МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»

УТВЕРЖДЕНО
Декан факультета
Информационных технологий
_____ / А.Ю. Филиппович /
« 28 » мая 2020 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Безопасность операционных систем»

Направление подготовки
10.03.01 «Информационная безопасность»

Образовательная программа (профиль)
«Безопасность компьютерных систем»

Квалификация (степень) выпускника
Бакалавр

Форма обучения
Очная

Год приема 2020

Москва 2020 г.

1. Цели освоения дисциплины.

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

- приобретение студентами базовых теоретических знаний и практических навыков в области эксплуатации и обеспечения эффективного применения современных операционных систем (ОС);
- подготовка студентов к деятельности в соответствии с квалификационной характеристикой специалитета по направлению, в том числе формирование у них умений и привитие навыков в использовании механизмов и сервисов обеспечения защиты информации средствами ОС.

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

- приобретение теоретических знания в области назначения, функций и принципов работы современных ОС, в вопросах управления ресурсами и задачами операционной системы; приобретение практических навыков по организации эффективной и безопасной эксплуатации ОС, администрированию и восстановлению ОС после сбоев, освоение методов и средств разграничения доступа и шифрования данных средствами современных ОС.

2. Место дисциплины в структуре ООП бакалавриата.

Дисциплина «Безопасность операционных систем» относится к числу профессиональных учебных дисциплин базовой части цикла (Б.1.1.16) основной образовательной программы бакалавриата.

Дисциплина «Безопасность операционных систем» взаимосвязана логически и содержательно-методически со следующими дисциплинами и практиками ООП:

В базовой и вариативной части цикла (Б1):

- Основы информационной безопасности
- Языки программирования
- Программно-аппаратные средства защиты информации
- Комплексная система защиты информации на предприятии

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 - 2	способностью применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач	**знать:** • принципы построения и функционирования, примеры реализаций современных операционных систем; • отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценки защищенности компьютерных систем **уметь:** • использовать средства операционных систем для обеспечения эффективного и безопасного функционирования автоматизированных систем; • формулировать и настраивать политику безопасности распространенных операционных систем, а также локальных вычислительных сетей, построенных на их основе **владеть:** • навыками установки и настройки операционных систем семейств Windows и Linux с учетом требований по обеспечению информационной безопасности; • навыками эксплуатации и администрирования (в части, касающейся разграничения доступа, аутентификации и аудита) баз данных, локальных компьютерных сетей, программных систем с учетом требований по обеспечению информационной безопасности

4. Структура и содержание дисциплины.

Общая трудоемкость дисциплины составляет 2 зачетных единицы, т.е. 72 академических часа (лабораторные занятия – 36 часов, самостоятельная работа – 36 часов, форма контроля - зкзамен) во втором семестре.

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

Содержание разделов дисциплины

Тема 1. Общая характеристика операционных систем.

Понятие программного обеспечения ЭВМ и его классификация. Состав системного ПО, место в нем ОС. Функции и организация ОС ЭВМ. Принципы построения и функционирования, примеры реализаций современных операционных Утилиты. Архитектура виртуальной ОС. Эффекты виртуализации. Классификация ОС. Факторы, оказывающие влияние на структуру ОС. Тенденции развития ОС, версии и разновидности ОС. Назначение и возможности систем клона UNIX, систем группы Windows.

Тема 2. Организация вычислительного процесса

Концепция процессов и потоков. Задание, процессы, потоки (нити), волокна. Формы мультипрограммной работы. Управление процессами и потоками. Планирование заданий, процессов и потоков. Взаимодействие и синхронизация процессов и потоков. Методы взаимодействия. Тупики и семафоры. Синхронизирующие объекты. Обработка исключений, сохранение и восстановление процессов, контекст устройства, контекст процесса Аппаратно-программные средства поддержки мультипрограммирования. Системные вызовы.
.

Тема 3. Управление памятью.

Функции ОС по управлению памятью. Распределение памяти. Алгоритмы распределения. Виртуальное адресное пространство. Страничная организация виртуальной памяти. Оптимизация функционирования страничной виртуальной памяти. Сегментная организация виртуальной памяти. Сегментно-страничная виртуальная память. Защита памяти.

