Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Максимов Алексей Борисович
Должность: директор департамента по образовательной политике
Дата подписания: 23.10.2023 17:39:31
Уникальный программный ключ:
8db180d1a3f02ac9e60521a5672742735c18b1d6

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное автономное образовательное учреждение высшего образования

«МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»

УТВЕРЖДАЮ

Декан факультета информационных технологий

/Д. Г. Демидов/

«30» августа 2021 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Безопасность операционных систем Windows»

Направление подготовки

10.05.03 «Информационная безопасность автоматизированных систем»

Образовательная программа (профиль)

«Безопасность открытых информационных систем»

Квалификация (степень) выпускника

Специалист по защите информации

Очная

Год приема - 2021

Москва 2021 г.

1. Цели освоения дисциплины.

К **основным целям** освоения дисциплины «Безопасность операционных систем Windows» следует отнести:

- обучение студентов принципам построения операционных систем (ОС) Windows;
- обучение принципам построения защиты информации в ОС Windows и анализа надежности защиты ОС Windows.

К **основным задачам** освоения дисциплины «Безопасность операционных систем Windows» следует отнести:

- знание принципов функционирования ОС Windows;
- знание принципов построения подсистем защиты в ОС Windows;
- знание средств и методов несанкционированного доступа (НСД) к ресурсам ОС Windows .

2. Место дисциплины в структуре ООП.

Дисциплина «Безопасность операционных систем Windows» относится к числу профессиональных учебных элективной части цикла (Б.1.ДВ) основной образовательной программы (Б.1.ДВ.1).

Изучение дисциплины опирается на знания, умения и навыки, приобретенные в предшествующих дисциплинах: «Основы информационной безопасности», «Основы ИКТ», «Криптографические методы защиты информации».

3. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенные с планируемыми результатами освоения образовательной программы.

В результате освоения дисциплины (модуля) у обучающихся формируются следующие компетенции и должны быть достигнуты следующие результаты обучения как этап формирования соответствующих компетенций:

Код компетенции	**В результате освоения образовательной программы обучающийся должен обладать**	**Перечень планируемых результатов обучения по дисциплине**
ПК-18	Способен администрировать подсистему информационной безопасности автоматизированной системы	**знать:** Виды ОС. Процессы. Алгоритмы и механизмы синхронизации. Тупики. Управления памятью. Файлы. Реализация файловой системы. Система управления вводом-выводом. Угрозы безопасности ОС. Требования к защите ОС. Разграничение доступа в ОС. Идентификация и аутентификация пользователей ОС. Аудит в ОС. **уметь:** Управлять процессами в операционных системах. Разграничивать доступ к процессам. Работать с системами ввода-вывода. Строить модель угроз для ОС. Работать с правами и привилегиями для пользователей. Проводить аудит ОС. **владеть:** Средствами управления процессами. Методами и средствами работы с файловой системой. Навыками работы с конфигурационными файлами ОС. Средствами разграничения доступа. Средствами управления политиками безопасности ОС. Системами логирования.

4. Структура и содержание дисциплины.

Общая трудоемкость дисциплины составляет 4 зачетных единицы, т.е. **144** академических часов (лабораторные занятия – 72 час, самостоятельная работа - 72 часов, форма контроля – экзамен) в 3 семестре.

Структура и содержание дисциплины «Безопасность операционных систем Windows» по срокам и видам работы отражены в приложении.

5. Образовательные технологии.

Методика преподавания дисциплины «Безопасность операционных систем Windows» и реализация компетентностного подхода в изложении и восприятии материала предусматривает использование следующих активных и интерактивных форм проведения групповых, индивидуальных, аудиторных занятий в сочетании с внеаудиторной работой с целью формирования и развития профессиональных навыков обучающихся:

- подготовка к выполнению лабораторных работ;

Удельный вес занятий, проводимых в интерактивных формах по дисциплине, составляет 20 % аудиторных занятий

6. Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины и учебно-методическое обеспечение самостоятельной работы студентов.

В процессе обучения используются следующие оценочные формы самостоятельной работы студентов, оценочные средства текущего контроля успеваемости и промежуточных аттестаций:

- компьютерное тестирование;
- экзамен.

