МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования "Российский государственный геологоразведочный университет имени Серго Орджоникидзе"

(МГРИ)

Безопасность операционных систем

рабочая программа дисциплины (модуля)

Закреплена за кафедрой **Промышленной кибербезопасности и защиты геоданных**

Учебный план b090302_25_BIS25.plx
09.03.02 Информационные системы и технологии

Квалификация **Бакалавр**

Форма обучения **очная**

Общая трудоемкость **4 ЗЕТ**

Часов по учебному плану 0
в том числе:
аудиторные занятия 0
самостоятельная работа 0

Виды контроля в семестрах:

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	**5 (3.1)**		Итого	
Недель	16			
Вид занятий	УП	РП	УП	РП
Лекции	32	28	32	28
Практические	32	70	32	70
Иные виды контактной работы	2,35	2,35	2,35	2,35
Итого ауд.	66,35	100,35	66,35	100,35
Контактная работа	66,35	100,35	66,35	100,35
Сам. работа	50,65	52,65	50,65	52,65
Часы на контроль	27	27	27	27
Итого	144	180	144	180

Москва 2025

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)	
1.1	Целью преподавания дисциплины является теоретическая и практическая подготовка специалистов в области эксплуатации современных операционных систем (ОС) для обеспечения их эффективного применения с учетом требований информационной безопасности и привитие навыков в использовании методов обеспечения защиты информации в ОС.
1.2	Задачи дисциплины:
1.3	-изучение назначения и функций ОС;
1.4	- приобретение навыков управления ресурсами и задачами в ОС;
1.5	- освоение администрирования ОС; - изучение требований к защите ОС;
1.6	- изучение методов и средств разграничения доступа в ОС;
1.7	- изучение аудита в ОС;
1.8	- формирование специальных теоретических и практических знаний, обеспечивающих возможность планирования политики безопасности ОС;
1.9	- приобретение навыков эффективной и безопасной эксплуатацию ОС автоматизированных систем;
1.10	- формирование специальных теоретических и практических знаний, обеспечивающих возможность проектировании средств защиты информации и средств контроля защищенности автоматизированных систем;
1.11	- приобретение навыков эффективного применения информационно-технологических ресурсов ОС с учетом требований информационной безопасности;
1.12	- приобретение навыков эффективного применения средств защиты информационно-технологических ресурсов ОС;
1.13	- формирование специальных теоретических и практических знаний, позволяющих администрировать подсистему информационной безопасности автоматизированной системы;
1.14	- формирование специальных теоретических и практических знаний, позволяющих обеспечить восстановление работоспособности систем защиты информации при возникновении нештатных ситуаций.

2. МЕСТО ДИСЦИПЛИНЫ (МОДУЛЯ) В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ	
Цикл (раздел) ОП:	Б1.В
2.1	**Требования к предварительной подготовке обучающегося:**
2.1.1	Информационные технологии
2.1.2	Сети и системы передачи информации
2.1.3	Ознакомительная практика
2.2	**Дисциплины (модули) и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:**
2.2.1	Безопасность систем баз данных
2.2.2	Мониторинг информационной безопасности и активный поиск киберугроз
2.2.3	Измерительная аппаратура контроля защищенности объектов информатизации
2.2.4	Управление информационной безопасностью
2.2.5	Информационная безопасность открытых систем

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)
ПК-8.3: Способен проводить администрирование систем защиты информации автоматизированных систем
Знать:
Уметь:
Владеть:

В результате освоения дисциплины (модуля) обучающийся должен

3.1	**Знать:**
3.1.1	устройство и принципы работы операционных систем, структуру и возможности подсистем защиты операционных систем семейств UNIX и Windows;
3.1.2	методы администрирования и принципы работы операционных систем семейств UNIX и Windows;
3.2	**Уметь:**
3.2.1	использовать средства управления работой операционной системы;
3.2.2	формулировать политику безопасности операционных систем семейств UNIX и Windows;
3.2.3	настраивать политику безопасности операционных систем семейств UNIX и Windows;
3.3	**Владеть:**

