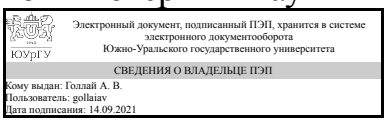
ЮЖНО-УРАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

УТВЕРЖДАЮ:
Директор института
Высшая школа электроники и компьютерных наук



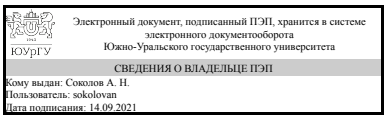
А. В. Голлай

РАБОЧАЯ ПРОГРАММА

дисциплины В.1.06 Безопасность операционных систем
для направления 10.03.01 Информационная безопасность
уровень бакалавр **тип программы** Бакалавриат
профиль подготовки Безопасность автоматизированных систем
форма обучения очная
кафедра-разработчик Защита информации

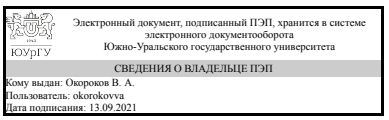
Рабочая программа составлена в соответствии с ФГОС ВО по направлению подготовки 10.03.01 Информационная безопасность, утверждённым приказом Минобрнауки от 01.12.2016 № 1515

Зав.кафедрой разработчика,
к.техн.н., доц.



А. Н. Соколов

Разработчик программы,
к.физ.-мат.н., доц., доцент



В. А. Окороков

Челябинск

1. Цели и задачи дисциплины

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. Задачи дисциплины: - изучение назначения и функций ОС; - приобретение навыков управления ресурсами и задачами в ОС; - освоение администрирования ОС; - изучение требований к защите ОС; - изучение методов и средств разграничения доступа в ОС; - изучение аудита в ОС; - формирование специальных теоретических и практических знаний, обеспечиващих возможность планирования политики безопасности ОС; - приобретение навыков эффективной и безопасной эксплуатацию ОС автоматизированных систем; - формирование специальных теоретических и практических знаний, обеспечиващих возможность проектировании средств защиты информации и средств контроля защищенности автоматизированных систем; - приобретение навыков эффективного применения информационно-технологических ресурсов ОС с учетом требований информационной безопасности; - приобретение навыков эффективного применения средств защиты информационно-технологических ресурсов ОС; - формирование специальных теоретических и практических знаний, позволяющих администрировать подсистему информационной безопасности автоматизированной системы; - формирование специальных теоретических и практических знаний, позволяющих обеспечить восстановление работоспособности систем защиты информации при возникновении нештатных ситуаций.

Краткое содержание дисциплины

Раздел 1. Основы функционирования ОС. Аппаратная поддержка работы ОС. Понятие супервизора. Назначение и функции операционных систем. Особенности архитектуры мобильных ОС на примере ОС Андроид. Управление задачами и ресурсами в ОС. Управления задачами в мобильных ОС. Автоматизация решения задач администрирования в ОС с использованием языков сценариев. Раздел 2. Безопасность ОС Требования к защите ОС. Классификация угроз безопасности ОС. Стандарты безопасности ОС. Концепция виртуализации. Виртуальные машины. Гипервизоры. Разграничение доступа в ОС. Субъекты, объекты, методы и права доступа. Идентификация и аутентификация с помощью аппаратных средств. Принцип минимизации привилегий. Понятие attack surface и его использование при организации защиты ОС. Аудит в ОС. Подсистемы безопасности ОС семейств Windows и Linux.