Образцы тестовых заданий, экзаменационных билетов, приведены в приложении.

6.1. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине (модулю).

6.1.1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы.

В результате освоения дисциплины (модуля) формируются следующие компетенции:

Код компетенции	В результате освоения образовательной программы обучающийся должен обладать
ПК-18	Способен администрировать подсистему информационной безопасности автоматизированной системы

В процессе освоения образовательной программы данные компетенции, в том числе их отдельные компоненты, формируются поэтапно в ходе освоения обучающимися дисциплин (модулей), практик в соответствии с учебным планом и календарным графиком учебного процесса.

6.1.2. Описание показателей и критериев оценивания компетенций, формируемых по итогам освоения дисциплины (модуля), описание шкал оценивания

Показателем оценивания компетенций на различных этапах их формирования является достижение обучающимися планируемых результатов обучения по дисциплине (модулю):

ПК-18 Способен администрировать подсистему информационной безопасности автоматизированной системы				
Показатель	**Критерии оценивания**			
	2	**3**	**4**	**5**
знать: Виды ОС. Процессы. Алгоритмы и механизмы синхронизации. Тупики. Управления памятью. Файлы. Реализация файловой системы. Система управления вводом-выводом. Угрозы безопасности ОС. Требования к защите ОС. Разграничение доступа в ОС. Идентификация и аутентификация пользователей ОС. Аудит в ОС.	Обучающийся демонстрирует полное отсутствие или недостаточное соответствие следующих знаний: Виды ОС. Процессы. Алгоритмы и механизмы синхронизации. Тупики. Управления памятью. Файлы. Реализация файловой системы. Система управления вводом-выводом. Угрозы безопасности ОС. Требования к защите ОС. Разграничение доступа в ОС. Идентификация и аутентификация пользователей ОС. Аудит в ОС. .	Обучающийся демонстрирует неполное соответствие следующих знаний: Виды ОС. Процессы. Алгоритмы и механизмы синхронизации. Тупики. Управления памятью. Файлы. Реализация файловой системы. Система управления вводом-выводом. Угрозы безопасности ОС. Требования к защите ОС. Разграничение доступа в ОС. Идентификация и аутентификация пользователей ОС. Аудит в ОС. Допускаются значительные ошибки, проявляется недостаточность знаний, по ряду показателей, обучающийся испытывает значительные затруднения при оперировании знаниями при их переносе на новые ситуации.	Обучающийся демонстрирует частичное соответствие следующих знаний: Виды ОС. Процессы. Алгоритмы и механизмы синхронизации. Тупики. Управления памятью. Файлы. Реализация файловой системы. Система управления вводом-выводом. Угрозы безопасности ОС. Требования к защите ОС. Разграничение доступа в ОС. Идентификация и аутентификация пользователей ОС. Аудит в ОС, но допускаются незначительные ошибки, неточности, затруднения при аналитических операциях.	Обучающийся демонстрирует полное соответствие следующих знаний: Виды ОС. Процессы. Алгоритмы и механизмы синхронизации. Тупики. Управления памятью. Файлы. Реализация файловой системы. Система управления вводом-выводом. Угрозы безопасности ОС. Требования к защите ОС. Разграничение доступа в ОС. Идентификация и аутентификация пользователей ОС. Аудит в ОС, свободно оперирует приобретенными знаниями.

