МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ ТАДЖИКИСТАН
МЕЖГОСУДАРСТВЕННОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«РОССИЙСКО-ТАДЖИКСКИЙ (СЛАВЯНСКИЙ) УНИВЕРСИТЕТ»

«Утверждаю»
Декан естественнонаучного факультета
_____ Пещукович А.И.
«____»_____2026 г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

Защита в операционных системах

Направление подготовки - 10.03.01 «Информационная безопасность»
Профиль подготовки – Безопасность компьютерных систем (по отрасли или в сфере профессиональной деятельности)
Форма подготовки – Очная
Уровень подготовки – Бакалавриат

ДУШАНБЕ - 2026

Рабочая программа составлена на основе требований федерального государственного образовательного стандарта высшего образования по направлению подготовки 10.03.01 «Информационная безопасность» **(**уровень Бакалавриат), утвержденного приказом Министерства образования и науки РФ №524 от 08.06.2017 г., Концепции преподавания Защита в операционных системах для специальностей и направлений подготовки, реализуемых в образовательных организациях высшего образования, утвержденной протоколом Экспертного совета по развитию исторического образования Минобрнауки РФ от 06.08.2024 г. №ВФ/35-ПР

При разработке рабочей программы учитываются

- содержание программ дисциплин, изучаемых на предыдущих и последующих этапах обучения;
- новейшие достижения в данной предметной области.

Рабочая программа обсуждена на заседании кафедры Кафедра информатики и информационных технологий протокол №1 от «___» _____ 2025 г.

Рабочая программа утверждена УМС естественнонаучного факультета протокол №1 от «___» _____ 2025 г.

Рабочая программа утверждена Ученым советом естественнонаучного факультета, протокол № 1 от «___» _____ 2025 г.

1. ЦЕЛИ И ЗАДАЧИ ИЗУЧЕНИЯ ДИСЦИПЛИНЫ

Актуальность изучения дисциплины «Защита в операционных системах»

1.1 Цели изучения дисциплины Целью освоения дисциплины "Защита в операционных системах" является формирование у студентов теоретических знаний и практических навыков в области защиты информации в операционных системах. Дисциплина направлена на изучение механизмов защиты, уязвимостей, угроз и способов противодействия им. В результате изучения дисциплины студенты должны уметь проектировать и внедрять эффективные решения по защите ОС.

1.2 Задачи изучения дисциплины Изучение архитектуры и принципов работы операционных систем с точки зрения безопасности. Ознакомление с различными типами угроз и уязвимостей, характерными для операционных систем. Изучение механизмов защиты, реализованных в современных операционных системах (Linux, Windows). Формирование практических навыков настройки и администрирования систем защиты. Развитие навыков анализа безопасности и разработки мер противодействия угрозам.

1.3 В результате изучения дисциплины «Защита в операционных системах» у обучающихся формируются следующие универсальные и общепрофессиональные компетенции:

Код	Результаты освоения ООП	Индикаторы достижения компетенции	Вид оценочного знания
УК-2.	Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений	"ИУК-2.1 Формулирует совокупность взаимосвязанных задач. ИУК-2.2 Определяет ресурсное обеспечение. ИУК-2.3 Выявляет правовые нормы, предъявляемые к способам решения профессиональных задач. ИУК-2.4 Выполняет задачи в рамках своей ответственности и при	

		необходимости корректирует способы их решения."	
ПК-2.	Способен разрабатывать и адаптировать прикладное программное обеспечение	ИПК-2.1 Применяет современные технологии разработки и адаптации прикладного ПО. ИПК-2.2 Разрабатывает и адаптирует ПО на современных языках программирования. ИПК-2.3 Применяет современные технологии для разработки веб-приложений.	
ПК-3.	Способен проектировать информационные системы по видам обеспечения	ИПК-3.1 Обосновывает выбор проектных решений по видам обеспечения ИС. ИПК-3.2 Участвует в проектировании экономических ИС и их модулей.	

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

2.1. Дисциплина **«Защита в операционных системах»** входит в обязательную часть Блока Дисциплины (модули) ОПОП ВО и является её базовой частью **(Б1.В.11).** В процессе преподавания данного курса учитываются знания студентов по таким дисциплинам, как история таджикского народа, история первобытного общества, история древнего мира и средних веков, изучавшихся ими в общеобразовательной средней школе.

2.2 Преподавание данной дисциплины является необходимым для дальнейшего освоения студентами дисциплин в структуре ОПОП бакалавриата по направлению **«Информационная безопасность».**

Таблица 2.