2. Компетенции обучающегося, формируемые в результате освоения дисциплины

Планируемые результаты освоения ОП ВО (компетенции)	Планируемые результаты обучения по дисциплине (ЗУНы)
ПСК-4.3 способностью планировать и организовывать комплекс мероприятий по защите информации, связанных с обеспечением надежности функционирования и отказоустойчивости аппаратных и программных	Знать:критерии оценки эффективности и надежности средств защиты операционных систем
	Уметь:использовать средства операционных

средств обработки информации	систем для обеспечения эффективного и безопасного функционирования систем обработки информации
	Владеть:навыками работы в операционных системах семейств Windows и Unix
ПК-3 способностью администрировать подсистемы информационной безопасности объекта защиты	Знать:базовые принципы организации и структуру подсистем защиты информации и разграничения доступа в операционных системах семейств UNIX и Windows; основные методы администрирования операционных систем семейств UNIX и Windows
	Уметь:формулировать политику безопасности операционных систем семейств UNIX и Windows
	Владеть:
ПК-9 способностью осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности	Знать:основные литературные источники, принципы построения и функционирования, примеры реализаций современных операционных систем
	Уметь:
	Владеть:
ОПК-5 способностью использовать нормативные правовые акты в профессиональной деятельности	Знать:критерии оценки эффективности и надежности средств защиты операционных систем
	Уметь:оценивать эффективность и надежность защиты операционных систем
	Владеть:
ПСК-4.2 способностью выполнять комплекс задач администрирования подсистем информационной безопасности операционных систем, систем управления базами данных, компьютерных сетей	Знать:принципы организации и структуру подсистем защиты операционных систем семейств UNIX и Windows; методы администрирования операционных систем семейств UNIX и Windows
	Уметь:формулировать и настраивать политику безопасности операционных систем семейств UNIX и Windows
	Владеть:навыками установки и настройки операционных систем семейств Windows и Unix с учетом требований по обеспечению информационной безопасности
ПСК-4.1 способностью учитывать и использовать особенности информационных технологий, применяемых в автоматизированных системах, при организации защиты обрабатываемой в них информации	Знать:принципы организации и структуру подсистем хранения данных в операционных системах семейств UNIX и Windows
	Уметь:
	Владеть:использования операционных систем семейств Windows и Unix с учетом требований по обеспечению информационной безопасности

3. Место дисциплины в структуре ОП ВО

Перечень предшествующих дисциплин, видов работ учебного плана	Перечень последующих дисциплин, видов работ
Б.1.16 Основы информационной безопасности, Б.1.17 Языки программирования	В.1.08 Безопасность систем баз данных, Б.1.21 Программно-аппаратные средства защиты информации

Требования к «входным» знаниям, умениям, навыкам студента, необходимым при освоении данной дисциплины и приобретенным в результате освоения предшествующих дисциплин:

Дисциплина	Требования
Б.1.16 Основы информационной безопасности	Знать: основные методы информационной безопасности. Уметь: применять основные методы обеспечения информационной безопасности на практике. Владеть: навыками обеспечения информационной безопасности
Б.1.17 Языки программирования	Знать: Методы разработки программ. Уметь: разрабатывать и проверять правильность программ. Владеть: навыками алгоритмизации.

4. Объём и виды учебной работы

Общая трудоемкость дисциплины составляет 5 з.е., 180 ч.

Вид учебной работы	Всего часов	Распределение по семестрам в часах
		Номер семестра
		5
Общая трудоёмкость дисциплины	180	180
Аудиторные занятия:	80	80
Лекции (Л)	32	32
Практические занятия, семинары и (или) другие виды аудиторных занятий (ПЗ)	32	32
Лабораторные работы (ЛР)	16	16
Самостоятельная работа (СРС)	100	100
Выполнение домашних заданий к практическим работам	100	100
Вид итогового контроля (зачет, диф.зачет, экзамен)	-	экзамен

5. Содержание дисциплины

№ раздела	Наименование разделов дисциплины	Объем аудиторных занятий по видам в часах			
		Всего	Л	ПЗ	ЛР
1	Основы функционирования ОС	54	22	16	16
2	Безопасность ОС	26	10	16	0

5.1. Лекции

№ лекции	№ раздела	Наименование или краткое содержание лекционного занятия	Кол-во часов
1	1	Назначение и функции операционных систем. Особенности архитектуры мобильных ОС на примере ОС Андроид..	4
2	1	Управление задачами в ОС. Управления задачами в мобильных ОС.	4
3	1	Управление данными и файловые системы	6