уметь: Управлять процессами в операционных системах. Разграничивать доступ к процессам. Работать с системами ввода-вывода. Строить модель угроз для ОС. Работать с правами и привилегиями для пользователей. Проводить аудит ОС.	Обучающийся не умеет или в недостаточной степени умеет Управлять процессами в операционных системах. Разграничивать доступ к процессам. Работать с системами ввода-вывода. Строить модель угроз для ОС. Работать с правами и привилегиями для пользователей. Проводить аудит ОС.	Обучающийся демонстрирует неполное соответствие следующих умений: Управлять процессами в операционных системах. Разграничивать доступ к процессам. Работать с системами ввода-вывода. Строить модель угроз для ОС. Работать с правами и привилегиями для пользователей. Проводить аудит ОС. . Допускаются значительные ошибки, проявляется недостаточность умений.	Обучающийся демонстрирует частичное соответствие следующих умений: Управлять процессами в операционных системах. Разграничивать доступ к процессам. Работать с системами ввода-вывода. Строить модель угроз для ОС. Работать с правами и привилегиями для пользователей. Проводить аудит ОС. . Умения освоены, но допускаются незначительные ошибки, неточности.	Обучающийся демонстрирует полное соответствие следующих умений: Управлять процессами в операционных системах. Разграничивать доступ к процессам. Работать с системами ввода-вывода. Строить модель угроз для ОС. Работать с правами и привилегиями для пользователей. Проводить аудит ОС. Свободно оперирует приобретенными умениями, применяет их в ситуациях повышенной сложности.
владеть: Средствами управления процессами. Методами и средствами работы с файловой системой. Навыками работы с конфигурационными файлами ОС. Средствами разграничения доступа. Средствами управления политиками безопасности ОС. Системами логирования.	Обучающийся не владеет или в недостаточной степени владеет Средствами управления процессами. Методами и средствами работы с файловой системой. Навыками работы с конфигурационным и файлами ОС. Средствами разграничения доступа. Средствами управления политиками безопасности ОС. Системами логирования.	Обучающийся владеет Средствами управления процессами. Методами и средствами работы с файловой системой. Навыками работы с конфигурационными файлами ОС. Средствами разграничения доступа. Средствами управления политиками безопасности ОС. Системами логирования. но допускаются значительные ошибки, проявляется недостаточность владения	Обучающийся частично владеет Средствами управления процессами. Методами и средствами работы с файловой системой. Навыками работы с конфигурационным и файлами ОС. Средствами разграничения доступа. Средствами управления политиками безопасности ОС. Системами логирования, навыки освоены, но допускаются незначительные ошибки, неточности, затруднения.	Обучающийся в полном объеме владеет Средствами управления процессами. Методами и средствами работы с файловой системой. Навыками работы с конфигурационными файлами ОС. Средствами разграничения доступа. Средствами управления политиками безопасности ОС. Системами логирования, свободно применяет полученные навыки в ситуациях повышенной сложности.

Шкалы оценивания результатов промежуточной аттестации и их описание:

Форма промежуточной аттестации: экзамен.

Промежуточная аттестация обучающихся в форме экзамена проводится по результатам выполнения всех видов учебной работы, предусмотренных учебным планом по данной дисциплине (модулю), при этом учитываются результаты текущего контроля успеваемости в течение семестра. Оценка степени достижения обучающимися планируемых результатов обучения по дисциплине (модулю) проводится преподавателем, ведущим занятия по дисциплине (модулю) методом экспертной оценки. По итогам промежуточной аттестации по дисциплине (модулю) выставляется оценка «отлично», «хорошо», «удовлетворительно» или «неудовлетворительно».

Шкала оценивания	**Описание**
Отлично	Выполнены все виды учебной работы, предусмотренные учебным планом. Студент демонстрирует соответствие знаний, умений, навыков приведенным в таблицах показателей, оперирует приобретенными знаниями, умениями, навыками, применяет их в ситуациях повышенной сложности. При этом могут быть допущены незначительные ошибки, неточности, затруднения при аналитических операциях, переносе знаний и умений на новые, нестандартные ситуации.
Хорошо	Выполнены все виды учебной работы, предусмотренные учебным планом. Студент демонстрирует неполное, правильное соответствие знаний, умений, навыков приведенным в таблицах показателей, либо если при этом были допущены 2-3 несущественные ошибки.
Удовлетворительно	Выполнены все виды учебной работы, предусмотренные учебным планом. Студент демонстрирует соответствие знаний, в котором освещена основная, наиболее важная часть материала, но при этом допущена одна значительная ошибка или неточность.
Неудовлетворительно	Не выполнен один или более видов учебной работы, предусмотренных учебным планом. Студент демонстрирует неполное соответствие знаний, умений, навыков приведенным в таблицах показателей, допускаются значительные ошибки, проявляется отсутствие знаний, умений, навыков по ряду показателей, студент испытывает значительные затруднения при оперировании знаниями и умениями при их переносе на новые ситуации.