3.3.1	установки операционных систем семейств Windows и Unix;
3.3.2	администрирования операционных систем семейств Windows и Unix с учетом требований по обеспечению информационной безопасности;

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Код занятия	Наименование разделов и тем /вид занятия/	Семестр / Курс	Часов	Компетен-ции	Литература	Инте ракт.	Примечание
	Раздел 1. Основы функционирования ОС						
1.1	Назначение и функции операционных систем. Особенности архитектуры мобильных ОС. /Лек/	5	2		Л1.1	0	
1.2	Управление задачами в ОС. Управления задачами в мобильных ОС. /Лек/	5	2		Л1.1	0	
1.3	Управление данными и файловые системы /Лек/	5	6		Л1.1	0	
1.4	Диспетчеризация процессов /Лек/	5	4		Л1.1	0	
1.5	Управление памятью /Лек/	5	4		Л1.1	0	
1.6	Средства управления работой операционной системы /Пр/	5	2		Л1.1	0	
1.7	Разграничение доступа к файлам /Пр/	5	4		Л1.1	0	
1.8	Система команд для работы с файловой системой /Пр/	5	10		Л1.1	0	
1.9	Сервисные команды /Пр/	5	10		Л1.1	0	
1.10	Сценарии, параметры и переменные среды /Пр/	5	8		Л1.1	0	
1.11	Операторы оболочки /Пр/	5	8		Л1.1	0	
1.12	Средства разработки сценариев /Пр/	5	6		Л1.1	0	
1.13	Разработка сценариев /Пр/	5	2		Л1.1	0	
1.14	Выполнение заданий к лабораторным работам /Ср/	5	25,25		Л1.1	0	
	Раздел 2. Безопасность ОС						
2.1	Требования к защите ОС. Концепция виртуализации. Виртуальные машины. Гипервизоры. /Лек/	5	2		Л1.1	0	
2.2	Административные меры защиты. Аппаратно-программные средства защиты. Понятие attack surface и его использование при организации защиты ОС. /Лек/	5	2		Л1.1	0	
2.3	Аппаратные средства идентификации и аутентификации. Разграничение доступа в ОС. /Лек/	5	2		Л1.1	0	
2.4	Идентификация, аутентификация и учет в современных ОС /Лек/	5	2		Л1.1	0	
2.5	Аудит и его реализации в современных ОС /Лек/	5	2		Л1.1	0	
2.6	Управление пользователями /Пр/	5	2		Л1.1	0	
2.7	Управление данными /Пр/	5	2		Л1.1	0	
2.8	Управление процессами /Пр/	5	2		Л1.1	0	
2.9	Системные вызовы для управления процессами /Пр/	5	4		Л1.1	0	
2.10	Управление файловой системой /Пр/	5	4		Л1.1	0	
2.11	Разделяемая память и очереди сообщений /Пр/	5	4		Л1.1	0	
2.12	Сигналы /Пр/	5	2		Л1.1	0	
2.13	Выполнение домашних заданий к практическим работам /Ср/	5	27,4		Л1.1	0	