4	1	Диспетчеризация процессов	4
5	1	Управление памятью	4
6	2	Требования к защите ОС. Концепция виртуализации. Виртуальные машины. Гипервизоры.	2
7	2	Административные меры защиты. Аппаратно-программные средства защиты. Понятие attack surface и его использование при организации защиты ОС.	2
8	2	Аппаратные средства идентификации и аутентификации. Разграничение доступа в ОС.	2
9	2	Идентификация, аутентификация и учет в современных ОС	2
10	2	Аудит и его реализации в современных ОС	2

5.2. Практические занятия, семинары

№ занятия	№ раздела	Наименование или краткое содержание практического занятия, семинара	Кол-во часов
1	1	Средства управления работой операционной системы	4
2	1	Разграничение доступа к файлам	4
3	1	Система команд для работы с файловой системой	4
4	1	Сервисные команды	4
5	2	Сценарии, параметры и переменные среды	4
6	2	Операторы оболочки	4
7	2	Средства разработки сценариев	4
8	2	Разработка сценариев	4

5.3. Лабораторные работы

№ занятия	№ раздела	Наименование или краткое содержание лабораторной работы	Кол-во часов
1	1	Системные вызовы для управления процессами	4
2	1	Управление файловой системой	4
3	1	Разделяемая память и очереди сообщений	4
4	1	Сигналы	4

5.4. Самостоятельная работа студента

Выполнение СРС		
Вид работы и содержание задания	Список литературы (с указанием разделов, глав, страниц)	Кол-во часов
Выполнение домашних заданий	доп. лит. 6	100

6. Инновационные образовательные технологии, используемые в учебном процессе

Инновационные формы учебных занятий	Вид работы (Л, ПЗ, ЛР)	Краткое описание	Кол-во ауд. часов
Адаптивное обучение	Лабораторные занятия	Изучение темы системные вызовы для работы с файловой системой.	4
Проектный метод обучения	Практические занятия и семинары	Разработка проекта по теме "Защита памяти"	6
Интерактивная леция	Лекции	Групповое обсуждение темы	4

		"Управление данными"	

Собственные инновационные способы и методы, используемые в образовательном процессе

Не предусмотрены

Использование результатов научных исследований, проводимых университетом, в рамках данной дисциплины: нет

7. Фонд оценочных средств (ФОС) для проведения текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины

7.1. Паспорт фонда оценочных средств

Наименование разделов дисциплины	Контролируемая компетенция ЗУНы	Вид контроля (включая текущий)	№№ заданий
Все разделы	ПК-3 способностью администрировать подсистемы информационной безопасности объекта защиты	Защита отчета по практической работе	1
Все разделы	ПК-9 способностью осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности	Экзамен	2
Все разделы	ПСК-4.2 способностью выполнять комплекс задач администрирования подсистем информационной безопасности операционных систем, систем управления базами данных, компьютерных сетей	Тестирование	3
Все разделы	ОПК-5 способностью использовать нормативные правовые акты в профессиональной деятельности	Тестирование	1
Все разделы	ПСК-4.1 способностью учитывать и использовать особенности информационных технологий, применяемых в автоматизированных системах, при организации защиты обрабатываемой в них информации	Тестирование	4
Все разделы	ПСК-4.3 способностью планировать и организовывать комплекс мероприятий по защите информации, связанных с обеспечением надежности функционирования и отказоустойчивости аппаратных и программных средств обработки информации	Тестирование	5
Безопасность ОС	ПК-3 способностью администрировать подсистемы информационной безопасности объекта защиты	Практическая работа	8-14

7.2. Виды контроля, процедуры проведения, критерии оценивания

Вид контроля	Процедуры проведения и оценивания	Критерии оценивания
Тестирование	Каждый правильный ответ оценивается в 0,5 балла	Отлично: 10 правильных ответов Хорошо: 8 правильных ответов Удовлетворительно: 6 правильных ответов Неудовлетворительно: менее 6 правильных

