Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
**«Владимирский государственный университет
имени Александра Григорьевича и Николая Григорьевича Столетовых»
(ВлГУ)**

Институт информационных технологий и радиоэлектроники

УТВЕРЖДАЮ:
Директор института
_____ Галкин А.А.
«_01_» _июня_ 2023 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Безопасность операционных систем»

направление подготовки / специальность

10.03.01 «Информационная безопасность»
(код и наименование направления подготовки (специальности)

направленность (профиль) подготовки

**Безопасность автоматизированных систем
(по отраслям или в сфере профессиональной деятельности)**
(направленность (профиль) подготовки))

г. Владимир

2023 год

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Целями освоения дисциплины *Безопасность операционных систем* являются обеспечение подготовки бакалавров в соответствии с требованиями ФГОС ВО и учебного плана по направлению 10.03.01 «Информационная безопасность», ознакомление студентов с основными методами и технологиями, назначением и функционированием механизмов обеспечения информационной безопасности операционных систем (ОС). Курс предусматривает углубленное изучение внутреннего устройства и алгоритмов работы основных компонентов современных операционных систем MS Windows, и UNIX, освоение функций системного программного интерфейса Win32 API и принципов обеспечения безопасности для ОС MS Windows.

Задачей изучения дисциплины является освоение следующих разделов:

- организации процессов и потоков, моделирование режима многозадачности. Потоки в POSIX. Реализация потоков в пользовательском пространстве, в ядре, гибридная реализация;

- взаимодействия процессов. Критические области. Синхронизационные примитивы;

- планирование в пакетных системах и в интерактивных системах. Системы реального времени. Планирование потоков. Классические задачи взаимодействия процессов;

-вопросы управление памятью. Страничная организация памяти, таблицы страниц. Алгоритмы замещения страниц: алгоритм LRU, алгоритм WSClock, алгоритм "рабочий набор";

изучение системы страничной организации памяти. Сегментация со страничной организацией памяти;

- файловые системы. Файловые системы с журнальной структурой. Журналируемые файловые системы. Оценка производительности ФС;

- ПО ввода-вывода. Ввод-вывод, управляемый прерываниями. Ввод-вывод с помощью DMA. Обработчики прерываний, драйверы устройств. Слой абстракции от оборудования (HAL);

- взаимоблокировка. Выгружаемые и невыгружаемые ресурсы. Условия возникновения ресурсных взаимоблокировок. Обнаружение взаимоблокировок разных типов. Уклонение от взаимоблокировок;

-технологии виртуализации. Гипервизоры первого и второго типа. Аппаратная поддержка вложенных таблиц страниц. Домены устройств;

-виртуальные машины на мультиядерных центральных процессорах. Виртуализация на примере продуктов VmWare;

-управление доступом к ресурсам. Реализация формальных моделей безопасности в операционных системах. Криптопроцессоры и криптопровайдеры. Аутентификация и авторизация в современных операционных системах;

- атаки переполнения буфера. Атаки, использующие форматирующую строку. Указатели на несуществующие объекты. Атаки, использующие внедрение команд. Инсайдерские атаки. Вредоносные программы;

-брандмауэры. Антивирусные технологии. Электронная подпись программ. Инкапсулированный код. Современные исследования в области безопасности операционных систем и т.д.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Дисциплина *Безопасность операционных систем* относится к обязательным дисциплинам обязательной части Блока Б1 (код Б1.О.03). В учебном плане предусмотрены виды учебной деятельности, обеспечивающие синтез теоретических лекций, лабораторных работ и самостоятельной работы студентов. Курс тесно взаимосвязан с другими дисциплинами данного цикла.

3. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ

Планируемые результаты обучения по дисциплине, соотнесенные с планируемыми результатами освоения ОПОП (компетенциями и индикаторами достижения компетенций)

Формируемые компетенции (код, содержание компетенции)	Планируемые результаты обучения по дисциплине, в соответствии с индикатором достижения компетенции		Наименование оценочного средства
	Индикатор достижения компетенции *(код, содержание индикатора)*	Результаты обучения по дисциплине	
ОПК-2 Способен применять информационно-коммуникационные технологии, программные средства системного и прикладного назначения, в том числе отечественного производства, для решения задач профессиональной деятельности	ОПК-2.1.1.	Знать эталонную модель взаимодействия открытых систем, методы коммутации и маршрутизации, сетевые протоколы	Тестовые вопросы
	ОПК-2.1.2.	Знать основные виды политик управления доступом и информационными потоками в компьютерных системах	
	ОПК-2.1.3.	Знать защитные механизмы и средства обеспечения безопасности операционных систем	
	ОПК-2.1.4.	Знать средства и методы хранения и передачи аутентификационной информации	
	ОПК-2.1.5.	Знать требования к подсистеме аудита и политике аудита	
	ОПК-2.1.6.	Знать принципы построения современных операционных систем и особенности их применения	
	ОПК-2.2.1.	Уметь выбирать необходимые инструментальные средства для разработки программ в различных операционных системах и средах	
	ОПК-2.2.2.	Уметь формулировать и настраивать политику безопасности операционных систем, а также локальных вычислительных сетей, построенных на их основе	
	ОПК-2.2.3.	Уметь осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты	
	ОПК-2.2.4.	Уметь применять основные виды политик управления доступом и информационными потоками в компьютерных системах	
	ОПК-2.2.5.	Уметь основные формальные модели дискреционного, мандатного, ролевого управления доступом, модели изолированной программной среды и безопасности информационных потоков	
	ОПК-2.2.6.	Уметь формулировать и настраивать политику безопасности основных операционных систем, а также локальных компьютерных сетей, построенных на их основе	
	ОПК-2.3.1.	Владеть навыками формирования частных политик безопасности компьютерных систем, в том числе политики управления доступом и информационными потоками	

	ОПК-2.3.2.	Владеть навыками разработки программных модулей, реализующих задачи, связанные с обеспечением безопасности операционных систем распространенных семейств	
	ОПК-2.3.3.	Владеть навыками конфигурирования и администрирования операционных систем	
ОПК-10 Способен в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты	ОПК-10.1.1	Знать основные виды политик управления доступом и информационными потоками в компьютерных системах	Тестовые вопросы
	ОПК-10.1.2	Знать защитные механизмы и средства обеспечения безопасности операционных систем	
	ОПК-10.1.3	Знать средства и методы хранения и передачи аутентификационной информации	
	ОПК-10.1.4	Знать требования к подсистеме аудита и политике аудита	
	ОПК-10.2.1	Уметь формулировать и настраивать политику безопасности операционных систем, а также локальных вычислительных сетей, построенных на их основе	
	ОПК-10.2.2	Уметь применять основные виды политик управления доступом и информационными потоками в компьютерных системах	
	ОПК-10.2.3	Уметь основные формальные модели дискреционного, мандатного, ролевого управления доступом, модели изолированной программной среды и безопасности информационных потоков	
	ОПК-10.2.4	Уметь формулировать и настраивать политику безопасности основных операционных систем, а также локальных компьютерных сетей, построенных на их основе	
	ОПК-10.3.1	Владеть навыками формирования частных политик безопасности компьютерных систем, в том числе политики управления доступом и информационными потоками	
	ОПК-10.3.2	Владеть навыками конфигурирования и администрирования операционных систем	
ОПК-4.2 Способен администрировать операционные системы, системы управления базами данных, вычислительные сети	ОПК-4.2-1.1	Знать средства, методы и протоколы идентификации, аутентификации и авторизации	Тестовые вопросы
	ОПК-4.2-2.1	Уметь устанавливать и настраивать операционные системы, системы управления базами данных, компьютерные сети и программные системы с учетом требований по обеспечению защиты информации	
	ОПК-4.2-2.2	Уметь управлять полномочиями пользователей	
	ОПК-4.2-3.1	Владеть навыками формирования частных политик безопасности компьютерных систем, в том числе политики управления доступом и информационными потоками	

