МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«Воронежский государственный технический университет»

УТВЕРЖДАЮ

Декан факультета _____ Гусев П.Ю.

«31» августа 2021 г.

РАБОЧАЯ ПРОГРАММА

дисциплины

«Безопасность операционных систем»

Специальность 10.05.03 Информационная безопасность автоматизированных систем

Специализация специализация N 7 "Анализ безопасности информационных систем"

Квалификация выпускника специалист по защите информации

Нормативный период обучения 5 лет и 6 м.

Форма обучения очная

Год начала подготовки 2021

Автор программы _____ /Белоножкин В.И. /

Заведующий кафедрой
Систем информационной
безопасности _____ /Остапенко А.Г./

Руководитель ОПОП _____ /Остапенко А.Г./

Воронеж 2021

1. ЦЕЛИ И ЗАДАЧИ ДИСЦИПЛИНЫ

1.1. Цели дисциплины

Формирование и закрепление профессиональных компетенций, направленных на знание и владение методами обеспечения безопасности современных операционных систем в процессе разработки и применения автоматизированных систем

1.2. Задачи освоения дисциплины:

- ознакомление с методами, способами, средствами обеспечения безопасности операционных систем при разработке автоматизированных систем;
- формирование умений применения защитных механизмов операционных систем в процессе проектирования защищенных автоматизированных систем;
- приобретение навыков настройки и использования механизмов и инструментов обеспечения безопасности операционных систем.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Дисциплина «Безопасность операционных систем» относится к дисциплинам обязательной части блока Б1.

3. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ

Процесс изучения дисциплины «Безопасность операционных систем» направлен на формирование следующих компетенций:

ОПК-11 - Способен разрабатывать компоненты систем защиты информации автоматизированных систем;

ОПК-12 - Способен применять знания в области безопасности вычислительных сетей, операционных систем и баз данных при разработке автоматизированных систем.

Компетенция	Результаты обучения, характеризующие сформированность компетенции
ОПК-11	знать методы, способы, средства обеспечения безопасности операционных систем как основных компонентов автоматизированных систем
	уметь использовать защитные механизмы операционных систем в процессе разработки средств защиты информации автоматизированных систем
	владеть навыками использования средств операционных систем для обеспечения безопасного функционирования автоматизированных систем
ОПК-12	знать принципы построения и механизмы функционирования, современных операционных систем,

	создания на их основе компьютерных сетей и автоматизированных систем
	уметь конфигурировать параметры защиты операционных систем, оценивать эффективность и надежность мер защиты
	владеть навыками установки, настройки и применения механизмов и средств обеспечения безопасности операционных систем

4. ОБЪЕМ ДИСЦИПЛИНЫ

Общая трудоемкость дисциплины «Безопасность операционных систем» составляет 9 з.е.

Распределение трудоемкости дисциплины по видам занятий

очная форма обучения

Виды учебной работы	Всего часов	Семестры	
		5	6
Аудиторные занятия (всего)	162	108	54
В том числе:			
Лекции	72	54	18
Лабораторные работы (ЛР)	90	54	36
Самостоятельная работа	90	36	54
Курсовой проект	+	+	
Часы на контроль	72	36	36
Виды промежуточной аттестации - экзамен	+	+	+
Общая трудоемкость: академические часы зач.ед.	 324 9	 180 5	 144 4

5. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

5.1 Содержание разделов дисциплины и распределение трудоемкости по видам занятий

очная форма обучения

№ п/п	Наименование темы	Содержание раздела	Лекц	Лаб. зан.	СРС	Всего, час
1	Автоматизированные системы и их безопасность	Типы автоматизированных систем (АС). Архитектуры и компоненты АС. Роль операционных систем (ОС) в функционировании АС. Требования безопасности в процессе разработки АС.	6	8	10	24
2	Архитектура и функционирование современных операционных систем	Разновидности архитектур ОС. Основные функции, подсистемы, компоненты, механизмы и процессы ОС. Требования, политики и модели безопасности ОС.	10	8	10	28
3	Структура, механизмы и компоненты	Характеристика подсистем безопасности ОС. Механизмы аутентификациии, контроля доступа, мониторнга, защиты от вторжений.	10	10	10	30

