МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Магнитогорский государственный технический университет им. Г.И. Носова»

УТВЕРЖДАЮ
Директор ИЭиАС
_____ С.И. Лукьянов

26.02.2020 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

БЕЗОПАСНОСТЬ ОПЕРАЦИОННЫХ СИСТЕМ

Направление подготовки (специальность)
10.05.03 Информационная безопасность автоматизированных систем

Направленность (профиль/специализация) программы
10.05.03 специализация N 7 "Обеспечение информационной безопасности распределенных информационных систем";

Уровень высшего образования - специалитет

Форма обучения
очная

Институт/ факультет	Институт энергетики и автоматизированных систем
Кафедра	Информатики и информационной безопасности
Курс	3, 4
Семестр	6, 7

Магнитогорск
2019 год

Лист актуализации рабочей программы

Рабочая программа пересмотрена, обсуждена и одобрена для реализации в 2020 - 2021 учебном году на заседании кафедры Информатики и информационной безопасности

Протокол от 1 сентября 2020 г. № 1
Зав. кафедрой _____ И.И. Баранкова

Рабочая программа пересмотрена, обсуждена и одобрена для реализации в 2021 - 2022 учебном году на заседании кафедры Информатики и информационной безопасности

Протокол от __ _____ 20__ г. № __
Зав. кафедрой _____ И.И. Баранкова

Рабочая программа пересмотрена, обсуждена и одобрена для реализации в 2022 - 2023 учебном году на заседании кафедры Информатики и информационной безопасности

Протокол от __ _____ 20__ г. № __
Зав. кафедрой _____ И.И. Баранкова

Рабочая программа пересмотрена, обсуждена и одобрена для реализации в 2023 - 2024 учебном году на заседании кафедры Информатики и информационной безопасности

Протокол от __ _____ 20__ г. № __
Зав. кафедрой _____ И.И. Баранкова

Рабочая программа пересмотрена, обсуждена и одобрена для реализации в 2024 - 2025 учебном году на заседании кафедры Информатики и информационной безопасности

Протокол от __ _____ 20__ г. № __
Зав. кафедрой _____ И.И. Баранкова

1 Цели освоения дисциплины (модуля)

Целями освоения дисциплины (модуля) «Безопасность операционных систем» являются:

1. Знакомство студентов с назначением, разновидностями и основными принципами организации современных операционных систем в объеме, достаточном для понимания задач обеспечения безопасности операционных систем.

2. Обучение студентов принципам построения защиты информации в операционных системах (ОС) и методам анализа надежности защиты ОС.

2 Место дисциплины (модуля) в структуре образовательной программы

Дисциплина Безопасность операционных систем входит в базовую часть учебного плана образовательной программы.

Для изучения дисциплины необходимы знания (умения, владения), сформированные в результате изучения дисциплин/ практик:

Информатика

Безопасность сетей ЭВМ

Сети и системы передачи информации

Организация ЭВМ и вычислительных систем

Основы информационной безопасности

Знания (умения, владения), полученные при изучении данной дисциплины будут необходимы для изучения дисциплин/практик:

Разработка и эксплуатация защищенных автоматизированных систем

Информационная безопасность распределенных информационных систем

Управление информационной безопасностью

Моделирование угроз информационной безопасности

Программно-аппаратные средства обеспечения информационной безопасности

Производственная-практика по получению профессиональных умений и опыта профессиональной деятельности

Производственная-преддипломная практика

3 Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля) и планируемые результаты обучения

В результате освоения дисциплины (модуля) «Безопасность операционных систем» обучающийся должен обладать следующими компетенциями:

Структурный элемент компетенции	Планируемые результаты обучения
ПК-23 способностью формировать комплекс мер (правила, процедуры, методы) для защиты информации ограниченного доступа	
Знать	- правила, процедуры, практические приемы для обеспечения информационной безопасности операционных систем - критерии оценки эффективности и надежности средств защиты операционных систем; специализированные средства выявления уязвимостей ОС;
Уметь	- реализовывать политику учетных записей пользователей операционной системы; - сформировать комплекс мер защиты информации ограниченного доступа для операционной системы;

Владеть	- навыками формальной постановки задачи обеспечения информационной безопасности операционной системы. - навыками эксплуатации операционных систем и программных систем с учетом требований по защиты информации ограниченного доступа; - навыками использования программно-аппаратных средств обеспечения информационной безопасности
ПК-25 способностью обеспечить эффективное применение средств защиты информационно-технологических ресурсов автоматизированной системы и восстановление их работоспособности при возникновении нештатных ситуаций	
Знать	- иметь представление об основных средствах защиты ОС в составе информационно-технологических ресурсов автоматизированной системы; - критерии защищенности ОС и сети ЭВМ; - критерии оценки эффективности и надежности средств защиты операционных систем; - принципы организации и структуру подсистем защиты операционных систем семейств UNIX и Windows;
Уметь	использовать средства операционных систем для обеспечения эффективного и безопасного функционирования автоматизированных систем; - проводить мониторинг угроз безопасности операционных систем - обеспечивать защиту сетевых подключений средствами операционной системы;
Владеть	- профессиональной терминологией в области информационной безопасности; - навыками работы с конкретными программными и аппаратными продуктами средств телекоммуникаций, удаленного доступа и сетевыми ОС; - навыками конфигурирования встроенных средств защиты информации ОС; - навыками противодействия угрозами типа «недоверенная загрузка (НДЗ) операционной системы» и несанкционированный доступ (НСД) к операционной системе и вычислительной сети;
ОПК-8 способностью к освоению новых образцов программных, технических средств и информационных технологий	
Знать	- основные определения и понятия, используемые в теории операционных систем; - современные подходы к организации и проведению научных исследований с использованием сетевых технологий; - принципы построения и современные технологии, используемые в современных операционных системах, автоматизированных системах и сетях ЭВМ;
Уметь	- разрабатывать политику учетных записей пользователей ОС; - обосновать выбор решения по обеспечению требуемого уровня защиты ОС (ИС); готовить публикации по результатам выполненных работ;
Владеть	- навыками использования операционных систем семейств Unix и Windows в системах защиты информации ; - методами и технологиями исследования безопасности операционных систем.

