Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Макаренко Елена Николаевна
Должность: Ректор
Дата подписания: 20.06.2026 11:53:55
Уникальный программный ключ:
c098bc0c1041cb2a4cf926cf171d6715d99a6ae00adc8e27b55cbe1e2dbd7c78

Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Ростовский государственный экономический университет (РИНХ)»

УТВЕРЖДАЮ
Начальник
учебно-методического управления
Т.К. Платонова
«25» мая 2026 г.

Рабочая программа дисциплины
Программно-аппаратные методы защиты информации

Направление подготовки
10.04.01 Информационная безопасность

Направленность (профиль) программы магистратуры
10.04.01.02 Программно-аппаратные методы расследования компьютерных преступлений

Для набора 2026 года

Квалификация
магистр

КАФЕДРА **Информационная безопасность**

Распределение часов дисциплины по семестрам / курсам

Семестр (<Курс>.<Семестр на курсе>)	**4 (2.2)**		Итого	
Недель	10 3/6			
Вид занятий	УП	РП	УП	РП
Лекции	14	14	14	14
Лабораторные	14	14	14	14
Итого ауд.	28	28	28	28
Контактная работа	28	28	28	28
Сам. работа	76	76	76	76
Часы на контроль	4	4	4	4
Итого	108	108	108	108

ОСНОВАНИЕ

Учебный план утвержден учёным советом Университета (протокол № 9 от 03.03.2026 г.).

Программу составил(и): к.ф.-м.н., доцент, Карнаухов С.Н.

Зав. кафедрой: к.э.н., доцент Ю.В. Радченко

Методический совет направления: д.э.н., профессор Е.Н. Тищенко

Директор института магистратуры: д.э.н., профессор Е.А. Иванова

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

1.1	ознакомление обучающихся с основными принципами использования программно-аппаратных комплексов защиты информации, сравнивать технико-эксплуатационные возможности устройств и систем защиты информации;
1.2	расшифровывать и анализировать информацию о параметрах и характеристиках устройств с использованием различных источников;
1.3	проектировать, планировать и разворачивать элементы комплексной системы защиты информации;
1.4	устанавливать, настраивать, использовать программно-аппаратные средства защиты информации.

2. ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ

УК-4. Способен применять современные коммуникативные технологии, в том числе на иностранном(ых) языке(ах), для академического и профессионального взаимодействия

ПК-1. Способен разрабатывать программно-аппаратные системы и комплексы обеспечения информационной безопасности

В результате освоения дисциплины обучающийся должен:

Знать:

современные коммуникативные технологии на государственном и иностранном языках; закономерности деловой устной и письменной коммуникации (соотнесено с индикатором УК-4.1.)
нормативно-правовые акты и методы обеспечения информационной безопасности объекта информатизации;
основные разделы технического задания, методы, способы и содержание этапов проектирования и разработки программно-аппаратных систем и комплексов обеспечения информационной безопасности;
технологии, методы, языки и средства программирования систем и комплексов обеспечения информационной безопасности (соотнесено с индикатором ПК-1.1.)

Уметь:

применять на практике коммуникативные технологии, методы и способы делового общения (соотнесено с индикатором УК-4.2.)
проводить сбор и анализ исходных данных для разработки, проектирования программно-аппаратных систем и комплексов обеспечения информационной безопасности с учетом нормативно-правовых актов и методических документов (соотнесено с индикатором ПК-1.2.)

Владеть:

методикой межличностного делового общения на государственном и иностранном языках, с применением профессиональных языковых форм и средств (соотнесено с индикатором УК-4.3.)
навыками формирования разделов технического задания на разработку программно-аппаратных систем и комплексов обеспечения информационной безопасности;
навыками проектирования и разработки программно-аппаратных систем и комплексов обеспечения информационной безопасности.(соотнесено с индикатором ПК-1.3.)

3. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Раздел 1. Основные понятия программно-аппаратной защиты информации. Управление доступом к компонентам информационных систем

№	Наименование темы, краткое содержание	Вид занятия / работы / форма ПА	Семестр / Курс	Количество часов	Компетенции
1.1	Тема 1.1 "Основные понятия программно-аппаратной защиты информации" Предмет и задачи программно-аппаратной защиты информации. Основные понятия. Уязвимость информационных систем. Политика безопасности в информационных системах. Оценка защищенности. Механизмы защиты.	Лекционные занятия	4	2	УК-4 ПК-1
1.2	Тема 1.2 "Идентификация пользователей информационных систем-субъектов доступа к данным" Идентификация и аутентификация пользователей. Взаимная проверка подлинности. Протоколы идентификации.	Лекционные занятия	4	2	УК-4 ПК-1
1.3	Тема 1.3 "Средства и методы ограничения доступа к ресурсам информационных систем" Защита информации от несанкционированного доступа. Система разграничения доступа к информации в компьютерных системах. Методы и средства ограничения доступа к компонентам ЭВМ.	Лекционные занятия	4	2	УК-4 ПК-1
1.4	Тема 1.5 "Применение средств защиты информации от несанкционированного доступа для организации защищенных компьютерных систем" Методы противодействия несанкционированному доступу.	Лекционные занятия	4	4	УК-4 ПК-1