№ п/п	Название дисциплины	Семестр	Место дисциплины в структуре ОПОП

-	—	—	Предшествующая дисциплина
-	—	—	Последующая дисциплина

При освоении данной дисциплины необходимы умения и готовность («входные» знания) обучающегося по дисциплинам, указанных в Таблице 2. Дисциплины взаимосвязаны с данной дисциплиной, они изучаются параллельно. Теоретическими дисциплинами, для которых освоение данной дисциплины необходимо как предшествующее являются:

3. СТРУКТУРА И СОДЕРЖАНИЕ КУРСА, КРИТЕРИИ НАЧИСЛЕНИЯ БАЛЛОВ

Преподавание курса «Защита в операционных системах» планируется студентам Очная формы обучения по направлению «Информационная безопасность».

Объем дисциплины составляет __ зачетные единицы. Всего запланировано 126 часа, из которых: лекции – 32 часов, практические занятия – 14 часов, лабораторные работы 16 часов, иная контактная работа – 32 часа, самостоятельная работа – 46. Всего часов аудиторной нагрузки – 80 часа.

По итогам 7 семестра планируется сдача студентами зачета с оценкой.

3.1 Структура и содержание теоретической части курса

Лекция 1 Введение в защиту информации в ОС. Основные понятия и определения.

Обзор дисциплины. Актуальность защиты информации. Модели угроз и нарушителей. Политики безопасности. Стандарты в области информационной безопасности.

Лекция 2 Архитектура операционных систем и её влияние на безопасность.

Обзор архитектуры ОС. Ядро, системные вызовы. Взаимодействие процессов. Привилегированный и непривилегированный режимы.

Лекция 3 Механизмы аутентификации и авторизации.

Пароли, биометрия, многофакторная аутентификация. Ролевая модель доступа. Списки управления доступом (ACL).

Лекция 4 Управление целостностью ОС. Криптографические методы защиты.

Хеширование. Цифровые подписи. Контроль изменений файлов. Обнаружение вредоносного ПО.

Лекция 5 Защита памяти и процессов.

Сегментация и страничная организация памяти. Защита памяти от переполнения буфера. ASLR, DEP.

Лекция 6 Безопасность файловых систем.

Механизмы шифрования файловых систем. Журналирование. Управление доступом к файлам.

Лекция 7 Безопасность сети в ОС.

Межсетевые экраны. Обнаружение вторжений. VPN. Безопасность протоколов.

Лекция 8 Аудит безопасности и анализ журналов.

Системы аудита. Анализ журналов событий. Обнаружение аномалий и инцидентов.

Лекция 9 Безопасность виртуализации

Основные понятия виртуализации. Угрозы безопасности в виртуализированных средах. Защита виртуальных машин.

Лекция 10 Безопасность облачных вычислений

Основные понятия облачных вычислений. Угрозы безопасности в облачных средах. Защита облачных ресурсов.

Лекция 11 Правовые аспекты информационной безопасности

Законодательство в области ИБ. Ответственность за нарушения. Защита персональных данных.

Лекция 12 Стандарты и лучшие практики информационной безопасности

Обзор стандартов ISO 27000, NIST. Лучшие практики, инструменты и методы защиты.

Лекция 13 Особенности защиты в Windows

Архитектура Windows, механизмы защиты (UAC, BitLocker, AppLocker), уязвимости.

Лекция 14 Особенности защиты в Linux

Архитектура Linux, механизмы защиты (SELinux, AppArmor), уязвимости.

Лекция 15 Современные атаки и методы защиты.

Атаки на операционные системы. Методы защиты от современных угроз.

Лекция 16 Перспективы развития защиты информации в ОС

Новые технологии и подходы к защите. Квантовая криптография. Искусственный интеллект в ИБ.

Структура и содержание практической части курса

Практическое занятие 1 Установка и настройка виртуальной машины. Обзор операционных систем. (Практика)

Установка и настройка виртуальной машины (VirtualBox, VMware). Обзор различных операционных систем и их интерфейсов.

Практическое занятие 2 Практикум по анализу политик безопасности. (Практика)

Анализ и настройка политик безопасности в Windows.

Практическое занятие 3 Практикум по настройке политик безопасности

Анализ и настройка политик безопасности в Linux.

Практическое занятие 4 Практикум по настройке аутентификации и авторизации. (Практика)

Настройка парольной политики, двухфакторной аутентификации.

Практическое занятие 5 Настройка механизмов защиты файловых систем. (Практика)

Шифрование файловых систем, настройка прав доступа.

