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
_____ В.Р. Храмшин

03.03.2021 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
2021 год

Рабочая программа составлена на основе ФГОС ВО по специальности 10.05.03 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ АВТОМАТИЗИРОВАННЫХ СИСТЕМ (приказ Минобрнауки России от 01.12.2016 г. № 1509)

Рабочая программа рассмотрена и одобрена на заседании кафедры Информатики и информационной безопасности
19.02.2021, протокол № 9

Зав. кафедрой _____ И.И. Баранкова

Рабочая программа одобрена методической комиссией ИЭиАС
03.03.2021 г. протокол № 5

Председатель _____ В.Р. Храмшин

Рабочая программа составлена:
зав. кафедрой ИиИБ, д-р техн. наук _____ И.И. Баранкова

Рецензент:
Начальник отдела информационной безопасности "КУБ" (АО),
_____ М.М. Близнецов

Лист актуализации рабочей программы

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

Рабочая программа пересмотрена, обсуждена и одобрена для реализации в 2025 - 2026 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 2026 - 2027 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 2027 - 2028 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 принципа-ми 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 обязательную 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

Технология построения защищенных распределенных приложений

Учебная - ознакомительная практика

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

Производственная-практика по получению профессиональных умений и опыта профессиональной деятельности

Производственная-преддипломная практика

Методы выявления нарушений информационной безопасности

Защита информационно-технологических ресурсов автоматизированных систем

Защита программного обеспечения

Обеспечение информационной безопасности критической информационной инфраструктурой

Методы и стандарты оценки защищенности компьютерных систем

Анализ рисков информационной безопасности

Безопасность Интернета вещей

Разработка эксплуатационной документации на системы защиты информации автоматизированных систем

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:

Код индикатора	Индикатор достижения компетенции
ОПК-12 Способен применять знания в области безопасности вычислительных сетей, операционных систем и баз данных при разработке автоматизированных систем;	
ОПК-12.1	Применяет знания в области безопасности вычислительных сетей при разработке автоматизированных систем

ОПК-12.2	Применяет знания в области безопасности операционных систем при разработке автоматизированных систем
ОПК-12.3	Применяет знания в области безопасности баз данных при разработке автоматизированных систем

4. Структура, объём и содержание дисциплины (модуля)

Общая трудоемкость дисциплины составляет 5 зачетных единиц 180 акад. часов, в том числе:

– контактная работа – 106,1 акад. часов:

– аудиторная – 102 акад. часов;

– внеаудиторная – 4,1 акад. часов;

– самостоятельная работа – 38,2 акад. часов;

– в форме практической подготовки – 0 акад. час;

– подготовка к экзамену – 35,7 акад. час

Форма аттестации - зачет, экзамен

Раздел/ тема дисциплины	Семестр	Аудиторная контактная работа (в акад. часах)			Самостоятельная работа студента	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	ОПК-12.1, ОПК-12.2, ОПК-12.3
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	
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	4/1И		2	Поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями)	Устный опрос	ОПК-12.1, ОПК-12.2, ОПК-12.3
2.2 ОС семейства Unix и Windows. Концепции в обеспечении защиты		1	4/1И		2	Поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями)	Устный опрос	
Итого по разделу		2	8/2И		4			
3. Структурная схема ОС								
3.1 Центральные элементы ОС – ядро, пользовательская оболочка, файловая подсистема, сетевая подсистема	6	2	4/1,9И		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. "	ОПК-12.1, ОПК-12.2, ОПК-12.3
3.2 Периферийные подсистемы ОС. Загрузка ОС и ее этапы		2	4/1И		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."	ОПК-12.1, ОПК-12.2, ОПК-12.3
Итого по разделу		4	8/2,9И		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"	ОПК-12.1, ОПК-12.2, ОПК-12.3
4.2 Принципы организации межпрограммного взаимодействия		2	4/2И		1	Поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями)	Устный опрос	
Итого по разделу		4	8/3И		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	
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"	
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	
Итого по разделу					3			
Итого за семестр		17	34/11,9И		20,05		зачёт	
7. Подсистема безопасности ОС								
7.1 Подсистема безопасности ОС. Основные компоненты	7	2	4/0,9И		2	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"	
7.2 Модели безопасности в различных семействах ОС		2	4		2	Поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями)	Устный опрос	
7.3 Дискреционный и мандатный принципы управления доступом – сравнительный анализ		2	4/1И		2	Поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями)	Устный опрос	
Итого по разделу		6	12/1,9И		6			
8. Администрирование операционных систем								