ПСК-7.4 способностью проводить удаленное администрирование операционных систем и систем баз данных в распределенных информационных системах	
Знать	- основы администрирования в операционных системах семейств UNIX и Windows; - средства и службы удаленного управления и администрирования ОС; - модели разделения администрирования операционных систем семейств UNIX и Windows;
Уметь	-выполнять настройку служб терминала; -создавать и выполнять настройку доменов, групп и учетный записей пользователей; -выполнять настройку и удаленное администрирование файлового сервера для ОС семейств UNIX и Windows;
Владеть	- Навыками удаленного администрирования ОС семейств UNIX и Windows; -Навыками настройки и управления службами терминала; -Навыками использования командной строки для настройки и проведения удаленного администрирования ОС семейств UNIX и Windows

4. Структура, объём и содержание дисциплины (модуля)

Общая трудоемкость дисциплины составляет 6 зачетных единиц 216 акад. часов, в том числе:
– контактная работа – 123,95 акад. часов:
– аудиторная – 119 акад. часов;
– внеаудиторная – 4,95 акад. часов
– самостоятельная работа – 56,35 акад. часов;
– подготовка к экзамену – 35,7 акад. часа

Форма аттестации - зачет, экзамен

Раздел/ тема дисциплины	Семестр	Аудиторная контактная работа (в акад. часах)			Самостоятельная работа обучающегося	Вид самостоятельной работы	Форма текущего контроля успеваемости и промежуточной аттестации	Код компетенции
		Лек.	лаб. зан.	практ. зан.				
1. Предмет безопасности операционных систем								
1.1 Определение предмета безопасности операционных систем (ОС)	6	1	2/1И		2	Поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями)	Устный опрос	ПК-23, ПК-25, ОПК-8

1.2 Общее понятие безопасности операционных систем, история развития вопроса, характеристика подходов к обеспечению безопасности операционных систем		1	2/1И		2	Поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями)	Устный опрос	ПК-23, ПК-25, ОПК-8
Итого по разделу		2	4/2И		4			
2. Операционная система с точки зрения специалиста по информационной								
2.1 Общая концепция построения ОС, виды ОС.	6	1	4/2И		2	Поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями)	Устный опрос	ПК-23, ПК-25, ОПК-8
2.2 ОС семейства Unix и Windows. Концепции в обеспечении защиты		1	4/2И		2	Поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями)	Устный опрос	ПК-23, ПК-25, ОПК-8
Итого по разделу		2	8/4И		4			
3. Структурная схема ОС								
3.1 Центральные элементы ОС – ядро, пользовательская оболочка, файловая подсистема, сетевая подсистема	6	2	4/2И		1	Поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями)	Лабораторная работа "Основные структурные элементы операционной системы. Отличительные свойства операционных систем на примере сравнения ОС семейства Microsoft Windows и Linux. "	ПК-23, ПК-25, ОПК-8

3.2 Периферийные подсистемы ОС. Загрузка ОС и ее этапы		2	4/2И		2	Поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями)	Лабораторная работа "Загрузка ОС. Порядок загрузки ОС. Известные способы перехвата загрузки ОС. Понятие доверенной загрузки."	ПК-23, ПК-25, ОПК-8
Итого по разделу		4	8/4И		3			
4. Многозадачные ОС								
4.1 Принципы организации многозадачной ОС. Виды многозадачности, технологии обеспечения многозадачности ОС	6	2	4/1И		1	Поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями). Подготовка к практическому занятию	Лабораторная работа "Файловые подсистемы ОС. Характеристики, разновидности, принципы организации. Известные уязвимости наиболее распространенных файловых систем"	ПК-23, ПК-25, ОПК-8
4.2 Принципы организации межпрограммного взаимодействия		2	4/1И		1	Поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями)	Устный опрос	ПК-23, ПК-25, ОПК-8
Итого по разделу		4	8/2И		2			
5. Сетевая подсистема ОС								
5.1 Сетевые сервисы ОС	6	2	2/1И		2	Поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями)	Устный опрос	ПК-23, ПК-25, ОПК-8

5.2 Принципы построения сетевой подсистемы ОС Характерные уязвимости сетевой подсистемы ОС		3	4/1И		2,05	Поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями)	Лабораторная работа "Сетевая подсистема ОС. Принципы организации, основные структурные элементы"	ПК-23, ПК-25, ОПК-8
Итого по разделу		5	6/2И		4,05			
6. Подготовка к промежуточной аттестации(зачет)								
6.1 Подготовка к промежуточной аттестации	6				3	Поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями)	Зачет	ПК-23, ПК-25, ОПК-8
Итого по разделу					3			
Итого за семестр		17	34/14И		20,05		зачёт	
7. Подсистема безопасности ОС								
7.1 Подсистема безопасности ОС. Основные компоненты	7	4	4/1И		4	Поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями)	Лабораторная работа "Подсистема безопасности ОС. Сравнительный анализ подсистем безопасности ОС семейства Microsoft Windows и Linux"	ПК-23, ПК-25, ОПК-8
7.2 Модели безопасности в различных семействах ОС		4	4/1И		2	Поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями)	Устный опрос	ПК-23, ПК-25, ОПК-8