Тема 4. Подсистема ввода-вывода. Файловые системы

Устройства ввода-вывода. Назначение, задачи и технологии подсистемы ввода-вывода. Согласование скоростей обмена и кэширование данных. Разделение устройств и данных между процессами. Обеспечение логического интерфейса между устройствами и системой. Классификация драйверов, управление драйверами. Динамическая загрузка и выгрузка драйверов. Поддержка синхронных и асинхронных операций ввода-вывода. Многослойная (иерархическая) модель ввода-вывода. Логическая организация файловой системы. Типы файлов. Монтирование файловой структуры. Физическая организация и адресация файловой. Контроль доступа к файлам. Физическая и логическая организация FAT и NTFS. Файловые операции. Восстановление файловой системы после сбоя.

Тема 5 Автоматизация решения задач администрирования в ОС с использованием языков сценариев

Общая характеристика языка командного интерпретатора POSIX-совместимых ОС. Переменные языка командного интерпретатора POSIX-совместимых ОС и их использование. Встроенные переменные. Управление порядком выполнения действий в языке командного интерпретатора POSIX-совместимых ОС. Команды для работы с файлами, каталогами, процессами, перенаправление ввода-вывода. Отладка сценариев. Назначение и функции систем выполнения сценариев Windows. Объектные модели и языки систем выполнения сценариев ОС Windows. Удаленное выполнение сценариев ОС Windows. Цифровая подпись сценариев в ОС Windows.

Тема 6. Требования к защите ОС

Классификация угроз безопасности ОС. Наиболее распространенные угрозы. Требования к защите ОС. Понятие защищенной ОС. Подходы к организации защиты. Этапы по-

строения защиты. Административные меры защиты. Стандарты безопасности ОС. Виртуальные машины. Изоляция процессов и пользователей. Политики безопасности в ОС Windows.

Тема 7. Структура подсистемы безопасности ОС

Типовая структура подсистемы безопасности ОС и выполняемые ей функции. Средства обеспечения безопасности в ОС семейств UNIX и Windows. Домены безопасности. Критерии защищенности ОС. Модели разграничения доступа Подсистема идентификации и аутентификации. Подсистема разграничения доступа. Подсистема аудита. Требования к подсистеме аудита. Централизованный аудит. Определение параметров аудита. Штатный аудит в ОС Windows и Unix. Реализация аудита в современных ОС. Криптографическая подсистема. Подотчетность действий. Повторное использование объектов. Точность и надежность обслуживания. Защита обмена данных. Реализация подсистем безопасности. Административные меры защиты операционных систем. задачи и принципы сопровождения системного программного обеспечения. Организация и поддержка политик безопасности. Применение групповых политик.

Тема 8. Разграничение доступа в ОС

Субъекты, объекты, методы и права доступа. Привилегии субъектов доступа. Избирательное и полномочное разграничение доступа, изолированная программная среда. Примеры реализации разграничения доступа в современных ОС. Понятия идентификации, аутентификации и учета. Аутентификация на основе паролей, методы подбора паролей, средства и методы повышения защищенности ОС от подбора паролей. Аутентификация на основе внешних носителей ключа, биометрических характеристик пользователя. Примеры реализации идентификации, аутентификации и учета в современных ОС. Разграничение доступа к объектам в операционной системе Microsoft Windows: дескриптор безопасности объекта, виды доступа, алгоритм проверки прав доступа. Служба Bit Locker. Разграничение доступа к объектам в операционной системе Unix.

5. Образовательные технологии.

Методика преподавания дисциплины «Безопасность операционных систем» 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;
- обсуждение и защита рефератов по дисциплине;
- подготовка, представление и обсуждение презентаций по темам рефератов на семинарских занятиях;
- организация и проведение текущего контроля знаний студентов в форме бланкового тестирования;
- проведение мастер-классов экспертов и специалистов по администрированию и аудиту безопасности операционных систем.

Удельный вес занятий, проводимых в интерактивных формах, определен главной целью образовательной программы, особенностью контингента обучающихся, содержанием дисци-

плины «Безопасность операционных систем» и в целом по дисциплине составляет 40% аудиторных занятий. Занятия лекционного типа составляют 30% от объема 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:

- подготовка к выполнению лабораторных работ и их защита.
- реферат по теме: «Структура подсистемы безопасности ОС и выполняемые ею функции»;

Оценочные средства текущего контроля успеваемости включают контрольные вопросы и задания в форме бланкового и (или) компьютерного тестирования, контрольные работы для контроля освоения обучающимися разделов дисциплины.

Образцы тестовых заданий, вариантов контрольных работ, тем рефератов, контрольных вопросов и заданий для проведения текущего контроля, экзаменационных билетов приведены в приложении.

