

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 УР

Н.А. Андреева

«28» 04 2026 г.

Рабочая программа дисциплины

Б1.О.36.01 Безопасность операционных систем

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	ОФ	
	ЗЕ	Часов/семестр
Общая трудоемкость дисциплины, в том числе (по семестрам, курсам):	3	108/5
Контактная работа, в том числе (по семестрам, курсам):		54/5
Лекции		18/5
Лабораторных работ		18/5
Практических занятий		18/5
Семинаров		
Самостоятельная работа		54/5
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
Число экзаменов с разбивкой по семестрам (курсам)		

Программу составил:

Кандидат технических наук, с.н.с. Ткачук Е.О.

Рабочая программа дисциплины

«Безопасность операционных систем»

Разработана в соответствии с ФГОС ВО

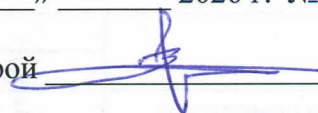
направление подготовки 10.03.01 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ,
утвержденное приказом Министерства науки и высшего образования Российской
Федерации от 17 ноября 2020 г. № 1427.

Составлена на основании учебного плана

направления 10.03.01 «Информационная безопасность», профиля «Безопасность
компьютерных систем», одобренного Учёным советом СКФ МТУСИ, протокол № 8 от
31.03 2026 г., и утвержденного директором СКФ МТУСИ 31.03 2026 г.

Рассмотрена и одобрена на заседании кафедры
Информационной безопасности

Протокол от «28» 04 2026 г. № 9

И.О.Зав. кафедрой  Жуковский А.Г.

1. Цели изучения дисциплины

Целью освоения дисциплины "Безопасность операционных систем" (БОС) является изучение принципов функционирования операционных систем и основных методов и средств обеспечивающих их безопасность.

2. Планируемые результаты обучения

Изучение дисциплины направлено на формирование у обучающегося способности решать профессиональные задачи в соответствии с *эксплуатационным* видом деятельности:

Результатом освоения дисциплины являются сформированные у обучающегося следующие компетенции:

ОПК-1.1: Способен разрабатывать и реализовывать политики управления доступом в компьютерных системах
Знать:
- понятия информации и информационной безопасности, место и роль информационной безопасности в системе национальной безопасности Российской Федерации; - направления обеспечения информационной безопасности; - классификацию методов криптографического преобразования информации; - структуру и принципы функционирования современных вычислительных систем; - основные способы защиты от потери информации и нарушений работоспособности сетей и систем.
Уметь:
- классифицировать и оценивать угрозы информационной безопасности; - проводить работы по сокрытию информации, проведению резервного копирования, восстановления информации; - использовать механизмы идентификации и аутентификации; - использовать антивирусные средства защиты; - восстанавливать потерянные компьютерные данные; - производить резервное копирование.
Владеть:
- основными понятиями, связанными с обеспечением информационно-психологической безопасности личности, общества и государства; - механизмами поддержания информационной безопасности ОС; - навыками работы по основам защиты информации с использованием программно-аппаратных комплексов
ОПК-1.2: Способен администрировать средства защиты информации в компьютерных системах и сетях
Знать:
- архитектуру и принципы построения и защиты операционных систем; - программные интерфейсы настроек политик управления доступом в операционных системах.
Уметь:
- работать со средствами защиты информации, встроенными в операционные системы; - использовать средства защиты информации операционных систем для противодействия угрозам безопасности информации.
Владеть:
- основными понятиями, связанными с обеспечением информационной безопасности операционных систем; - навыками работы по основам защиты информации операционных систем с использованием программно-аппаратных комплексов.

3. Место дисциплины в структуре образовательной программы

Требования к предварительной подготовке обучающегося (предшествующие дисциплины, модули, темы):	
1	Дисциплина «Безопасность операционных систем» является логическим продолжением дисциплины Б1.О.27 «Основы информационной безопасности», знание которой в объеме требований образовательной программы является необходимым.
2	Успешное освоение дисциплины «Безопасность операционных систем» базируется также на знаниях, приобретенных из дисциплин: Б1.О.20 «Физика», Б1.О.07 «Иностранный язык», Б1.О.05 «Введение в информационные технологии».
Последующие дисциплины и практики, для которых освоение данной дисциплины необходимо:	
1	Дисциплина является базовой для успешного освоения дисциплин: Б1.О.29 «Методы и средства криптографической защиты информации», Б1.О.32 «Основы управления информационной безопасностью», Б1.О.33 «Комплексное обеспечение защиты информации», Б1.В.02 «Программно-аппаратные средства защиты информации»

4. Структура и содержание дисциплины

4.1 Очная форма обучения, 4 года (всего 108 часов, 60 аудиторных часов, 48 часов самостоятельной работы)

Код зан.	Тема и краткое содержание занятия	Вид зан.	Кол. часов	Компет енции	УМИО
Курс 3, Семестр 5					
Модуль 1. Принципы работы и угрозы безопасности ОС – (28+27=55)					
1.1	Лекция 1. ОСОБЕННОСТИ РАБОТЫ ОПЕРАЦИОННЫХ СИСТЕМ 1. Управление системными службами и процессами в ОС 2. Управление сетевыми подключениями в ОС 3. Применение консольного управления ОС 4. Действия, приводящие к неправомерному овладении конфиденциальной информацией	Лек 1	4	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	Лек 2	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 визуальным оптическим каналам 2. Защита информации от утечки по сетевым каналам 3. Защита информации от утечки по материально - вещественным каналам	Лек 3	2	ОПК-1.1	Л1.1 Л1.2 Л1.3
1.4	Лабораторная работа 1 Управление системными службами и процессами в ОС	ЛР1	4	ОПК-1.1	Л3.1 Л3.2
1.5	Лабораторная работа 2	ЛР2	4	ОПК-	Л3.1

	Управление сетевыми подключениями в ОС			1.1	ЛЗ.2
1.6	Лабораторная работа 3 Применение консольного управления ОС	ЛР3	4	ОПК-1.1	ЛЗ.1 ЛЗ.2
1.7	Лабораторная работа № 4 Средства защиты ОС	ЛР4	6	ОПК-1.1	ЛЗ.1 ЛЗ.2
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 на современные ОС. Классификация методов и их сравнительная статистика	СРС	27	ОПК-1.1	Л1.1 Л1.2 Л1.3
Модуль 2 Основы защиты информации в инфокоммуникационных системах и сетях – (26+27=53)					
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	Лек 4	4	ОПК-1.2	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	Лек 5	2	ОПК-1.2	Л1.1 Л1.2 Л1.3
2.3	Лекция 6. ПРОТОКОЛИРОВАНИЕ И СРЕДСТВА АУДИТА Средства аудита в ОС. Протоколирование событий в операционных системах	Лек 6	2	ОПК-1.2	Л1.1 Л1.2 Л1.3
2.4	Практическое занятие 1 Управление средствами обеспечения безопасности ОС	ПЗ1	4	ОПК-1.2	ЛЗ.1 ЛЗ.2
2.5	Практическое занятие 2 Исследование характеристик и возможностей программ по восстановлению потерянных данных	ПЗ2	4	ОПК-1.2	ЛЗ.1 ЛЗ.2
2.6	Практическое занятие 3 Разграничение доступа к файловым объектам и устройствам	ПЗ3	4	ОПК-1.2	ЛЗ.1 ЛЗ.2
2.7	Практическое занятие 4 Разграничение доступа к запуску программного обеспечения	ПЗ4	4	ОПК-1.2	ЛЗ.1 ЛЗ.2
2.8	Практическое занятие 5 Средства аудита в ОС. Протоколирование событий в	ПЗ5	2	ОПК-1.2	ЛЗ.1 ЛЗ.2

	операционных системах				
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	27	ОПК-1.2	Л1.1 Л1.2 Л1.3
	Зачет			ОПК-1.1 ОПК-1.2	Л1.1 Л1.2 Л1.3 Л2.1 Л2.2 Л3.1 Л3.2
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	А. Ю. Гарькушев, А. В. Липис, И. Л. Карпова.	Основы обеспечения безопасности операционных систем : учебное пособие	Москва, Вологда : Инфра-Инженерия, 2024	Э1
Л1.2	Винокуров И. В.	Операционные системы : учебное пособие для бакалавров	Москва : Ай Пи Ар Медиа, 2022.	Э2
Л1.3	Шаньгин В. Ф.	Информационная безопасность и защита информации	Саратов: Профобразование, 2019.	Э3
5.1.2. Дополнительная литература				
Код	Авторы, составители	Заглавие	Издательство, год	Кол.
Л2.1	Гончарук, С. В.	Администрирование ОС Linux : учебное пособие	Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2024.	Э4
Л2.2	Нестеров С.А.	Основы информационной безопасности [Электронный ресурс]: учебное пособие/— Электрон. текстовые данные.	СПб.: Санкт-Петербургский политехнический университет Петра Великого, 2014	Э5
5.1.3. Учебно-методическое обеспечение				
Код	Авторы, составители	Заглавие	Издательство, год	Кол.
Л3.1	Потерпеев Г.Ю., Трубиенко О.В., Абрамов Д.П.	Сборник практических занятий для дисциплины безопасность операционных систем: Практикум : учебное пособие.	Москва : РТУ МИРЭА, 2023 — Часть 1 — 2023. — 65 с.	Э6
Л3.2	Потерпеев Г.Ю., Трубиенко О.В.,	Сборник практических занятий для дисциплины безопасность	Москва : РТУ МИРЭА, 2024 — Часть 2 — 2024. — 79 с.	Э7

	Абрамов Д.П.	операционных систем: Практикум : учебное пособие.		
5.2. Электронные образовательные ресурсы				
Э1	https://www.iprbookshop.ru/143546.html			
Э2	https://www.iprbookshop.ru/115696.html			
Э3	https://www.iprbookshop.ru/87995.html			
Э4	https://www.iprbookshop.ru/133916.html			
Э5	https://www.iprbookshop.ru/43960			
Э6	https://e.lanbook.com/book/368750			
Э7	https://e.lanbook.com/book/448808			
5.3 Информационно-справочные системы и профессиональные базы данных				
5.3.1	Консультант Плюс – https://www.consultant.ru/			
5.3.2	Гарант – https://www.garant.ru/			
5.3.2	Консорциум Кодекс – https://docs.cntd.ru/			
5.3.3	Научная электронная библиотека – https://www.elibrary.ru/			
5.3.4	Профессиональная база данных: Федеральный портал «Российское образование»: [Электронный ресурс] – Режим доступа: http://www.edu.ru/ (открытый доступ)			
5.3.5	Профессиональная база данных: Федеральный центр информационно-образовательных ресурсов: [Электронный ресурс] – Режим доступа: http://fcior.edu.ru/ (открытый доступ)			
5.4. Программное обеспечение				
СКФ МТУСИ обеспечен необходимым комплектом лицензионного и свободно распространяемого программного обеспечения, в том числе отечественного производства:				
П.1	1. AVAST Free Antivirus	Антивирусное ПО. Свободное, условно свободное или триал-версии.		
	2. AVG AntiVirus Free			
	3. Dr.Web Antivirus			
	4. Антивирус Касперского			
	5. ESET NOD32 Антивирус			
	6. AVZ Antivirus			
	7. Avira Free Antivirus			
	8. Norton AntiVirus			
	9. McAfee Antivirus			
	10. Emsisoft Anti-Malware			
	11. BullGuard Antivirus			
	12. Protector Plus Antivirus			
	13. Panda Antivirus			
	14. Ashampoo Anti-Virus			
	14. G Data AntiVirus			
	16. K7 AntiVirus			
	17. VIRUSfighter			
	18. Twister Antivirus			
П.2	1. Wise Folder Hider	Программное обеспечение по защите и сокрытию файлов и папок. Свободное, условно свободное или триал-версии.		
	2. Secure Folders			
	3. Anvide Lock Folder			
	4. Folder Lock			
	5. Easy File Locker			
	6. Folder Guard			
	7. DEKSI USB Security			
	8. Locker (защита папок и дисков)			
	9. Advanced Hider			

	10. Hide Folders XP	
	11. Hide Files	
П.3	1. TrustPort Tools	Программное обеспечение по шифрованию, безвозвратному удалению, стеганографии. Свободное, условно свободное или триал-версии.
	2. Cryptic Disk	
	3. Locker (скрытие файлов)	
	4. Max File Encryption	
	5. Secure Disk	
	6. Masker 7.1	
	7. Fox Secret	
	8. HideInPicture 1.0	
	9. Шифровальщик	
	10. Advanced Encryption Package	
	11. Gpg4win	
	12. Cryptic Disk Professional	
	13. CyberSafe Files Encryption	
	14. Steganos Privacy Suite	
	15. Lavasoft Privacy Toolbox	
	16. pkiImage Free Edition	
П.4	1. Hetman Partition Recovery	Программное обеспечение по восстановлению данных. Свободное, условно свободное или триал-версии.
	2. Active File Recovery	
	3. R-Studio 7.6	
	4. Auslogics File Recovery	
	5. Active UNDELETE	
	6. Paragon Rescue Kit	
	7. Wise Data Recovery	
	8. Puran File Recovery	
	9. O&O DiskRecovery	
	10. Tenorshare Any Data Recovery	
	11. Power Data Recovery	
	12. GetDataBack	
	13. Recover My Files	
	14. R-Undelete	
	15. Handy Recovery	
	16. Ashampoo Undeleter	
П.5	1. Iperius Backup	Программное обеспечение по резервному копированию данных. Свободное, условно свободное или триал-версии.
	2. FBackup	
	3. Backup4all	
	4. Uranium Backup Free	
	5. Simple Data Backup	
	6. Personal Backup	
	7. Back4Sure	
	8. SyncBackFree	
	9. Handy Backup	
	10. EASEUS Todo Backup 8.0 Free Edition	
	11. Exiland Backup Free 4.0	
	12. Nero BackItUp	
	13. Paragon Rescue Kit 14.0 Free	
	14. Action Backup	

	15. LimBackup	
	16. AVSbackup	
	17. ExtraBackup	
	18. Cobian Backup	
	19. Backup & Recovery 10 Build 9169 Free Edition	
	20. Information Backup System	
П.6	MS Word, Power Point – с лицензией	
П.7	Операционная система Linux – свободное ПО	

6. Материально-техническое обеспечение дисциплины

6.1 МТО лекционных занятий	
1	Лекционная аудитория, оснащенная интерактивной доской, проектором, ПК (ноутбуком), экраном.
6.2 МТО лабораторных работ и практических занятий	
1	Лаборатория «Программно-аппаратные средства защиты информации», укомплектованная специализированной мебелью, оснащенную программно-аппаратными комплексами защиты информации, включающими в том числе средства криптографической защиты информации
6.3 МТО рубежных контролей, зачетов, экзаменов	
1	Учебные аудитории, оборудованные компьютерной техникой с возможностью выхода в локальную сеть Филиала и Интернет.
6.4 МТО самостоятельной работы обучающихся	
1	Помещение для самостоятельной работы обучающихся оснащено компьютерной техникой с возможностью подключения к сети Интернет и обеспечением доступа в электронную информационно-образовательную среду СКФ МТУСИ

7. Оценочные материалы

Оценочные материалы и перечень видов оценочных средств текущего контроля и промежуточной аттестации представлены в Приложении 1 к рабочей программе дисциплины.

8. Методические рекомендации для обучающихся по освоению дисциплины

Методические рекомендации по освоению дисциплины представлены в Приложении 2 к рабочей программе дисциплины.