		ответов
Экзамен	Вопросы к экзамену выдаются не менее чем за месяц до начала сессии. Экзамен проводится письменно. Ответы студентов хранятся до начала следующего семестра. Письменные ответы проверяются преподавателем. По результатам проверки выставляется экзаменационная оценка	Отлично: Оценка «Отлично» выставляется за ответ, который полностью раскрывает поставленный вопрос. Студент показывает глубокое знание вопросов темы, свободно оперирует терминами предметной области и легко отвечает на поставленные вопросы. Хорошо: Оценка «Хорошо» выставляется за ответ, который полностью соответствует поставленному вопросу. Ответ демонстрирует хорошее владение материалом и наличие навыков решения поставленных задач. Ответ содержит последовательное изложение материала с соответствующими выводами, однако, положения ответа не всегда достаточной степени обоснованы, а используемая терминология не всегда корректна. Удовлетворительно: Оценка «Удовлетворительно» выставляется за ответ, который не полностью соответствует поставленному вопросу, содержит незначительные пробелы в излагаемом материале. Студент в недостаточной степени владеет общепринятой терминологией, а также слабыми навыками решения прикладных задач Неудовлетворительно: Неудовлетворительно: Оценка «Неудовлетворительно» выставляется за ответ, который не соответствует поставленному вопросу. Студент демонстрирует существенные пробелы в знаниях и недостаточный уровень навыков при решении практических задач. В ответе допускаются существенные ошибки.

7.3. Типовые контрольные задания

Вид контроля	Типовые контрольные задания
Тестирование	При замене пользовательского контекста процесса: а) Заменяется содержимое областей кода, данных и стека. б) Удаляются области кода, данных и стека. в) Заменяется содержимое области кода. г) Удаляется стек старой программы. Тесты ОС 10.03.01 .pdf
Экзамен	1. Понятие операционной системы. ОС как расширенная машина. ОС как система управления ресурсами. 2. Поколения ОС. Классификация ОС. 3. Понятие мультипрограммирования. Концептуальная схема компьютера. 4. Общее устройство и принципы работы. Переключение процессора с выполнения одной программы на другую. Централизации управления устройствами. Планирование процессора. 5. Прерывания. Понятие прерывания. Типы прерываний. Общая схема обработки прерываний. Маскирование прерываний. Контроллер прерываний. 6. Память. Методы сокращения времени доступа к памяти и обеспечения

	достаточного объема памяти. Принципы распределения и защиты основной памяти. 7. Процессы. 8. Устройства ввода-вывода и хранения данных. Контроллеры и их функции. 9. Интерфейс ОС с прикладными программами. 10. Абстрактная модель файлов. Базовые структурные свойства файлов. Базовые операции с файлами. 11. Понятие, компоненты и функции файловой системы. 12. Логическая структура файловой системы. Директории и их структура. 13. Иерархические файловые системы. 14. Идентификация файлов. Преобразование имени файла в ссылку на его местоположение. Основные операции над директориями. 15. Связывание файлов. 16. Монтирование файловых систем. 17. Защита файлов и контроль доступа. 18. Реализация модели файлов и основные управляющие структуры. Структура интерфейса процессов с файловой системой. 19. Методы выделения дискового пространства. Преобразование текущей позиции в адрес дискового блока. 20. Управление свободным дисковым пространством.. Распределение дискового пространства. 21. Реализация директорий. Примеры реализация директорий в различных ОС. 22. Надежность файловой системы. Целостность файловой системы. Средства и методы обеспечения целостности. 23. Алгоритмы восстановления целостности. 24. Производительность файловой системы. 25. Алгоритмы реализации некоторых файловых операций в UNIX: открытие файла; чтение файла; запись в файл; закрытие файла. 26. Состояния процессов. Блок управления процессом. Контекст процесса. 27. Операции над процессами. Одноразовые операции, их свойства и методы реализации. Процессы-зомби. 28. Многоразовые операции. Переключение контекста. 29. Нити исполнения. Модель потока и понятие нити исполнения. Состояния нитей и их связь с состояниями процесса. Методы реализации нитей. 30. Управление процессами в UNIX. Состояния процессов в UNIX. Управляющие структуры данных. Алгоритмы работы системных функций и операции над процессами в UNIX. 31. Взаимодействие между процессами. Причины взаимодействия процессов. Категории средств обмена информацией. 32. Конфликты и состояние состязания. Критические области. Взаимное исключение. 33. Условия правильной реализации взаимного исключения. 34. Алгоритмы синхронизации процессов. 35. Проблема производителя и потребителя. 36. Семафоры. Решение проблемы производителя и потребителя с помощью семафоров. Сообщения. Решение проблемы производителя и потребителя с помощью сообщений. 37. Уровни планирования. Критерии планирования и требования к алгоритмам. Параметры планирования. 38. Вытесняющее и невытесняющее планирование. 39. Алгоритм «Первым пришел - первый обслужен» (FCFS). Алгоритм планирования «Карусель» (RR). 40. Оценки среднего времени ожидания и среднего полного времени выполнения. Приоритетное планирование. 41. Статические приоритеты и многоуровневые очереди. Динамические приоритеты и многоуровневые очереди с обратной связью. 42. Базовые принципы управления памятью. Основные функции ОС по управлению