4. ОБЪЕМ И СТРУКТУРА ДИСЦИПЛИНЫ

Трудоемкость дисциплины составляет 3 зачетных единиц, 108 часов

Тематический план
форма обучения – очная

№ п/п	Наименование тем и/или разделов/тем дисциплины	Семестр	Неделя семестра	Контактная работа обучающихся с педагогическим работником				Самостоятельная работа	Формы текущего контроля успеваемости, форма промежуточной аттестации *(по семестрам)*
				Лекции	Практические занятия	Лабораторные работы	*в форме практической подготовки*		
1.	Введение. Понятия операционной системы: процесс, адресное пространство, файл, ввод-вывод, шины. Системные вызовы.	4	1	2				2	
2.	Процессы и потоки. Модель процесса, состояние процессов, моделирование режима многозадачности.	4	2	2		4		2	
3.	Взаимодействие процессов. Состязательные ситуации. Критические области. Синхронизационные примитивы	4	3	2				2	
4.	Планирование в пакетных системах. Планирование в интерактивных системах. Системы реального времени.	4	4	2		4		2	
5.	Управление памятью. Виртуальная память. Страничная организация памяти, таблицы страниц.	4	5	2				2	
6.	Системы страничной организации памяти. Управление загрузкой. Разделение пространства команд и данных.	4	6	2		4		2	Рейтинг-контроль №1
7.	Файловые системы. Свойства файлов. Файловые системы с журнальной структурой.	4	7	2				2	
8	Ввод и вывод информации. Устройства и контроллеры устройств ввода-вывода.	4	8	2		4		2	
9.	ПО ввода-вывода. Ввод-вывод, управляемый прерываниями. Ввод-вывод с помощью DMA. Обработчики прерываний, драйверы устройств.	4	9	2				2	
10.	Аппаратная часть дисков. Алгоритмы планирования перемещения блока головок. Обработка ошибок.	4	10	2		4		2	
11.	Взаимоблокировка. Выгружаемые и невыгружаемые ресурсы. Условия возникновения ресурсных взаимоблокировок	4	11	2				2	

12.	Предотвращение взаимоблокировки. Атака условия взаимного исключения. Атака условия удержания и ожидания.	4	12	2		4		2	Рейтинг-контроль №2
13.	Технологии виртуализации. Гипервизоры первого и второго типа. Аппаратная поддержка вложенных таблиц страниц. Возвращение памяти.	4	13	2				2	
14.	Виртуальные машины на мультиядерных центральных процессорах. Облака в качестве услуги.	4	14	2		4		2	
15.	Многопроцессорные системы. Низкоуровневые коммуникационные программы мультикомпьютеров	4	15	2				2	
16.	Управление доступом к ресурсам. Реализация формальных моделей безопасности в операционных системах. Реализация криптографических схем в ОС.	4	16	2		4		2	
17.	Атаки переполнения буфера. Атаки, использующие форматирующую строку. Указатели на несуществующие объекты. Разыменование нулевого указателя.	4	17	2				2	
18	Брандмауэры. Антивирусные технологии. Электронная подпись программ.	4	18	2		4		2	Рейтинг-контроль №3
Всего за 4 семестр:		108		36		36		36	Зачет
Наличие в дисциплине КП/КР		нет							
Итого по дисциплине		108		36		36		36	Зачет

Содержание лекционных занятий по дисциплине

Тема 1. *Понятия операционной системы: процесс, адресное пространство, файл, ввод-вывод, шины. Системные вызовы* Содержание темы. Монолитные системы, микроядра, виртуальные машины.

Тема 2. *Модель процесса, состояние процессов, моделирование режима многозадачности. Потоки в POSIX.* Содержание темы. Реализация потоков в пользовательском пространстве, в ядре, гибридная реализация. Алгоритм активации планировщика.

Тема 3. *Состязательные ситуации. Критические области.* Содержание темы. Синхронизационные примитивы: семафор, мьютекс, монитор. Барьеры. Передача сообщений

Тема 4. *Планирование в интерактивных системах. Системы реального времени. Планирование потоков.* Содержание темы. Классические задачи взаимодействия процессов.

Тема 5. *Страничная организация памяти, таблицы страниц.* Содержание темы. Алгоритмы замещения страниц: алгоритм LRU, алгоритм WSClock, алгоритм "рабочий набор".

Тема 6. *Управление загрузкой. Разделение пространства команд и данных.* Содержание темы. Совместно используемые страницы и библиотеки. Политика очистки страниц. Интерфейс виртуальной памяти. Сегментация со страничной организацией памяти.