2.14	Экзамен /ИВКР/	5	2,35		Л1.1	0	

5. ОЦЕНОЧНЫЕ СРЕДСТВА

5.1. Контрольные вопросы и задания

Тема 1: Назначение и функции операционных систем. Особенности архитектуры мобильных ОС
1. Каково назначение операционной системы?
2. Перечислите основные функции современной операционной системы.
3. Чем отличаются монолитная и микроядерная архитектура ОС?
4. Каковы особенности архитектуры мобильных операционных систем?
5. Какие мобильные ОС являются наиболее популярными на сегодняшний день?
Тема 2: Управление задачами в ОС. Управления задачами в мобильных ОС
6. Что такое процесс и поток в контексте ОС?
7. Как осуществляется планирование задач в многозадачной ОС?
8. Какие режимы управления задачами реализованы в мобильных ОС?
9. Какие ограничения накладывает мобильная платформа на управление задачами?
10. Как обеспечивается энергоэффективное управление задачами в мобильных ОС?
Тема 3: Управление данными и файловые системы
11. Что такое файловая система и какие её основные компоненты?
12. Чем отличаются логическая и физическая организация хранения данных?
13. Какие типы файловых систем используются в современных ОС?
14. Как организуется доступ к данным в условиях многозадачности?
15. Какие механизмы обеспечивают целостность и восстановление данных?
Тема 4: Диспетчеризация процессов
16. Что такое планировщик процессов и какие у него функции?
17. Какие алгоритмы диспетчеризации процессов вы знаете?
18. Какие критерии используются при выборе алгоритма планирования?
19. Как решается проблема тупиков (deadlock) в системах с множеством процессов?
20. Как влияет диспетчеризация на производительность и безопасность ОС?
Тема 5: Управление памятью
21. Какие виды памяти существуют в составе компьютерной системы?
22. Что такое виртуальная память и как она реализуется?
23. Как происходит преобразование виртуальных адресов в физические?
24. Что такое страничная и сегментная организация памяти?
25. Какие угрозы безопасности связаны с управлением памятью?
Тема 6: Требования к защите ОС. Концепция виртуализации. Гипервизоры
26. Какие основные требования предъявляются к безопасности ОС?
27. Что такое виртуализация и зачем она применяется?
28. Чем отличаются гипервизоры типа 1 и типа 2?
29. Как виртуализация влияет на безопасность вычислений?
30. Какие уязвимости могут возникнуть при использовании виртуальных машин?
Тема 7: Административные меры защиты. Аппаратно-программные средства защиты. Attack surface
31. Какие административные меры способствуют повышению безопасности ОС?
32. Что такое минимальная привилегия и как она используется?
33. Какие аппаратно-программные средства обеспечивают защиту ОС?
34. Что означает термин *attack surface* и как его минимизировать?
35. Как роль принципа "минимизации поверхности атаки" влияет на безопасность ОС?
Тема 8: Аппаратные средства идентификации и аутентификации. Разграничение доступа в ОС
36. Какие аппаратные средства идентификации и аутентификации существуют?
37. Что такое двухфакторная аутентификация и как она реализуется?
38. Какие модели разграничения доступа реализованы в современных ОС?
39. Чем отличаются дискреционный и мандатный доступ?
40. Как биометрические системы влияют на безопасность идентификации?
Тема 9: Идентификация, аутентификация и учет в современных ОС
41. Что такое идентификация и аутентификация в контексте ОС?
42. Какие методы учёта действий пользователей реализуются в ОС?
43. Как обеспечивается уникальность идентификаторов пользователей?
44. Какие протоколы аутентификации используются в сетевых средах?
45. Как обеспечивается безопасность хранения учетных данных?
Тема 10: Аудит и его реализации в современных ОС
46. Что такое аудит безопасности и какова его цель?
47. Какие события обычно регистрируются в журналах аудита?
48. Какие инструменты используются для анализа журналов аудита?
49. Какие политики аудита поддерживаются в Windows/Linux/Android?
50. Как аудит помогает в расследовании инцидентов информационной безопасности?

5.2. Темы письменных работ

Не предусмотрены

5.3. Оценочные средства

Рабочая программа "Безопасность операционных систем" обеспечена оценочными средствами для проведения текущего контроля и промежуточной аттестации, включающими контрольные вопросы для проведения промежуточной аттестации, критерии оценивания учебной деятельности обучающихся по балльно-рейтинговой системе, примеры заданий для практических и лабораторных занятий, билеты для проведения промежуточной аттестации.
Все оценочные средства представлены в Приложении 1.

5.4. Перечень видов оценочных средств

Оценочные средства разработаны для всех видов учебной деятельности студента - лекций, практических занятий, самостоятельной работы и промежуточной аттестации. Оценочные средства представлены в виде:
- средства текущего контроля: проверочных работ по решению задач, дискуссии по теме;
- средств итогового контроля - промежуточной аттестации: экзамена в 4 семестре.