9. Особенности реализации дисциплины (модуля) при обучении инвалидов и лиц с ограниченными возможностями здоровья

Рабочая программа дисциплины (модуля) при необходимости может быть адаптирована для обучения (в том числе с применением дистанционных образовательных технологий) лиц с ограниченными возможностями здоровья, инвалидов. Для этого требуется заявление

обучающихся, являющихся лицами с ограниченными возможностями здоровья, инвалидами, или их законных представителей и рекомендации психолого-медико-педагогической комиссии. При обучении лиц с ограниченными возможностями здоровья учитываются их индивидуальные психофизические особенности. Обучение инвалидов осуществляется также в соответствии с индивидуальной программой реабилитации инвалида (при наличии).

Для лиц с нарушением слуха возможно предоставление учебной информации в визуальной форме (краткий конспект лекций; тексты заданий, напечатанные увеличенным шрифтом), на аудиторных занятиях допускается присутствие ассистента, а также сурдопереводчиков и тифлосурдопереводчиков.

Текущий контроль успеваемости осуществляется в письменной форме: обучающийся письменно отвечает на вопросы, письменно выполняет практические задания.

Доклад (реферат) также может быть представлен в письменной форме, при этом требования к содержанию остаются теми же, а требования к качеству изложения материала (понятность, качество речи, взаимодействие с аудиторией и т. д.) заменяются на соответствующие требования, предъявляемые к письменным работам (качество оформления текста и списка литературы, грамотность, наличие иллюстрационных материалов и т.д.).

Промежуточная аттестация для лиц с нарушениями слуха проводится в письменной форме, при этом используются общие критерии оценивания. При необходимости время подготовки к ответу может быть увеличено.

Для лиц с нарушением зрения допускается аудиальное предоставление информации, а также использование на аудиторных занятиях звукозаписывающих устройств (диктофонов и т.д.). Допускается присутствие на занятиях ассистента (помощника), оказывающего обучающимся необходимую техническую помощь.

Текущий контроль успеваемости осуществляется в устной форме.

При проведении промежуточной аттестации для лиц с нарушением зрения тестирование может быть заменено на устное собеседование по вопросам.

Для лиц с ограниченными возможностями здоровья, имеющих нарушения опорно-двигательного аппарата, на аудиторных занятиях, а также при проведении процедур текущего контроля успеваемости и промежуточной аттестации могут быть предоставлены необходимые технические средства (персональный компьютер, ноутбук или другой гаджет); допускается присутствие ассистента (ассистентов), оказывающего обучающимся необходимую техническую помощь (занять рабочее место, передвигаться по аудитории, прочитать задание, оформить ответ, общаться с преподавателем).

10. Дополнения и изменения в Рабочей программе

Лист актуализации рабочей программы дисциплины «Безопасность операционных систем Б1.О.36.01» для использования в 20__/20__ учебном году

Утверждаю

Зам. директора по УР _____
«__» _____ 20__ г.

Направление: 10.03.01 Информационная безопасность

Профиль: Безопасность компьютерных систем

Форма обучения: очная

(Возможны следующие варианты):

а) Рабочая программа действует без изменений.

б) В рабочую программу вносятся следующие изменения:

1)

2)

3)

Разработчик (и): _____

(ФИО, ученая степень, ученое звание)

«__» _____ 20__ г.

Рабочая программа пересмотрена и одобрена на заседании кафедры ИБ

Протокол № _____ от «__» _____ 20__ г.

Заведующий кафедрой _____

Оценочные материалы для проведения текущего контроля и промежуточной аттестации по дисциплине

1. Оценочные материалы для проведения промежуточной аттестации по дисциплине

1.1 Шкала оценивания компетенций

Шкала оценивания компетенций		
Оценка	Уровень освоения компетенции	Критерии оценивания
«Отлично»	Высокий уровень	Обучающийся показывает всестороннее, систематическое и глубокое знание основного и дополнительного учебного материала, дает полные, профессиональные и грамотные ответы на поставленные вопросы, что свидетельствует об освоении обучающимся взаимосвязи основных понятий дисциплины; усвоил основную и знаком с дополнительной рекомендованной литературой; проявляет творческие способности в понимании, изложении и использовании учебно-программного материала.
«Хорошо»	Повышенный уровень	Обучающийся показывает достаточный уровень знания основного и дополнительного учебного материала, дает в целом грамотные ответы на поставленные вопросы, что свидетельствует об освоении обучающимся взаимосвязи основных понятий дисциплины; усвоил основную и знаком с дополнительной рекомендованной литературой. Допускает не существенные погрешности в ответах, устраняет их без помощи преподавателя.
«Удовлетворительно»	Пороговый уровень	Обучающийся демонстрирует знание основного учебного материала в минимальном объеме, необходимом для дальнейшей учебы; в целом отвечает на поставленные вопросы, допуская не принципиальные ошибки; знаком с основной литературой. Допускает ошибки в ответах различного уровня, которые исправляет после наводящих вопросов и под руководством преподавателя.
«Неудовлетворительно»	Минимальный уровень не достигнут	Обучающийся обнаруживает существенные пробелы в знаниях основного учебно-программного материала, допустившему принципиальные ошибки в выполнении, предусмотренных программой, заданий; не знаком с рекомендованной литературой, не может исправить допущенные ошибки. Как правило, оценка «неудовлетворительно»

		ставится обучающимся, которые не могут продолжить обучение или приступить к профессиональной деятельности по окончании вуза без дополнительных занятий по соответствующей дисциплине.
--	--	---

1.2 Показатели, критерии и шкалы оценивания компетенций

Показатели компетенции	Критерии оценивания	Шкала оценивания
ОПК-1.1: Способен разрабатывать и реализовывать политики управления доступом в компьютерных системах		
Знать:		
- понятия информации и информационной безопасности, место и роль информационной безопасности в системе национальной безопасности Российской Федерации; - направления обеспечения информационной безопасности; - классификацию методов криптографического преобразования информации; - структуру и принципы функционирования современных вычислительных систем; - основные способы защиты от потери информации и нарушений работоспособности сетей и систем	Тестовый контроль	Модуль 1 0÷10 «Неудовлетворительно» - 0-3 «Удовлетворительно» - 4-6 «Хорошо» - 7-8- «Отлично» - 9-10
Уметь		
- классифицировать и оценивать угрозы информационной безопасности; - проводить работы по сокрытию информации, проведению резервного копирования, восстановления информации; - использовать механизмы идентификации и аутентификации; - использовать антивирусные средства защиты; - восстанавливать потерянные компьютерные данные; - производить резервное копирование.	Лабораторные работы 1-2	Модуль 1 0÷10 «Неудовлетворительно» - 0-3 «Удовлетворительно» - 4-6 «Хорошо» - 7-8- «Отлично» - 9-10
Владеть		
- основными понятиями, связанными с обеспечением информационно-психологической безопасности личности, общества и государства; - механизмами поддержания информационной безопасности ОС; - навыками работы по основам защиты	Лабораторные работы 3-4	Модуль 1 0÷10 «Неудовлетворительно» - 0-7 «Удовлетворительно» - 8-12 «Хорошо» - 13-16 «Отлично» - 17-20

информации с использованием программно-аппаратных комплексов		
ОПК-1.2: Способен администрировать средства защиты информации в компьютерных системах и сетях		
Знать:		
- архитектуру и принципы построения и защиты операционных систем; - программные интерфейсы настроек политик управления доступом в операционных системах;	Тестовый контроль	Модуль 2 0÷10 «Неудовлетворительно» - 0-3 «Удовлетворительно» - 4-6 «Хорошо» - 7-8- «Отлично» - 9-10
Уметь		
- работать со средствами защиты информации, встроенными в операционные системы; - использовать средства защиты информации операционных систем для противодействия угрозам безопасности информации;	Практические занятия 1-2	Модуль 2 0÷8 «Неудовлетворительно» - 0-3 «Удовлетворительно» - 4-5 «Хорошо» - 6-7 «Отлично» - 8
Владеть		
- основными понятиями, связанными с обеспечением информационной операционных систем; - навыками работы по основам защиты информации операционных систем с использованием программно-аппаратных комплексов	Практические занятия 3-5	Модуль 2 0÷8 «Неудовлетворительно» - 0-3 «Удовлетворительно» - 4-5 «Хорошо» - 6-7 «Отлично» - 8
	Зачет	0-100 баллов «Не зачтено» - 0-40 «Зачтено» - 41-100

1.3 Оценочные материалы: типовые контрольные задания, иные материалы

1.3.1 Оценочные средства текущего контроля для очной формы обучения

Модуль 1 (50 баллов):

Модуль содержит 3 лекционных занятия и 4 лабораторных работы. Знание лекционного материала оценивается по результатам тестового контроля, как выполнения письменных заданий или устных опросов, максимальное количество баллов - 10. За выполненные и защищенные лабораторных работы обучающийся получает максимум 40 баллов. Общее максимальное количество баллов за модуль 1 составляет 50.