Тема 7. *Файловые системы с журнальной структурой. Журналируемые файловые системы*. Содержание темы. Виртуальные файловые системы. Непротиворечивость ФС. Оценка производительности ФС.

Тема 8. *Устройства и контроллеры устройств ввода-вывода.* Содержание темы. Ввод-вывод, отображаемый на адресное пространство. Прямой доступ к памяти.

Тема 9. *Ввод-вывод, управляемый прерываниями. Ввод-вывод с помощью DMA.*

Содержание темы. Обработчики прерываний, драйверы устройств. Слой абстракции от оборудования (HAL).

Тема 10. *Алгоритмы планирования перемещения блока головок. Обработка ошибок.* Содержание темы. Аппаратная составляющая часов. Программируемые таймеры. Пользовательский интерфейс ввода-вывода. Управление энергопотреблением.

Тема 11. *Выгружаемые и невыгружаемые ресурсы*. Содержание темы. Условия возникновения ресурсных взаимоблокировок. Обнаружение взаимоблокировок разных типов. Уклонение от взаимоблокировок, алгоритм банкира.

Тема 12. *Атака условия взаимного исключения. Атака условия удержания и ожидания. Атака условия невыгружаемости*. Содержание темы. Атака условия циклического ожидания. Двухфазное блокирование. Активная взаимоблокировка. Зависание.

Тема 13. *Гипервизоры первого и второго типа. Аппаратная поддержка вложенных таблиц страниц.* Содержание темы. Возвращение памяти. Виртуализация ввода-вывода. Блоки управления памятью при вводе-выводе. Домены устройств.

Тема 14. *Облака в качестве услуги. Миграция виртуальных машин.* Содержание темы. Установка контрольных точек. Виртуализация на примере продуктов VmWare.

Тема 15. *Низкоуровневые коммуникационные программы мультикомпьютеров. Распределенная совместно используемая память.* Содержание темы. Планирование мультикомпьютеров. Вызовы удаленных процедур. Балансировка нагрузки.

Тема 16. *Реализация формальных моделей безопасности в операционных системах.*

Содержание темы. Реализация криптографических схем в ОС. Криптопроцессоры и криптопровайдеры. Аутентификация и авторизация в современных операционных системах.

Тема 17. *Атаки, использующие форматирующую строку. Указатели на несуществующие объекты.* Содержание темы. Разыменование нулевого указателя. Переполнение целочисленных значений. Атаки, использующие внедрение команд. Инсайдерские атаки. Вредоносные программы.

Тема 18. *Антивирусные технологии.* Содержание темы. Электронная подпись программ. "Тюремное заключение". Обнаружение проникновения на основе модели. Инкапсулированный код. Современные исследования в области безопасности операционных систем.

Содержание лабораторных занятий по дисциплине

Лабораторная работа №1. *Создание многопоточного приложения для обмена текстовыми сообщениями*. Содержание. Проектирование клиент-серверной архитектуры приложения.

Лабораторная работа №2. *Создание многопоточного приложения для обмена текстовыми сообщениями.* Содержание. Разработка потоков, реализующих доступ к базе данных, пользовательский ввод-вывод, доступ к сокетам и сетевым интерфейсам.

Лабораторная работа №3. *Создание многопоточного приложения для обмена текстовыми сообщениями.* Содержание. Синхронизация потоков, разработка необходимых примитивов синхронизации, задействование моделей "произвдитель-потребитель". Реализация обмена информацией между потоками на базе синхронизированных структур данных.

Лабораторная работа №4. *Создание многопоточного приложения для обмена текстовыми сообщениями.* Содержание. Защита клиента и сервера от копирования. Реализация статической защиты (от обратной разработки), динамической защиты (от отладки)

и контроля целостности для предотвращения несанкционированной модификации исполняемых файлов.

Лабораторная работа №5. *Создание многопоточного приложения для обмена текстовыми сообщениями.* Содержание. Тестирование, отладка. Упаковка приложения в дистрибутив. Нагрузочное тестирование приложения.

Лабораторная работа №6. *Анализ защищенности приложения.* Содержание. Знакомство со средой дизассемблирования. Статический анализ кода. Анализ строк и системных вызовов. Обнаружение упаковщика и шифратора кода.

