



**РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ**  
**Б1.В.01.01 Безопасность операционных систем**

**Направление подготовки:** *10.03.01 Информационная безопасность*

**Направленность (профиль):** *Организация и технологии защиты информации (по отрасли или в сфере профессиональной деятельности)*

**Квалификация (степень):** *бакалавр*

**Форма обучения:** *очная*

**Институт:** математики, естествознания и техники

**Кафедра:** математического моделирования, компьютерных технологий и информационной безопасности

	очная форма	очно-заочная форма	заочная форма
Курс	3		
Семестр/триместр	5		

Лекции	18		
Лабораторные занятия	18		
Практические (семинарские) занятия			
в т. ч. практическая подготовка	2		
Консультации	-		
Форма(ы) промежуточной аттестации	Зачет		
Контроль	-		
Иные формы работы	-		
Самостоятельная работа	72		

**Всего часов:** 108

**Трудоемкость:** 3 зачетные единицы.

Разработчик(и) рабочей программы:

кандидат педагогических наук, доцент Д.А. Таров

# I. ОРГАНИЗАЦИОННО-МЕТОДИЧЕСКИЙ РАЗДЕЛ

## Цель изучения дисциплины:

Целью освоения дисциплины «Б1.В.01.03 Безопасность операционных систем» 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.

## Задачи изучения дисциплины:

Задачами изучения дисциплины «Б1.В.01.03 Безопасность операционных систем» являются:

- получение знаний о защитных механизмах и средствах обеспечения безопасности операционных систем, средствах и методах аутентификации пользователей в операционных системах, средствах и методах управления доступом в операционных системах, средствах и методах реализации политики аудита в операционных системах, средствах и методах управления процессами в операционных системах, средствах и методах антивирусной защиты в операционных системах, средствах и методах интеграции операционных систем в компьютерную сеть;
- приобретение умения применять средства обеспечения безопасности операционных систем; определять и классифицировать угрозы информационной безопасности операционных систем; формулировать, настраивать и реализовывать политику безопасности операционных систем;
- приобретение практических навыков применения защитных механизмов и средств обеспечения информационной безопасности операционных систем, определения и классификации угроз информационной безопасности операционных систем, формулирования требований информационной безопасности к операционным системам,

**Место дисциплины в структуре ОПОП** реализуется в рамках вариативной части (части, формируемой участниками образовательных отношений) блока Б1. Дисциплины (модули).

## Планируемые результаты обучения по дисциплине:

Код компетенции	Индикаторы компетенции	Планируемые результаты обучения по дисциплине
ПКС-1	<b>Знать:</b> <ul style="list-style-type: none"><li>- сущность и понятие информационной безопасности, характеристику ее составляющих, источники угроз и меры по их предотвращению;</li><li>- методы и средства управления информационной безопасностью, а также основные подходы к разработке, реализации, эксплуатации, диагностике, анализу, сопровождению и совершенствованию систем защиты информации.</li></ul>	<b>Знает:</b> <ul style="list-style-type: none"><li>- требования к политике безопасности основных операционных систем;</li><li>- требования к подсистеме аудита и политике аудита;</li><li>- источники и классификацию угроз информационной безопасности;</li><li>- защитные механизмы и средства обеспечения безопасности операционных систем.</li></ul>
	<b>Уметь:</b> <ul style="list-style-type: none"><li>- оценивать защищенность, классифицировать основные угрозы, обеспечивать информационную безопасность компьютерных систем, применяя необходимые программно-аппаратные средства и си-</li></ul>	<b>Умеет:</b> <ul style="list-style-type: none"><li>- формулировать и настраивать политику безопасности основных операционных систем, а также локальных компьютерных сетей, построенных на их основе;</li><li>- применять защитные механизмы и средства обеспечения безопасности опе-</li></ul>

	<p>стемы защиты информации;</p> <ul style="list-style-type: none"> <li>- принимать управленческие и административные решения в сфере защиты информации.</li> </ul>	рациональных систем.
	<p><b>Владеть:</b></p> <ul style="list-style-type: none"> <li>- категориальным аппаратом в области обеспечения комплекса мер по администрированию и диагностике систем защиты информации;</li> <li>- правилами, методами, средствами, процедурами управления и администрирования информационной безопасностью объекта.</li> </ul>	<p><b>Владеет:</b></p> <ul style="list-style-type: none"> <li>– навыками определения и классификации угроз информационной безопасности;</li> <li>– навыками конфигурирования и администрирования операционных систем в рамках реализации политики безопасности;</li> <li>– навыками применения защитных механизмов и средств обеспечения безопасности операционных систем.</li> </ul>