Вопросы тестовых заданий для контроля лекционного материала (ОПК-1.1):

1. Каким образом производится управление системными службами и процессами в ОС
2. Как управлять сетевыми подключениями в ОС
3. Опишите применение консольного управления ОС
4. Какие действия, могут привести к неправомерному овладению конфиденциальной информацией

5. Назовите основные средства защиты ОС
6. В чем сущность организационной защиты ОС
7. Как организуется инженерно-техническая защита ОС
8. Защита информации от утечки по визуальным оптическим каналам
9. Защита информации от утечки по сетевым каналам
10. Защита информации от утечки по материально - вещественным каналам

Лабораторная работа 1. Управление системными службами и процессами в ОС

Контрольные вопросы ЛРН№1 (ОПК-1.1):

1. История развития средств безопасности операционных систем.
2. Связь аппаратной и программной составляющих.
3. Функции безопасности современных ОС.
4. Назначение и функции BIOS и UEFI.
5. Файловые системы и их особенности.

Лабораторная работа 2. Управление сетевыми подключениями в ОС

Контрольные вопросы ЛРН№2 (ОПК-1.1):

1. Взаимодействие пользователей с ОС.
2. Прерывания.
3. Прикладные и системные программы.
4. Системные вызовы.
5. Драйверы

Лабораторная работа 3. Применение консольного управления ОС

Контрольные вопросы ЛРН№3 (ОПК-1.1):

1. Планирование и диспетчеризация в ОС.
2. Управление памятью в ОС.
3. Прямой доступ к памяти. Достоинства и недостатки.
4. Субъекты и объекты.
5. Определение прав доступа субъектов к объектам.

Лабораторная работа 4. Средства защиты ОС

Контрольные вопросы ЛРН№4 (ОПК-1.1):

1. Субъектно-объектная модель доступа.
2. Защита информации в вычислительной системе.
3. Потокковая модель доступа.
4. Понятие политики безопасности.
5. Применение политик безопасности.

Модуль 2: (50 баллов):

Модуль содержит 3 лекционных занятия и 5 практических занятий. Знание лекционного материала оценивается по результатам тестового контроля, как выполнения письменных заданий или устных опросов, максимальное количество баллов - 10. За выполненные и защищенные практические работы обучающийся получает максимум 40 баллов. Общее максимальное количество баллов за модуль 1 составляет 50.

Вопросы тестовых заданий для контроля лекционного материала (ОПК-1.2):

1. Структуризация методов обеспечения информационной безопасности
2. Классификация злоумышленников

3. Основные направления и методы реализации угроз информационной безопасности
4. Аутентификация пользователей в ОС.
5. Разграничение доступа к файловым объектам и устройствам.
6. Разграничение доступа к запуску программного обеспечения
7. Средства аудита в ОС.
8. Протоколирование событий в операционных системах

Практическое занятие 1. Управление средствами обеспечения безопасности ОС

Контрольные вопросы ПЗ №1 (ОПК-1.2):

1. Подходы к построению защищенной системы.
2. Адекватная политика безопасности.
3. Этапы построения и поддержания защиты.
4. Стандарты безопасности ОС.
5. Обеспечение безопасности функционирования ОС.

Практическое занятие 2. Исследование характеристик и возможностей программ по восстановлению потерянных данных

Контрольные вопросы ПЗ №2 (ОПК-1.2):

1. Механизмы защиты ОС.
2. Проблемы обеспечения безопасности ОС.
3. Контроль доступа к данным.
4. Анализ защищенности современных ОС.
5. Управление доступом.

Практическое занятие 3. Разграничение доступа к файловым объектам и устройствам

Контрольные вопросы ПЗ №3 (ОПК-1.2):

1. Требования к защите информации от НСД.
2. Основные встроенные механизмы защиты ОС.
3. Необходимость наличия средств защиты в ОС.
4. Достоинства и недостатки основных систем защиты ОС.
5. Системы защиты от несанкционированного доступа. и недостатки программы Backup & Recovery 10 Build 9169 Free Edition

Практическое занятие 4. Разграничение доступа к запуску программного обеспечения

Контрольные вопросы ПЗ №4 (ОПК-1.2):

1. Системы «привязки» ПО.
2. Программно-аппаратные средства защиты ПО с электронными ключами.
3. Показатели эффективности систем защиты. Критерии оценки.
4. Понятие аутентификации и авторизации.
5. Аутентификация с использованием паролей.

Практическое занятие 5. Средства аудита в ОС. Протоколирование событий в операционных системах

Контрольные вопросы ПЗ №5 (ОПК-1.2):

1. Аутентификация с использованием биометрических данных.
2. Аутентификация с использованием физических объектов.
3. Угрозы безопасности ОС.
4. Протоколирование.
5. Проблемы организации протоколирования

1.3.2 Вопросы, выносимые на зачет по дисциплине «Безопасность операционных систем» (ОПК-1.1, ОПК-1.2) (промежуточная аттестация):

1. История развития средств безопасности операционных систем.
2. Связь аппаратной и программной составляющих.
3. Функции безопасности современных ОС.
4. Назначение и функции BIOS и UEFI.
5. Файловые системы и их особенности.
6. Взаимодействие пользователей с ОС.
7. Прерывания.
8. Прикладные и системные программы.
9. Системные вызовы.
10. Драйверы.
11. Планирование и диспетчеризация в ОС.
12. Управление памятью в ОС.
13. Прямой доступ к памяти. Достоинства и недостатки.
14. Субъекты и объекты.
15. Определение прав доступа субъектов к объектам.
16. Субъектно-объектная модель доступа.
17. Защита информации в вычислительной системе.
18. Потокковая модель доступа.
19. Понятие политики безопасности.
20. Применение политик безопасности.
21. Подходы к построению защищенной системы.
22. Адекватная политика безопасности.
23. Этапы построения и поддержания защиты.
24. Стандарты безопасности ОС.
25. Обеспечение безопасности функционирования ОС.
26. Механизмы защиты ОС.
27. Проблемы обеспечения безопасности ОС.
28. Контроль доступа к данным.
29. Анализ защищенности современных ОС.
30. Управление доступом.
31. Требования к защите информации от НСД.
32. Основные встроенные механизмы защиты ОС.
33. Необходимость наличия средств защиты в ОС.
34. Достоинства и недостатки основных систем защиты ОС.
35. Системы защиты от несанкционированного доступа.
36. Системы «привязки» ПО.
37. Программно-аппаратные средства защиты ПО с электронными ключами.
38. Показатели эффективности систем защиты. Критерии оценки.
39. Понятие аутентификации и авторизации.
40. Аутентификация с использованием паролей.
41. Аутентификация с использованием биометрических данных.
42. Аутентификация с использованием физических объектов.
43. Угрозы безопасности ОС.
44. Протоколирование.
45. Проблемы организации протоколирования.

2. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Порядок и методика проведения текущего контроля и промежуточной аттестаций

Предусмотрены следующие виды контроля:

- текущий контроль по каждому модулю – в форме написания письменных заданий или устных опросов для оценки теоретических знаний;
- текущий контроль по каждому модулю – в форме отчетов по лабораторным работам и практическим занятиям для оценки практических навыков;
- промежуточная аттестация по дисциплине – в форме зачета.

Текущий контроль успеваемости в форме защиты лабораторных и практических проводится в два этапа:

- 1-й этап: допуск к выполнению лабораторной работы – проводится в форме письменной «летучки» (5-10 мин) с целью контроля знаний обучающихся теоретической части лабораторной работы и готовности к выполнению практических исследований;
- 2-й этап выполняется по окончании каждой лабораторной работы (практического занятия) в форме индивидуального собеседования по выполненным исследованиям или расчетам. Проводится с целью контроля закрепления теоретической части материала и степени отработки обучающимся практических навыков исследования на аппаратуре.

Тестовый контроль усвоения лекционного материала выполняются в виде короткого письменного или устного ответа на один вопрос, изученный на предыдущей лекции в начале каждой последующей лекции. Ответ на вопрос дается в течение 5-10 минут. Таким образом, после лекционного курса каждого модуля формируется общая оценка за теоретические знания.

С целью повышения качества обучения за счет побуждения обучающихся к активной текущей учебной работе, четкого и оперативного контроля всего хода учебного процесса, снижения роли случайных и субъективных факторов при оценивании учебной деятельности обучающихся в образовательном процессе реализована модульно-рейтинговая система.

Правила ее использования прописаны в «Положении об МРС».

Набранные обучающимся в рамках текущего контроля баллы переводятся в оценку в соответствии со следующей шкалой:

- «не зачтено» - от 0 до 40 от максимального количества баллов;
- «зачтено» - от 41 до 100 максимального количества баллов.

Соотношения максимального количества баллов, полученных обучающимся по блокам модулей, показаны в Таблице 1.

Таблица 1 - Распределение баллов по модулям дисциплины «Основы информационной безопасности»

Модуль	Всего баллов (Максимальное значение)	Теоретический блок (Тестовый контроль)	Практический блок
Модуль 1	50	10	40
Модуль 2	50	10	40
Зачет	100		

Теоретический блок оценивается по результатам тестового контроля. Практический блок оценивается по результатам выполнения лабораторных работ и заданий на практических занятиях.

На зачете производится оценка тех компетенций, которые должны быть в той или иной форме освоены в процессе изучения. Рекомендуются формировать вопросы в билетах к зачету таким образом, чтобы преподаватель смог оценить все компетенции данной дисциплины.

3 Промежуточная аттестация

Промежуточная аттестация проводится в форме зачета. Зачет проводится по расписанию в устном виде по билетам к зачету. Результаты аттестации заносятся в ведомость и зачетную книжку обучающегося.

Образец билета к зачету.

	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 И.о.зав. кафедрой «ИБ» _____ А.Г.Жуковский « ____ » _____ 20__ г.
Направление подготовки: 10.03.01 <i>Информационная безопасность</i> Курсы: 3 Дисциплина: <i>Безопасность операционных систем</i>		
Билет №1 1. История развития средств безопасности операционных систем. 2. Связь аппаратной и программной составляющих. « ____ » _____ 20__ г. Кандидат технических наук, с.н.с. _____ Ткачук Е.О.		

Один комплект отпечатанных билетов к зачету, подписанных преподавателем кафедры и утвержденных заведующим кафедрой хранится у заведующего кафедрой, другой комплект – у преподавателя, ведущего дисциплину

4 Тестовые задания по дисциплине «Безопасность операционных систем»

Тестовые задания позволяют оценить уровень сформированности 2-х компетенций ОПК-1.1; ОПК-1.2.

Задания распределены по блокам в соответствии с уровнем сложности. Каждый блок содержит номер задания, и текст задания.

Базовый уровень содержит примерно 50 % заданий.

Он формируется из заданий с выбором одного или нескольких верных ответов из предложенных или воспроизведения фактического материала (терминология, факты, классификация, параметры и др.);

Повышенный уровень в среднем составляет 35 % заданий.

В нем используются задания на сопоставление, сравнение, установление последовательности;

Высокий уровень в среднем составляют – 15 % заданий.

В задании используются: решения нетиповых задач, алгоритмы, доказательства, задания с развернутым ответом – определения, перечисление, изображение схемы, структуры и др.

Количество заданий по каждой компетенции равно 20. Всего 40 заданий.

Один комплект тестовых вопросов с указанием правильных ответов хранится у заведующего кафедрой, другой комплект – у преподавателя, ведущего дисциплину.

ОПК-1.1

Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства

БЛОК А (базовый уровень) – Задание с выбором одного или нескольких верных ответов из предложенных

Инструкция по тестам Блока А: Прочитайте текст и выберите один или несколько правильных ответов

№ задания	Тексты заданий
1	К правовым методам, обеспечивающим информационную безопасность, относятся: 1. Разработка аппаратных средств обеспечения правовых данных 2. Разработка и установка во всех компьютерных правовых сетях журналов учета действий 3. Разработка и конкретизация правовых нормативных актов обеспечения безопасности 4. Проверка уровня защищенности информационных ресурсов
2	Основные объекты информационной безопасности: 1. Компьютерные сети, базы данных 2. Информация, системы и сети, пользователи и каналы связи 3. Бизнес ориентированные, коммерческие системы 4. Операционные системы
3	Какова основная цель обеспечения безопасности операционной системы? 1. Целостность данных 2. Аутентификация пользователя 3. Распределение ресурсов 4. Оптимизация производительности
4	Что из перечисленного ниже является распространённой угрозой безопасности операционной системы? 1. Вредоносное ПО 2. Брандмауэры 3. Антивирусное программное обеспечение 4. Шифрование
5	Основными субъектами информационной безопасности являются: 1. Руководители, менеджеры, администраторы компаний 2. Органы права, государства, бизнеса 3. Сетевые базы данных, файерволы
6	Какой механизм в основном используется для аутентификации пользователей в операционных

№ задания	Тексты заданий
	системах? 1. Пароль 2. Брандмауэр 3. Шифрование 4. Резервное копирование
7	К основным функциям системы безопасности ОС можно отнести все перечисленное: 1. Установление регламента, аудит операционной системы, выявление рисков 2. Установка новых офисных приложений, смена хостинг-компаний 3. Внедрение аутентификации, проверки контактных данных пользователей
8	Какой распространённый метод используется для защиты данных при передаче? 1. Журналы аудита 2. Установка права доступа к файлу 3. Списки контроля доступа 4. Шифрование данных
9	Какого типа пользователей нет в Linux? 1. Владелец 2. Группа 3. Сотрудники 4. Друзья 5. Прочее
10	В чем слабость парольной защиты? 1. Трудность распознавания 2. Возможность раскрытия пароля путём подбора 3. Возможность обхода парольной защиты

БЛОК Б (повышенный уровень) – Задание закрытого типа на установление соответствия
Инструкция: Прочитайте текст и установите соответствие

№ задания	Тексты заданий
11	Установите соответствие между программным обеспечением и реализуемой технологией обеспечения безопасности: 1. Операционная система (ОС) Windows. 2. Сервер аутентификации. 3. ОС семейства Unix. Достигаются следующими действиями: А. Разграничение прав доступа к объектам на основе дискреционной модели доступа. Б. Возможность создания и применения различных политик безопасности, таких как политики паролей, политики аудита и т.д. В. Наличие доверенной третьей стороны, которой доверяют все субъекты аутентификации, владеющей секретными ключами обслуживаемых субъектов и помогающей им в попарной проверке подлинности.
12	Для операционной системы возможны следующие риски 1. Потеря целостности; 2. Потеря конфиденциальности; 3. Потеря функциональности, Это приводит к А. Манипуляции с данными; Б. Несанкционированное получение информации; В. Потеря или разрушение данных.
13	Установите соответствие между типами мероприятий по защите операционных систем (ОС) и их описаниями: 1. Технические мероприятия; 2. Процедурные (или административные) мероприятия; 3. Физические мероприятия; А. Применение организационных мер и совокупности средств, создающих препятствие для проникновения или доступа неуполномоченных физических лиц к защищаемой; Б. Обеспечение защиты (конфиденциальности, целостности, доступности) содержащейся в ОС информации при помощи программных и технических средств; В. Разработка и применение стандартов, требований, регламентов и прочих нормативных документов,

№ задания	Тексты заданий
	направленных на обеспечение защиты, содержащейся в системе информации;
14	Установите соответствие между основными типами угроз, характерных для операционных систем (ОС), и примерами их реализации: 1. Логические угрозы; 2. Физические угрозы; 3. Неправильное управление доступом; Поставьте в соответствие примеры их реализации А. Несанкционированный доступ к оборудованию. Б. Вредоносный код, встроенный в приложения. В. Назначение избыточных прав пользователям.