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

6.1. Рекомендуемая литература

6.1.1. Основная литература

	Авторы, составители	Заглавие	Издательство, год
Л1.1	Баланов А. Н.	Комплексная информационная безопасность: учебное пособие для вузов	Санкт-Петербург: Лань, 2025

6.3.1 Перечень программного обеспечения

6.3.1.1	Office Professional Plus 2019	
6.3.1.2	Windows 10	
6.3.1.3	МТС-Линк	Комплексная платформа для коммуникаций, обучения и совместной работы, разработанная с использованием современных технологий. Доступны десктопные и мобильные приложения для удобной работы с системой.

6.3.2 Перечень информационных справочных систем

6.3.2.1	Электронно-библиотечная система «Книжный Дом Университета» ("БиблиоТех")
6.3.2.2	Электронно-библиотечная система "Лань" Доступ к коллекциям электронных изданий ЭБС "Издательство "Лань"
6.3.2.3	База данных научных электронных журналов "eLibrary"

7. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Аудитория	Назначение	Оснащение	Вид
1	Специализированная многофункциональная учебная аудитория № 1 для проведения учебных занятий лекционного и семинарского типов, групповых и индивидуальных консультаций, текущего контроля и промежуточной/ итоговой аттестации	Столы обучающихся; Стулья обучающихся; Письменный стол педагогического работника; Стул педагогического работника; Кафедра; Магнитно-маркерная доска; Мультимедийный проектор; Экран; Ноутбук с возможностью подключения к сети «Интернет» и обеспечением доступа к электронной информационно-образовательной среде	

3	Специализированная многофункциональная учебная аудитория № 3 для проведения учебных занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной/ итоговой аттестации	Компьютерные столы обучающихся; Стулья обучающихся; Письменный стол педагогического работника; Стул педагогического работника; Стеллаж для учебно-методических материалов, в том числе учебно-наглядных пособий; Многофункциональное устройство (принтер, сканер, ксерокс); Интерактивная доска; Мультимедийный проектор; Ноутбуки с возможностью подключения к сети «Интернет» и обеспечением доступа к электронной информационно-образовательной среде	
5	Помещение № 5 для самостоятельной работы обучающихся	Письменный стол обучающегося; Стул обучающегося; Письменный стол обучающегося с ограниченными возможностями здоровья; Стул обучающегося с ограниченными возможностями здоровья; Ноутбук с возможностью подключения к сети «Интернет» и обеспечением доступа к электронной информационно-образовательной среде лицензиата; Моноблок (в том числе, клавиатура, мышь, наушники) с возможностью подключения к сети «Интернет» и обеспечением доступа к электронной информационно-образовательной среде	

Ауд. 8	Аудитория для научно-исследовательской работы обучающихся, курсового и дипломного проектирования № 8	Рабочие места на базе вычислительной техники с набором необходимых для проведения и оформления результатов исследований дополнительных аппаратных и/или программных средств; Письменный стол обучающегося; Стул обучающегося; Письменный стол обучающегося с ограниченными возможностями здоровья; Стул обучающегося с ограниченными возможностями здоровья; Ноутбук с возможностью подключения к сети «Интернет» и обеспечением доступа к электронной информационно-образовательной среде лицензиата; Моноблок (в том числе, клавиатура, мышь, наушники) с возможностью подключения к сети «Интернет» и обеспечением доступа к электронной информационно-образовательной среде; Многофункциональное устройство (принтер, сканер, ксерокс).	

8. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

Методические указания по изучению дисциплины "Безопасность операционных систем" представлены в Приложении 2 и включают в себя:
1. Методические указания для обучающихся по организации учебной деятельности.
2. Методические указания по организации самостоятельной работы обучающихся.
3. Методические указания по организации процедуры оценивания знания, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций.