МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ, СВЯЗИ
И МАССОВЫХ КОММУНИКАЦИЙ РОССИЙСКОЙ ФЕДЕРАЦИИ
Северо-Кавказский филиал
ордена Трудового Красного Знамени федерального государственного
бюджетного образовательного учреждения высшего образования
«Московский технический университет связи и информатики»

Утверждаю
Зам. директора по УВР
_____ Н.А. Андреева
«29» 04 2024 г.

Безопасность операционных систем Б1.О.36.01

рабочая программа дисциплины

Кафедра: **Информационной безопасности**
Направление подготовки: **10.03.01 Информационная безопасность**
Профиль: **Безопасность компьютерных систем (по отрасли или в сфере профессиональной деятельности)**
Формы обучения: **очная**

Распределение часов дисциплины по семестрам (для очной формы обучения (ОФО))

Вид учебной работы	ОФО	
	ЗЕ	часов
Общая трудоемкость дисциплины, в том числе (по семестрам, курсам):	3	108/5 сем
Контактная работа, в том числе (по семестрам, курсам):		52/5 сем
Лекции		18/5 сем
Лабораторных работ		18/5 сем
Практических занятий		16/5 сем
Семинаров		
Самостоятельная работа		56/5 сем
Контроль		
Число контрольных работ (по курсам)		
Число КР (по семестрам, курсам)		
Число КП (по семестрам, курсам)		
Число зачетов с разбивкой по семестрам (курсам)		1/5 сем
Число экзаменов с разбивкой по семестрам (курсам)		

Программу составил:
Доцент кафедры ИВТ, к.т.н., с.н.с. Ткачук Е.О.

Рецензенты:
Ведущий сотрудник ФГУП «РНИИРС», д.т.н., доцент Елисеев А.В.

Рабочая программа дисциплины
«Безопасность операционных систем»

разработана в соответствии с ФГОС ВО:
направления подготовки 10.03.01 «Информационная безопасность», утвержденным приказом Министерства образования и науки Российской Федерации от 17 ноября 2020 г. N 1427.

Составлена на основании учебного плана
направления 10.03.01 «Информационная безопасность», профиля «Безопасность компьютерных систем (по отрасли или в сфере профессиональной деятельности)», одобренного Учёным советом СКФ МТУСИ, протокол № 9 от 22.04.2024, и утвержденного директором СКФ МТУСИ 22.04.2024 г.

Рассмотрена и одобрена на заседании кафедры
«Информационная безопасность»

Протокол от «24» апреля 2024 г. № 9

Зав. кафедрой _____ Д.В. Маршаков

Визирование для использования в 20__/20__ уч. году

Утверждаю
Зам. директора по УВР _____
-__ _____ 20__ г.
Рабочая программа пересмотрена, обсуждена и одобрена на заседании кафедры
"Информационная безопасность"

Протокол от _ _____ 20__ г. № _
Зав. кафедрой _____

Визирование для использования в 20__/20__ уч. году

Утверждаю
Зам. директора по УВР _____
-__ _____ 20__ г.
Рабочая программа пересмотрена, обсуждена и одобрена на заседании кафедры

"Информационная безопасность"

Протокол от _ _____ 20__ г. № _
Зав. кафедрой _____

Визирование для использования в 20__/20__ уч. году

Утверждаю
Зам. директора по УВР _____
-__ _____ 20__ г.
Рабочая программа пересмотрена, обсуждена и одобрена на заседании кафедры
"Информационная безопасность"

Протокол от _ _____ 20__ г. № _
Зав. кафедрой _____

---

1. Цели изучения дисциплины

Целями изучения дисциплины **"Безопасность операционных систем"** является изучение принципов функционирования операционных систем и основных методов и средств обеспечивающих их безопасность.