БЛОК Б (повышенный уровень) – Задание закрытого типа на установление последовательности

Инструкция: Прочитайте текст и установите правильную последовательность

№ задания	Тексты заданий
15	Установите правильную последовательность этапов контроля доступа пользователя при входе в операционную систему семейства Unix: 1) Пользователь вводит пароль, который преобразуется в хеш и сравнивается с хешем, содержащимся в специальном хранилище 2) Пользователь вводит символьное имя (логин), для которого проверяется его наличие в специализированном хранилище 3) Реализуется доступ пользователя к объектам системы в соответствии с правами доступа к ним на основе дискреционной модели 4) Происходит присвоение пользователю числовых идентификаторов UID и GID
16	Установите правильную последовательность этапов доступа пользователя к информационной системе: 1). Авторизация, 2). Идентификация 3). Аутентификация 4). Расшифрование зашифрованных данных
17	Установите правильную последовательность этапов процесса реагирования на инциденты – 1. Идентификация, 2. Ликвидация, 3. Улучшение, 4. Подготовка, 5. Возвращение к работе, 6. Сдерживание.

БЛОК В (высокий уровень) – Задание открытого типа с развернутым ответом

Инструкция: Прочитайте текст и запишите обоснованный ответ

№ задания	Тексты заданий
18	Криптографическая подсистема, подсистема управления доступом, подсистема обеспечения целостности и подсистема регистрации и учета позволяют организовать защиту ОС от
19	Для сокрытия информации используется
20	В документе «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации» сформулированы _____ по достижению требуемого уровня защиты информации в автоматизированной системе.

Система оценивания выполнения тестовых заданий по компетенции ОПК-1.1

Номер задания	Указания по оцениванию	Результат оценивания (баллы, полученные за выполнение задания/характеристика правильности ответа)
Задания 1-10	Задания с выбором одного или нескольких верных ответов из предложенных считается верным, если правильно указана цифра или цифры, означающие верные ответы.	Совпадение с верным ответом оценивается 1 баллом; неверный ответ или его отсутствие - 0 баллов.
Задания 11-14	Задания закрытого типа на установление соответствия считается верным, если правильно установлены все соответствия (позиции из одного столбца верно сопоставлены с позициями другого)	Полное совпадение с верным ответом оценивается 1 баллом; неверный ответ или его отсутствие - 0 баллов.
Задания 15-17	Задания закрытого типа на установление последовательности считается верным, если правильно указана вся последовательность цифр	Полное совпадение с верным ответом оценивается 1 баллом; если допущены ошибки или ответ отсутствует - 0 баллов.
Задания 18-20	Задание открытого типа с развернутым ответом считается верным, если ответ совпадает с эталонным по содержанию и полноте.	Полный правильный ответ на задание оценивается 1 баллом. Если в ответе используются перечисления, то различный порядок следования правильных ответов в перечислении не считается ошибкой. Если допущена ошибка, ответ не полный, неправильный или отсутствует - 0 баллов.

ОПК-1.2

Способен администрировать средства защиты информации в компьютерных системах и сетях

БЛОК А (базовый уровень) – Задание с выбором одного или нескольких верных ответов из предложенных

Инструкция по тестам Блока А: Прочитайте текст и выберите один или несколько правильных ответов

№ задания	Тексты заданий
1	Какие из перечисленных компонентов операционной системы связаны с управлением ресурсами компьютера? 1. Системные вызовы 2. Управление базой данных 3. Графический интерфейс пользователя, текстовый процессор 4. Диспетчер задач, планировщик процессов, драйверы устройств
2	Какова роль системного программного обеспечения в архитектуре операционной системы? 1. Предоставление графического интерфейса 2. Создание пользовательских приложений 3. Управление ресурсами компьютера и обеспечение взаимодействия с аппаратурой 4. Организация базы данных
3	Какие из перечисленных функций ОС относятся к уровню пользовательского интерфейса? 1. Управление вводом и выводом данных 2. Поддержка графического и текстового интерфейсов, взаимодействие с пользователем 3. Управление ресурсами компьютера 4. Управление процессами и потоками
4	В OS UNIX каждый новый процесс может быть образован (порожден) только ... 1. одним из существующих процессов 2. двумя из существующих процессов 3. несколькими родительскими процессами 4. четным количеством родительских процессов
5	Политика безопасности в операционной системе – это комплекс: 1. Руководств, требований обеспечения необходимого уровня безопасности 2. Инструкций, алгоритмов поведения пользователя в сети 3. Нормы информационного права, соблюдаемые в сети
6	В операционной системе UNIX сигналы можно рассматривать как простейшую форму взаимодействия между ... 1. процессорами 2. процессами 3. каналами 4. сегментами
7	Защита с применением меток безопасности, согласно «Оранжевой книге», используется в системах класса 1. B1 2. C1 3. C2 4. B2
8	Какую угрозу можно назвать преднамеренной? Сотрудник: 1. Открыл письмо содержащее вредоносное ПО 2. Совершил не авторизованный доступ 3. Включил компьютер без разрешения 4. Ввел неправильные данные
9	Что записывается в таблицу сегментов процесса? 1. признак обращения к данному сегменту за все время существования сегмента 2. правила доступа

№ задания	Тексты заданий
	3. размер сегмента 4. признак модификации 5. начальный физический адрес
10	Машинные коды с настроенными адресами по месту размещения в основной памяти называются ... 1. объектным модулем 2. абсолютным модулем 3. загрузочный модуль 4. исходным модулем

БЛОК Б (повышенный уровень) – Задание закрытого типа на установление соответствия
Инструкция: Прочитайте текст и установите соответствие

№ задания	Тексты заданий
11	Установите соответствие между схемами администрирования и их описанием: 1. Централизованная схема, 2. Распределенная схема, 3. Смешанная схема ; Установите соответствие между схемами администрирования и их описанием А. Каждый объект инфраструктуры имеет свои собственные средства управления и может функционировать автономно. Б. Наличие единой точки управления, откуда администраторы могут управлять всей инфраструктурой системы. В. главный администратор безопасности обеспечивает единую политику безопасности в масштабах всей системы, а подчиненные администраторы – безопасность закрепленных за ними элементов системы..
12	Соотнесите периоды эволюции ОС с характеристиками ОС 1. Первый период эволюции ОС 2. Второй период эволюции ОС 3. Третий период эволюции ОС 4. Четвёртый период эволюции ОС Установите соответствие периодов эволюции ОС их описанию. А. Классические, сетевые и распределённые ОС. Б. Нет ОС. В. Пакетные ОС. Г. Многозадачные ОС
13	Соотнесите первые 4 записи MFT и их назначение: 1. \$MftMirr, 2. \$Mft, 3. \$Volume, 4. \$LogFile Установите соответствие записей их содержанию. А. Файл журнала; Б. Резервная копия начала файла MFT В. Информация о томе; Г. Описывает сам файл MFT;
14	Соотнесите достоинства микроядра с точки зрения: 1. Надежность, безопасность, 2. Повышение производительности, 3. Дисковое пространство, 4. Переносимость. Поставьте в соответствие перечисленные достоинства микроядра. А. Минимизация количества обращений к диску за счёт кэширования Б. Простота переноса на новое оборудование В. Управляемость сохраняется даже если не выделено ни одному файлу Г. Меньше кода выполняется в режиме ядра, ошибки программ не влияют на остальную часть системы