Практическое занятие 6 Настройка межсетевых экранов и обнаружение вторжений. (Практика)

Настройка межсетевых экранов (firewall) в Windows и Linux. Обнаружение вторжений с помощью Snort.

Практическое занятие 7 Практикум по анализу журналов событий. (Практика)

Анализ журналов Windows и Linux, поиск подозрительной активности.

Практическое занятие 8 Практикум по настройке VPN. (Практика)

Настройка VPN-соединения.

Структура и содержание лабораторной части курса

Лабораторная работа 1 Установка и настройка виртуальной машины. Обзор операционных систем.

Установка и настройка виртуальной машины (VirtualBox, VMware). Обзор различных операционных систем и их интерфейсов.

Лабораторная работа 2 Практикум по анализу политик безопасности.

Анализ и настройка политик безопасности в Windows.

Лабораторная работа 3 Практикум по настройке политик безопасности

Анализ и настройка политик безопасности в Linux.

Лабораторная работа 4 Практикум по настройке аутентификации и авторизации.

Настройка парольной политики, двухфакторной аутентификации.

Лабораторная работа 5 Настройка механизмов защиты файловых систем.

Шифрование файловых систем, настройка прав доступа.

Лабораторная работа 6 Настройка межсетевых экранов и обнаружение вторжений.

Настройка межсетевых экранов (firewall) в Windows и Linux. Обнаружение вторжений с помощью Snort.

Лабораторная работа 7 Практикум по анализу журналов событий.

Анализ журналов Windows и Linux, поиск подозрительной активности.

Лабораторная работа 8 Практикум по настройке VPN.

Настройка VPN-соединения.

Структура и содержание КСР

КСР 1 Анализ угроз и уязвимостей ОС.

Анализ конкретной операционной системы (Windows/Linux) с точки зрения угроз безопасности.

КСР 2 Разработка модели угроз.

Построение модели угроз для заданной информационной системы.

КСР 3 Разработка политик безопасности для ОС.

Разработка политик безопасности для конкретного сценария использования ОС.

КСР 4 Настройка системы аудита безопасности.

Настройка системы аудита безопасности на примере Windows или Linux.

КСР 5 Оценка защищенности ОС.

Проведение оценки защищенности ОС с использованием сканеров уязвимостей.

КСР 6 Разработка мер по защите от атак.

Разработка плана мероприятий по защите от конкретной атаки.

КСР 7 Анализ журналов безопасности.

Анализ журналов безопасности для выявления инцидентов.

КСР 8 Защита информации в виртуализированных средах

Анализ безопасности виртуализированных сред.

Структура и содержание СРС

СРС 1 Изучение истории развития ОС и угроз безопасности.

Подготовка реферата по истории развития ОС и угроз безопасности.

СРС 2 Анализ современных угроз и атак на ОС.

Обзор современных угроз и атак на ОС. Подготовка презентации.

СРС 3 Изучение стандартов и лучших практик безопасности.

Изучение стандартов и лучших практик безопасности (ISO, NIST).

СРС 4 Исследование механизмов защиты в Windows.

Изучение конкретных механизмов защиты в Windows. Подготовка презентации.

СРС 5 Исследование механизмов защиты в Linux.

Изучение конкретных механизмов защиты в Linux. Подготовка презентации.

СРС 6 Изучение инструментов аудита безопасности.

Обзор и практическое применение инструментов аудита безопасности. Подготовка отчета.

СРС 7 Анализ уязвимостей ОС с помощью сканеров.

Самостоятельная работа по сканированию уязвимостей. Подготовка отчета.

СРС 8 Разработка плана защиты от конкретной атаки.

Подготовка плана действий по защите от конкретной атаки.

СРС 9 Исследование безопасности облачных сервисов

Изучение безопасности облачных сервисов. Подготовка презентации.

СРС 10 Исследование безопасности виртуализированных систем

Изучение безопасности виртуализированных систем. Подготовка презентации.

СРС 11 Анализ правовых аспектов информационной безопасности

Изучение законодательства в области ИБ. Подготовка реферата.

СРС 12 Анализ современных методов защиты

Изучение современных методов защиты. Подготовка презентации.

СРС 13 Разработка модели угроз для организации

Разработка модели угроз для заданной организации. Подготовка отчета.

СРС 14 Изучение уязвимостей zero-day

Изучение уязвимостей zero-day. Подготовка реферата.