	памятью. 43. Схема с фиксированными разделами, таблица разделов. Оверлейная структура программ. 44. Схема с переменными разделами. Свопинг. Внешняя фрагментация и методы борьбы с ней. Учет свободных и занятых участков памяти. 45. Виртуальная память. Страничная память. Таблицы страниц. Общая структура и назначение полей таблицы страниц. 46. Буфер быстрого преобразования адреса. Многоуровневые таблицы страниц. Инвертированные таблицы страниц. 47. Исключительные ситуации при работе с памятью. Стратегии выборки и замещения. Алгоритмы замещения страниц. 48. Оптимальный алгоритм. Алгоритм FIFO. Алгоритм NRU. Алгоритм LRU. Алгоритм NFU и его реализация. 49. Пробуксовка. Модель рабочего множества. Замещение страниц в многозадачной среде. Демоны системы управления памятью. 50. Безопасные системы и угрозы безопасности. Роль операционных систем в обеспечении информационной безопасности. 51. Идентификация и аутентификация пользователя. 52. Авторизация и методы разграничения доступа. 53. Методы реализации дискреционной модели доступа. 54. Многоуровневый доступ. 55. Контроль повторного использования объектов. Анализ тайных каналов передачи информации. Аудит и протоколирование системы защиты. 56. Требования надежности систем безопасности. 57. Понятие классов безопасности. 58. Средства обеспечения безопасности современных операционных системах.

8. Учебно-методическое и информационное обеспечение дисциплины

Печатная учебно-методическая документация

а) основная литература:

Не предусмотрена

б) дополнительная литература:

1. Партыка, Т. Л. Операционные системы, среды и оболочки Учеб. пособие для сред. проф. образования по специальностям информтики и вычисл. техники Т. Л. Партыка, И. И. Попов. - М.: Форум, 2006. - 399 с.
2. Окороков, В. А. Операционные системы [Текст] курс лекций В. А. Окороков ; Челяб. гос. ун-т. - Челябинск: Издательство Челябинского государственного универси, 2011

в) отечественные и зарубежные журналы по дисциплине, имеющиеся в библиотеке:

1. IEEE transactions on automatic control: науч. журн./IEEE Control Systems Soc.New York : Institute of Electrical and Electronics Engineers
2. IEEE/ACM transactions on networking: науч.-техн. журн. / IEEE Communications Soc.;IEEE Computer Soc. ; ACM with its Special Interest Group on Data Communication; New York : Institute of Electrical and Electronics Engineers : The Association for Computing Machinery
3. IEEE transactions on computers: науч. журн. / IEEE Computer Soc. New York : Institute of Electrical and Electronics Engineers
4. IEEE software:науч. журн./IEEE Computer Soc.Los Alamitos, CA : IEEE Computer Society