7.3 Дискреционный и мандатный принципы управления доступом – сравнительный анализ		4	4/1И		2	Поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями)	Устный опрос	ПК-23, ПК-25, ОПК-8
Итого по разделу		12	12/3И		8			
8. Администрирование операционных систем								
8.1 Модели пользователей в различных ОС	7	4	4/2И		3	Поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями). Подготовка к практическому занятию	Выполнение лабораторной работы «Создание пользователя ОС Linux»	ПК-23, ПК-25, ОПК-8
8.2 Профиль пользователя, бюджет, авторизация, аутентификация пользователя ОС		4	4/2И		3	Поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями). Подготовка к практическому занятию	Выполнение лабораторной работы «Создание пользователя ОС Windows»	ПК-23, ПК-25, ОПК-8
8.3 Назначение прав пользователю ОС и аудит его действий		4	4/2И		3	Поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями). Подготовка к практическому занятию	Выполнение лабораторной работы «Аудит действий пользователя ОС Windows»	ПК-23, ПК-25, ОПК-8

8.4 Аудит системных событий ОС		4	4/2И		3	Поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями)	Устный опрос	ПК-23, ПК-25, ОПК-8
Итого по разделу		16	16/8И		12			
9. Противодействие атакам на информационные системы								
9.1 Методология атаки и их разновидности	7	3	3/1И		3	Поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями). Подготовка к практическому занятию	Выполнение лабораторной работы «Работа со сканером уязвимостей»	ПК-23, ПК-25, ОПК-8
9.2 Методы обнаружения и предотвращения атак на информационные системы		3	3/2И		3,3	Поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями)	Лабораторная работа "Средства шифрования и их роль в современных ОС. Сравнительный анализ использования средств шифрования в различных ОС."	ПК-23, ПК-25, ОПК-8
Итого по разделу		6	6/3И		6,3			
10. Подготовка к итоговой аттестации								
10.1 Экзамен	7				10	Поиск дополнительной информации по заданной теме	Экзамен	ПК-23, ПК-25, ОПК-8
Итого по разделу					10			
Итого за семестр		34	34/14И		36,3		экзамен	
Итого по дисциплине		51	68/28И		56,35		зачет, экзамен	ПК-23,ПК-25,ОПК-8

5 Образовательные технологии

Для реализации предусмотренных видов учебной работы в качестве образовательных технологий в преподавании дисциплины «Безопасность операционных систем» используются традиционная и модульно-компетентностная технологии.

Реализация компетентностного подхода предусматривает использование в учебном процессе активных и интерактивных форм проведения занятий в сочетании с внеаудиторной работой с целью формирования и развития профессиональных навыков обучающихся.

При проведении учебных занятий преподаватель обеспечивает развитие у обучающихся навыков командной работы, межличностной коммуникации, принятия решений, лидерских качеств посредством проведения интерактивных лекций, групповых дискуссий, ролевых игр, тренингов, анализа ситуаций, учета особенностей профессиональной деятельности выпускников и потребностей работодателей.

6 Учебно-методическое обеспечение самостоятельной работы обучающихся

По дисциплине «Безопасность операционных систем » предусмотрена аудиторная и внеаудиторная самостоятельная работа обучающихся.

Аудиторная самостоятельная работа обучающихся на практических занятиях осуществляется под контролем преподавателя в виде выполнения лабораторных работ, которые определяет преподаватель для обучающегося.

Внеаудиторная самостоятельная работа обучающихся осуществляется в виде изучения литературы по соответствующему разделу с проработкой материала; выполнения домашних заданий, подготовки к аудиторным контрольным работам и выполнения домашних заданий с консультациями преподавателя, а так же с применением кейс-технологий.

Перечень лабораторных работ по курсу «Безопасность операционных систем»

Лабораторная работа №1.

Основные структурные элементы операционной системы. Отличительные свойства операционных систем на примере сравнения ОС семейства Microsoft Windows и Linux.

Лабораторная работа №2.

Загрузка ОС. Порядок загрузки ОС. Известные способы перехвата загрузки ОС. Понятие доверенной загрузки.

Лабораторная работа №3.

Файловые подсистемы ОС. Характеристики, разновидности, принципы организации. Известные уязвимости наиболее распространенных файловых систем.

Лабораторная работа №4.

Сетевая подсистема ОС. Принципы организации, основные структурные элементы.

Лабораторная работа №5.

Подсистема безопасности ОС. Сравнительный анализ подсистем безопасности ОС семейства Microsoft Windows и Linux.

Лабораторная работа №6.

Известные уязвимости наиболее популярных ОС. Принципы обнаружения уязвимостей, приемы использования, методы обнаружения и устранения уязвимостей ОС. Специализированное ПО для поиска и анализа уязвимостей ОС.

Лабораторная работа №7.

Использование встроенных межсетевых экранов на примере настройки межсетевого экрана Iptables ОС Linux.

Лабораторная работа №8.

Средства шифрования и их роль в современных ОС. Сравнительный анализ использования средств шифрования в различных ОС.

Примерный перечень индивидуальных домашних заданий

1. Исследование методов идентификации и аутентификации в ОС Windows.
2. Исследование методов идентификации и аутентификации в ОС Unix.
3. Исследование методов разграничение доступа к ресурсам в ОС Windows, Unix.
4. Настройка системы аудита в Windows.
5. Настройка системы аудита в Unix.
6. Изучение средств защиты сетевого взаимодействия Windows. Конфигурирование средств защиты каналов средствами Windows XP/2003/Vista, Windows Firewall. Виртуальные частные сети, протоколы L2TP и PPTP.

7 Оценочные средства для проведения промежуточной аттестации

Структурный элемент компетенции	Планируемые результаты обучения	Оценочные средства
ОПК-8 - способность к освоению новых образцов программных, технических средств и информационных технологий		
Знать	- основные определения и понятия, используемые в теории операционных систем; - современные подходы к организации и проведению научных исследований с использованием сетевых технологий; - принципы построения и современные технологии, используемые в современных операционных системах, автоматизированных системах и сетях ЭВМ;	Перечень вопрос: 1. Принципы классификации операционных систем, их основные характеристики и функциональное назначение; 2. Основные структурные элементы и подсистемы операционной системы, их характеристики и функциональное назначение; 3. Принципы функционирования ядра, дисковой, файловой, сетевой подсистем операционной системы 4. Основные принципы построения подсистем безопасности операционных систем
Уметь	- разрабатывать политику учетных записей пользователей ОС; - обосновать выбор решения по обеспечению требуемого уровня защиты ОС (ИС); готовить публикации по результатам выполненных работ;	1. Провести сравнительный анализ различных операционных систем с точки зрения защищенности информации; 2. Обосновать выбор операционной системы при построении информационной системы на ее базе;
Владеть	- навыками использования операционных систем семейств Unix и Windows в системах защиты информации ; - методами и технологиями исследования безопасности операционных систем.	1. Используя средства администрирования файловой подсистемы произвести настройку операционной систем семейств Windows 2. Используя средства администрирования произвести настройку подсистемы безопасности операционной системы семейств Windows 3. Разработать сценарий администрирования для операционных систем семейств Windows и UNIX/Linux 4. Произвести и обосновать выбор операционной системы для построения информационной системы на ее базе с точки зрения требований по защищенности информации
ПК-23 - способность формировать комплекс мер (правила, процедуры, методы) для защиты информации ограниченного доступа		
	- правила, процедуры, практические приемы для обеспечения информационной безопасности операционных систем	Перечень вопросов: 1. Классификация уязвимостей ОС, методы их нейтрализации 2. Критерии надежности средств

7 Оценочные средства для проведения промежуточной аттестации

Структурный элемент компетенции	Планируемые результаты обучения	Оценочные средства
ОПК-8 - способность к освоению новых образцов программных, технических средств и информационных технологий		
Знать	- основные определения и понятия, используемые в теории операционных систем; - современные подходы к организации и проведению научных исследований с использованием сетевых технологий; - принципы построения и современные технологии, используемые в современных операционных системах, автоматизированных системах и сетях ЭВМ;	Перечень вопрос: 1. Принципы классификации операционных систем, их основные характеристики и функциональное назначение; 2. Основные структурные элементы и подсистемы операционной системы, их характеристики и функциональное назначение; 3. Принципы функционирования ядра, дисковой, файловой, сетевой подсистем операционной системы 4. Основные принципы построения подсистем безопасности операционных систем
Уметь	- разрабатывать политику учетных записей пользователей ОС; - обосновать выбор решения по обеспечению требуемого уровня защиты ОС (ИС); готовить публикации по результатам выполненных работ;	1. Провести сравнительный анализ различных операционных систем с точки зрения защищенности информации; 2. Обосновать выбор операционной системы при построении информационной системы на ее базе;
Владеть	- навыками использования операционных систем семейств Unix и Windows в системах защиты информации ; - методами и технологиями исследования безопасности операционных систем.	1. Используя средства администрирования файловой подсистемы произвести настройку операционной систем семейств Windows 2. Используя средства администрирования произвести настройку подсистемы безопасности операционной системы семейств Windows 3. Разработать сценарий администрирования для операционных систем семейств Windows и UNIX/Linux 4. Произвести и обосновать выбор операционной системы для построения информационной системы на ее базе с точки зрения требований по защищенности информации
ПК-23 - способность формировать комплекс мер (правила, процедуры, методы) для защиты информации ограниченного доступа		
	- правила, процедуры, практические приемы для обеспечения информационной безопасности операционных систем	Перечень вопросов: 1. Классификация уязвимостей ОС, методы их нейтрализации 2. Критерии надежности средств

7 Оценочные средства для проведения промежуточной аттестации

Структурный элемент компетенции	Планируемые результаты обучения	Оценочные средства
ОПК-8 - способность к освоению новых образцов программных, технических средств и информационных технологий		
Знать	- основные определения и понятия, используемые в теории операционных систем; - современные подходы к организации и проведению научных исследований с использованием сетевых технологий; - принципы построения и современные технологии, используемые в современных операционных системах, автоматизированных системах и сетях ЭВМ;	Перечень вопрос: 1. Принципы классификации операционных систем, их основные характеристики и функциональное назначение; 2. Основные структурные элементы и подсистемы операционной системы, их характеристики и функциональное назначение; 3. Принципы функционирования ядра, дисковой, файловой, сетевой подсистем операционной системы 4. Основные принципы построения подсистем безопасности операционных систем
Уметь	- разрабатывать политику учетных записей пользователей ОС; - обосновать выбор решения по обеспечению требуемого уровня защиты ОС (ИС); готовить публикации по результатам выполненных работ;	1. Провести сравнительный анализ различных операционных систем с точки зрения защищенности информации; 2. Обосновать выбор операционной системы при построении информационной системы на ее базе;
Владеть	- навыками использования операционных систем семейств Unix и Windows в системах защиты информации ; - методами и технологиями исследования безопасности операционных систем.	1. Используя средства администрирования файловой подсистемы произвести настройку операционной систем семейств Windows 2. Используя средства администрирования произвести настройку подсистемы безопасности операционной системы семейств Windows 3. Разработать сценарий администрирования для операционных систем семейств Windows и UNIX/Linux 4. Произвести и обосновать выбор операционной системы для построения информационной системы на ее базе с точки зрения требований по защищенности информации
ПК-23 - способность формировать комплекс мер (правила, процедуры, методы) для защиты информации ограниченного доступа		
	- правила, процедуры, практические приемы для обеспечения информационной безопасности операционных систем	Перечень вопросов: 1. Классификация уязвимостей ОС, методы их нейтрализации 2. Критерии надежности средств