Фонды оценочных средствпредставлены в приложении к рабочей программе.

7. Учебно-методическое и информационное обеспечение дисциплины.

а) основная литература:

1. Астапчук В. А., Терещенко П. В. КОРПОРАТИВНЫЕ ИНФОРМАЦИОННЫЕ СИСТЕМЫ: ТРЕБОВАНИЯ ПРИ ПРОЕКТИРОВАНИИ 2-е изд., испр. и доп. Учебное пособие для вузов: М.:Издательство Юрайт ЭБС Юрайт, 2018 https://biblio-online.ru/book/7AEBE7EE-EB71-453C-A3D9-ABEB7F46D73D
2. Гостев И.М. ОПЕРАЦИОННЫЕ СИСТЕМЫ 2-е изд., испр. и доп. Учебник и практикум для академического бакалавриата: Гриф УМО ВО М.:Издательство Юрайт ЭБС Юрайт, 2018 https://biblio-online.ru/book/A14759F4-CD1C-441C-A929-64B9D29C6010

б) дополнительная литература:

1. Гордеев А.В. Операционные системы: учеб. для вузов СПб.[и др.]: Питер, 2007
2. Синицын С.В., Батаев А.В., Налютин Н.Ю. Операционные системы: учебникМ.: Академия, 2010

в) программное обеспечение и интернет-ресурсы:

Microsoft Windows

9. Материально-техническое обеспечение дисциплины.

Для проведения всех видов занятий необходимо презентационное оборудование (мультимедийный проектор, экран) – 1 комплект.

10. Оборудование и аппаратура.

Для проведения лабораторных занятий необходимо наличие компьютерных классов оборудованных современной вычислительной техникой из расчета одно рабочее место на одного обучаемого.

11. Методические рекомендации для самостоятельной работы студентов

Изучение дисциплины осуществляется в строгом соответствии с целевой установкой в тесной взаимосвязи учебным планом. Основой теоретической подготовки студентов являются лекции.

В процессе самостоятельной работы студенты закрепляют и углубляют знания, полученные во время аудиторных занятий, готовятся к экзамену, а также самостоятельно изучают отдельные темы учебной программы.

12. Методические рекомендации для преподавателя

Программа составлена в соответствии с Федеральным государственным образовательным стандартом высшего образования по направлению подготовки **10.05.03 «Информационная безопасность автоматизированных систем»**.

Программу составил: ст. преп. Пиков В.А.

Программа утверждена на заседании кафедры “Информационная безопасность” «30» августа 2021 г., протокол № 1

Заведующий кафедрой
«Информационная безопасность»



к.т.н., доцент Н.В. Федоров

Приложение.

Структура и содержание дисциплины «Безопасность операционных систем Windows»
по направлению подготовки
10.05.03 «Информационная безопасность автоматизированных систем»
(специалист)

n/n	Раздел	Семестр	Неделя семестра	Виды учебной работы, включая самостоятельную работу студентов, и трудоемкость в часах					Виды самостоятельной работы студентов					Формы аттестации	
				Л	П/С	Лаб	СРС	КСР	К.Р.	К.П.	ДЗ	Реферат	К/р	Э	З
	3 семестр														
1	Введение в операционные системы. Процессы. Алгоритмы и механизмы синхронизации. Тупики.	3	1-4			16	16								
2	Управление памятью. Файловая система. Система ввода-вывода.		5-9			20	20								
3	Механизмы синхронизации процессов и потоков		10-12			12	12								
4	Угрозы безопасности ОС. Требования к защите ОС. Разграничение доступа в ОС.		13-14			8	8								
5	Идентификация и аутентификация пользователей ОС. Аудит в ОС.		15-18			16	16								
	Форма аттестации	3	19-21							.				Э	
	Всего часов по дисциплине во 3 семестре					72	72								
	Всего часов по дисциплине					72	72								

Приложение к
рабочей программе

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ

РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ

ВЫСШЕГО ОБРАЗОВАНИЯ

«МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»
(МОСКОВСКИЙ ПОЛИТЕХ)

Направление подготовки: 10.05.03 «Информационная безопасность автоматизированных систем»

ОП (профиль): «Безопасность открытых информационных систем»

Форма обучения: очная

Вид профессиональной деятельности: эксплуатационная; проектно-технологическая; экспериментально-исследовательская; организационно-управленческая

.