СРС 15 Анализ реальных инцидентов ИБ

Изучение реальных инцидентов ИБ. Подготовка презентации.

СРС 16 Подготовка к контрольной работе / экзамену

Повторение материала дисциплины.

СРС 17 Подготовка к экзамену

Систематизация знаний, подготовка к итоговому контролю.

СРС 18 Работа над курсовым проектом

Работа над курсовым проектом.

СРС 19 Разработка сценария реагирования на инциденты

Разработка сценария реагирования на инциденты.

СРС 20 Анализ и сравнение различных инструментов ИБ

Сравнение и анализ различных инструментов ИБ. Подготовка обзора.

СРС 21 Изучение лучших практик управления безопасностью

Изучение лучших практик управления безопасностью. Подготовка презентации.

СРС 22 Работа над курсовым проектом

Завершение работы над курсовым проектом.

СРС 23 Самостоятельное изучение дополнительных материалов

Поиск и изучение материалов по выбранной теме.

Структура и содержание теоретической, лабораторной части курса, КСР и СРС

Таблица 3.

№ п/п	Наименование темы	Виды учебной работы, включая самостоятельную работу студентов и трудоемкость (в часах)						Литература	Количество баллов
		Лек	Прак	КСР	Лаб	СРС	ИКР		
1	Введение в защиту информации в ОС. Основные понятия и определения.	2						5	12,5

	Установка и настройка виртуальной машины. Обзор операционных си-стем.		2			3	3	4	
2	Архитектура операционных систем и её влияние на безопасность.	2						7	12,5
	Установка и настройка виртуальной машины. Обзор операционных си-стем.				2		3	5	
	Анализ угроз и уязвимостей ОС.			2					
3	Механизмы аутентификации и авторизации.	2						6	12,5
	Практикум по анализу политик безопасности.		2			3	3	7	
4	Управление целостностью ОС. Криптографические методы защиты.	2						5	12,5
	Практикум по анализу политик безопасности.				2		4	2	
	Разработка модели угроз.			2					
5	Защита памяти и процессов.	2						3	12,5
	Практикум по настройке политик безопасности		2			4	3	2	
6	Безопасность файловых систем.	2						1	12,5
	Практикум по настройке политик безопасности				2		3	4	
	Разработка политик безопасности для ОС.			2					
7	Безопасность сети в ОС.	2						5	12,5
	Практикум по настройке аутентификации и авторизации.		2			3	4	2	
8	Аудит безопасности и анализ журналов.	2						7	12,5
	Практикум по настройке аутентификации и авторизации.				2		3	1	
	Настройка системы аудита безопасности.			2					
9	Безопасность виртуализации	2						5	12,5
	Настройка механизмов защиты файловых систем.		2			4	3	4	
10	Безопасность облачных вычислений	2						6	12,5
	Настройка механизмов защиты файловых систем.				2		4	2	
	Оценка защищенности ОС.			2					
11	Правовые аспекты информационной безопасности	2						4	12,5

	Настройка межсетевых экранов и обнаружение вторжений.		2			3	3	7	
12	Стандарты и лучшие практики информационной безопасности	2						5	12,5
	Настройка межсетевых экранов и обнаружение вторжений.				2		4	2	
	Разработка мер по защите от атак.			2					
13	Особенности защиты в Windows	2						1	12,5
	Практикум по анализу журналов событий.		2			4	3	2	
14	Особенности защиты в Linux	2						3	12,5
	Практикум по анализу журналов событий.				2		3	5	
	Анализ журналов безопасности.			2					
15	Современные атаки и методы защиты.	2						2	12,5
	Практикум по настройке VPN.		2			4	4	4	
16	Перспективы развития защиты информации в ОС	2						6	12,5
	Практикум по настройке VPN.				2		3	7	
	Защита информации в виртуализированных средах			2					
Итого:		**32**	**16**	**16**	**16**	**28**	**53**		**200**

Формы контроля и критерии начисления баллов

Контроль усвоения студентом каждой темы осуществляется в рамках балльно-рейтинговой системы (БРС), включающей текущий, рубежный и итоговый контроль. Студенты **4 -го курса**, обучающиеся по кредитно-рейтинговой системе обучения, могут получить максимально возможное количество баллов - 300. Из них на текущий и рубежный контроль выделяется 200 баллов или 49% от общего количества.

На итоговый контроль знаний студентов выделяется 51% или 100 баллов.