Перечень теоретических вопросов к зачету:

1. Общее понятие безопасности операционных систем, история развития вопроса, характеристика подходов к обеспечению безопасности операционных систем.
2. Анализ угроз информационной безопасности ОС. Методы обеспечения информационной безопасности в ОС. Классификация злоумышленников. Основные направления и методы реализации угроз информационной безопасности ОС.
3. Операционная система с точки зрения специалиста по информационной безопасности
4. Общая концепция построения ОС, виды ОС, история развития, семейства ОС. Разграничение доступа в ОС. Идентификация и аутентификация пользователей ОС.
5. Разграничение доступа в ОС.
6. Субъекты, объекты, методы и права доступа. Привилегии субъектов доступа. Избирательное и полномочное разграничение доступа, изолированная программная среда. Примеры реализации разграничения доступа в современных ОС.
7. Формальная процедура установки прав доступа к системным сервисам и ресурсам.
8. Идентификация и аутентификация пользователей ОС.
9. Понятия идентификации и аутентификации пользователей. Аутентификация на основе паролей, методы подбора паролей, средства и методы повышения защищенности ОС от подбора паролей.
10. Аутентификация на основе внешних носителей ключа, биометрических характеристик пользователя. Примеры реализации идентификации и аутентификации в современных ОС.
11. Необходимость аудита. Требования к подсистеме аудита. Примеры реализации аудита в современных ОС.
12. Состав операционной системы. Группы компонентов ОС: ядро, пользовательская оболочка, файловая подсистема, сетевая подсистема.
13. Принципы организации многозадачной ОС. Виды многозадачности, технологии обеспечения многозадачности ОС.
14. Принципы организации межпрограммного взаимодействия.

Критерии оценки для получения зачета

«зачтено» – обучающийся показывает средний уровень сформированности компетенций.

«не зачтено» – результат обучения не достигнут, студент не может показать знания на уровне воспроизведения и объяснения информации, не может показать интеллектуальные навыки решения простых задач, не может показать знания на уровне воспроизведения и объяснения информации.

Перечень теоретических вопросов к экзамену:

1. Подсистема безопасности ОС. Модели безопасности в различных семействах ОС.
2. Анализ защищенности современных операционных систем. Встроенные средства защиты Windows, Unix.
3. Многопользовательские ОС. Методы авторизации и аутентификации пользователей. Известные уязвимости.
4. Обеспечение безопасности ОС – журналирование системных событий, системный аудит и анализ инцидентов. Угрозы безопасности информации в информационно-вычислительных системах.
5. Угрозы безопасности ОС.
6. Инциденты информационной безопасности.
7. Организация режима информационной безопасности.

8. Мониторинг информационной безопасности.
9. Понятие защищенной ОС. Подходы к организации защиты ОС и их недостатки. Этапы построения защиты. Административные меры защиты. Стандарты безопасности ОС.
10. Классификация требований к системам защиты. Формализованные требования к защите информации от НСД.
11. Общие подходы к построению систем защиты компьютерной информации.
12. Требования к защите ОС. Использование средств шифрования в современных ОС. Понятие криптоядра.
13. Сравнительный анализ использования средств шифрования в ОС семейства Microsoft Windows и Linux.
14. Анализ защищенности операционных систем семейства Windows.
15. Анализ защищенности операционных систем семейства Unix.

Критерии оценки (в соответствии с формируемыми компетенциями и планируемыми результатами обучения):

– на оценку **«отлично»** (5 баллов) – обучающийся демонстрирует высокий уровень сформированности компетенций, всестороннее, систематическое и глубокое знание учебного материала, свободно выполняет практические задания, свободно оперирует знаниями, умениями, применяет их в ситуациях повышенной сложности.

– на оценку **«хорошо»** (4 балла) – обучающийся демонстрирует средний уровень сформированности компетенций: основные знания, умения освоены, но допускаются незначительные ошибки, неточности, затруднения при аналитических операциях, переносе знаний и умений на новые, нестандартные ситуации.

– на оценку **«удовлетворительно»** (3 балла) – обучающийся демонстрирует пороговый уровень сформированности компетенций: в ходе контрольных мероприятий допускаются ошибки, проявляется отсутствие отдельных знаний, умений, навыков, обучающийся испытывает значительные затруднения при оперировании знаниями и умениями при их переносе на новые ситуации.

– на оценку **«неудовлетворительно»** (2 балла) – обучающийся демонстрирует знания не более 20% теоретического материала, допускает существенные ошибки, не может показать интеллектуальные навыки решения простых задач.

– на оценку **«неудовлетворительно»** (1 балл) – обучающийся не может показать знания на уровне воспроизведения и объяснения информации, не может показать интеллектуальные навыки решения простых задач.