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

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 - 2	способностью применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач

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.

ПК - 2 способностью применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач				
Показатель	**Критерии оценивания**			
	2	**3**	**4**	**5**
знать: принципы построения и функционирования, примеры реализаций современных операционных систем; отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценки защищенности компьютерных систем	Обучающийся демонстрирует полное отсутствие или недостаточное соответствие знаний принципов построения и функционирования, примеры реализаций современных операционных систем; отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценки защищенности компьютерных систем	Обучающийся демонстрирует неполное знание принципов построения и функционирования ОС, отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценки защищенности компьютерных систем, допускает значительные затруднения в реализаций функций современных операционных систем	Обучающийся демонстрирует частичные знания принципов построения и функционирования ОС, отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценки защищенности компьютерных систем, допускаются незначительные затруднения в реализаций функций современных операционных систем	Обучающийся демонстрирует полное соответствие знаний принципов построения и функционирования, примеры реализаций современных операционных систем, отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценки защищенности компьютерных систем и свободно оперирует приобретёнными знаниями.
уметь: использовать средства операционных систем для обеспечения эффективного и безопасного функционирования автоматизированных систем; формулировать и настраивать политику безопасности распространенных операционных систем, а также локальных вычислительных сетей, построенных на их основе .	Обучающийся не умеет или в недостаточной степени умеет использовать средства операционных систем для обеспечения эффективного и безопасного функционирования автоматизированных систем, формулировать и настраивать политику безопасности распространенных операционных систем, а также локальных вычислительных сетей, построенных на их основе	Обучающийся умеет использовать средства операционных систем для обеспечения эффективного и безопасного функционирования автоматизированных систем в недостаточной степени, формулировать и настраивать политику безопасности распространенных операционных систем, а также локальных вычислительных сетей, построенных на их основе допускаются значительные ошибки.	Обучающийся демонстрирует частичное соответствие следующих умений: -может использовать средства операционных систем для обеспечения эффективного и безопасного функционирования автоматизированных систем, формулировать и настраивать политику безопасности распространенных операционных систем, а также локальных вычислительных сетей, построенных на их основе, но допускает незначительные ошибки, неточности, затруднения при переносе умений на новые, нестандартные ситуации	Обучающийся демонстрирует полное соответствие следующих умений: - может использовать средства операционных систем для обеспечения эффективного и безопасного функционирования автоматизированных систем, формулировать и настраивать политику безопасности распространенных операционных систем, а также локальных вычислительных сетей, построенных на их основе, обучающийся свободно оперирует приобретенным умениями, применяет их в ситуациях повы-

				шенной сложности.
владеть: навыками установки и настройки операционных систем семейств Windows и Linux с учетом требований по обеспечению информационной безопасности.	Обучающийся не владеет навыками установки и настройки операционных систем семейств Windows и Linux с учетом требований по обеспечению информационной безопасности	Обучающийся владеет навыками установки и настройки операционных систем семейств Windows и Linux с учетом требований по обеспечению информационной безопасности в неполном объеме, допускаются значительные ошибки, испытывает значительные затруднения при применении навыков в новых ситуациях.	Обучающийся частично владеет навыками установки и настройки операционных систем семейств Windows и Linux с учетом требований по обеспечению информационной безопасности, навыки освоены, но допускаются незначительные ошибки, затруднения при переносе умений на новые, нестандартные ситуации.	Обучающийся в полном объеме владеет навыками установки и настройки операционных систем семейств Windows и Linux с учетом требований по обеспечению информационной безопасности, 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, при этом учитываются результаты текущего контроля успеваемости в течение семестра. Оценка степени достижения обучающимися планируемых результатов обучения по дисциплине проводится преподавателем, ведущим занятия по дисциплине методом экспертной оценки. По итогам промежуточной аттестации по дисциплине (модулю) выставляется оценка «отлично», «хорошо», «удовлетворительно» или «неудовлетворительно».

К промежуточной аттестации допускаются только студенты, выполнившие все виды учебной работы, предусмотренные рабочей программой по дисциплине «Безопасность операционных систем» (прошли промежуточный контроль, представили рефераты, выполнили контрольные работы, защитили лабораторные работы)

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 приведенных 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 средств представлены в приложение к рабочей программе**.**

7. Учебно-методическое и информационное обеспечение дисциплины.