Кафедра: «Информационная безопасность»

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

ПО ДИСЦИПЛИНЕ

«Безопасность операционных систем Windows»

Состав: 1. Паспорт фонда оценочных средств

2. Описание оценочных средств:

Компьютерное тестирование

Экзамен

Составители: ст. преп. Пиков В.А.

Москва, 2021 год

Таблица 1

ПОКАЗАТЕЛЬ УРОВНЯ СФОРМИРОВАННОСТИ КОМПЕТЕНЦИЙ

Безопасность операционных систем Windows					
ФГОС ВО **10.05.03 «Информационная безопасность автоматизированных систем»**					
В процессе освоения данной дисциплины студент формирует и демонстрирует следующие **общепрофессиональные и профессиональные компетенции**:					
КОМПЕТЕНЦИИ		**Перечень компонентов**	**Технология формирования компетен**	**Форма оценоч-ного**	**Степени уровней освоения компетенций**
ИН-ДЕКС	**ФОРМУЛИРОВКА**				

ПК-18	Способен администрировать подсистему информационной безопасности автоматизированной системы	**знать:** Виды ОС. Процессы. Алгоритмы и механизмы синхронизации. Тупики. Управления памятью. Файлы. Реализация файловой системы. Система управления вводом-выводом. Угрозы безопасности ОС. Требования к защите ОС. Разграничение доступа в ОС. Идентификация и аутентификация пользователей ОС. Аудит в ОС. **уметь:** Управлять процессами в операционных системах. Разграничивать доступ к процессам. Работать с системами ввода-вывода. Строить модель угроз для ОС. Работать с правами и привилегиями для пользователей. Проводить аудит ОС. **владеть:** Средствами управления процессами. Методами и средствами работы с файловой системой. Навыками работы с конфигурационными файлами ОС. Средствами разграничения доступа. Средствами управления политиками безопасности ОС. Системами логирования.	самостоятельная работа, лабораторные занятия	КТ, экзамен	Базовый уровень: знать: Виды ОС. Процессы. Алгоритмы и механизмы синхронизации. Тупики. Управления памятью. Файлы. Реализация файловой системы. Система управления вводом-выводом. Угрозы безопасности ОС. Требования к защите ОС. Разграничение доступа в ОС. Идентификация и аутентификация пользователей ОС. Аудит в ОС. умеет Управлять процессами в операционных системах. Разграничивать доступ к процессам. Работать с системами ввода-вывода. Строить модель угроз для ОС. Работать с правами и привилегиями для пользователей. Проводить владеть: Средствами управления процессами. Методами и средствами работы с файловой системой. Навыками работы с конфигурационными файлами ОС. Средствами разграничения доступа. Средствами управления политиками безопасности ОС. Системами логирования

Приложение 2
к рабочей программе

Оценочные средства для текущей аттестации

Компьютерное тестирование.

По каждой теме предлагается 10 вопросов по каждой теме. Освоение темы зависит от результата написания теста: 9-10 баллов - тема считается освоенной на продвинутом уровне; 6-8 баллов - тема считается освоенной на базовом уровне; 0-5 баллов – тема считается не освоенной.

Оценочные средства для промежуточной аттестации

Экзамен.

Список вопросов для экзамена по дисциплине

1. Процессы.
2. Алгоритмы и механизмы синхронизации.
3. Тупики.
4. Управление памятью.
5. Файловая система.
6. Система ввода-вывода.
7. Механизмы синхронизации процессов и потоков
8. Угрозы безопасности ОС.
9. Требования к защите ОС.
10. Разграничение доступа в ОС.
11. Идентификация и аутентификация пользователей ОС.
12. Аудит в ОС.

Пример билета.

3. Алгоритмы и механизмы синхронизации.
4. Разграничение доступа в ОС.