8 Учебно-методическое и информационное обеспечение дисциплины (модуля)

а) Основная литература:

1. Внуков, А. А. Защита информации : учебное пособие для вузов / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2020. — 161 с. — (Высшее образование). — ISBN 978-5-534-07248-8. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/422772 (дата обращения: 31.08.2020).

2. Бабенко, Л. К. Криптографическая защита информации: симметричное шифрование : учебное пособие для вузов / Л. К. Бабенко, Е. А. Ищукова. — Москва : Издательство Юрайт, 2019. — 220 с. — (Университеты России). — ISBN 978-5-9916-9244-1. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/437667 (дата обращения: 31.08.2020).

3. Зашита информации : учеб. пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. - 3-е изд. - Москва : РИОР: ИНФРА-М, 2019. - 400 с. - (Высшее образование). - DOI: https://doi.org/10.12737/1759-3. - ISBN 978-5-16-106478-8. - Текст : электронный. - URL: https://new.znanium.com/catalog/product/1018901 (дата обращения: 31.08.2020).

б) Дополнительная литература:

1. Сухарев, А. Г. Методы оптимизации : учебник и практикум для бакалавриата и магистратуры / А. Г. Сухарев, А. В. Тимохов, В. В. Федоров. — 3-е изд., испр. и доп. — Москва : Издательство Юрайт, 2019. — 367 с. — (Бакалавр и магистр. Академический курс). — ISBN 978-5-9916-3859-3. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/444155 (дата обращения: 31.08.2020).

2. Казарин, О. В. Надежность и безопасность программного обеспечения : учебное пособие для бакалавриата и магистратуры / О. В. Казарин, И. Б. Шубинский. — Москва : Издательство Юрайт, 2019. — 342 с. — (Бакалавр и магистр. Модуль). — ISBN 978-5-534-05142-1. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/441287 (дата обращения: 31.08.2020).

3. Ищукова, Е. А. Криптографические протоколы и стандарты: Учебное пособие / Ищукова Е.А., Лобова Е.А. - Таганрог:Южный федеральный университет, 2016. - 80 с.: ISBN 978-5-9275-2066-4. - Текст : электронный. - URL: https://new.znanium.com/catalog/product/991903 (дата обращения: 31.08.2020)

4. Душкин, А. В. Методологические основы построения защищенных автоматизированных систем: Монография / Душкин А.В. - Воронеж:Научная книга, 2016. - 76 с. ISBN 978-5-4446-0902-6. - Текст : электронный. - URL: https://new.znanium.com/catalog/product/923295 (дата обращения: 31.08.2020)

МАКРОЭЛЕМЕНТЫ:

5. Баранкова, И. И. Определение критически значимых ресурсов объекта защиты при составлении модели угроз информационной безопасности : учебное пособие / И. И. Баранкова, О. В. Пермякова ; МГТУ. - Магнитогорск : МГТУ, 2017. - 1 электрон. опт. диск (CD-ROM). - Загл. с титул. экрана. - URL: https://magtu.informsystema.ru/uploader/fileUpload?name=3323.pdf&show=dcatalogues/1/1138331/3323.pdf&view=true (дата обращения: 31.08.2020). - Макрообъект. - Текст : электронный. - ISBN 978-5-9967-1031-7. - Сведения доступны также на CD-ROM.

6.Сетевая защита информации. Лабораторный практикум : учебное пособие [для вузов] / Д. Н. Мазнин [и др.] ; Магнитогорский гос. технический ун-т им. Г. И. Носова. - Магнитогорск : МГТУ им. Г. И. Носова, 2019. - 1 CD-ROM. - Загл. с титул. экрана. - URL: https://magtu.informsystema.ru/uploader/fileUpload?name=3824.pdf&show=dcatalogues/1/1530260/3824.pdf&view=true (дата обращения: 31.08.2020). - Макрообъект. - ISBN 978-5-9967-1605-0. - Текст : электронный. - Сведения доступны также на CD-ROM.

*РЕЖИМ ПРОСМОТРА МАКРООБЪЕКТОВ

в) Методические указания:

1. Методические указания по выполнению лабораторных работ по дисциплине «Безопасность операционных систем» (Приложение 1) .

2. Методические указания по выполнению внеаудиторных самостоятельных работ по дисциплине «Безопасность операционных систем» (Приложение 2).

г) Программное обеспечение и Интернет-ресурсы:

Программное обеспечение

Наименование ПО	№ договора	Срок действия лицензии

MS Windows 7 Professional(для классов)	Д-1227-18 от 08.10.2018	11.10.2021
MS Office 2007 Professional	№ 135 от 17.09.2007	бессрочно
7Zip	свободно распространяемое	бессрочно
LibreOffice	свободно распространяемое	бессрочно
Adobe Reader	свободно распространяемое	бессрочно
MS Windows 10 Professional (для классов)	Д-1227-18 от 08.10.2018	11.10.2021
MS Windows Server(для классов)	Д-1227-18 от 08.10.2018	11.10.2021
VIP Net Client	Д-946-14 от 22.07.2014	бессрочно
VIP Net CryptoService	Д-946-14 от 22.07.2014	бессрочно
Браузер Mozilla Firefox	свободно распространяемое ПО	бессрочно
Браузер Yandex	свободно распространяемое	бессрочно
FAR Manager	свободно распространяемое	бессрочно