а) основная литература:

основная литература:

1. Назаров С.В., Широков А.И. Современные операционные системы: учебное пособие –М.: НОУ «Интуит»: БИНОМ. Лаборатория знаний, 2013 г. - 367 с. **(15 экз.)**

б) дополнительная литература:

1. Федоров Н.В. Проектирование информационных систем: лаб. практикум - М.: МГИУ, 2009 г.-180 с. **(м/у № 28-9 — 200 экз.)**
2. Хорев П.Б. Методы и средства защиты информации в компьютерных системах – М., Изд. Центр «Академия», 2008 г. -256 с. **(т.1- 49 экз.)**
3. Ларина И.Е. Экономика защиты информации. Учебное пособие- М., МГИУ, 2007 г. - 97 с. **(37 экз.)**

в) программное обеспечение и интернет-ресурсы:

1. Операционная система Windows 7(или ниже) - MicrosoftOpenLicense Лицензия № 61984214, 61984216,61984217, 61984219, 61984213, 61984218, 61984215
2. Офисные приложения, MicrosoftOffice 2013(или ниже) - MicrosoftOpenLicense Лицензия № 61984042
3. Virtual Box 5.2.0.118431 свободно распространяемое ПО

4. Журнал «информационная безопасность» Режим доступа:http://itsec.ru/imag/

Полезные учебно-методические и информационные материалы представлены на сайтах:

1. «Информационная безопасность», журнал – Режим доступа - http://itsec.ru/imag/
2. Плашенков В.В. Обеспечение безопасности бизнеса промышленных предприятий: теория и практика: учебное пособие. Издательство ЧГУ, 2014 г. -Режим доступа - http://biblioclub.ru

8. Материально-техническое обеспечение дисциплины.

Проведение лекционных занятий осуществляется в мультимедийной аудитории, а практических и лабораторных работ в компьютерном классе

9. 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.* При рассмотрении учебного материалы рекомендуется делать акцент на структуру и взаимосвязь аспектов безопасности - методологии, информационного обеспечения, организации, методах кадрового обеспечения и нормативно-правовой базы. Полезно также сосредоточить внимание студентов на анализе угроз и оценке рисков информационной безопасности операционных систем, оценке прямого и косвенного ущерба от риска потери информации, методах оценки целесообразности и эффективности мер на обеспечение информационной безопасности операционных систем.

В процессе самостоятельной работы студенты закрепляют и углубляют знания, полученные во время аудиторных занятий, дорабатывают конспекты лекций, готовятся к зачету и экзамену, а также самостоятельно изучают отдельные темы учебной программы. Преподаватель направляет самостоятельную работу студентов, отвечает на возникающие вопросы, дает рекомендации по методике изучения тем.

Практические занятия проводятся по наиболее важным темам дисциплины. Осуществляется закрепление знаний, полученных студентами на лекциях и в процессе самостоятельной работы. Особое внимание обращается на развитие умений и навыков установления связи положений теории с профессиональной деятельностью будущего специалиста по ИБ. Практическое занятие предполагает творческие дискуссии, активный обмен мнениями по поставленным *вопросам,* заслушивание и обсуждение докладов по предложенным преподавателем темам.

Важным обстоятельством является привлечение внимания студентов к обсуждаемой проблеме, стимулирование интереса к ней и организация активного обсуждения, как структуры проблемы, так и составляющих ее наиболее актуальных тем. Для повышения эффективности проведения занятия требуется предварительная подготовка всех его участников. В этой связи рекомендуется заблаговременно (не менее, чем за неделю) оповестить студентов о теме занятия, дать перечень литературы по теме, назначить из числа студентов докладчиков и содокладчиков.

При проведении практического занятия преподаватель *выполняет, в основном,* функции ведущего - следит за регламентом времени, помогает уточнить формулировки, обобщает результаты дискуссии, подводит итог занятию в целом. При высоком уровне подготовки студенческой группы отдельные функции ведущего можно поручить одному из студентов. В случае необходимости, преподаватель оказывает ему поддержку, а при подведении итогов - дает оценку работе ведущего.

Активная работа студента на практическом занятии учитывается при определении итоговой оценки его знаний по дисциплине на экзамене.

Самостоятельная работа по дисциплине «Безопасность операционных систем» предполагает: выполнение студентами домашних заданий. Домашние задания являются, как правило, продолжением практических занятий и содействуют овладению практическими навыками по основным разделам дисциплины. Самостоятельная работа студентов предполагает изучение теоретического и практического материала по актуальным вопросам дисциплины. Рекомендуется самостоятельное изучение учебной и научной литературы, использование справочной литературы и др.