Порядок выставления баллов: 1-й рейтинг (1-7 недели до 12,5 баллов+12,5 баллов (8 неделя – Рубежный контроль №1) = 100 баллов), 2-й рейтинг (9-15 недели до 12,5 баллов+12,5 баллов (16 неделя – Рубежный контроль №2) = 100 баллов), итоговый контроль 100 баллов.

К примеру, за текущий и 1-й рубежный контроль выставляется 100 баллов:

лекционные занятия – 21 балл, за практические занятия (КСР, лабораторные) – 31,5 балл, за СРС – 17,5 баллов, требования ВУЗа – 17,5 баллов, рубежный контроль – 12,5 баллов.

В случае пропуска студентом занятий по уважительной причине (при наличии подтверждающего документа) в период академической недели деканат факультета обращается к проректору по учебной работе с представлением об отработке студентом баллов за пропущенные дни по каждой отдельной дисциплине с последующим внесением их в электронный журнал.

Итоговая форма контроля по дисциплине (зачет, экзамен) проводится как в форме тестирования, так и в традиционной (устной) форме. Тестовая форма итогового контроля по дисциплине предусматривает: для естественнонаучных направлений – 10 тестовых вопросов на одного студента, где правильный ответ оценивается в 10 баллов, для гуманитарных направлений – 25 тестовых вопросов, где правильный ответ оценивается в 4 балла. Тестирование проводится в электронном виде, устный экзамен на бумажном носителе с выставлением оценки в ведомости по аналогичной системе с тестированием.

Таблица 4.

Неделя	Активное участие на лекционных занятиях, написание конспекта и выполнение других видов работ*	Активное участие на практических (семинарских) занятиях, КСР	СРС Написание реферата, доклада, эссе Выполнение других видов работ	Выполнение положения высшей школы (установленная форма одежды, наличие рабочей папки, а также других пунктов устава высшей школы)	РК №1	Всего
1	2	3	4	5	6	7
1	3	4,5	2,5	2,5	-	12,5
2	3	4,5	2,5	2,5	-	12,5
3	3	4,5	2,5	2,5	-	12,5
4	3	4,5	2,5	2,5	-	12,5
5	3	4,5	2,5	2,5	-	12,5
6	3	4,5	2,5	2,5	-	12,5
7	3	4,5	2,5	2,5	-	12,5
8	-	-	-	-	12,5	12,5
Первый рейтинг	21	31,5	17,5	17,5	12,5	100
1	2	3	4	5	6	7

1	3	4,5	2,5	2,5	-	12,5
2	3	4,5	2,5	2,5	-	12,5
3	3	4,5	2,5	2,5	-	12,5
4	3	4,5	2,5	2,5	-	12,5
5	3	4,5	2,5	2,5	-	12,5
6	3	4,5	2,5	2,5	-	12,5
7	3	4,5	2,5	2,5	-	12,5
8	-	-	-	-	12,5	12,5
Второй рейтинг	21	31,5	17,5	17,5	12,5	100
Итог						200

Формула вычисления результатов дистанционного контроля и итоговой формы контроля по дисциплине за семестр для студентов 4 -го курсов:

$$ИБ = \left[\frac{(P_1 + P_2)}{2}\right] \cdot 0{,}49 + Эи \cdot 0{,}51 \ ,$$

где ИБ –итоговый балл, P_1- итоги первого рейтинга, P_2- итоги второго рейтинга, *Эи*– результаты итоговой формы контроля (экзамен).

4. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ

Учебно-методическое обеспечение самостоятельной работы обучающихся по дисциплине «Методы обработки информации» включает в себя:

1. план-график выполнения самостоятельной работы по дисциплине, в том числе примерные нормы времени на выполнение по каждому заданию;

2. характеристика заданий для самостоятельной работы обучающихся и методические рекомендации по их выполнению;

3. требования к представлению и оформлению результатов самостоятельной работы;

4. критерии оценки выполнения самостоятельной работы.