Профессиональные базы данных и информационные справочные системы

Название ресурса	Ссылка
Электронная база периодических изданий East View Information Services, ООО «ИВИС»	https://dlib.eastview.com/
Национальная информационно-аналитическая система – Российский индекс научного цитирования (РИНЦ)	URL: https://elibrary.ru/project_risc.asp
Поисковая система Академия Google (Google Scholar)	URL: https://scholar.google.ru/
Информационная система - Единое окно доступа к информационным ресурсам	URL: http://window.edu.ru/
Федеральное государственное бюджетное учреждение «Федеральный институт промышленной собственности»	URL: http://www1.fips.ru/
Российская Государственная библиотека. Каталоги	s/
Электронные ресурсы библиотеки МГТУ им. Г.И. Носова	asp
Федеральный образовательный портал – Экономика. Социология. Менеджмент	http://ecsocman.hse.ru/
Университетская информационная система РОССИЯ	https://uisrussia.msu.ru
Международная наукометрическая реферативная и полнотекстовая база данных научных изданий «Web of science»	http://webofscience.com
Международная реферативная и полнотекстовая справочная база данных научных изданий	http://scopus.com
Международная база полнотекстовых журналов Springer Journals	http://link.springer.com/
Международная коллекция научных протоколов по различным отраслям знаний Springer Protocols	http://www.springerprotocols.com/

Международная база научных материалов в области физических наук и инжиниринга SpringerMaterials	http://materials.springer.com/
Международная база справочных изданий по всем отраслям знаний SpringerReference	http://www.springer.com/references
Международная реферативная база данных по чистой и прикладной математике zbMATH	http://zbmath.org/
Международная реферативная и полнотекстовая справочная база данных научных изданий «Springer Nature»	https://www.nature.com/siteindex
Архив научных журналов «Национальный электронно-информационный концорциум» (НП НЭИКОН)	https://archive.neicon.ru/xmlui/
Информационная система - Нормативные правовые акты, организационно-распорядительные документы, нормативные и методические документы и подготовленные проекты документов по технической защите информации ФСТЭК России	https://fstec.ru/normotvorcheskaya/tekhnicheskaya-zashchita-informatsii
Информационная система - Банк данных угроз безопасности информации ФСТЭК России	https://bdu.fstec.ru/

9 Материально-техническое обеспечение дисциплины (модуля)

Материально-техническое обеспечение дисциплины включает:

Лекционная аудитория Мультимедийные средства хранения, передачи и

ПРИЛОЖЕНИЕ 1

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ВЫПОЛНЕНИЮ ЛАБОРАТОРНЫХ РАБОТ

Рекомендации направлены на оказание методической помощи обучающимся при выполнении лабораторных занятий.

Лабораторное занятие – это занятие, проводимое под руководством преподавателя в учебной аудитории (компьютерном классе университета или учебной специализированной лаборатории университета), направленное на углубление научно-теоретических знаний и получение лабораторных навыков решения типовых и прикладных задач.

Целью лабораторных занятий является формирование и отработка лабораторных умений и навыков, необходимых в последующей деятельности обучающихся.

Основными задачами лабораторных занятий являются:

- углубление уровня освоения общекультурных и профессиональных компетенций;
- обобщение, систематизация, углубление, закрепление полученных лабораторных знаний по конкретным темам дисциплин различных циклов;
- приобретение обучающимися умений и навыков использования современных теоретических знаний в решении конкретных прикладных задач;
- развитие профессионального мышления, профессиональной и познавательной мотивации.

Перечень тем лабораторных работ определяется рабочей программой дисциплины. План лабораторных занятий отвечает общей направленности лекционного курса и соотнесен с ним в последовательности тем.

Структура лабораторного занятия включает следующие компоненты: вступительная часть; ответы на вопросы обучающихся; практическая часть; заключительное слово преподавателя. Во вступительной части объявляется тема текущей лабораторной работы, ставится ее цели и задачи, проводиться инструктаж по технике безопасности выполнения работы, проверяется исходный уровень готовности обучающихся к лабораторной работе (выполнение тестов, контрольные вопросы и т.п.), выдается порядок и условия выполнения лабораторной работы.

На лабораторном занятии преподаватель может использовать разнообразные образовательные технологии (методы IT, работа в команде, case-study, проблемное обучение, учебные дискуссии и т.п.) по своему выбору для достижения качественного уровня обучения.

Правила по технике безопасности для обучающихся при проведении лабораторных работ

Общие правила:

1. Лабораторные работы проводятся под наблюдением преподавателя. К выполнению лабораторных работ обучающиеся допускаются только после прослушивания инструктажа по технике безопасности, правилам поведения, противопожарным мерам в компьютерном классе и специализированных лабораториях.

2. Обучаемый должен строго выполнять правила техники безопасности и санитарно-гигиенические нормы при работе в компьютерных классах и специализированных лабораториях университета.

Порядок выполнения лабораторных работ

При подготовке к выполнению лабораторных работ обучающийся должен повторить теоретический материал, необходимый для выполнения заданий по текущей теме.

Лабораторная работа выполняется каждым обучающимся самостоятельно, согласно

индивидуальному заданию.

Обучающиеся, пропустившие занятия, выполняют лабораторные работы во внеурочное время.

После выполнения каждой лабораторной работы обучающийся демонстрирует результат выполнения преподавателю в виде отчета по лабораторной работе и отвечает на вопросы. Преподаватель оценивает работу в соответствии с заданными критериями оценки лабораторных работ.

Правила оформления результатов и оценивания лабораторной работы

Результаты выполненной лабораторной работы оформляются в соответствии с требованиями к выполнению конкретной работы.

Практическая работа считается выполненной, если обучающийся набрал балл, который составляет половину максимального количества баллов.

Для оценивания работы прилагаются следующие критерии.