БЛОК Б (повышенный уровень) – Задание закрытого типа на установление последовательности

Инструкция: Прочитайте текст и установите правильную последовательность

№ задания	Тексты заданий
15	Упорядочьте технологии резервного копирования и восстановления данных в зависимости от объема дискового пространства, требуемого для их реализации (от наименьшего к наибольшему объему): 1) полное резервное копирование 2) дифференциальное резервное копирование 3). инкрементальное резервное копирование
16	Установите правильную последовательность этапов получения клиентом (C1) доступа к серверу (C2) в соответствии с протоколом Kerberos:.. 1) C1 посылает серверу Kerberos запрос, содержащий сведения о себе и о запрашиваемой услуге сервера C2 2) сервер Kerberos возвращает так называемый билет, зашифрованный секретным ключом C2, и копию части информации из билета, зашифрованную при помощи алгоритма симметричного шифрования секретным ключом клиента C1 3) C2, расшифровав билет своим секретным ключом, может сравнить его содержимое с дополнительной информацией, присланной клиентом; при совпадении C1 может получить доступ к 4) C2C1 расшифровывает порцию данных, зашифрованную при помощи алгоритма симметричного шифрования, своим секретным ключом и пересылает ее вместе с билетом C2
17	Расставьте в правильном порядке действия при запуске операционной системы: 1. Запуск ядра ОС, 2. Поиск загрузчика ОС, 3. Запуск BIOS, 4. Действия загрузчика, 5. Запуск POST.

БЛОК В (высокий уровень) – Задание открытого типа с развернутым ответом

Инструкция: Прочитайте текст и запишите обоснованный ответ

№ задания	Тексты заданий
18	Добавить недостающие слова в определение доступа к информации: Для обеспечения _____ данных при передаче по сети используется VPN (Virtual Private Network) соединение, который _____ трафик между двумя точками.
19	Политика информационной безопасности определяет _____ корпоративных ресурсов и должна включать в себя требования по _____ и ответственности пользователей.
20	Межсетевой экран (Firewall) позволяет _____ входящий и исходящий сетевой трафик, _____ нежелательные соединения и защищая сеть от атак.

Система оценивания выполнения тестовых заданий по компетенции ООПК-1.2.4

Номер задания	Указания по оцениванию	Результат оценивания (баллы, полученные за выполнение задания/характеристика правильности ответа)
Задания 1-10	Задания с выбором одного или нескольких верных ответов из предложенных считается верным, если правильно указана цифра или цифры, означающие верные ответы.	Совпадение с верным ответом оценивается 1 баллом; неверный ответ или его отсутствие - 0 баллов.
Задания 11-14	Задания закрытого типа на установление соответствия считается верным, если правильно установлены все соответствия (позиции из одного столбца верно сопоставлены с позициями другого)	Полное совпадение с верным ответом оценивается 1 баллом; неверный ответ или его отсутствие - 0 баллов.
Задания 15-17	Задания закрытого типа на установление последовательности считается верным, если правильно указана вся последовательность цифр	Полное совпадение с верным ответом оценивается 1 баллом; если допущены ошибки или ответ отсутствует - 0 баллов.
Задания 18-20	Задание открытого типа с развернутым ответом считается верным, если ответ совпадает с эталонным по содержанию и полноте.	Полный правильный ответ на задание оценивается 1 баллом. Если в ответе используются перечисления, то различный порядок следования правильных ответов в перечислении не считается ошибкой. Если допущена ошибка, ответ не полный, неправильный или отсутствует - 0 баллов.

Методические рекомендации по освоению дисциплины

1. Методические рекомендации преподавателю

Перед началом изучения дисциплины преподаватель должен ознакомить обучающихся с рабочей программой и оценочными материалами по дисциплине, с видами учебной и самостоятельной работы, перечнем литературы и интернет-ресурсов, с формами текущей и промежуточной аттестации, с критериями оценки качества знаний для итоговой оценки по дисциплине.

При проведении лекций, преподаватель:

- 1) формулирует тему и цель занятия, объявляет учебные вопросы;
- 2) излагает основные теоретические положения;
- 3) с помощью технических средств обучения и/или под запись дает определения основных понятий, расчетных формул;
- 4) проводит примеры из отечественного и зарубежного опыта, дает текущие статистические данные для наглядного и образного представления изучаемого материала;
- 5) в конце занятия выдает вопросы для самостоятельного изучения.

На занятиях лабораторного цикла следует обратить внимание на соответствие выбираемых обучающимся средств выполнения решаемым в работе задачам.

Каждая лабораторная работа должна быть оформлена и защищена в соответствии с требованиями. Защита производится после оформления отчета по работе.

Во время выполнения заданий в учебной аудитории обучающийся может консультироваться с преподавателем, определять наиболее эффективные методы решения поставленных задач. Если какая-то часть задания остается не выполненной, обучающийся может продолжить её выполнение во время внеаудиторной самостоятельной работы.

Для оценки полученных знаний и освоения учебного материала по каждому разделу и в целом по дисциплине преподаватель использует формы текущего, промежуточного и итогового контроля знаний обучающихся.

2. Методические рекомендации обучающимся

Приступая к изучению новой учебной дисциплины, обучающиеся должны ознакомиться с рабочей программой, оценочными материалами, учебной, научной и методической литературой, имеющейся в ЭИОС СКФ МТУСИ,

Глубина усвоения дисциплины зависит от активной и систематической работы обучающегося на лекциях и практических занятиях, а также в ходе самостоятельной работы, по изучению рекомендованной литературы.

2.1 Методические указания для обучающихся по лекционным занятиям

Важно сосредоточить внимание на содержании лекции. Это поможет лучше воспринимать учебный материал и уяснить взаимосвязь проблем по всей дисциплине.

Основное содержание лекции целесообразнее записывать в тетради в виде ключевых фраз, понятий, тезисов, обобщений, схем, опорных выводов. Необходимо обращать внимание на термины, формулировки, раскрывающие содержание тех или иных явлений и процессов, научные выводы и практические рекомендации. Желательно оставлять в конспектах поля, на которых делать пометки из рекомендованной литературы, дополняющей материал прослушанной лекции, а также подчеркивающие особую важность тех или иных теоретических положений.

С целью уяснения теоретических положений, разрешения спорных ситуаций необходимо задавать преподавателю уточняющие вопросы. Для закрепления содержания лекции в памяти,

необходимо во время самостоятельной работы внимательно прочесть свой конспект и дополнить его записями из учебников и рекомендованной литературы.

Конспектирование читаемых лекций и их последующая доработка способствует более глубокому усвоению знаний, и поэтому являются важной формой учебной деятельности обучающихся.

2.2 Методические указания для обучающихся по подготовке к лабораторным работам

Лабораторные занятия по любой учебной дисциплине проводятся в соответствии с рабочей программой этой учебной дисциплины в установленные расписанием часы.

Инструктаж по технике безопасности, правилам пожарной безопасности и правилам внутреннего распорядка в лаборатории проводится преподавателем на первом лабораторном занятии. На этом же занятии обучающимся сообщаются:

- программа всего предстоящего лабораторного цикла;
- условия взаимодействия обучающихся с преподавателем в процессе выполнения лабораторных работ;
- условия контроля самостоятельной работы обучающихся, включая правила оформления отчетов по лабораторным работам и их последующей защиты;
- другая необходимая информация.