План-график выполнения самостоятельной работы по дисциплине

4.1. План-график выполнения самостоятельной работы по дисциплине

№	Объем СРС, ч.	Тема СРС	Форма и вид результатов самостоятельной работы	Форма контроля
1	4	Понятие защиты в операционных системах	Вопросы 1–4. Описание технологии разработки, реферат	Опрос
2	4	Архитектура операционных систем и безопасность	Вопросы 5–8. Презентация методов	Выступление
3	6	Модели безопасности операционных систем	Вопросы 8–10. Презентация, доклад	Выступление
4	6	Управление пользователями и правами доступа	Вопросы 11–13. Выполнение задания 1 (1–10)	Защита работы, выступление
5	4	Аутентификация и авторизация в ОС	Выполнение задания 1. Конспект, презентация (вопросы 14–15)	Опрос, выступление
6	4	Разграничение доступа к файлам и каталогам	Выполнение задания 2	Защита работы
7	6	Защита процессов и памяти	Вопросы 16–17. Выполнение задания 3	Защита работы
8	6	Журналирование и аудит событий безопасности	Вопросы 16–17. Выполнение задания 4	Защита работы
9	4	Защита загрузки и целостности ОС	Выполнение задания 5	Защита работы
10	4	Встроенные средства защиты ОС (брандмауэр, антивирус)	Вопросы 18–25. Выполнение задания 6	Защита работы
11	4	Управление обновлениями и патчами	Вопросы 26–29. Выполнить задания 2 и описать в терминах классов	Опрос, защита работы
12	4	Виртуализация и безопасность	Вопросы 30–31. Реферат. Выполнение задания 7	Защита реферата, защита работы
13	4	Контейнеризация и безопасность	Вопросы 32–37. Презентация	Опрос, выступление
14	4	Защита мобильных операционных систем	Вопросы 38–40. Выполнение задания 8 (1–4)	Защита работы
15	4	Реагирование на инциденты в ОС	Вопросы 41–44. Выполнение задания 9	Защита работы
16	4	Комплексная настройка безопасности операционной системы	Вопросы 45–46. Выполнение задания 8 (4–10)	Защита работы

4.2 Характеристика заданий для самостоятельной работы обучающихся и методические рекомендации по их выполнению;

Для выполнения задания, прежде всего, необходимо ознакомиться и изучить основные положения теоретических материалов соответствующей темы из литературных источников. Они указаны в разделе «Содержание и структура дисциплины». Конспекты и задания можно выполнить в отдельном тетради или в

лекционной (практической) тетради в произвольной форме.

4.3 Критерии оценки выполнения самостоятельной работы.

Критерии оценки выполнения самостоятельной работы является полнота освещения вопроса, логичность изложения, проявления самостоятельность в обработке материала.

4.4. Критерии оценки выполнения самостоятельной работы.

Самостоятельная работа прививает студентам навыки работы с источниками и учебной литературой, помогает повысить уровень знаний по предмету, которые можно использовать на практике.

Оценка «отлично» выставляется студенту, если индивидуальное задание выполнено полностью и по данной теме защищена лабораторная работа.

Оценка «хорошо» выставляется студенту, если лабораторная работа по теме индивидуального задания защищена, а само индивидуальное задание выполнено с отдельными замечаниями.

Оценка «удовлетворительно» выставляется студенту, если лабораторная работа по теме индивидуального задания защищена, а само индивидуальное задание выполнено не до конца, т.е. не полностью.

Оценка «неудовлетворительно» выставляется студенту, если лабораторная работа по теме индивидуального задания не защищена, а само индивидуальное задание выполнено не до конца, т.е. не полностью.

5. СПИСОК УЧЕБНОЙ ЛИТЕРАТУРЫ И ИНФОРМАЦИОННО-МЕТОДИЧЕСКОЕ ОБЕСПЕ- ЧЕНИЕ ДИСЦИПЛИНЫ

5.1. Основная литература:

1. 1. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы. 2019. 944 стр.

2. Ромашов П.А. Защита информации в операционных системах: Учебник и практикум для вузов. 2020. 320 стр.

3. Гаврилов А.В. Безопасность операционных систем. 2020. 256 стр.

4. Хорев А.А. Защита информации в компьютерных системах: учеб. пособие. 2020. 336 с.

5. Щербаков А.Ю. Безопасность Linux. 2020. 416 стр.

6. Андреев А.В. Основы информационной безопасности. 2019. 288 стр.

7. Стоцкий А.Ю. Информационная безопасность: Учебное пособие. 2019. 256 стр.

5.2. Учебники и учебные пособия в сети Интернет:

1. 1. Курбанов Р.А. Информационная безопасность: учебник. 2018. 320 с.

2. Малкин В.И. Защита информации в компьютерных системах. 2018. 272 с.

3. Петров А.А. Безопасность компьютерных сетей. 2017. 352 с.

4. Сенин А.В. Безопасность операционных систем Windows: практическое руководство. 2017. 224 с.

5. Гусев А.В. Теория и практика защиты информации. 2017. 480 с.

6. Воробьев С.А. Безопасность операционных систем. 2016. 192 с.

7. Долинский А.В. Безопасность Linux: практическое руководство. 2016. 288 с.