2. Планируемые результаты обучения

Изучение дисциплины направлено на формирование у выпускника способности решать профессиональные задачи в соответствии с ***организационно-управленческой деятельностью.***

Результатом освоения дисциплины являются сформированные у выпускника следующие компетенции:

Компетенции выпускника, формируемые в результате освоения дисциплины (в части, обеспечиваемой дисциплиной)
ОПК-1.1: способен разрабатывать и реализовывать политики управления доступом в компьютерных системах
Знать:
- принципы организации современных операционных систем и их администрирования - архитектуру и принципы построения и защиты операционных систем;
Уметь:
- устанавливать, настраивать, вводить в эксплуатацию, следить за правильной эксплуатацией различных операционных систем - работать со средствами защиты информации, встроенными в операционные системы
Владеть:
- навыками установки, настройки, администрирования операционных систем - основными понятиями, связанными с обеспечением информационной безопасности операционных систем

3. Место дисциплины в структуре образовательной программы

Требования к предварительной подготовке обучающегося (предшествующие дисциплины, модули, темы):	
1	Б1.О.27 Основы информационной безопасности
2	Б1.О.28 Организационное и правовое обеспечение информационной безопасности
3	Б1.О.05Введение в информационные технологии
Последующие дисциплины и практики, для которых освоение данной дисциплины необходимо:	
1	Б1.В.01 Обеспечение безопасности персональных данных в информационных системах
2	Б1.О.30 Программно-аппаратные средства защиты информации
3	Б1.О.36.06 Администрирование средств защиты информации в компьютерных системах и сетях

Рабочая программа дисциплины для инвалидов и лиц с ограниченными возможностями здоровья разрабатывается индивидуально с учетом особенностей психофизического развития, индивидуальных возможностей и состояния здоровья таких обучающихся.

4. Структура и содержание дисциплины

4.1 Очная форма обучения, 4 года (всего 108 часов, 52 аудиторных часов, 56 часов самостоятельной работы)

Код зан.	Тема и краткое содержание занятия	Вид зан.	Кол. часов	Компетенции	УМИО
Курс 3, Семестр 5					
Модуль 1. Принципы работы и угрозы безопасности ОС.					
1.1	Лекция 1. ОСОБЕННОСТИ РАБОТЫ ОПЕРАЦИОННЫХ СИСТЕМ 1. Управление системными службами и процессами в ОС 2. Управление сетевыми подключениями вОС 3. Применение консольного управления ОС 4. Действия, приводящие к неправомерному овладении конфиденциальной информацией	Л1.	2	ОПК-1.1	Л1.1 Л1.2 Л1.3
1.2	Лекция 2. ТРЕБОВАНИЯ К БЕЗОПАСНОСТИ ОС 1. Средства защиты ОС 2. Организационная защита 3. Инженерно-техническая защита	Л2.	4	ОПК-1.1	Л1.1 Л1.2 Л1.3
1.3	Лекция 3. УГРОЗЫ БЕЗОПАСНОСТИ ОС 1.Общие положения 2.Защита информации от утечки по визуально оптическим каналам 2.Защита информации от утечки по сетевым каналам 3.Защита информации от утечки по материально - вещественным каналам	Л3.	4	ОПК-1.1	Л1.1 Л1.2 Л1.3
1.4	Практическое занятие 1 Управление системными службами и процессами в ОС	ПЗ1	4	ОПК-1.1	Л3.1
1.5	Практическое занятие 2 Управление сетевыми подключениями в ОС	ПЗ2	4	ОПК-1.1	Л3.1
1.6	Лабораторная работа 1 Применение консольного управления ОС	ЛР1	4	ОПК-1.1	Л3.1
1.7	Лабораторная работа № 2 Средства защиты ОС	ЛР2	4	ОПК-1.1	
1.8	Анализ защищенности современных операционных систем 1. Анализ выполнения современными ОС формализованных требований к защите информации от несанкционированных действий 2. Основные встроенные механизмы защиты ОС и их недостатки 3. Анализ существующей статистики угроз для современных универсальных ОС. Семейства ОС и общая статистика угроз 4. Обзор и статистика методов, лежащих в основе атак	СРС	28	ОПК-1.1	Л1.1 Л1.2 Л1.3