	подсистем безопасности ОС	Основные типы средств, реализующих защитные механизмы. Оценка эффективности защиты ОС.				
4	Реализация механизмов и компонентов защиты ОС семейства Windows	Политики безопасности Windows. Механизмы и службы безопасности. Active Directory. Шифрованная файловая система. Виртуализация. Поддержание работоспособности и восстановление. Аудит.	16	20	20	56
5	Реализация механизмов и компонентов защиты ОС семейства Linux	Основные механизмы и средства защиты ОС Linux. Проекты расширений безопасности Linux. Средства обеспечения безопасности сетей под управлением Linux.	14	20	16	50
6	Реализация механизмов и компонентов защиты других типов ОС	Механизмы и инструменты защиты сертифицированных в России релизов ОС. Механизмы и средства защиты ОС компании Apple. Механизмы и средства защиты ОС семейства Android.	10	14	14	38
7	Использование механизмов и инструментов защиты ОС в процессе создания и функционирования автоматизированных систем	Порядок разработки АС с учетом требований безопасности. Подходы к использованию механизмов и инструментов защиты ОС при выработке политик безопасности АС. Примеры защищенных АС.	6	10	10	26
		Итого	**72**	**90**	**90**	**252**

5.2 Перечень лабораторных работ

1. Анализ операций, выполняемых ОС в разных типах автоматизированных систем.
2. Анализ функций подсистем безопасности для ОС различной архитектуры и платформы.
3. Сравнение механизмов аутентификации различных типов ОС.
4. Сравнение механизмов контроля доступа к объектам в различных типах ОС.
5. Изучение основных команд и элементов интерфейса ОС семейства Windows.
6. Изучение средств управления ресурсами компьютера в ОС семейства Windows.
7. Изучение основных оснасток и ролей в ОС семейства Windows.
8. Изучение основных служб ОС семейства Windows.
9. Настройка инструментов аутентификации в ОС семейства Windows.
10. Настройка инструментов контроля доступа в ОС семейства Windows.
11. Изучение Active Directory.
12. Настройка шифрующей файловой системы ОС семейства Windows.
13. Установка и настройка виртуальных машин в среде ОС семейства Windows.
14. Изучение средств аудита в ОС семейства Windows.
15. Изучение средств поддержки работоспособности ОС семейства Windows.
16. Изучение основных команд и элементов интерфейса ОС семейства

Linux.

17. Изучение основных команд и элементов интерфейса ОС семейства Linux.

18. Изучение средств управления ресурсами компьютера в ОС семейства Linux.

19. Изучение основных системных демонов ОС семейства Linux.

20. Настройка инструментов аутентификации в ОС семейства Linux.

21. Настройка инструментов контроля доступа в ОС семейства Linux.

22. Изучение средств аудита в ОС семейства Linux.

23. Изучение средств поддержки работоспособности ОС семейства Linux.

24. Анализ функций различных расширений безопасности ОС семейства Linux.

25. Изучение инструментов защиты ОС семейства Android.

26. Выработка политики безопасности автоматизированных систем с учетом функциональности ОС.

6. ПРИМЕРНАЯ ТЕМАТИКА КУРСОВЫХ ПРОЕКТОВ (РАБОТ) И КОНТРОЛЬНЫХ РАБОТ

В соответствии с учебным планом освоение дисциплины предусматривает выполнение курсового проекта в 5 семестре для очной формы обучения.

Примерная тематика курсового проекта: «Реализация компонента обеспечения безопасности автоматизированной системы средствами операционной системы»

Задачи, решаемые при выполнении курсового проекта:

• Определение технических требований к разработке заданного компонента обеспечения безопасности АС.

• Анализ и выбор средств ОС для реализации заданного компонента.

• Проектирование заданного компонента на основе использования выбранных средств ОС.

Курсовой проект включат в себя графическую часть и расчетно-пояснительную записку.

7. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

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

7.1.1 Этап текущего контроля

Результаты текущего контроля знаний и межсессионной аттестации оцениваются по следующей системе:

«аттестован»;

«не аттестован».