## II. СОДЕРЖАНИЕ И ОБЪЕМ ДИСЦИПЛИНЫ

с указанием количества часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу

### Очная форма обучения

№ п/п	Наименование разделов и тем	Всего	Аудиторные занятия			Сам. раб.
			ЛК	ПЗ	ЛБ	
1.	Тема 1. «Понятия операционной системы: процесс, адресное пространство, файл, ввод-вывод, шины. Системные вызовы. Монолитные системы, микроядра, виртуальные машины»	12	2		2	8
2.	Тема 2. «Процессы и потоки. Модель процесса, состояние процессов, моделирование режима многозадачности. Реализация потоков. Алгоритм активации планировщика»	12	2		2	8
3.	Тема 3. «Планирование в пакетных и интерактивных системах. Системы реального времени. Планирование потоков. Управление памятью. Виртуальная память. Страничная организация памяти»	12	2		2	8
4.	Тема 4. «Системы страничной организации памяти. Управление загрузкой. Разделение пространства команд и данных. Совместно используемые страницы и библиотеки. Политика очистки страниц. Интерфейс виртуальной памяти. Сегментация со страничной организацией памяти. Файловые системы. Файловые системы с журнальной структурой. Виртуальные файловые системы.»	12	2		2	8
	Тема 5. «Ввод и вывод информации. Устройства и контроллеры устройств ввода-вывода. ПО ввода-вывода. Ввод-вывод, управляемый прерываниями. Ввод-вывод с помощью	12	2		2	8

	DMA. Аппаратная часть дисков. Алгоритмы планирования перемещения блока головок. Обработка ошибок. Аппаратная составляющая часов. Программируемые таймеры. Управление энергопотреблением.»					
	Тема 6. «Взаимоблокировка. Выгружаемые и невыгружаемые ресурсы. Условия возникновения ресурсных взаимоблокировок. Предотвращение взаимоблокировки. Двухфазное блокирование. Активная взаимоблокировка. Зависание.»	12	2		2	8
	Тема 7. «Технологии виртуализации. Гипервизоры первого и второго типа. Аппаратная поддержка вложенных таблиц страниц. Возвращение памяти. Виртуализация ввода-вывода. Домены устройств»	12	2		2	8
	Тема 8. «Многопроцессорные системы. Низкоуровневые коммуникационные программы мультимикомпьютеров. Планирование мультимикомпьютеров. Вызовы удаленных процедур. Балансировка нагрузки. Управление доступом к ресурсам. Аутентификация и авторизация в современных операционных системах. Атаки переполнения буфера. Атаки, использующие форматирующую строку. Указатели на несуществующие объекты»	12	2		2	8
	Тема 9. «Брандмауэры. Антивирусные технологии. Электронная подпись программ. Современные исследования в области безопасности операционных систем»	12	2		2	8
	<i>Контроль</i>					
	<i>Консультация</i>					
	<i>Зачет</i>					
	<i>Итого за 5 семестр</i>	108	18		18	72
	<i>в т.ч. практическая подготовка</i>				2	
	<b>ИТОГО:</b>	108	18		18	72

**Очно-заочная форма обучения (не реализуется)**

**Заочная форма обучения (не реализуется)**

### **III. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕЙ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ**

Текущая аттестация проводится в форме теста.

#### **Типовой вариант теста**

### **Вопросы теста №1**

1. Понятие процесса.
2. Понятие адресного пространства.
3. Понятие файла.
4. Понятие ввода-вывода.
5. Понятие шины.
6. Системные вызовы.
7. Монолитные системы.
8. Микроядра.
9. Виртуальные машины.
10. Модель процесса.
11. Планирование в интерактивных системах.
12. Планирование в системах реального времени.

### **Вопросы теста №2**

1. Атака условия невыгружаемости.
2. Атака условия циклического ожидания.
3. Двухфазное блокирование. Активная взаимоблокировка. Зависание.
4. Технологии виртуализации. Гипервизоры первого и второго типа.
5. Аппаратная поддержка вложенных таблиц страниц. Возвращение памяти.
6. Планирование мультимикомпьютеров.
7. Вызовы удаленных процедур.
8. Балансировка нагрузки.
9. Аутентификация и авторизация в современных операционных системах.
10. Атаки переполнения буфера.
11. Атаки, использующие форматирующую строку.
12. Указатели на несуществующие объекты.

Промежуточная аттестация обучающихся осуществляется в форме зачета с использованием следующих оценочных материалов: вопросы к зачету.

### **Вопросы к зачету (5 семестр, очная форма обучения)**

1. Понятие процесса. Понятие адресного пространства. Понятие файла.
2. Понятие ввода-вывода. Понятие шины.
3. Системные вызовы.
4. Монолитные системы. Микроядра.
5. Виртуальные машины.
6. Модель процесса. Состояние процессов. Моделирование режима многозадачности.
7. Реализация потоков в пользовательском пространстве, Реализация потоков в ядре.
8. Алгоритм активации планировщика. Планирование в пакетных, интерактивных системах и системах реального времени.
9. Виртуальная память. Страничная организация памяти.
10. Файловые системы. Свойства файлов. Файловые системы с журнальной структурой. Виртуальные файловые системы.
11. ПО ввода-вывода. Ввод-вывод, управляемый прерываниями. Ввод-вывод с помощью DMA.
12. Условия возникновения ресурсных взаимоблокировок. Обнаружение взаимоблокировок разных типов. Двухфазное блокирование. Активная взаимоблокировка. Зависание.
13. Технологии виртуализации. Гипервизоры первого и второго типа. Виртуализация ввода-вывода. Домены устройств.