	на современные ОС. Классификация методов и их сравнительная статистика				
Модуль 2 Основы защиты информации в инфокоммуникационных системах и сетях					
2.1	Лекция 4. МЕТОДЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ОС И ИХ АДМИНИСТРИРОВАНИЕ Структуризация методов обеспечения информационной безопасности Классификация злоумышленников Основные направления и методы реализации угроз информационной безопасности	Л3	4	ОПК-1.1	Л1.1 Л1.2 Л1.3
2.2	Лекция 5. УПРАВЛЕНИЕ ДОСТУПОМ В ОС. Аутентификация пользователей в ОС. Разграничение доступа к файловым объектам и устройствам. Разграничение доступа к запуску программного обеспечения	Л5	2	ОПК-1.1	Л1.1 Л1.2 Л1.3
2.3	Лекция 6. ПРОТОКОЛИРОВАНИЕ И СРЕДСТВА АУДИТА Средства аудита в ОС. Протоколирование событий в операционных системах	Л6	2	ОПК-1.1	Л1.1 Л1.2 Л1.3
2.4	Практическое занятие 3 Управление средствами обеспечения безопасности ОС	ПЗ3	4	ОПК-1.1	Л3.1
2.5	Практическое занятие 4 Исследование характеристик и возможностей программ по восстановлению потерянных данных	ПЗ4	4	ОПК-1.1	Л3.1
2.6	Лабораторная работа № 3 Разграничение доступа к файловым объектам и устройствам	ЛР3	4	ОПК-1.1	Л3.1
2.7	Лабораторная работа № 4 Разграничение доступа к запуску программного обеспечения	ЛР4	4	ОПК-1.1	
2.8	Лабораторная работа № 5 Средства аудита в ОС. Протоколирование событий в операционных системах	ЛР5	2	ОПК-1.1	
2.9	Подходы к построению защищенной системы. Адекватная политика безопасности. Этапы построения и поддержания защиты. Стандарты безопасности ОС. Обеспечение безопасности функционирования ОС. Механизмы защиты ОС. Проблемы обеспечения безопасности ОС. Контроль доступа к данным	СРС	28	ОПК-1.1	Л1.1 Л1.2 Л1.3
Итого – 108 часов					

5. Учебно-методическое и информационное обеспечение дисциплины

5.1. Рекомендуемая литература				
5.1.1. Основная литература				
Код	**Авторы, составители**	**Заглавие**	**Издательство, год**	**Кол.**
Л1.1	Ю.Ф. Мартемьянов, А.В. Яковлев, А.В. Яковлев	Операционные системы. Концепции построения и обеспечения безопасности	Москва : Гор. линия-Телеком, 2011. - 332 с.: ил.;	Э1
Л1.2	Винокуров И. В.	Операционные системы : учебное пособие для бакалавров	Москва : Ай Пи Ар Медиа, 2022. — 133 с.	Э2
Л1.3	Шаньгин В. Ф.	Информационная безопасность и защита информации	Саратов: Профобразование, 2019. — 702 с. — ISBN 978-5-4488-0070-2	Э3
5.1.2. Дополнительная литература				
Код	**Авторы, составители**	**Заглавие**	**Издательство, год**	**Кол.**
Л2.1	Гатчин Ю.А., Климова Е.В.	Введение в комплексную защиту объектов информатизации	СПб.: Университет ИТМО, 2011. — 112 с. — 2227-8397. —	Э4
5.1.3. Учебно-методическое обеспечение для самостоятельной работы обучающихся				
Код	**Авторы, составители**	**Заглавие**	**Издательство, год**	**Кол.**
Л3.1	Нестеров С.А.	Основы информационной безопасности [Электронный ресурс]: учебное пособие/— Электрон. текстовые данные.	СПб.: Санкт-Петербургский политехнический университет Петра Великого, 2014. — 322 с.	Э5

5.2. Электронные образовательные ресурсы	
Э1	https://znanium.com/catalog/product/308932
Э2	https://www.iprbookshop.ru/115696.html
Э3	https://www.iprbookshop.ru/87995.html
Э4	http://www.iprbookshop.ru/65808.html
Э5	https://www.iprbookshop.ru/43960
5.3. Программное обеспечение	
П.1	Linux (свободное ПО)
П.2	LibreOffice (свободное ПО)
П.3	Kaspersky Endpoint Security (лицензия)

6. Материально-техническое обеспечение дисциплины

6.1 МТО лекционных занятий	
1	Лекционная аудитория, оборудованная интерактивной доской, проектором
6.2 МТО лабораторных работ и практических занятий	
1	Компьютерные аудитории с возможностью выхода в локальную сеть Филиала и Интернет
6.3 МТО рубежных контролей, экзамена	
1	Компьютерные аудитории с возможностью выхода в локальную сеть Филиала и Интернет