Компе-тенция	Результаты обучения, характеризующие сформированность компетенции	Критерии оценивания	Аттестован	Не аттестован
ОПК-11	знать методы, способы, средства обеспечения безопасности операционных систем как основных компонентов автоматизированных систем	Ответ на вопрос преподавателя, выполнение теста	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	уметь использовать защитные механизмы операционных систем в процессе разработки средств защиты информации автоматизированных систем	Решение стандартных практических задач	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	владеть навыками использования средств операционных систем для обеспечения безопасного функционирования автоматизированных систем	Решение прикладных задач в конкретной предметной области	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
ОПК-12	знать принципы построения и механизмы функционирования, современных операционных систем, создания на их основе компьютерных сетей и автоматизированных систем	Ответ на вопрос преподавателя, выполнение теста	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	уметь конфигурировать параметры защиты операционных систем, оценивать эффективность и надежность мер защиты	Решение стандартных практических задач	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	владеть навыками установки, настройки и применения механизмов и средств обеспечения безопасности операционных	Решение прикладных задач в конкретной предметной области	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах

	систем			

7.1.2 Этап промежуточного контроля знаний

Результаты промежуточного контроля знаний оцениваются в 5, 6 семестре для очной формы обучения по четырехбалльной системе:

«отлично»;

«хорошо»;

«удовлетворительно»;

«неудовлетворительно».

Компе-тенция	Результаты обучения, характеризующие сформированность компетенции	Критерии оценивания	Отлично	Хорошо	Удовл.	Неудовл.
ОПК-11	знать методы, способы, средства обеспечения безопасности операционных систем как основных компонентов автоматизированных систем	Тест	Выполнение теста на 90-100%	Выполнение теста на 80-90%	Выполнение теста на 70-80%	В тесте менее 70% правильных ответов
	уметь использовать защитные механизмы операционных систем в процессе разработки средств защиты информации автоматизированных систем	Решение стандартных практических задач	Задачи решены в полном объеме и получены верные ответы	Продемонстрирован верный ход решения всех, но не получен верный ответ во всех задачах	Продемонстрирован верный ход решения в большинстве задач	Задачи не решены
	владеть навыками использования средств операционных систем для обеспечения безопасного функционирования автоматизированных систем	Решение прикладных задач в конкретной предметной области	Задачи решены в полном объеме и получены верные ответы	Продемонстрирован верный ход решения всех, но не получен верный ответ во всех задачах	Продемонстрирован верный ход решения в большинстве задач	Задачи не решены
ОПК-12	знать принципы построения и механизмы функционирования, современных операционных систем, создания на их основе компьютерных	Тест	Выполнение теста на 90-100%	Выполнение теста на 80-90%	Выполнение теста на 70-80%	В тесте менее 70% правильных ответов

	сетей и автоматизированных систем					
	уметь конфигурировать параметры защиты операционных систем, оценивать эффективность и надежность мер защиты	Решение стандартных практических задач	Задачи решены в полном объеме и получены верные ответы	Продемонстрирован верный ход решения всех, но не получен верный ответ во всех задачах	Продемонстрирован верный ход решения в большинстве задач	Задачи не решены
	владеть навыками установки, настройки и применения механизмов и средств обеспечения безопасности операционных систем	Решение прикладных задач в конкретной предметной области	Задачи решены в полном объеме и получены верные ответы	Продемонстрирован верный ход решения всех, но не получен верный ответ во всех задачах	Продемонстрирован верный ход решения в большинстве задач	Задачи не решены

7.2 Примерный перечень оценочных средств (типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности)

7.2.1 Примерный перечень заданий для подготовки к тестированию

1. В автоматизированных системах ОС относится к:
а) аппаратным средствам;
б) общесистемному программному обеспечению;
в) специальному программному обеспечению.
2. К элементам архитектуры ОС относятся:
а) файлы;
б) процессы;
в) драйверы.
3. Степень защищенности ОС определяется:
а) количеством блокируемых угроз безопасности;
б) наличием или отсутствием уязвимостей;
в) уровнем риска.
4. В защищенной ОС базовые средства защиты располагаются в:
а) прикладных программах;
б) ядре;
в) системных службах.
5. К функциям подсистемы безопасности ОС относятся:
а) управление доступом к объектам;
б) выполнение файловых операций;
в) маршрутизация сетевых пакетов.
6. Основная идея принципа микроядра ОС заключатся в:

а) минимально возможном количестве модулей, выполняемых в привилегированном режиме;

б) минимально занимаемом объеме памяти;

в) минимально возможном количестве реализуемых функций.

7. Процессы в ОС можно классифицировать с точки зрения соотношения их исполнения и ввода-вывода как:

а) ориентированные на ввод-вывод, ориентированные на вычисления активные и ленивые;

б) ресурсоемкие и экономные;

в) выполняющие ввод-вывод и не выполняющие ввод-вывод.

8. Разграничение доступа на основе дискреционного принципа контроля использует механизм:

а) ролей;

б) меток безопасности;

в) набора правил.

