПК-12.2-В ОПК-12.3-З ОПК-12.3-У ОПК-12.3-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2Л3.1 Л3.2 Э1 Э2 Э3 Э4 Э5 Э6	Отчет по ЛР Защита ЛР.
	Раздел 4. Безопасность мобильных ОС					
4.1	/Тема/	8	0			
4.2	Актуальные угрозы безопасности мобильных ОС. Особенности защиты в ОС Android: - аутентификация и технология Smart Lock, - цифровые подписи приложений, - полномочия, - ограничения (полномочий, API, на доступ к информации и устройствам, на работу в сети, на запуск приложений, на доступ к памяти, - шифрование данных, - доверенная среда исполнения, - доверенная загрузка, - защита от срыва стека, - технология SELinux, - технология Seccomp, - технология SafetyNet. Особенности защиты в ОС iOS. /Лек/	8	8	ОПК-9.1-З ОПК-9.2-З ОПК-12.2-З ОПК-12.3-З	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2Л3.1 Л3.2 Э1 Э2 Э3 Э4 Э5 Э6	Конспект лекций.

4.3	Изучение литературы по защите информации в ОС Android. /Ср/	8	4	ОПК-9.1-З ОПК-9.2-З ОПК-12.2-З ОПК-12.3-З	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2Л3.1 Л3.2 Э1 Э2 Э3 Э4 Э5 Э6	Подготовка конспекта по вопросам темы. Краткий опрос по теме на консультации к экзамену (зачету).
4.4	Сдача (прием) экзамена /ИКР/	8	0,35		Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2Л3.1 Л3.2 Э1 Э2 Э3 Э4 Э5 Э6	Ответы на Контрольные вопросы Результаты решения задач. Ответы на дополнительные вопросы. Результаты тестирования.
4.5	Консультирование перед экзаменом /Кнс/	8	2	ОПК-9.1-З ОПК-9.2-З ОПК-12.2-З ОПК-12.3-З	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2Л3.1 Л3.2 Э1 Э2 Э3 Э4 Э5 Э6	Вопросы к экзамену. Решение типовых задач. Ответы на вопросы.
4.6	Подготовка к экзамену /Экзамен/	8	35,65	ОПК-9.1-З ОПК-9.1-У ОПК-9.1-В ОПК-9.2-З ОПК-9.2-У ОПК-9.2-В ОПК-12.2-З ОПК-12.2-У ОПК-12.2-В ОПК-12.3-З ОПК-12.3-У ОПК-12.3-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2Л3.1 Л3.2 Э1 Э2 Э3 Э4 Э5 Э6	Задачи к экзамену. Билеты к экзамену. Тесты к экзамену.

5. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

Оценочные материалы по данной дисциплине приведены в Приложении 1 к рабочей программе дисциплины (см. документ «Оценочные материалы по дисциплине «Защита в операционных системах

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	Ермаков Д. Г., Присяжный А. В.	Применение антивирусных программ для обеспечения информационной безопасности	Екатеринбург: Уральский федеральный университет, ЭБС АСВ, 2013, 64 с.	2227-8397, http://www.iprbookshop.ru/66577.html
Л1.2	Сычев Ю. Н.	Стандарты информационной безопасности. Защита и обработка конфиденциальных документов : учебное пособие	Саратов: Вузовское образование, 2018, 195 с.	978-5-4487-0128-3, http://www.iprbookshop.ru/72345.html

№	Авторы, составители	Заглавие	Издательство, год	Количество/ название ЭБС
Л1.3	Глотина И. М.	Средства безопасности операционной системы Windows Server 2008 : учебно-методическое пособие	Саратов: Вузовское образование, 2018, 141 с.	978-5-4487-0136-8, http://www.iprbookshop.ru/72538.html
Л1.4		Администрирование ОС Unix	Москва: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016, 303 с.	2227-8397, http://www.iprbookshop.ru/73659.html
Л1.5	Айвенс К.	Администрирование Microsoft Windows Server 2003	Москва: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016, 486 с.	2227-8397, http://www.iprbookshop.ru/73725.html
6.1.2. Дополнительная литература				
№	Авторы, составители	Заглавие	Издательство, год	Количество/ название ЭБС
Л2.1	Ложников П. С., Михайлов Е. М.	Обеспечение безопасности сетевой инфраструктуры на основеоперационных систем Microsoft : практикум	Москва, Саратов: Интернет-Университет Информационных Технологий (ИНТУИТ), Вузовское образование, 2017, 264 с.	978-5-4487-0080-4, http://www.iprbookshop.ru/67389.html
Л2.2	Руденков Н. А., Пролетарский А. В., Смирнова Е. В., Суровов А. М.	Технологии защиты информации в компьютерных сетях	Москва: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016, 368 с.	2227-8397, http://www.iprbookshop.ru/73732.html
6.1.3. Методические разработки				
№	Авторы, составители	Заглавие	Издательство, год	Количество/ название ЭБС
Л3.1	Засорин С.В., Кузьмин Ю.М., Пржегорлинский В.Н.	Защита в операционных системах : метод. указ. к лаб.работам	Рязань, 2016, 76с.	60
Л3.2	Засорин С.В., Кузьмин Ю.М., Пржегорлинский В.Н.	Защита в операционных системах : метод. указ. к лаб. работам	Рязань, 2016, 44с.	60
6.2. Перечень ресурсов информационно-телекоммуникационной сети "Интернет"				
Э1	1. Электронно-библиотечная система «Лань». – Режим доступа: доступ из корпоративной сети РГРТУ – свободный (без пароля). URL: https://e.lanbook.com/			

Э2	2. Электронно-библиотечная система «IPRbooks». – Режим доступа: доступ из корпоративной сети РГРТУ – свободный (без пароля), доступ из сети Интернет - по паролю. URL: https://iprbookshop.ru/
Э3	3. Электронная библиотека РГРТУ. URL: http://elib.rsreu.ru/ . Режим доступа: из корпоративной сети РГРТУ – по паролю
Э4	4. Научная электронная библиотека eLibrary. URL: http//e.lib/vlsu.ru/www.uisrussia.msu.ru/elibrary.ru
Э5	5. Библиотека и форум по программированию. URL: http://www.cyberforum.ru
Э6	6. Национальный открытый университет ИНТУИТ. URL: http://www.intuit.ru/

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
Операционная система Windows	Коммерческая лицензия
Kaspersky Endpoint Security	Коммерческая лицензия
Adobe Acrobat Reader	Свободное ПО
LibreOffice	Свободное ПО
VMware Player	Свободное ПО

6.3.2 Перечень информационных справочных систем

6.3.2.1	Система КонсультантПлюс http://www.consultant.ru

7. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

1	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.
2	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.

8. МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

Методические материалы по данной дисциплине приведены в Приложении 2 к рабочей программе дисциплины (см. документ «Методическое обеспечение дисциплины «Защита в операционных системах