	Программно-аппаратные комплексы защиты информации от несанкционированного доступа				
1.5	Тема 1.4 "Организация и контроль доступа к файлам" Шифрование, контроль доступа и разграничение доступа, иерархический доступ к файлу, защита сетевого файлового ресурса, фиксация доступа к файлам. Способы фиксации факта доступа. Надежность систем ограничения доступа. Защита файлов от изменения.	Лекционные занятия	4	4	УК-4 ПК-1
1.6	Тема 1.2 "Идентификация пользователей информационных систем-субъектов доступа к данным" Запуск менеджера виртуальных машин. Установка виртуальных машин: REDOS. Настройка одноранговой сети. Создание учетных записей пользователей. Настройка локальных политик паролей. Создание иерархической структуры сети. Установка контроллера домена. Управление учетными записями пользователей.LibreOffice	Лабораторные занятия	4	2	УК-4 ПК-1
1.7	Тема 1.3 "Средства и методы ограничения доступа к ресурсам информационных систем" Ознакомление с аппаратными комплексами защиты от несанкционированного доступа к ИС. Программно-аппаратный комплекс "Соболь": ознакомление, установка, настройка. Аппаратные средства биометрической идентификации.LibreOffice	Лабораторные занятия	4	4	УК-4 ПК-1
1.8	Тема 1.4 "Организация и контроль доступа к файлам" Создание на виртуальном сервере сетевого ресурса. Настройка доступа к созданному ресурсу в одноранговой и иерархической сети. Виды доступа. Наследование прав на сетевые ресурсы. Использование групп безопасности для организации доступа к сетевым рессурсам.	Лабораторные занятия	4	4	УК-4 ПК-1
1.9	Тема 1.5 "Применение средств защиты информации от несанкционированного доступа для организации защищенных компьютерных систем" Установка, настройка, эксплуатация программно-аппаратных средств защиты информации от несанкционированного доступа	Лабораторные занятия	4	4	УК-4 ПК-1
1.10	Удаленные сетевые атаки	Самостоятельная работа	4	44	УК-4 ПК-1
1.11	Основы межсетевого взаимодействия	Самостоятельная работа	4	32	УК-4 ПК-1
1.12	Подготовка к промежуточной аттестации	Зачет	4	4	УК-4 ПК-1

4. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

Структура и содержание фонда оценочных средств для проведения текущего контроля и промежуточной аттестации представлены в Приложении 1 к рабочей программе дисциплины.

5. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

5.1. Учебные, научные и методические издания

	Авторы, составители	Заглавие	Издательство, год	Библиотека / Количество
1		Информационная безопасность: журнал	Москва: Гротек, 2014	ЭБС «Университетская библиотека онлайн»
2	Алакоз Г. М., Котов А. В., Попов А. А., Курак М. В., Сериков А. П.	Программно-аппаратные платформы и вычислительные наноструктуры: учебное пособие	Москва: Национальный Открытый Университет «ИНТУИТ», 2016	ЭБС «Университетская библиотека онлайн»
3	Денисов, И. А.	Лабораторный практикум по дисциплине Программно-аппаратные средства защиты информации	Москва: Московский технический университет связи и информатики, 2016	ЭБС «IPR SMART»
4	Громов Ю. Ю., Иванова О. Г., Стародубов К. В., Кадыков А. А.	Программно-аппаратные средства защиты информационных систем: учебное пособие	Тамбов: Тамбовский государственный технический университет (ТГТУ), 2017	ЭБС «Университетская библиотека онлайн»

5.2. Профессиональные базы данных и информационные справочные системы

ИСС "КонсультантПлюс"
ИСС "Гарант" http://www.internet.garant.ru/
ФСТЭК России/fstec.ru

5.3. Перечень программного обеспечения
Операционная система РЕД ОС LibreOffice ПАК Соболь
5.4. Учебно-методические материалы для обучающихся с ограниченными возможностями здоровья
При необходимости по заявлению обучающегося с ограниченными возможностями здоровья учебно-методические материалы предоставляются в формах, адаптированных к ограничениям здоровья и восприятия информации. Для лиц с нарушениями зрения: в форме аудиофайла; в печатной форме увеличенным шрифтом. Для лиц с нарушениями слуха: в форме электронного документа; в печатной форме. Для лиц с нарушениями опорно-двигательного аппарата: в форме электронного документа; в печатной форме.