8.1 Модели пользователей в различных ОС	7	2	4/1И		2	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»	
8.2 Профиль пользователя, бюджет, авторизация, аутентификация пользователя ОС		2	4/2И		2	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»	
8.3 Назначение прав пользователю ОС и аудит его действий		2	4/2И		2	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»	
8.4 Аудит системных событий ОС		2	4/2И		2	Поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями)	Устный опрос	
Итого по разделу		8	16/7И		8			
9. Противодействие атакам на информационные								

9.1 Методология атаки и их разновидности	7	1	3/1И		2	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»	
9.2 Методы обнаружения и предотвращения атак на информационные системы		2	3/2И		2	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."	
Итого по разделу		3	6/3И		4			
10. Подготовка к итоговой аттестации								
10.1 Экзамен	7				0,15	Поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями)	Экзамен	
Итого по разделу					0,15			
Итого за семестр		17	34/11,9И		18,15		экзамен	
Итого по дисциплине		34	68/23,8И		38,2		зачет, экзамен	

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

Представлено в приложении 1.

7 Оценочные средства для проведения промежуточной аттестации

Представлены в приложении 2.

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)

МАКРООБЪЕКТЫ:

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

1. Перейти по адресу электронного каталога https://magtu.informsystema.ru
2. Произвести авторизацию (Логин: Читатель1 Пароль: 111111)
3. Активизировать гиперссылку макрообъекта.

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 ПО	бессрочно
LibreOffice	свободно распространяемое ПО	бессрочно
Adobe Reader	свободно распространяемое ПО	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
Браузер Mozilla Firefox	свободно распространяемое ПО	бессрочно
Браузер Yandex	свободно распространяемое	бессрочно
FAR Manager	свободно распространяемое	бессрочно
Linux Calculate	свободно распространяемое	бессрочно

Профессиональные базы данных и информационные справочные системы

Название курса	Ссылка
Электронная база периодических изданий East View Information Services, ООО «ИВИС»	https://dlib.eastview.com/
Национальная информационно-аналитическая система – Российский индекс научного цитирования	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	https://www.rsl.ru/ru/4readers/catalogues/
Электронные ресурсы библиотеки МГТУ им. Г.И. Носова	http://magtu.ru:8085/marcweb2/Default.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	http://scopus.com
Международная база полнотекстовых журналов Springer Journals	http://link.springer.com/
Международная коллекция научных протоколов по различным отраслям знаний	http://www.springerprotocols.com/
Международная база научных материалов в области физических наук и инжиниринга	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	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	https://fstec.ru/normotvorcheskaya/tekhnicheskaya-zashchita-informatsii
Информационная система - Банк данных угроз	https://bdu.fstec.ru/

9 Материально-техническое обеспечение дисциплины (модуля)

Материально-техническое обеспечение дисциплины включает:

Лекционная аудитория Мультимедийные средства хранения, передачи и представления информации

Лаборатория сетей и систем передачи данных. Лаборатория безопасности сетей ЭВМ:

1. Учебно-лабораторный стенд "Кодирование и модуляция информации в системах связи", комплектация полная

2. Учебно-лабораторный стенд "Системы спутниковой навигации" GPS.(2 шт)

3. Комплект типового учебного оборудования "Сети сотовой связи GSM"

4. Комплект типового учебного оборудования "Телекоммуникационные линии связи" ТЛС-01

5. Комплект типового учебного оборудования "Сетевая безопасность типа SECURITY-3M"(2шт. cisco и d-link)

6. Комплект учебного оборудования "Беспроводные компьютерные сети ЭВМ"

7. Модуль учебно-лабораторный для изучения низкоуровнего контроллера Ethernet

8. Стенд коммуникационного оборудования сервером для моделирования облачного сервиса

9. Комплекс программно-аппаратный ViPNet

Компьютерный класс (ауд. 372, ауд. 245, ауд. 247, ауд. 144, ауд. 142 и т.д.) - Персональные компьютеры с ПО и выходом в Интернет и доступом в электронную информационно-образовательную среду университета.