9. Обеспечение работоспособности ОС – это:

а) оптимизация нагрузки;

б) поддержание доступности и целостности;

в) защита системных настроек.

10. К функциям аудита безопасности в ОС относятся:

а) мониторинг несанкционированного доступа;

б) контроль полномочий пользователей;

в) фиксация настроек ОС.

7.2.2 Примерный перечень заданий для решения стандартных задач

1. Типовая структура подсистемы безопасности ОС включает в себя:

а) средства аутентификации;

б) сетевые драйверы;

в) модуль ввода-вывода.

2. К основным действиям по управлению процессами ОС относятся:

а) визуализация выполнения процесса на дисплее;

б) сопровождение выполнения каждого процесса записью в журнале;

в) создание и удаление процессов.

3. Независимый процесс – это:

а) процесс, выполняемый независимо от других процессов;

б) процесс, выполняемый независимо от ОС;

в) процесс с непредсказуемым поведением.

4. Открытие файла – это:

а) запись на носитель;

б) обнуление признаков защиты;

в) считывание заголовка и одного или нескольких смежных блоков в оперативную память.

5. К причинам фрагментации памяти относятся:

а) несовпадение размеров блоков свободной памяти и требуемых

размеров запрашиваемых участков;

б) большое число запросов;

в) ненадежность операционной системы.

6. По управлению оперативной памятью ОС выполняет:

а) выделение памяти требуемого размера, освобождение заданной области памяти;

б) шифрование содержимого заданного участка памяти;

в) автоматический сброс содержимого памяти на диск в случае сбоя.

7. В процессе аутентификации ОС проверяет:

а) полномочия пользователя

б) наличие учетной записи пользователя

в) совпадения атрибутов, предъявляемых пользователем и сохраненных в системе.

8. Настройки межсетевого экрана регулируют:

а) входящий трафик;

б) отображение графики на экране;

в) количество запускаемых приложений.

9. К средствам восстановления ОС после сбоя относятся:

а) утилиты сканирование и дефрагментация дисков;

б) загрузка в безопасном режиме работы;

в) средства устранения “зависаний” программ.

10. В журнал безопасности ОС записываются:

а) данные сеанса работы пользователей;

б) события нарушения политик безопасности;

в) запуск системных служб.

7.2.3 Примерный перечень заданий для решения прикладных задач

1. При установке ОС проверяется:

а) наличие достаточного свободного места на диске установки;

б) степень фрагментирования диска установки;

в) присутствие данных на диске установки.

2. Настройка параметров ОС при установке включает:

а) максимальное количество хранимых файлов;

б) период обновления системы;

в) пароль учетной записи администратора.

3. В режиме разделения времени в ОС:

а) машинное время предоставляется пользователям по очереди;

б) пользователь планирует время в какое время какие задания пропускаются;

в) ОС обрабатывает задания, вводимые и управляемые несколькими пользователями.

4. В процессе управления памятью в режиме мультипрограммирования:

а) в каждый момент в памяти размещается только одно задание;

б) в памяти хранится одновременно несколько заданий;

в) выделяется область памяти, куда поочередно загружаются различные задания.

5. Коммуникация между процессами организуется:

а) по электронной почте;

б) с помощью файловых операций;

в) с помощью передачи сообщений или общей области памяти.

6. Для авторизации действий пользователя в ОС:

а) запускается специальная программа:

б) используется его идентификатор;

в) проверяется системный журнал.

7. Структура прав доступа к файлам в ОС Linux:

а) владелец – группа владельца – все остальные;

б) администратор – остальные пользователи;

в) root — владелец – остальные пользователи.

8. Отличным правом доступа к файлам в ОС Windows от Linux является:

а) чтение;

б) запись;

в) изменение

9. Настройка средств аудита включает в себя:

а) выбор вида событий регистрации;

б) выбор фиксируемых пользователей;

в) выбор места размещения журнала.

10. Регламент резервирования ОС устанавливает:

а) количество сохраняемых файлов;

б) ответственного пользователя;

в) периодичность проведения операции резервирования.