6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Помещения для всех видов работ, предусмотренных учебным планом, укомплектованы необходимой специализированной учебной мебелью и техническими средствами обучения:
- столы, стулья;
- персональный компьютер / ноутбук (переносной);
- проектор;
- экран / интерактивная доска.

Лабораторные занятия проводятся в компьютерных классах, рабочие места в которых оборудованы необходимыми лицензионными и/или свободно распространяемыми программными средствами и выходом в Интернет, и/или в специализированных лабораториях, предусмотренных образовательной программой.

Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой с возможностью подключения к сети "Интернет" и обеспечением доступа к электронной информационно-образовательной среде.

7. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Методические указания по освоению дисциплины представлены в Приложении 2 к рабочей программе дисциплины.

Приложение 1

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

1 Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

1.1 Показатели и критерии оценивания компетенций:

ЗУН, составляющие компетенцию	Показатели оценивания	Критерии оценивания	Средства оценивания
УК-4: Способен применять современные коммуникативные технологии, в том числе на иностранном(ых) языке(ах), для академического и профессионального взаимодействия			
З. - современные коммуникативные технологии на государственном и иностранном языках; закономерности деловой устной и письменной коммуникации	Этапы установки REDOS. Аппаратные требования REDOS.	полнота и содержательность ответа умение приводить примеры	О (1-45) З(1-46)
У. - сравнивать технико-эксплуатационные возможности устройств и систем защиты информации;	RAID. Аппаратный и программный. Типы. RAID в REDOS. Работа с дисками в REDOS.	полнота и содержательность ответа умение приводить примеры умение самостоятельно находить решение поставленных задач	ЛЗ (5-8) ПОЗЗ (1-5)
В. методикой межличностного делового общения на государственном и иностранном языках, с применением профессиональных языковых форм и средств	Источники резервного питания Резервное копирование данных. Аппаратные устройства для разграничения доступа в сети.	полнота и содержательность ответа умение приводить примеры умение самостоятельно находить решение поставленных задач	ЛЗ (5-8) ПОЗЗ (1-5)
ПК-1: Способен разрабатывать программно-аппаратные системы и комплексы обеспечения информационной безопасности			
З. - нормативно-правовые акты и методы обеспечения информационной безопасности объекта информатизации; основные разделы технического задания, методы, способы и содержание этапов	Политика безопасности, наследование политики безопасности Протокол безопасности Kerberos. Firewall: назначение, принцип работы.	полнота и содержательность ответа умение приводить примеры	О (1-45) З(1-46)

проектирования и разработки программно-аппаратных систем и комплексов обеспечения информационной безопасности; технологии, методы, языки и средства программирования систем и комплексов обеспечения информационной безопасности			
У. - проводить сбор и анализ исходных данных для разработки, проектирования программно-аппаратных систем и комплексов обеспечения информационной безопасности с учетом нормативно-правовых актов и методических документов	Виды адресаций в TCP/IP сетях IP адрес: назначение, структура, применение	полнота и содержательность ответа умение приводить примеры умение самостоятельно находить решение поставленных задач	ЛЗ (1-4) ПОЗЗ (1-5)
В. навыками формирования разделов технического задания на разработку программно-аппаратных систем и комплексов обеспечения информационной безопасности; навыками проектирования и разработки программно-аппаратных систем и комплексов обеспечения информационной безопасности	DNS имя: назначение, структура, применение Семиуровневая модель OSI. Характеристика стэка протоколов TCP/IP.	полнота и содержательность ответа умение приводить примеры умение самостоятельно находить решение поставленных задач	ЛЗ (1-4) ПОЗЗ (1-5)

З – зачет О – опрос, ЛЗ- лабораторная работа, ПОЗЗ – практико-ориентированные задания к зачету

1.2 Шкалы оценивания:

Текущий контроль успеваемости и промежуточная аттестация осуществляется в рамках накопительной балльно-рейтинговой системы в 100-балльной шкале.

- 50-100 баллов (зачет);
- 0-49 баллов (незачет).

2. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы

Вопросы к зачету

1) Семейство ОС REDOS.
2) Этапы установки REDOS.
3) Аппаратные требования REDOS.
4) RAID. Аппаратный и программный. Типы.
5) RAID в REDOS.
6) Работа с дисками в REDOS.
7) Источники резервного питания
8) Резервное копирование данных.
9) Аппаратные устройства для разграничения доступа в сети.
10) Служба каталогов REDOS.
11) Домен, дерево, лес в службе каталогов REDOS.
12) Выбор аппаратных компонентов для организации серверных центров.
13) Служба каталогов Active Directory.
14) Установка и настройка AD.
15) Управление пользователями с помощью AD.
16) Группы в AD. Типы групп.
17) Разграничение доступа к ресурсам.
18) Система безопасности REDOS.
19) Политика безопасности, наследование политики безопасности
20) Протокол безопасности Kerberos.
21) Firewall: назначение, принцип работы.
22) Microsoft ISA Server: особенности установки и настройки.
23) Виды адресаций в TCP/IP сетях
24) IP адрес: назначение, структура, применение
25) DNS имя: назначение, структура, применение
26) Семиуровневая модель OSI.
27) Характеристика стэка протоколов TCP/IP.
28) Виды адресации в IP сетях.
29) Протокол IP: назначение, структура заголовка, принципы работы
30) Протокол TCP: назначение, структура заголовка, основные режимы работы
31) Маршрутизация. Таблицы маршрутизации
32) Службы REDOS для мониторинга и оптимизации.
33) Мониторинг и оптимизация производительности дисков.
34) Работа с дисковыми квотами.
35) Сжатие и шифрование данных средствами ОС.
36) Консоль "Производительность": назначение, состав.

37) Оснастка "Системный монитор"
38) Оснастка "Журналы"
39) Утилита "Диспетчер задач": назначение, функции.
40) Описание протоколов VPN
41) Компоненты VipNet
42) Secret Net назначение и функции
43) Основные особенности использования Secret Net
44) Сравнительная характеристика Proxy и Nat серверов
45) Протокол безопасности IpSec
46) Программно-аппаратный комплекс "Соболь": назначение, установка, настройка

Практико-ориентированные задания к зачету

1. Установить угрозы, атаки и риски сетевой безопасности.
1. Установить антивирусное программное обеспечение.
2. Установить Linux-подобную операционную систему.
3. Настроить впервые установленную Linux-подобную операционную систему.
4. Установить шифровальную систему.

Критерии оценивания*:*

- 50-100 баллов (зачтено) – наличие твердых знаний в объеме пройденного курса в соответствии с целями обучения, изложение ответов с отдельными ошибками, уверенно исправленными после дополнительных вопросов; правильные в целом действия по применению знаний на практике;

- 0-49 баллов (Не зачтено) – ответы не связаны с вопросами, наличие грубых ошибок в ответе, непонимание сущности излагаемого вопроса, неумение применять знания на практике, неуверенность и неточность ответов на дополнительные и наводящие вопросы.

Задания для опроса

1. Семейство ОС REDOS.
2. Этапы установки REDOS.
3. Аппаратные требования REDOS.
4. RAID. Аппаратный и программный. Типы.
5. RAID в REDOS.
6. Работа с дисками в REDOS.
7. Источники резервного питания
8. Резервное копирование данных.
9. Аппаратные устройства для разграничения доступа в сети.
10. Служба каталогов REDOS.
11. Домен, дерево, лес в службе каталогов REDOS.
12. Выбор аппаратных компонентов для организации серверных центров.
13. Служба каталогов Active Directory.
14. Установка и настройка AD.
15. Управление пользователями с помощью AD.
16. Группы в AD. Типы групп.
17. Разграничение доступа к ресурсам.
18. Система безопасности REDOS.
19. Политика безопасности, наследование политики безопасности
20. Протокол безопасности Kerberos.
21. Firewall: назначение, принцип работы.

22. Microsoft ISA Server: особенности установки и настройки.
23. Виды адресаций в TCP/IP сетях
24. IP адрес: назначение, структура, применение
25. DNS имя: назначение, структура, применение
26. Семиуровневая модель OSI.
27. Характеристика стэка протоколов TCP/IP.
28. Виды адресации в IP сетях.
29. Протокол IP: назначение, структура заголовка, принципы работы
30. Протокол TCP: назначение, структура заголовка, основные режимы работы
31. Маршрутизация. Таблицы маршрутизации
32. Службы REDOS для мониторинга и оптимизации.
33. Мониторинг и оптимизация производительности дисков.
34. Работа с дисковыми квотами.
35. Сжатие и шифрование данных средствами ОС.
36. Консоль "Производительность": назначение, состав.
37. Оснастка "Системный монитор"
38. Оснастка "Журналы"
39. Утилита "Диспетчер задач": назначение, функции.
40. Описание протоколов VPN
41. Компоненты VipNet
42. Secret Net назначение и функции
43. Основные особенности использования Secret Net
44. Сравнительная характеристика Proxy и Nat серверов
45. Протокол безопасности IpSec

Критерии оценки:

- 1-20 баллов выставляется обучаемому. За один правильный ответ обучаемый получает 1 балл.