Аудитория для самостоятельной работы читальные залы библиотеки, ауд 132а - Персональные компьютеры с ПО и выходом в Интернет и доступом в электронную информационно-образовательную среду университета.

Приложение 1

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 также 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.

Приложение 2

Оценочные средства для проведения промежуточной аттестации

Оценочные средства
ОПК-12 Способен применять знания в области безопасности вычислительных сетей, операционных систем и баз данных при разработке автоматизированных систем.
ОПК-12.1 Применяет знания в области безопасности вычислительных сетей при разработке автоматизированных систем
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 5. Провести сравнительный анализ различных операционных систем с точки зрения защищенности информации; 6. Обосновать выбор операционной системы при построении информационной системы на ее базе; 7. Провести администрирования дисковой, файловой, сетевой подсистемами, подсистемой безопасности операционных систем семейств Windows и UNIX/Linux 8. Разработать сценарии администрирования для операционных систем семейств Windows и UNIX/Linux 9. Провести выбор операционной системы для построения информационной системы на ее базе с точки зрения требований по защищенности информации
ОПК-12.2 Применяет знания в области безопасности операционных систем при разработке автоматизированных систем
1. Классификация уязвимостей ОС, методы их нейтрализации 2. Критерии надежности средств защиты информации (СЗИ) для операционных систем 3. Методы разработки политики безопасности для автоматизированных систем 4. Разработать комплекс организационных и технических мер для реализации политики безопасности для операционной системы; 5. Разработать политику внедрения мер, направленных на повышения безопасности информации при эксплуатации ОС 6. Провести администрирование операционных систем семейств Windows и UNIX/Linux 7. Навыками установки, настройки, конфигурирования ОС семейств Windows и UNIX/Linux 8. Установить настройки средств защиты информации для ОС семейств Windows и UNIX/Linux 9. Технологии аудита событий безопасности операционной системы
ОПК-12.3 Применяет знания в области безопасности баз данных при разработке автоматизированных систем

1. Принципы функционирования средств защиты информации при их эксплуатации в составе информационных систем
2. Современные технологии построения средств и систем защиты информации и их применение в составе систем защиты автоматизированных систем и сетей ЭВМ
3. Дискреционная и мандатная модели подсистем безопасности
4. Понятие «политика безопасности», «контекст безопасности», «бюджет безопасности»
5. Использовать средства мониторинга уязвимостей операционных систем для проведения проверки ОС
6. Провести анализ уязвимостей
7. Разработать методику нейтрализации обнаруженных уязвимостей операционных систем
8. Првести администрирование подсистемы информационной безопасности автоматизированных систем; принимать меры по устранению неисправностей;
9. Провести администрирование подсистем защиты информации ОС семейств Windows и UNIX/Linux

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. Методы обеспечения информационной безопасности. Классификация злоумышленников. Основные направления и методы реализации угроз информационной безопасности.
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» – студент должен показать высокий уровень знаний, умений и навыков в соответствии с формируемыми компетенциями; т.е. всесторонние, систематизированные, глубокие знания учебной программы дисциплины и умение уверенно применять их на практике при решении конкретных задач, свободно и правильно обосновывать принятые решения;

– на оценку «хорошо» – студент должен показать средний уровень знаний, умений и навыков в соответствии с формируемыми компетенциями; т.е. твердо знает материал, грамотно и по существу излагает его, умеет применять полученные знания на практике;

– на оценку «удовлетворительно» – студент должен показать пороговый уровень знаний, умений и навыков в соответствии с формируемыми компетенциями; т.е. владеет

основными разделами учебной программы, необходимыми для дальнейшего обучения и может применять полученные знания по образцу в стандартной ситуации;

– на оценку «неудовлетворительно» – студент не может показать знания на уровне воспроизведения и объяснения информации, не умеет использовать полученные знания при решении типовых практических задач.