7.2.4 Примерный перечень вопросов для подготовки к зачету

Не предусмотрено учебным планом

7.2.5 Примерный перечень вопросов для подготовки к экзамену

1. Типы современных автоматизированных систем и используемых для их создания ОС.
2. Классификация угроз безопасности ОС.
3. Характеристика типовых уязвимостей ОС.
4. Требования безопасности ОС.
5. Понятие защищенной ОС.
6. Содержание системного подхода к обеспечению безопасности ОС.
7. Этапы построения защиты ОС.
8. Стандарты безопасности ОС.
9. Подходы к оценке эффективности реализации защиты ОС.
10. Способы аутентификации пользователей ОС.
11. Средства и методы повышения надежности аутентификации в ОС.
12. Механизмы управления доступом в ОС.
13. Методы, права доступа и привилегии субъектов по отношению к объектам ОС.

14. Встроенные средства защиты файлов в ОС.
15. Реализация дискреционного и мандатного принципов в защищенных ОС.
16. Задачи аудита в ОС.
17. Средства реализации аудита в современных ОС.
18. Методы резервирования информации в ОС.
19. Подходы к организации восстановления работоспособности в современных ОС.
20. Направления использования инструментов защиты ОС в процессе функционирования автоматизированных систем.

7.2.6. Методика выставления оценки при проведении промежуточной аттестации

Экзамен проводится по тест-билетам, каждый из которых содержит 10 вопросов и задачу. Каждый правильный ответ на вопрос в тесте оценивается 1 баллом, задача оценивается в 10 баллов (5 баллов верное решение и 5 баллов за верный ответ). Максимальное количество набранных баллов – 20.

1. Оценка «Неудовлетворительно» ставится в случае, если студент набрал менее 6 баллов.
2. Оценка «Удовлетворительно» ставится в случае, если студент набрал от 6 до 10 баллов
3. Оценка «Хорошо» ставится в случае, если студент набрал от 11 до 15 баллов.
4. Оценка «Отлично» ставится, если студент набрал от 16 до 20 баллов.

7.2.7 Паспорт оценочных материалов

№ п/п	Контролируемые разделы (темы) дисциплины	Код контролируемой компетенции	Наименование оценочного средства
1	Автоматизированные системы и их безопасность	ОПК-11, ОПК-12	Тест, контрольная работа, защита лабораторных работ
2	Архитектура и функционирование современных операционных систем	ОПК-11, ОПК-12	Тест, защита лабораторных работ, защита реферата
3	Структура, механизмы и компоненты подсистем безопасности ОС	ОПК-11, ОПК-12	Тест, защита лабораторных работ, требования к курсовому проекту
4	Реализация механизмов и компонентов защиты ОС семейства Windows	ОПК-11, ОПК-12	Тест, защита лабораторных работ, требования к курсовому проекту
5	Реализация механизмов и компонентов защиты ОС семейства Linux	ОПК-11, ОПК-12	Тест, контрольная работа, защита лабораторных работ
6	Реализация механизмов и компонентов защиты других типов ОС	ОПК-11, ОПК-12	Тест, защита лабораторных работ, защита реферата
7	Использование механизмов и инструментов защиты ОС в процессе создания и функционирования автоматизированных систем	ОПК-11, ОПК-12	Тест, защита лабораторных работ

7.3. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности

Тестирование осуществляется, либо при помощи компьютерной системы тестирования, либо с использованием выданных тест-заданий на

бумажном носителе. Время тестирования 30 мин. Затем осуществляется проверка теста экзаменатором и выставляется оценка согласно методики выставления оценки при проведении промежуточной аттестации.

Решение стандартных задач осуществляется, либо при помощи компьютерной системы тестирования, либо с использованием выданных задач на бумажном носителе. Время решения задач 30 мин. Затем осуществляется проверка решения задач экзаменатором и выставляется оценка, согласно методики выставления оценки при проведении промежуточной аттестации.

Решение прикладных задач осуществляется, либо при помощи компьютерной системы тестирования, либо с использованием выданных задач на бумажном носителе. Время решения задач 30 мин. Затем осуществляется проверка решения задач экзаменатором и выставляется оценка, согласно методики выставления оценки при проведении промежуточной аттестации.

Защита курсового проекта осуществляется согласно требованиям, предъявляемым к работе, описанным в методических материалах. Примерное время защиты на одного студента составляет 20 мин.