Оценка «отлично» – работа выполнена в полном объеме и без замечаний.

Оценка «хорошо» – работа выполнена правильно с учетом 2-3 несущественных ошибок, исправленных самостоятельно по требованию преподавателя.

Оценка «удовлетворительно» – работа выполнена правильно не менее чем на половину или допущена существенная ошибка.

Оценка «неудовлетворительно» – допущены две (и более) существенные ошибки в ходе работы, которые обучающийся не может исправить даже по требованию преподавателя, или работа не выполнена.

ПРИЛОЖЕНИЕ 2

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ВЫПОЛНЕНИЮ ВНЕАУДИТОРНЫХ САМОСТОЯТЕЛЬНЫХ РАБОТ

Общие положения

Настоящие методические указания предназначены для организации внеаудиторной самостоятельной работы обучающихся и оказания помощи в самостоятельном изучении теоретического и реализации компетенций обучаемых.

Данные методические указания не являются учебным пособием, поэтому перед началом выполнения самостоятельного задания следует изучить соответствующие разделы лекционных занятий, материалов образовательного портала, разделов основной и дополнительной литературы, представленных в пункте 8. «Учебно-методическое и информационное обеспечение дисциплины (модуля)» данной РПД.

Цели и задачи самостоятельной работы

Цель самостоятельной работы – содействие оптимальному усвоению учебного материала обучающимися, развитие их познавательной активности, готовности и потребности в самообразовании.

Задачи самостоятельной работы:

- повышение исходного уровня владения информационными технологиями;
- углубление и систематизация знаний;
- постановка и решение стандартных задач профессиональной деятельности;
- развитие работы с различной по объему и виду информацией, учебной и научной литературой;
- практическое применение знаний, умений;
- самостоятельно использование стандартных программных средств сбора, обработки, хранения и защиты информации
- развитие навыков организации самостоятельного учебного труда и контроля за его эффективностью.

Виды внеаудиторной самостоятельной работы и формы контроля и время на выполнение каждого вида самостоятельной работы указаны в пункте 4. «Структура и содержание дисциплины» данной РПД.

Порядок выполнения

При выполнении текущей внеаудиторной самостоятельной работы обучающемуся следует придерживаться следующего порядка действий:

1) внимательно изучить соответствующие теоретические разделы дисциплины, пользуясь материалами (лекционными, презентационными, аудио-визуальными):
   a) предоставляемыми преподавателем на лекционных занятиях;
   b) предоставляемыми преподавателем в рамках электронных образовательных курсов;
   c) содержащимися в учебниках и учебных пособиях ЭБС (электронно-библиотечных систем), электронных каталогов университета и интернет-ресурсов.
2) Подробно разобрать типовые примеры решения задач, рассмотренные в рамках аудиторной контактной работы с преподавателем.
3) Применить полученные теоретические знания и практические навыки к решению индивидуальных заданий, к прохождению компьютерных тестирований.
4) При необходимости, сформировать перечень вопросов, вызвавших затруднения в процессе самостоятельной работы. Обсудить возникшие вопросы с обучающимися группы, в рамках командно-проектной работы, и с преподавателем, в рамках консультационной помощи, реализованной либо в контактной форме, либо средствами информационно-образовательной среды ВУЗа.

Критерии оценки внеаудиторных самостоятельных работ

Качество выполнения внеаудиторной самостоятельной работы обучающихся оценивается посредством текущего контроля самостоятельной работы обучающихся с использованием балльно-рейтинговой системы.

В качестве форм текущего контроля по дисциплине используются: индивидуальные задания, аудиторные контрольные работы, компьютерное тестирование.

Максимальное количество баллов обучающийся получает, если:

- выполняет индивидуальные задания в соответствии со всеми заявленными требованиями;
- дает правильные формулировки, точные определения, понятия терминов;
- может обосновать рациональность решения текущей задачи.;
- обстоятельно с достаточной полнотой излагает соответствующую теоретический раздел;
- правильно отвечает на дополнительные вопросы преподавателя, имеющие целью выяснить степень понимания им данного материала.

50~85% от максимального количества баллов обучающийся получает, если:

- неполно (не менее 70% от полного), но правильно выполнено задание;
- при изложении были допущены 1-2 несущественные ошибки, которые он исправляет после замечания преподавателя;
- дает правильные формулировки, точные определения, понятия терминов;
- может обосновать свой ответ, привести необходимые примеры;
- правильно отвечает на дополнительные вопросы преподавателя, имеющие целью выяснить степень понимания им данного материала.

36~50% от максимального количества баллов обучающийся получает, если:

- неполно (не менее 50% от полного), но правильно изложено задание;
- при изложении была допущена 1 существенная ошибка;
- знает и понимает основные положения данной темы, но допускает неточности в формулировке понятий;
- излагает выполнение задания недостаточно логично и последовательно;
- затрудняется при ответах на вопросы преподавателя.

35% и менее от максимального количества баллов обучающийся получает, если:

- неполно (менее 50% от полного) изложено задание;
- при изложении были допущены существенные ошибки. В "0" баллов преподаватель вправе оценить выполненное обучающимся задание, если оно не удовлетворяет требованиям, установленным преподавателем к данному виду работы или не было представлено для проверки.

Сумма полученных баллов по всем видам заданий внеаудиторной самостоятельной работы составляет рейтинговый показатель обучающегося. Рейтинговый показатель обучающегося влияет на выставление итоговой оценки по результатам изучения дисциплины.

Показатели и критерии оценивания полученных знаний представлены в пункте 7.б) «Оценочные средства для проведения промежуточной аттестации» данной РПД.