7. Методические рекомендации для обучающихся по самостоятельной работе

Указания по подготовке к различным видам занятий

Подготовка к лекционным занятиям осуществляется систематически и сводится к повторению изученного материала и отработке тем, вынесенных на самостоятельную работу. При этом должен быть доработан конспект лекций, а также получены ответы на контрольные вопросы, которые, как правило, приводятся в конце каждого раздела учебных пособий. Особое внимание необходимо уделить пониманию изучаемого материала. Зафиксировать вопросы, которые следует задать преподавателю.

Подготовка к лабораторным и практическим занятиям должна проводиться в объеме тех указаний, которые приводятся в каждом методическом пособии для проведения соответствующего занятия. Тема очередного занятия объявляется преподавателем накануне.

После повторения лекционного материала необходимо ознакомиться с предлагаемыми практическими заданиями, уяснить их суть, продумать порядок их выполнения, уточнить достаточность своих знаний для выполнения задания. Целесообразно выполнить возможные заготовки из состава отчета, который предстоит оформить на занятии. Это позволит выполнить и защитить работу в период плановых часов. Перед проведением каждого занятия должно быть полное представление о сути и порядке выполнения предстоящей работы.

Существенное значение имеет самостоятельная работа студента.

Темы для самостоятельного изучения для различных форм обучения, информационные источники и рекомендуемое время указаны в Разделе 4 настоящей Рабочей программы.

Самостоятельная работа студентов по дисциплине проводится в течение всего семестра и складывается из нескольких составляющих.

Подготовка к плановым аудиторным занятиям. В начале семестра студентов знакомят с календарным планом проведения всех видов учебных занятий. Чтобы студенты могли проверить качество своей подготовки к занятиям, в учебных пособиях и методических указаниях к лабораторным работам имеются вопросы для проверки уровня знаний перед выполнением работы и контрольные вопросы, позволяющие студенту оценить качество полученных результатов после выполнения работы. Предлагаемые студентам учебные пособия кроме контрольных вопросов содержат примеры с решениями и упражнения по основным темам.

Изучение технической литературы. Студенты самостоятельно изучают рекомендованную преподавателем техническую литературу.

Дополнительные самостоятельные исследования в лаборатории. Студенты, желающие получить более глубокие знания, имеют возможность выполнить дополнительные самостоятельные исследования в лаборатории. С этой целью в плановых лабораторных работах предусмотрены возможности для дополнительных исследований. Перечень разделов программы, предлагаемых для самостоятельных исследований, доводится до сведения студентов в начале семестра.

Самостоятельная работа на ПЭВМ. Для повышения эффективности самостоятельной работы студентам во второй половине дня предоставляется возможность выполнить в лаборатории самостоятельные исследования с использованием программно-аппаратного комплекса, состоящего из виртуальных электронных приборов, отображаемых на экране ПЭВМ, и моделирующих программ. Исследуемые схемы могут собираться из реальных компонентов на лабораторном стенде или виртуальных компонентов, хранящихся в библиотеке ПЭВМ.

Источники, рекомендуемые для углубленного изучения учебного материала

1. Шаньгин В.Ф. Информационная безопасность компьютерных систем и сетей: учебное пособие. – М.: ДМК Пресс, 2011. – 416 с.;
2. Бирюков А.А. Информационная безопасность: защита и нападение. 2-е изд., перераб. и доп. – М.: ДМК Пресс, 2017. – 434 с.
3. Маршаков, Д. В. Программно-аппаратные средства защиты информации: учебное пособие / Д. В. Маршаков, Д. В. Фатхи. — Ростов-на-Дону: Донской ГТУ, 2021. — 228 с.
4. Воронов В.А., Тихонов В.А. Концептуальные основы создания и применения системы