5.3. Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

1. 1. OWASP (Open Web Application Security Project): https://owasp.org/

2. NIST (National Institute of Standards and Technology): https://www.nist.gov/

3. CERT (Computer Emergency Response Team): https://www.cert.org/

4. SANS Institute: https://www.sans.org/

5. Хабр: https://habr.com/

5.4. Перечень информационных технологий и программного обеспечения

Используются лицензионное программное обеспечение ОС Windows -/11 и программное обеспечение открытого доступа (Open source), среды

программирования (Denwer, CodeBlock, Dev_C++ и др.). Для разработки моделей проекта ИС используются CASE – средства: ERWin, Visual UML, Rational Rose и т.д.

6. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Для обеспечения систематической и регулярной работы по изучению дисциплины «Защита в операционных системах» и успешного прохождения текущих и итоговых контрольных испытаний студенту рекомендуется придерживаться следующего порядка обучения:

1. Самостоятельно определить объем времени, необходимого для проработки каждой темы.

2. Регулярно изучать каждую тему дисциплины, используя различные формы индивидуальной работы.

3. Согласовывать с преподавателем виды работы по изучению дисциплины.

4. По завершении отдельных тем передавать выполненные работы (рефераты) преподавателю.

Обучение по дисциплине «Защита в операционных системах» строится следующим образом. На лекциях преподаватель дает общую характеристику рассматриваемого вопроса, различные научные концепции или позиции, которые есть по данной теме. Во время лекции рекомендуется составлять конспект, фиксирующий основные положения лекции и ключевые определения по пройденной теме. Во время лекционного занятия необходимо фиксировать все спорные моменты и проблемы, на которых останавливается преподаватель. Потом именно эти аспекты станут предметом самого пристального внимания и изучения на практических занятиях.

При подготовке к практическому занятию обязательно требуется изучение дополнительной литературы по теме занятия. Без использования нескольких источников информации невозможно проведение дискуссии на занятиях, обоснование собственной позиции, построение аргументации. Если обсуждаемый аспект носит дискуссионный характер, следует изучить существующие точки зрения и выбрать тот подход, который вам кажется наиболее верным. При этом

следует учитывать необходимость обязательной аргументации собственной позиции. Во время практических занятий рекомендуется активно участвовать в обсуждении рассматриваемой темы, выступать с подготовленными заранее рефератами, докладами и презентациями.

Самостоятельная работа должна соответствовать графику прохождения программы дисциплины. Самостоятельная работа по дисциплине «Защита в операционных системах» включает:

а) работу с литературой;

б) подготовку устного выступления на практическом занятии;

в) подготовку к занятию в интерактивной форме;

г) подготовку реферата с презентацией;

д) подготовку к дискуссии;

е) заполнение хронологической таблицы;

ж) подготовку к текущей и итоговой аттестации по дисциплине.

Для теоретического и практического усвоения дисциплины большое значение имеет самостоятельная работа студентов, которая может осуществляться студентами индивидуально и под руководством преподавателя.

Самостоятельная работа студентов предполагает самостоятельное изучение отдельных тем, дополнительную подготовку студентов к каждому практическому занятию.

Самостоятельная работа студентов является важной формой образовательного процесса. Она реализуется непосредственно в процессе аудиторных занятий, в контакте с преподавателем, а также в библиотеке, дома, при выполнении студентом учебных и творческих задач.

Цель самостоятельной работы студентов - научить студента осмысленно и самостоятельно работать сначала с учебным материалом, затем с научной информацией, заложить основы самоорганизации и самовоспитания с тем, чтобы привить умение в дальнейшем непрерывно повышать свою квалификацию.

При изучении дисциплины организация самостоятельной работы студентов форм представлена следующим образом:

1) внеаудиторная самостоятельная работа;

2)аудиторная самостоятельная работа, которая осуществляется под непосредственным руководством преподавателя.

Аудиторная самостоятельная работа может реализовываться при проведении практических занятий и во время чтения лекций.

На практических занятиях различные виды самостоятельной работы позволяют сделать процесс обучения более интересным и поднять активность значительной части студентов в группе.

Для проведения занятий необходимо иметь большой банк заданий, причем эти задания могут быть дифференцированы по степени сложности.

На каждом этапе самостоятельной работы следует разъяснять цели работы, контролировать понимание этих целей студентами, постепенно формируя у них умение самостоятельной постановки задачи и выбора цели.