8 УЧЕБНО МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ)

8.1 Перечень учебной литературы, необходимой для освоения дисциплины

1. Дейтел Х. М., Дейтел П. Дж., Чофнес Д. Р. Операционные системы. Т.1: Основы и принципы /; пер. с англ. под ред. А. С. Молявко. - 3-е изд. - М.: БИНОМ, 2011. - 1023 с.
2. Дейтел Х. М., Дейтел П. Дж., Чофнес Д. Р. Операционные системы . Т. 2: Распределённые системы, сети, безопасность / ; пер. с англ. под ред. А.С.Молявко. - 3-е изд. - М. : БИНОМ, 2011. - 704 с.
3. Проскурин В.Г. Защита в операционных системах. Учебное пособие для вузов. – М.: Горячая линия – Телеком, 2014. – 192 с.
4. Буренин П.В., Девянин П.Н., Лебеденко Е.В., Проскурин В.Г., Цибуля А.Н. Безопасность операционной системы специального назначения Astra Linux Special Edition. – М.: Горячая линия – Телеком, 2019. -404 с.
5. Линн С. Администрирование Microsoft Windows Server 2012. — СПб.: Питер, 2014. -304 с.
6. Хакер Р. Active Directory глазами хакера. — СПб.: БХВ-Петербург, 2021. -176 с.
7. Гончарук С.В. Администрирование ОС Linux. - М.: Национальный открытый университет «ИНТУИТ», 2016. -165 с.
8. Зобнин Е. Е. Android глазами хакера. — СПб.: БХВ-Петербург, 2021. — 272 с.

8.2 Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая

перечень лицензионного программного обеспечения, ресурсов информационно-телекоммуникационной сети «Интернет», современных профессиональных баз данных и информационных справочных систем:

- ЕИОС ВГТУ http://eios.vorstu.ru/;
- ЭБС «Консультант студента» http://www.studentlibrary.ru/;
- Портал «Anti-Malware» https://www.anti-malware.ru;
- портал «Information Security» https://www.itsec.ru;
- электронный журнал «Information Security» http://lib.itsec.ru/imag/;
- операционные системы Windows, Linux, Android.

9 МАТЕРИАЛЬНО-ТЕХНИЧЕСКАЯ БАЗА, НЕОБХОДИМАЯ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА

Аудитория с компьютерными рабочими местами, локальная сеть, презентационное оборудование.

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

По дисциплине «Безопасность операционных систем» читаются лекции, проводятся лабораторные работы, выполняется курсовой проект.

Основой изучения дисциплины являются лекции, на которых излагаются наиболее существенные и трудные вопросы, а также вопросы, не нашедшие отражения в учебной литературе.

Лабораторные работы выполняются на лабораторном оборудовании в соответствии с методиками, приведенными в указаниях к выполнению работ.

Методика выполнения курсового проекта изложена в учебно-методическом пособии. Выполнять этапы курсового проекта должны своевременно и в установленные сроки.

Контроль усвоения материала дисциплины производится тестированием, проверкой лабораторных работ, проверкой и защитой курсового проекта.

Вид учебных занятий	Деятельность студента
Лекция	Написание конспекта лекций: кратко, схематично, последовательно фиксировать основные положения, выводы, формулировки, обобщения; помечать важные мысли, выделять ключевые слова, термины. Проверка терминов, понятий с помощью энциклопедий, словарей, справочников с выписыванием толкований в тетрадь. Обозначение вопросов, терминов, материала, которые вызывают трудности, поиск ответов в рекомендуемой литературе. Если самостоятельно не удается разобраться в материале, необходимо сформулировать вопрос и задать преподавателю на лекции или на практическом занятии.
Лабораторная работа	Лабораторные работы позволяют научиться применять теоретические знания, полученные на лекции при решении конкретных задач. Чтобы наиболее рационально и полно использовать все возможности

	лабораторных для подготовки к ним необходимо: следует разобрать лекцию по соответствующей теме, ознакомится с соответствующим разделом учебника, проработать дополнительную литературу и источники, решить задачи и выполнить другие письменные задания.
Самостоятельная работа	Самостоятельная работа студентов способствует глубокому усвоения учебного материала и развитию навыков самообразования. Самостоятельная работа предполагает следующие составляющие: - работа с текстами: учебниками, справочниками, дополнительной литературой, а также проработка конспектов лекций; - выполнение домашних заданий и расчетов; - работа над темами для самостоятельного изучения; - участие в работе студенческих научных конференций, олимпиад; - подготовка к промежуточной аттестации.
Подготовка к промежуточной аттестации	Готовиться к промежуточной аттестации следует систематически, в течение всего семестра. Интенсивная подготовка должна начаться не позднее, чем за месяц-полтора до промежуточной аттестации. Данные перед экзаменом, экзаменом три дня эффективнее всего использовать для повторения и систематизации материала.