защиты объектов. – М.: Горячая линия - Телеком, 2013.
5. Хорев П.Б. Программно-аппаратная защита информации: учебное пособие. 3-е изд., испр. и доп. – Москва: ИНФРА-М, 2022. – 327 с.
6. Ерохин С.Д., Петухов А.Н., Пилюгин П.Л. Управление безопасностью критических информационных инфраструктур. – М.: Горячая линия – Телеком, 2021.
7. Климентьев, К. Е. Введение в защиту компьютерной информации: учебное пособие / К. Е. Климентьев. — Самара: Самарский университет, 2020. — 183 с.
8. Краковский, Ю. М. Методы защиты информации: учебное пособие для вузов / Ю. М. Краковский. — 3-е изд., перераб. — Санкт-Петербург: Лань, 2021. — 236 с..
9. Никифоров, С. Н. Методы защиты информации. Пароли, скрытие, шифрование: учеб-ное пособие для вузов / С. Н. Никифоров. — 4-е изд., стер. — Санкт-Петербург: Лань, 2022. — 124 с.
10. Язов Ю.К., Соловьев С.В. Организация защиты информации в информационных системах от несанкционированного доступа: монография / Ю.К. Язов, С.В. Соловьев. – Воронеж: Кварта, 2018. – 588 с.
11. Профильные журналы «Электросвязь», «T-Comm: Телекоммуникации и транспорт» и другие.

Использование Интернет-ресурсов

1. Электронный ресурс https://www.securitylab.ru/
2. Электронный ресурс https://securelist.ru/
3. Электронный ресурс https://www.kaspersky.ru/
4. Электронный ресурс https://encyclopedia.kaspersky.ru/
5. Электронный ресурс https://www.drweb.ru/
6. Электронный ресурс http://infoprotect.net/category/news
7. Электронный ресурс https://www.it-world.ru/it-news/security/
8. Электронный ресурс https://threatpost.ru/
9. Электронный ресурс https://www.anti-malware.ru/

Рекомендации по подготовке к рубежным аттестациям

Подготовка к сдаче модуля сводится защите на дату проведения последнего занятия в рамках модуля всех практических и лабораторных занятий, а также к подготовке к ответам по тестовым заданиям.

Объем вопросов по каждому лабораторному и практическому занятию отражен в методических указаниях по проведению соответствующего занятия. Кроме того студент должен быть готов к пояснениям по сути практических приемов работы и доказыванию обоснованности принятых решений. Если работа не выполнена или не защищена своевременно, то это следует сделать в часы самоподготовки и консультаций до даты последнего занятия в рамках сдаваемого модуля.

Подготовка к выполнению теста обеспечивается изучением и повторением того материала, который изучался на лекционных занятиях и входе лабораторных и практических занятий. Материал повторяется по конспектам и учебным пособиям, указанным в списке литературы и методических указаниях.

Подготовка к зачету осуществляется на протяжении всего времени изучения дисциплины.

Для более конкретной, целенаправленной и качественной подготовки к зачету необходимо перед началом изучения дисциплины познакомиться с содержанием рабочей программы. Уяснить логику и последовательность изучения материала, уточнить конкретные конечные результаты, которые должны быть достигнуты в итоге изучения конкретных тем и занятий. Познакомиться с перечнем вопросов и заданий, выносимых на экзамен.

В ходе каждого занятия необходимо изучить все учебные вопросы и выполнить практические задания. Для оперативного оценивания уровня достижения учебных целей следует ответить на контрольные вопросы, которые имеются в руководстве для каждого практического и лабораторного занятия. В случае выявленных затруднений следует провести дополнительное изучение материала в

часы самостоятельной работы или в период консультаций с преподавателем. Все учебные материалы должны быть отражены в конспекте, он должен дополняться и уточняться по мере отработки и уточнения учебных вопросов. Само ведение конспекта концентрирует внимание, упорядочивает знания, стимулирует активность в усвоении. К моменту выхода на непосредственную подготовку к зачету в конспекте не должно остаться непонятных вопросов.

В силу ограниченного времени, отводимого на непосредственную подготовку к зачету, целесообразно материал повторять в основном по отработанному конспекту. Это экономит время и дает возможность работать по уже знакомым записям, что улучшает запоминание материала. Остается спланировать работу в соответствии с имеющимся временем и жестко придерживаться намеченного плана. В период обязательных плановых предэкзаменационных консультаций необходимо уточнить организационные вопросы проведения экзамена и при необходимости - сложные вопросы по существу материала.

Дополнения и изменения в Рабочей программе