При чтении лекционного курса непосредственно в аудитории необходимо контролировать усвоение материала основной массой студентов

путем проведения экспресс-опросов по конкретным темам.

На практических занятиях различные виды самостоятельной работы позволяют сделать процесс обучения более интересным и поднять активность значительной части студентов в группе.

На практических занятиях нужно не менее 1 часа из двух (50% времени) отводить на самостоятельное рассмотрение заданий.

По результатам самостоятельного рассмотрения задания следует выставлять по каждому занятию оценку. Оценка предварительной подготовки студента к практическому занятию может быть сделана путем экспресс-опроса в течение 5, максимум - 10 минут.

По материалам раздела целесообразно выдавать студенту домашнее задание и на последнем практическом занятии по разделу подвести итоги его изучения (например, провести контрольную работу), обсудить оценки каждого студента, выдать дополнительные задания тем студентам, которые хотят повысить оценку.

Результативность самостоятельной работы студентов во многом

определяется наличием активных методов ее контроля. Существуют следующие виды контроля:

- входной контроль знаний и умений студентов при начале изучения очередной дисциплины;

- текущий контроль, то есть регулярное отслеживание уровня усвоения материала на лекциях, практических занятиях;

- самоконтроль, осуществляемый студентом в процессе изучения дисциплины при подготовке к контрольным мероприятиям;

- итоговый контроль по дисциплине в виде зачета, зачета с оценкой (в устной форме).

7. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Для реализации дисциплины при кафедре информатики и ИТ РТСУ имеются 4 компьютерных классов. Для занятий используются лицензионное программное обеспечение ОС Windows -7/8/10/11 и программное обеспечение открытого доступа (Open source), среды программирования (Denwer, CodeBlock, Dev_C++ и др.). Для разработки моделей проекта ИС используются CASE – средства: ERWin, Visual UML, Rational Rose и т.д.

В Университете созданы специальные условия для обучающихся с ограниченными возможностями здоровья - специальные учебники, учебные пособия и дидактические материалы, специальные технические средства обучения коллективного и индивидуального пользования, предоставление услуг ассистента (помощника), оказывающего обучающимся необходимую техническую помощь, проведение групповых и индивидуальных коррекционных занятий, обеспечение доступа в здания организаций и другие условия, без которых невозможно или затруднено освоение дисциплины обучающимися с ограниченными возможностями здоровья.

Обучающимся с ограниченными возможностями здоровья предоставляются бесплатно специальные учебники и учебные пособия, иная учебная литература, а также обеспечивается:

- наличие альтернативной версии официального сайта организации в сети "Интернет" для слабовидящих;

- присутствие ассистента, оказывающего обучающемуся необходимую помощь;

- обеспечение выпуска альтернативных форматов печатных материалов (крупный шрифт или аудиофайлы);

- возможность беспрепятственного доступа обучающихся в учебные помещения, столовые, туалетные и другие помещения организации, а также пребывания в указанных помещениях (наличие пандусов, поручней, расширенных дверных проёмов, лифтов).

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

Промежуточная аттестации осуществляется: для зачета – контрольная работа и опрос. Экзамен проводится в форме тестирования. Защита курсового проекта: представляется пояснительная записка и презентация выступления.

Текущий контроль студентов осуществляется путем защиты лабораторных работ, выполнения самостоятельного задания, обсуждения теоретических вопросов.

Контролирующие материалы по дисциплине содержат:

Контрольные вопросы и задания для текущего контроля знаний по дисциплине.

Тестовые задания для промежуточного контроля знаний по дисциплине;

Методические рекомендации и тематика курсового проектирования.

Также указаны критерии оценки курсового проекта.

Итоговая система оценок по кредитно-рейтинговой системе с использованием буквенных символов

Оценка по буквенной системе	Диапазон соответствующих наборных баллов	Численное выражение оценочного балла	Оценка по традиционной системе

A	10	95-100	Отлично
A-	9	90-94	
B+	8	85-89	Хорошо
B	7	80-84	
B-	6	75-79	
C+	5	70-74	Удовлетворительно
C	4	65-69	
C-	3	60-64	
D+	2	55-59	
D	1	50-54	
Fx	0	45-49	Неудовлетвори-тельно
F	0	0-44	

Содержание текущего контроля, промежуточной аттестации, итогового контроля раскрываются в фонде оценочных средств, предназначенных для проверки соответствия уровня подготовки по дисциплине требованиям ФГОС ВО.

ФОС по дисциплине является логическим продолжением рабочей программы учебной дисциплины. ФОС по дисциплине прилагается.