5. IEEE transactions on software engineering: науч. журн. / IEEE Computer Soc.Выходные данные: New York : Institute of Electrical and Electronics Engineers

6. IEEE transactions on computers: науч.-техн. журн./IEEE Computer Soc.Выходные данные: New York : Institute of Electrical and Electronics Engineers

г) методические указания для студентов по освоению дисциплины:

1. Конспект лекций "Безопасность операционных систем"

из них: учебно-методическое обеспечение самостоятельной работы студента:

2. Конспект лекций "Безопасность операционных систем"

Электронная учебно-методическая документация

№	Вид литературы	Наименование разработки	Наименование ресурса в электронной форме	Д (се ло авт / с
1	Дополнительная литература	Мартемьянов Ю.Ф., Яковлев Ал.В., Яковлев Ан.В. Операционные системы. Концепции построения и обеспечения безопасности. Изд "Горячая линия-Телеком", 2011, 332 с.	Электронно-библиотечная система издательства Лань	Ин Ав
2	Основная литература	Окороков, В. А. Безопасность операционных систем [Текст : непосредственный] : курс лекций для специальностей 10.03.01, 10.05.03 / В. А. Окороков ; Юж.-Урал. гос. ун-т, Каф. Защита информации ; ЮУрГУ, Челябинск : Издательский Центр ЮУрГУ , 2020 URL http://www.lib.susu.ac.ru/ftd?base=SUSU_METHOD&key=000569542 Объем 242, [1] с. : ил. + электрон. версия	Электронный каталог ЮУрГУ	Ин Сво
3	Основная литература	Староверова, Н. А. Операционные системы : учебник для спо / Н. А. Староверова. — Санкт-Петербург : Лань, 2021. — 412 с. — ISBN 978-5-8114-6385-5. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/162376 (дата обращения: 13.09.2021). — Режим доступа: для авториз. пользователей.	Электронно-библиотечная система издательства Лань	Ин Ав
4	Основная литература	Кручинин, А. Ю. Операционные системы : учебное пособие / А. Ю. Кручинин. — Оренбург : ОГУ, 2019. — 152 с. — ISBN 978-5-7410-2306-8. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/159896 (дата обращения: 13.09.2021). — Режим доступа: для авториз. пользователей.	Электронно-библиотечная система издательства Лань	Ин Ав

9. Информационные технологии, используемые при осуществлении образовательного процесса

Перечень используемого программного обеспечения:

1. Microsoft-Windows server(бессрочно)
2. Microsoft-Windows(бессрочно)
3. Microsoft-Office(бессрочно)
4. Microsoft-Visual Studio(бессрочно)

Перечень используемых информационных справочных систем:

1. -Thr Cambridge Cristallographic Data Centre(бессрочно)
2. -База данных ВИНИТИ РАН(бессрочно)

10. Материально-техническое обеспечение дисциплины

Вид занятий	№ ауд.	Основное оборудование, стенды, макеты, компьютерная техника, предустановленное программное обеспечение, используемое для различных видов занятий
Практические занятия и семинары	906 (3б)	Комплект компьютерного оборудования, проектор, коммутатор, экран для проектора, программное обеспечение: ОС Windows XP , MS Office 2007, Matlab, WinRar, Mozila Firefox, Virtual Box, Ms Visual Studio Express.
Лабораторные занятия	906 (3б)	Комплект компьютерного оборудования, проектор, коммутатор, экран для проектора, программное обеспечение: ОС Windows XP , MS Office 2007, Matlab, WinRar, Mozila Firefox, Virtual Box, Ms Visual Studio Express.
Лекции	912 (3б)	Комплект компьютерного оборудования, LCD Проектор, Экран проекционный, настенные стенды по защите информации (5 шт.), программное обеспечение: ОС Windows XP , MS Office 2007, Matlab, WinRar, Mozila Firefox, Консультант+.