Лабораторные работы

Лабораторная работа №1

Запуск менеджера виртуальных машин. Установка виртуальных машин: REDOS 7. Настройка одноранговой сети. Создание учетных записей пользователей. Настройка локальных политик паролей.

Создание иерархической структуры сети. Установка контроллера домена. Управление учетными записями пользователей.

Лабораторная работа №2

Ознакомление с аппаратными комплексами защиты от несанкционированного доступа к ИС. Программно-аппаратный комплекс «Соболь»: ознакомление, установка, настройка. Аппаратные средства биометрической идентификации.

Лабораторная работа №3

Создание на виртуальном сервере сетевого ресурса. Настройка доступа к созданному ресурсу в одноранговой и иерархической сети. Виды доступа. Наследование прав на сетевые ресурсы. Использование групп безопасности для организации доступа к сетевым рессурсам.

Лабораторная работа №4

Установка в виртуальную сетевую среду на сервер межсетевого экрана. Первичная настройка межсетевого экрана. Формирование правил фильтрации пакетов. Проверка уровня защищенности треброваниям.

Лабораторная работа №5

Установка в виртуальной среде антивирусного комплекса. Настройка основных параметров. Сканирование дисков и объектов.

Лабораторная работа №6

Работа с программным RAID в REDOS сервер. Создание дополнительного виртуального жесткого диска. Подключение диска к виртуальному серверу. Создание RAID–массива. Генерация события отказа и оценка работоспособности RAID-массива.

Лабораторная работа №7

Установка и настройка утилиты «Сетевой монитор». Оценка сетевого трафика. Сбор трафика. Анализ трафика. Определение принадлежности пакета. Перехват передаваемых данных.

Лабораторная работа №8

Разворачивание архитектуры VPN с использованием стандартных средств защиты REDOS сервер.

Критерии оценки: всего – 80 баллов.

- (для каждого задания):

10 б. – задание выполнено верно;

9-7 б. – при выполнении задания были допущены неточности, не влияющие на результат;

6-4 б. – при выполнении задания были допущены ошибки;

3-1. – при выполнении задания были допущены существенные ошибки;

0 б. – задание не выполнено.

3 Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Процедуры оценивания включают в себя текущий контроль и промежуточную аттестацию.

Текущий контроль успеваемости проводится с использованием оценочных средств, представленных в п. 2 данного приложения. Результаты текущего контроля доводятся до сведения студентов до промежуточной аттестации.

Промежуточная аттестация проводится в форме зачета.

Зачет проводится по окончанию теоретического обучения в соответствии с расписанием. Количество вопросов в задании – 3. Объявление результатов производится в день зачета. Результаты аттестации заносятся в ведомость и зачетную книжку студента. Студенты, не прошедшие промежуточную аттестацию по графику, должны ликвидировать задолженность в установленном порядке.

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Методические указания по освоению дисциплины «Программно-аппаратные средства защиты информации» адресованы студентам всех форм обучения.

Учебным планом по направлению подготовки предусмотрены следующие виды занятий:

лекционные

лабораторные

В ходе лекционных занятий рассматриваются основные теоретические вопросы, даются рекомендации для самостоятельной работы и подготовке к лабораторным занятиям.

При подготовке к лабораторным занятиям каждый студент должен:

– изучить рекомендованную учебную литературу;

– изучить конспекты лекций;

– подготовить ответы на все вопросы по изучаемой теме;

– письменно решить домашнее задание, рекомендованные преподавателем при изучении каждой темы.

По согласованию с преподавателем студент может подготовить реферат, доклад или сообщение по теме занятия. В процессе подготовки к лабораторным занятиям студенты могут воспользоваться консультациями преподавателя.

Вопросы, не рассмотренные на аудиторных занятиях, должны быть изучены студентами в ходе самостоятельной работы. Контроль самостоятельной работы студентов над учебной программой курса осуществляется в ходе занятий методом устного опроса или контрольной работы. В ходе самостоятельной работы каждый студент обязан прочитать основную и по возможности дополнительную литературу по изучаемой теме, дополнить конспекты недостающим материалом, выписками из рекомендованных первоисточников. Выделить непонятные термины, найти их значение в энциклопедических словарях.

Студент должен готовиться к предстоящим лабораторным занятиям по всем, обозначенным в рабочей программе дисциплины вопросам.

библиотеки или воспользоваться читальными залами вуза.