Лабораторная работа №7. *Анализ защищенности приложения.* Содержание. Динамический анализ и отладка. Мониторинг памяти. Деобфускация кода

Лабораторная работа №8. *Анализ защищенности приложения.* Содержание. Способы обхода механизмов контроля целостности. Обнаружение и подмена имитовставок, контрольных сумм, хэш-сумм.

Лабораторная работа №9. *Анализ защищенности приложения.* Содержание. Тестирование на защиту от атак типа "отказ в обслуживании", атак, подразумевающих удаленное исполнение кода и атак, заключающихся в динамической подмене библиотек.

5. ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ, ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ИТОГАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ И УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ СТУДЕНТОВ

5.1. Текущий контроль успеваемости

Вопросы рейтинг-контроля №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.
13. Планирование потоков.
14. Классические задачи взаимодействия процессов.
15. Виртуальная память.
16. Страничная организация памяти.
17. Алгоритмы замещения страниц.
18. Алгоритм LRU.

Вопросы рейтинг-контроля №2

1. Алгоритм WSClock.
2. Алгоритм "рабочий набор".
3. Управление загрузкой.
4. Разделение пространства команд и данных.
5. Совместно используемые страницы и библиотеки.
6. Политика очистки страниц.
7. Интерфейс виртуальной памяти.

8. Сегментация со страничной организацией памяти.
9. Файловые системы. Свойства файлов.
10. Файловые системы с журнальной структурой.
11. Аппаратная составляющая часов. Программируемые таймеры.
12. Пользовательский интерфейс ввода-вывода - клавиатура, мышь, монитор.
13. Управление энергопотреблением.
14. Выгружаемые и невыгружаемые ресурсы.
15. Условия возникновения ресурсных взаимоблокировок.
16. Обнаружение взаимоблокировок разных типов.
17. Уклонение от взаимоблокировок, алгоритм банкира.
18. Атака условия взаимного исключения.
19. Атака условия удержания и ожидания.

Вопросы рейтинг-контроля №3

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 мультикомпьютеров.
7. Вызовы удаленных процедур.
8. Балансировка нагрузки.
9. Реализация формальных моделей безопасности в операционных системах.
10. Реализация криптографических схем в ОС.
11. Криптопроцессоры и криптопровайдеры.
12. Аутентификация и авторизация в современных операционных системах.
13. Атаки переполнения буфера.
14. Атаки, использующие форматирующую строку.
15. Указатели на несуществующие объекты.
16. Разыменование нулевого указателя.
17. Переполнение целочисленных значений.
18. Атаки, использующие внедрение команд.
19. Антивирусные технологии.
20. Электронная подпись программ.
21. Защита кода типа "Тюремное заключение".
22. Обнаружение проникновения на основе модели.
103. Инкапсулированный код.

5.2. Промежуточная аттестация по итогам освоения дисциплины

Перечень вопросов к зачету

- Понятие процесса.
- Понятие адресного пространства.
- Понятие файла.
- Понятие ввода-вывода.
- Понятие шины.
- Системные вызовы.
- Монолитные системы.
- Микроядра.
- Виртуальные машины.
- Модель процесса.
- Состояние процессов.

• Моделирование режима многозадачности.
• Потоки в POSIX.
• Реализация потоков в пользовательском пространстве,
• Реализация потоков в ядре.
• Гибридная реализация потоков.
• Алгоритм активации планировщика.
• Состязательные ситуации.
• Критические области.
• Синхронизационные примитивы.
• Семафор.
• Мьютекс.
• Монитор.
• Барьеры.
• Передача сообщений.
• Планирование в пакетных системах.
• Планирование в интерактивных системах.
• Планирование в системах реального времени.
• Планирование потоков.
• Классические задачи взаимодействия процессов.
• Виртуальная память.
• Страничная организация памяти.
• Алгоритмы замещения страниц.
• Алгоритм LRU.
• Алгоритм WSClock.
• Алгоритм "рабочий набор".
• 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. Свойства файлов.
• Файловые системы с журнальной структурой.
• Журналируемые файловые системы.
• Виртуальные файловые системы.
• Непротиворечивость ФС.
• Оценка производительности ФС.
• Устройства и контроллеры устройств ввода-вывода.
• Ввод-вывод, отображаемый на адресное пространство.
• Прямой доступ к памяти.
• ПО ввода-вывода.
• Ввод-вывод, управляемый прерываниями.
• Ввод-вывод с помощью DMA.
• Обработчики прерываний, драйверы устройств.
• Слой абстракции от оборудования (HAL).
• Аппаратная часть дисков.
• Алгоритмы планирования перемещения блока головок.
• Обработка ошибок при обращении к жесткому диску.
• Аппаратная составляющая часов. Программируемые таймеры.
• Пользовательский интерфейс ввода-вывода - клавиатура, мышь, монитор.
• Управление энергопотреблением.
• Выгружаемые и невыгружаемые ресурсы.

