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
_____ А.Г. Жуковский
«29» 08 2022 г.

Безопасность операционных систем Б1.О.26
рабочая программа дисциплины

Кафедра: Информатика и вычислительная техника
Направление подготовки: **10.03.01 Информационная безопасность**
Профиль: **Безопасность компьютерных систем.**
Формы обучения: **очная**

Распределение часов дисциплины по семестрам (для очной формы обучения), курсам (для заочной формы обучения)

Вид учебной работы	ОФ		ЗФ	
	ЗЕ	часов	ЗЕ	часов
Общая трудоемкость дисциплины, в том числе (по семестрам, курсам):	3	108/5сем		
Контактная работа, в том числе (по семестрам, курсам):		60/5сем		
Лекции		24/5сем		
Лабораторных работ		36/5сем		
Практических занятий				
Семинаров				
Самостоятельная работа		48/5сем		
Контроль				
Число контрольных работ (по курсам)				
Число КР (по семестрам, курсам)				
Число КП (по семестрам, курсам)				
Число зачетов с оценкой с разбивкой по семестрам (курсам)		1/5сем		
Число экзаменов с разбивкой по семестрам (курсам)				

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

Рецензент:
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 2020г. N 1427.

Составлена на основании учебного плана
направления 10.03.01 «Информационная безопасность», профиля «Безопасность компьютерных систем», одобренного Учёным советом СКФ МТУСИ, протокол № 9 от 25.04.2022, и утвержденного директором СКФ МТУСИ 25.04.2022 г.

Рассмотрена и одобрена на заседании кафедры
«Информатика и вычислительная техника»

Протокол от «29» 08 2022г. №1

Зав. кафедрой _____ С.В. Соколов

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

Утверждаю
Зам. директора по УВР ________________
«___» _______ 20__ г.
Рабочая программа пересмотрена, обсуждена и одобрена на заседании кафедры

«Информатика и вычислительная техника»

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
«Информатика и вычислительная техника»

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
«Информатика и вычислительная техника»

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
«Информатика и вычислительная техника»

Протокол от «___» _______ 20__ г. № ____
Зав. кафедрой _____________________

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 выпускника способности решать профессиональные задачи в соответствии с ***эксплуатационным*** видом деятельности:

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:
- 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; информационного противоборства, информационной войны и формами их проявления в современном мире; - навыками работы по основам защиты информации с использованием программно-аппаратных комплексов.
ПК-1: Администрирование подсистем защиты информации в операционных системах
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.11 «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.06 «Физика», Б1.О.07 «Иностранный язык», Б1.О.12 «Введение в информационные технологии».
Последующие дисциплины и практики, для которых освоение данной дисциплины необходимо:	
1	Дисциплина является базовой для успешного освоения дисциплин: Б1.О.25 «Методы и средства криптографической защиты информации», Б1.О.26 «Безопасность операционных систем», Б1.О.29 «Основы управления информационной безопасностью», Б1.О.32 «Основы организационно-правового обеспечения информационной безопасности», Б1.О.33 «Программно-аппаратные средства защиты информации», Б1.О.37 «Комплексное обеспечение 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	Компетенции	УМИО
Курс 1, Семестр 2					
Модуль 1. Принципы работы и угрозы безопасности ОС. (30+24) часов					
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.	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	Л2.	4	ОПК-1.1	Л1.1 Л1.2 Л1.3

	3. Инженерно-техническая защита				
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	Лабораторная работа 1 Управление системными службами и процессами в ОС	ЛР1	4	ОПК-1.1	Л3.1
1.5	Лабораторная работа 2 Управление сетевыми подключениями в ОС	ЛР2	4	ОПК-1.1	Л3.1
1.6	Лабораторная работа 3 Применение консольного управления ОС	ЛР3	4	ОПК-1.1	Л3.1
1.7	Лабораторная работа № 4 Средства защиты ОС	ЛР4	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 на современные ОС. Классификация методов и их сравнительная статистика	СРС	24	ПК-1	Л1.1 Л1.2 Л1.3
Модуль 2 Основы защиты информации в инфокоммуникационных системах и сетях (30+24)					
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	Лабораторная работа 5 Управление средствами обеспечения безопасности ОС	ЛР5	4	ПК-1	Л3.1
2.5	Лабораторная работа 6 Исследование характеристик и возможностей программ по восстановлению потерянных данных	ЛР6	4	ПК-1	Л3.1
2.6	Лабораторная работа № 7 Разграничение доступа к файловым объектам и устройствам	ЛР7	4	ПК-1	Л3.1
2.7	Лабораторная работа № 8 Разграничение доступа к запуску программного обеспечения	ЛР8	4		
2.8	Лабораторная работа № 9 Средства аудита в ОС. Протоколирование событий в операционных системах	ЛР9	2		
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	24	ПК-1	Л1.1 Л1.2 Л1.3
	Зачет			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	1. AVAST Free Antivirus 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	Антивирусное ПО. Свободное, условно свободное или триал-версии.

	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 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	Программное обеспечение по защите и сокрытию файлов и папок. Свободное, условно свободное или триал-версии.
П.3	1. TrustPort Tools 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	Программное обеспечение по шифрованию, безвозвратному удалению, стеганографии. Свободное, условно свободное или триал-версии.
П.4	1. Hetman Partition Recovery 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	Программное обеспечение по восстановлению данных. Свободное, условно свободное или триал-версии.

	15. Handy Recovery	
	16. Ashampoo Undeleter	
П.5	1. Iperius Backup 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	Программное обеспечение по резервному копированию данных. Свободное, условно свободное или триал-версии.
П.6	MS Word – с лицензией	
П.7	Power Point – с лицензией	

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	Компьютерная аудитория с выходом в интернет
6.3 МТО рубежных контролей, экзамена	
1	Компьютерная аудитория

7. Методические указания для обучающихся по освоению дисциплины

7.1 Указания по самостоятельной работе студента

Достижение целей эффективной подготовки студентов 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 студентов 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 студентов 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.

Материал, подлежащий обработке на самостоятельных занятиях, намечается при разработке программы самостоятельной работы. Опыт, накопленный кафедрами в организации самостоятельных занятий, что материал выделяемый на такие занятия, должен удовлетворять следующим требованиям:

- быть изложенным в учебнике достаточно полно и с примерами;
- обеспечиваться достаточным количеством литературы, учебных пособий. учебно-методических материалов, образцов техники
- содержать материал. углубляющий знания, полученные на лекции;
- осваивать проблемные еще не полностью решенные вопросы.

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 занятия, предшествующему данному. Он разъясняет смысл занятия и указывает, что к нему студенты 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 студентов 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 баз) 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 5 настоящей Рабочей программы.

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

Таблица 7.1 – Учебный материал, выносимый на самостоятельное изучение студентам 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: 24	Неделя
Модуль 1 – 24 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	6	3,4
3	Анализ существующей статистики угроз для современных универсальных ОС. Семейства ОС и общая статистика угроз	6	5,6
4	Обзор и статистика методов, лежащих в основе атак на современные ОС. Классификация методов и их сравнительная статистика	6	7,8
Модуль 2 – 24 часа			
9	Адекватная политика безопасности.	3	9
10	Этапы построения и поддержания защиты.	3	10
11	Стандарты безопасности ОС.	3	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

Дополнения и изменения в рабочей программе