Организация лабораторных работ включает:

- самостоятельную внеаудиторную подготовку обучающегося к выполнению каждой отдельной лабораторной работы в соответствии с ее программой в рамках часов, выделенных на самостоятельную проработку материала в программе дисциплины;
- входной контроль преподавателем степени подготовленности каждого обучающегося к выполнению лабораторных работ;
- выполнение программы лабораторных работ в полном объеме;
- оформление отчета и его защиту каждым обучающимся в установленные сроки;
- формирование преподавателем рейтингов каждого из обучающихся по результатам выполнения и защиты им отдельных лабораторных работ и их циклов (используется Модульно-рейтинговая система).

Оценка качества выполнения лабораторных работ каждым обучающимся производится преподавателем отдельно за подготовку к работе, ее выполнение и защиту.

2.3 Методические указания для обучающихся по подготовке к практическим занятиям

Целью практических занятий является закрепление теоретических знаний, полученных при изучении дисциплины.

При подготовке к практическому занятию целесообразно выполнить следующие рекомендации:

- изучить основную литературу; ознакомиться с дополнительной литературой, новыми публикациями в периодических изданиях: журналах, газетах и т.д.;
- при необходимости доработать конспект лекций. При этом учесть рекомендации преподавателя и требования учебной программы.

При выполнении практических занятий основным методом обучения является самостоятельная работа обучающегося под управлением преподавателя. На них пополняются теоретические знания обучающихся, их умение творчески мыслить, анализировать, обобщать изученный материал, проверяется отношение обучающихся к будущей профессиональной деятельности.

Оценка выполненной работы осуществляется преподавателем комплексно: по результатам выполнения заданий, устному сообщению и оформлению работы.

После подведения итогов занятия обучающийся обязан устранить недостатки, отмеченные преподавателем при оценке его работы.

3. Методические рекомендации для обучающихся по самостоятельной работе

Достижение целей эффективной подготовки обучающихся в вузах невозможно без их целеустремленной самостоятельной работы. При этом, безусловно, нельзя обойтись без живого общения и консультирования со стороны профессорско-преподавательского состава. Самостоятельная работа обучающихся является составной частью учебной работы и имеет целью закрепление и углубление полученных знаний и навыков, поиск и приобретение новых знаний, в том числе с использованием автоматизированных обучающих курсов (систем), а также выполнение учебных заданий, подготовку к предстоящим занятиям, зачетам и экзаменам. Обязательным компонентом самостоятельной работы обучающихся является внеаудиторный практикум по иностранному языку.

Самостоятельная работа организуется преподавателями, обеспечивается и контролируется кафедрами. Она предусматривает, как правило, разработку рефератов, выполнение расчетно-графических, вычислительных работ, моделирования и других творческих заданий в соответствии с учебной программой (тематическим планом изучения дисциплины). Основная цель данного вида занятий состоит в обучении курсантов методам самостоятельной работы с учебным материалом.

Самостоятельная работа обучающихся является составной частью учебной работы и имеет целью закрепление и углубление полученных знаний и навыков, поиск и приобретение новых знаний, в том числе с использованием автоматизированных обучающих курсов (систем), а также выполнение учебных заданий, подготовку к предстоящим занятиям, зачетам и экзаменам.

Самостоятельная работа во внеаудиторное время включает в себя:

- повторение лекционного материала;
 - подготовки к лабораторным работам (практическим занятиям);
 - изучения учебной и научной литературы;
 - решения задач, выданных на практических занятиях;
 - подготовки к тестированию;
 - выделение наиболее сложных и проблемных вопросов по изучаемой теме, получение разъяснений и рекомендаций по данным вопросам с преподавателями кафедры на их еженедельных консультациях.
- проведение самоконтроля путем ответов на вопросы текущего контроля знаний, решения представленных в учебно-методических материалах кафедры задач, тестов, написания рефератов по отдельным вопросам изучаемой дисциплины.

Перед выполнением внеаудиторной самостоятельной работы преподаватель проводит инструктаж (консультацию) с определением цели задания, его содержания, сроков выполнения, основных требований к результатам работы, критериев оценки, форм контроля и перечня источников и литературы.

Обычно постановку задачи обучаемым на проведение самостоятельной работы преподаватель осуществляет на одном из занятий, предшествующем данному.

Методику самостоятельной работы все обучаемые выбирают индивидуально.

Проведению самостоятельной работы (как и любого другого вида занятий) должна предшествовать подготовка как преподавателя, так и обучаемых.

Постановку задачи обучаемым на проведение самостоятельного занятия преподаватель осуществляет на одном из занятий, предшествующем данному. Он разъясняет смысл занятия и указывает, что к нему обучающиеся должны приготовить. Задание на самостоятельную работу должно быть выдано заблаговременно с тем, чтобы слушатели имели время на информационный поиск в библиотеке необходимых пособий.

Методику самостоятельной работы все обучаемые выбирают индивидуально, но методика достижения конечной цели может определяться преподавателем и включать: последовательность изучения и усвоения учебно-методического материала, пособий, руководств, наставлений, техники и т.д.; определение главного в изучаемом материале, материале, который необходимо законспектировать; просмотр учебных кинофильмов и их обсуждение; работу обучающихся по индивидуальным заданиям; опрос обучаемых в течении 7-10 минут с целью проверки усвоения главного из прочитанного материала.

При возникновении затруднений у обучаемых в разрешении вопросов задания преподавателю необходимо предусмотреть, чтобы каждый обучаемый мог получить оперативную консультацию по любому вопросу, если же при самостоятельной работе возникают затруднения по одному и тому же материалу (вопросу) у многих обучаемых, то желательно провести групповую консультацию.

Для контроля усвоения учебного материала целесообразно проводить в групповое собеседование или обсуждение изучаемого материала, проведение контрольных работ и т.п. Контрольные мероприятия при должной их организации позволяют не только оценивать знания материала, но и углубить и закрепить его у обучаемых.

Приветствуется использование компьютеров, которое:

- расширяет информационную базу учебных занятий;
- повышает активность обучаемых, из пассивного получателя информации они превращаются в её добытчиков:
- способствует развитию способностей к анализу и обобщению, улучшает связанность, широту и глубину мышления;
- облегчает усвоение абстрактного материала, позволяет многое из него представить в виде конкретных образов;
- приучает к точности, аккуратности, последовательности действий способствует развитию самостоятельности.

Компьютерные технологии и программные продукты для выполнения самостоятельной работы по освоению учебного материала необходимо использовать в соответствии с указаниями методических разработок раздела 4 настоящей Рабочей программы.

Таблица – Учебный материал, выносимый на самостоятельное изучение обучающимся очной формы обучения

№	Темы, разделы, вынесенные на самостоятельную подготовку, вопросы для подготовки к практическим и лабораторным занятиям; курсовые работы, содержание контрольных работ; рекомендации по использованию литературы, ЭВМ и др.	Часов всего:	Неделя
Модуль 1 – 27 часа			
1	Анализ выполнения современными ОС формализованных требований к защите информации от несанкционированных действий	6	1,2
2	Основные встроенные механизмы защиты ОС и их недостатки	7	3,4
3	Анализ существующей статистики угроз для современных универсальных ОС. Семейства ОС и общая статистика угроз	7	5,6
4	Обзор и статистика методов, лежащих в основе атак на современные ОС. Классификация методов и их сравнительная статистика	7	7,8
Модуль 2 – 27 часа			
9	Адекватная политика безопасности.	4	9
10	Этапы построения и поддержания защиты.	4	10
11	Стандарты безопасности ОС.	4	11
12	Обеспечение безопасности функционирования ОС.	3	12
13	Механизмы защиты ОС.	3	13
14	Проблемы обеспечения безопасности ОС.	3	14
15	Контроль доступа к данным	3	15
16	Достоинства и недостатки основных систем защиты ОС.	3	16

Для более углубленного изучения материала по дисциплине целесообразно использовать учебные курсы сайта <http://www.intuit.ru/>.

Самостоятельная работа обучающихся над усвоением материала по дисциплине может выполняться в помещении для самостоятельной работы СКФ МТУСИ, посредством использования электронной библиотеки и ЭИОС