- Условия возникновения ресурсных взаимоблокировок.
- Обнаружение взаимоблокировок разных типов.
- Уклонение от взаимоблокировок, алгоритм банкира.
- Атака условия взаимного исключения.
- Атака условия удержания и ожидания.
- Атака условия невыгружаемости.
- Атака условия циклического ожидания.
- Двухфазное блокирование. Активная взаимоблокировка. Зависание.
- Технологии виртуализации. Гипервизоры первого и второго типа.
- Аппаратная поддержка вложенных таблиц страниц. Возвращение памяти.
- Виртуализация ввода-вывода.
- Блоки управления памятью при вводе-выводе.
- Домены устройств.
- Виртуальные машины на мультиядерных центральных процессорах.
- Облака в качестве услуги.
- Виртуализация на примере продуктов VmWare.
- Многопроцессорные системы.
- Коммуникационные программы мультикомпьютеров.
- Распределенная совместно используемая память.
- Планирование мультикомпьютеров.
- Вызовы удаленных процедур.
- Балансировка нагрузки.
- Реализация формальных моделей безопасности в операционных системах.
- Реализация криптографических схем в ОС.
- Криптопроцессоры и криптопровайдеры.
- Аутентификация и авторизация в современных операционных системах.
- Атаки переполнения буфера.
- Атаки, использующие форматирующую строку.
- Указатели на несуществующие объекты.
- Разыменование нулевого указателя.
- Переполнение целочисленных значений.
- Атаки, использующие внедрение команд.
- Инсайдерские атаки.
- Вредоносные программы.
- Брандмауэры.
- Антивирусные технологии.
- Электронная подпись программ.
- Защита кода типа "Тюремное заключение".
- Обнаружение проникновения на основе модели.
- Инкапсулированный код.

5.3. Самостоятельная работа обучающегося.

Вопросы и задания для самостоятельной работы студентов

1. Механизмы управления памятью в ОС Windows
2. Организация системных вызовов ОС Windows
3. Структура ядра операционной системы Windows
4. Механизмы управления памятью в ОС Linux
5. Организация системных вызовов ОС Linux
6. Структура ядра операционной системы Linux
7. Контексты безопасности SELinux
8. Механизмы Data Execution Prevention (DEP)

9. Рандомизация пространства адресов (ASLR)
10. Инкапсуляция кода в мобильных операционных системах
11. APT-угрозы и защита от них в современных операционных системах
12. EFI и системы доверенной загрузки.

Фонд оценочных материалов (ФОМ) для проведения аттестации уровня сформированности компетенций обучающихся по дисциплине оформляется отдельным документом.

6. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

6.1. Книгообеспеченность

Наименование литературы: автор, название, вид издания, издательство	Год издания	КНИГООБЕСПЕЧЕННОСТЬ
		Наличие в электронном каталоге ЭБС
Основная литература*		
1. Широков, А. И. Операционные системы и среды: основные понятия теории: учебник / А. И. Широков, Ф. Г. Кирдяшов, С. Э. Мурадханов; под ред. Е. А. Калашникова, Л. П. Рябова. - Москва: Изд. Дом НИТУ «МИСиС», 2018. - 192 с. - ISBN 978-5-906953-49-0.	2018	https://znanium.com/catalog/product/1232238
2. Бабичев, С. Л. Распределенные системы: учебное пособие для вузов / С. Л. Бабичев, К. А. Коньков. — Москва: Издательство Юрайт, 2020. — 507 с. —— ISBN 978-5-534-11380-8.	2020	https://urait.ru/bcode/457005
3. Гостев, И. М. Операционные системы: учебник и практикум для вузов / И. М. Гостев. — 2-е изд., испр. и доп. — Москва: Издательство Юрайт, 2021. — 164 с. ISBN 978-5-534-04520-8.	2021	https://urait.ru/bcode/470010
4. Басыня, Е. А. Системное администрирование и информационная безопасность: учебное пособие: [16+] / Е. А. Басыня. – Новосибирск: Новосибирский государственный технический университет, 2018. – 79с.– ISBN 978-5-7782-3484-0.	2018	https://biblioclub.ru/index.php?page=book&id=575325 (дата обращения: 08.09.2021)
5. Ложников, П. С. Средства безопасности операционной системы ROSA Linux : учебное пособие : [16+] / П. С. Ложников, А. О. Провоторский. – Омск : Омский государственный технический университет (ОмГТУ), 2017. – 94 с. – ISBN 978-5-8149-2502-2	2017	https://biblioclub.ru/index.php?page=book&id=493349 (дата обращения: 08.09.2021)
Дополнительная литература		
1.Операционные системы. Основы UNIX: Учебное пособие/ ВавренюкА.Б., КурышеваО.К., КутеповС.В. и др. - М.: НИЦ ИНФРА-М, 2015. - 184 с.: ISBN 978-5-16-010893-3.	2015	Режим доступа: http://znanium.com/catalog.php?bookinfo=504874
2. Куль, Т. П. Операционные системы: учебное пособие: [16+] / Т. П. Куль. – Минск: РИПО, 2019. – 312 с– ISBN 978-985-503-940-3	2019	https://biblioclub.ru/index.php?page=book&id=599951 (дата обращения: 08.09.2021)
3. Инфокоммуникационные системы и сети: курс лекций: [16+] / авт.-сост. З. М. Альбекова. – Ставрополь: Северо-Кавказский Федеральный университет (СКФУ), 2018. – 165 с.	2018	https://biblioclub.ru/index.php?page=book&id=562882 (дата обращения: 08.09.2021)

6.2. Периодические издания

1. Журнал «Вопросы защиты информации». Режим доступа: http://i-vimi.ru/editions/detail.php?SECTION_ID=155/;
2. Журнал "Information Security/Информационная безопасность". Режим доступа: http://www.itsec.ru/insec-about.php.

3. Ежемесячный теоретический и прикладной научно-технический журнал «Информационные технологии». Режим доступа http://novtex.ru/IT/.

6.3. Интернет-ресурсы

1.Образовательный сервер кафедры ИЗИ.– Режим доступа: http://edu.izi.vlsu.ru

2.Информационная образовательная сеть.- Режим доступа: http://ien.izi.vlsu.ru

3.Внутривузовские издания ВлГУ.– Режим доступа: http://e.lib.vlsu.ru/

4.ИНТУИТ. Национальный открытый университет.– Режим доступа: http://www.intuit.ru/

7. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Занятия проводятся в следующих аудиториях ВлГУ (корпус №2) по адресу г. Владимир, ул. Белоконской, д. 3.

ауд. 408-2, Лекционная аудитория, количество студенческих мест – 50, площадь 60 м2, оснащение: мультимедийное оборудование (интерактивная доска Hitachi FX-77WD, проектор BenQ MX 503 DLP 2700ANSI XGA), ноутбук Lenovo Idea Pad B5045

ауд. 427а-2, лаборатория сетевых технологий, количество студенческих мест – 14, площадь 36 м2, оснащение: компьютерный класс с 8 рабочими станциями Core 2 Duo E8400 с выходом в Internet, 3 маршрутизатора Cisco 2800 Series, 6 маршрутизаторов Cisco 2621, 6 коммутаторов Cisco Catalyst 2960 Series, 3 коммутатора Cisco Catalyst 2950 Series, коммутатор Cisco Catalyst Express 500 Series, проектор BenQ MP 620 P, экран настенный рулонный. Лицензионное программное обеспечение: операционная система Windows 7 Профессиональная, офисный пакет приложений Microsoft Office Профессиональный плюс 2007, бесплатно распространяемое программное обеспечение: линейка интегрированных сред разработки Visual Studio Express 2012, программный продукт виртуализации Oracle VM VirtualBox 5.0.4, симулятор сети передачи данных Cisco Packet Tracer 7.0, интегрированная среда разработки программного обеспечения IntelliJ IDEA Community Edition 15.0.3.