14. Многопроцессорные системы. Коммуникационные программы мультимедийных компьютеров. Планирование мультимедийных компьютеров.
15. Вредоносные программы. Брандмауэры. Антивирусные технологии. Электронная подпись программ.

## IV. ПЕРЕЧЕНЬ ЛИТЕРАТУРЫ, НЕОБХОДИМОЙ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ

### 4.1. Основная литература

1. Власенко, А.Ю. Операционные системы : учебное пособие : [16+] / А.Ю. Власенко, С.Н. Карабцев, Т.С. Рейн ; Кемеровский государственный университет. – Кемерово : Кемеровский государственный университет, 2019. – 161 с. : ил., табл. – Режим доступа: по подписке. – URL: <https://biblioclub.ru/index.php?page=book&id=574269> . – Библиогр. в кн. – ISBN 978-5-8353-2424-8. – Текст : электронный.

### 4.2. Дополнительная литература

1. Кобылянский, В.Г. Операционные системы, среды и оболочки : учебное пособие : [16+] / В.Г. Кобылянский ; Новосибирский государственный технический университет. – Новосибирск : Новосибирский государственный технический университет, 2018. – 80 с. : ил., табл. – Режим доступа: по подписке. – URL: <https://biblioclub.ru/index.php?page=book&id=576354> . – Библиогр.: с. 77. – ISBN 978-5-7782-3517-5. – Текст : электронный.
2. Курячий, Г.В. Операционная система Linux : учебник : [16+] / Г.В. Курячий, К.А. Маслинский. – 2-е изд., исправ. – Москва : Национальный Открытый Университет «ИНТУИТ», 2016. – 451 с. : ил. – Режим доступа: по подписке. – URL: <https://biblioclub.ru/index.php?page=book&id=578058> . – Библиогр.: с. 450. – ISBN 5-9556-0029-9. – Текст : электронный.

## V. ПЕРЕЧЕНЬ РЕСУРСОВ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ «ИНТЕРНЕТ», НЕОБХОДИМЫХ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ

№ пп	Ссылка на информационный ресурс	Наименование разработки в электронной форме	Доступность
1.	<a href="http://www.biblioclub.ru">http://www.biblioclub.ru</a>	Электронно-библиотечная система (ЭБС) Университетская библиотека онлайн	Свободный доступ
2.	<a href="http://edu.ru/">http://edu.ru/</a>	<b>Российское образование: Федеральный портал.</b> Включает ссылки на порталы и сайты образовательных учреждений; государственные образовательные стандарты; нормативные документы; каталог экскурсий и обучающих программ.	Свободный доступ
3.	<a href="http://www.elibrary.ru">www.elibrary.ru</a>	Российский информационный портал в области науки, технологии, медицины и образования	Свободный доступ

## **VI. СОВРЕМЕННЫЕ ПРОФЕССИОНАЛЬНЫЕ БАЗЫ ДАННЫХ И ИНФОРМАЦИОННЫЕ СПРАВОЧНЫЕ СИСТЕМЫ**

1.	<a href="http://ilib.mccme.ru">http://ilib.mccme.ru</a>	ЭБ с книгами по математике	Свободный доступ
2.	<a href="https://e.lanbook.com/">https://e.lanbook.com/</a>	ЭБС Лань	Регистрация через компьютер Научной библиотеки ЕГУ. Доступ с компьютеров библиотеки.

## **VII. ЛИЦЕНЗИОННОЕ И СВОБОДНО РАСПРОСТРАНЯЕМОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ**

При реализации учебной дисциплины применяется следующее лицензионное и свободно распространяемое программное обеспечение:

- Microsoft Windows;
- Microsoft Office;
- LibreOffice,
- Kaspersky Endpoint Security 11,
- Smart Notebook 17 и др.

## **VIII. ОБОРУДОВАНИЕ И ТЕХНИЧЕСКИЕ СРЕДСТВА ОБУЧЕНИЯ, НЕОБХОДИМЫЕ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ**

Учебные занятия проводятся в аудиториях, укомплектованных специализированной мебелью, в том числе стационарными или переносными техническими средствами обучения (проектор, экран, компьютер/ноутбук).

Лабораторные занятия, групповые и индивидуальные консультации, текущая и промежуточная аттестации проводятся в специализированных классах, оснащенных автоматизированными рабочими местами с компьютерами.

Самостоятельная работа проводится в кабинетах, оснащенных компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду университета.