ауд. 427б-2, УНЦ «Комплексная защита объектов информатизации», количество студенческих мест – 15, площадь 52 м2, оснащение: компьютерный класс с 7 рабочими станциями Alliance Optima P4 с выходом в Internet, коммутатор D-Link DGS-1100-16 мультимедийный комплект (проектор Toshiba TLP X200, экран настенный рулонный), прибор ST-031P «Пиранья-Р» многофункциональный поисковый, прибор «Улан-2» поисковый, виброакустический генератор шума «Соната АВ 1М», имитатор работы средств нелегального съема информации, работающих по радиоканалу «Шиповник», анализатор спектра «GoodWill GSP-827», индикатор поля «SEL SP-75 Black Hunter», устройство блокирования работы систем мобильной связи «Мозайка-3», устройство защиты телефонных переговоров от прослушивания «Прокруст 2000», диктофон Edic MINI Hunter, локатор «Родник-2К» нелинейный, комплекс проведения акустических и виброакустических измерений «Спрут мини-А», видеорегистратор цифровой Best DVR-405, генератор Шума «Гном-3»,учебно-исследовательский комплекс «Сверхширокополосные беспроводные сенсорные сети» (Nano Xaos), сканирующий приемник «Icom IC-R1500», анализатор сетей Wi-Fi Fluke AirCheck с активной антенной. Лицензионное программное обеспечение: Windows 8 Профессиональная, офисный пакет приложений Microsoft Office Профессиональный плюс 2010, бесплатно распространяемое программное обеспечение: линейка интегрированных сред разработки Visual Studio Express 2012, инструмент имитационного моделирования AnyLogic 7.2.0 Personal Learning Edition, интегрированная среда разработки программного обеспечения IntelliJ IDEA Community Edition 14.1.4.

Рабочую программу составил: доцент кафедры ИЗИ к.т.н. Монахов Ю.М.__________

Рецензент: Заместитель руководителя РАЦ ООО
«ИнфоЦентр» к.т.н. Вертилевский Н.В__________

Программа рассмотрена и одобрена на заседании кафедры ИЗИ

Протокол № 13 от 12.05.23 года
Заведующий кафедрой д.т.н., профессор__________/М.Ю. Монахов/

Рабочая программа рассмотрена и одобрена на заседании учебно-методической комиссии направления 10.03.01 «Информационная безопасность»

Протокол № 13 от 12.05.23 года
Председатель комиссии д.т.н., профессор__________/М.Ю. Монахов/

ЛИСТ ПЕРЕУТВЕРЖДЕНИЯ
РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ

Рабочая программа одобрена на 20___ / 20___ учебный год

Протокол заседания кафедры № ______ от _________ года

Заведующий кафедрой д.т.н., профессор__________/М.Ю.Монахов/
(ФИО, должность, подпись)

Рабочая программа одобрена на 20___ / 20___ учебный год

Протокол заседания кафедры № ______ от _________ года

Заведующий кафедрой д.т.н., профессор__________/М.Ю.Монахов/
(ФИО, должность, подпись)

Рабочая программа одобрена на 20___ / 20___ учебный год

Протокол заседания кафедры № ______ от _________ года

Заведующий кафедрой д.т.н., профессор__________/М.Ю.Монахов/
(ФИО, должность, подпись)

Рабочая программа одобрена на 20___ / 20___ учебный год

Протокол заседания кафедры № ______ от _________ года

Заведующий кафедрой д.т.н., профессор__________/М.Ю.Монахов/
(ФИО, должность, подпись)

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

в рабочую программу дисциплины
Безопасность операционных систем
образовательной программы направления подготовки *10.03.01. Информационная безопасность*,
профиль: *Безопасность автоматизированных систем*

Номер изменения	Внесены изменения в части/разделы рабочей программы	Исполнитель ФИО	Основание (номер и дата протокола заседания кафедры)
1			
2			

Заведующий кафедрой _____/М.Ю.Монахов/

Подпись *ФИО*