Самостоятельная работа осуществляется индивидуально.

Контроль самостоятельной работы организуется в двух формах:

- самоконтроль и самооценка студента;
- контроль со стороны преподавателей (текущий и промежуточный).

Критериями оценки результатов самостоятельной работы студента являются:

- уровень освоения студентом учебного материала;
- умения студента использовать теоретические знания при выполнении практических задач;
- сформированность умений;
- оформление материала в соответствии с требованиями.

Текущий контроль осуществляется на практических занятиях, промежуточный контроль осуществляется на зачете и экзамене в устной форме.

10. Методические рекомендации для преподавателя

Программа составлена в соответствии с Федеральным государственным образовательным стандартом высшего образования по направлению подготовки бакалавров **10.03.01 «Информационная безопасность».**

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

Программа утверждена на заседании кафедры “Информационная безопасность”
«29» августа 2020 г., протокол № 1

Заведующий кафедрой
«Информационная безопасность»

к.т.н., доцент Н.В. Федоров

Приложение

Структура и содержание дисциплины «Безопасность операционных систем» по направлению подготовки 10.03.01 «Информационная безопасность» (бакалавр)

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.	РГР	Реферат	К/р	Э	З
	Первый семестр														
1.1	**Общая характеристика операционных систем.**		**1**				**2**								
1.2	*Общая характеристика ОС. Задание на реферат*		**1-2**			2									
1.3	*Назначение и возможности систем клона UNIX, систем группы Windows*.		**1-2**			**1**	**1**								
1.4	*Команды работы с файлами и каталогами*		**1-2**			**1**	**1**	+							
1.5	**Организация вычислительного процесса**		**3**				**2**								
1.6	*Организация вычислительного процесса*		**3-4**			**2**									
1.7	*Мультипрограммные вычислительные процессы*		**3-4**			**1**	**1**								
1.8	*Мультипрограммирование*		**3-4**			**1**	**1**	+							
1.9	**Управление памятью**.		**5**				**2**								
1.10	*Управление памятью Контрольная работа*		**5-6**			**2**	**1**						+		
1.11	*Управление потоками*		**5-6**			**2**	**1**	+							
1.12	**Подсистема ввода- вывода. Файло-**		**7**				**2**								

	вые системы.														
1.13	*Подсистема ввода-вывода Защита рефератов*		**7-8**			**2**						+			
1.14	*Исследование алгоритма замены страниц*		**7-8**			**1**	**1**	+							
1.15	*Файловые системы*		**7-8**			**1**	**1**								
1.16	**Автоматизация решения задач администрирования в ОС с использованием языков сценариев**		**9**				**2**								
1.17	*Контроль доступа к файлам и каталогам*		**9-10**			**2**	**1**	+							
1.18	*Языки систем выполнения сценариев*		**9-10**			**1**		+							
1.19	*Языки систем выполнения сценариев*		**9-10**			**1**	**1**	+							
1.20	**Требования к защите ОС**		**11**				**2**								
1.21	*Административные меры защиты. Стандарты безопасности ОС*		**11-12**			**2**	**1**								
1.22	*Учетные записи пользователей и их права*		**11-12**			**2**	**1**	+							
1.23	**Структура подсистемы безопасности ОС**		**13**				**2**								
1.24	*Структура подсистемы безопасности ОС Защита рефератов*		**13-14**			**2**	**1**					+			
1.25	*Инструменты администрирования и контроля Windows Server*		**13-14**			**2**	**1**	+							
1.26	**Разграничение доступа в ОС**		**15**				**2**								
1.27	*Разграничение доступа в ОС Контрольная работа*		**15-18**			**2**	**1**	+					+		
1.28	*Безопасности локально-вычислительной сети*		**15-18**			**2**	**1**	+							
1.29	*Штатный аудит в ОС Windows и Unix.*		**15-18**			**1**	**1**								
1.30	*Защита лабораторных и рефератов*		**15-18**			**1**	**1**	+				+			
	Форма аттестации		19-21											**Э**	
	Всего часов по дисциплине					**36**	**36**								

Приложение

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Московский политехнический университет»
(МОСКОВСКИЙ ПОЛИТЕХ)

Направление подготовки: **10.03.01 «Информационная безопасность»**
ОП (профиль) «Безопасность автоматизированных 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»

Состав: 1. Паспорт фонда оценочных средств
2. Описание оценочных средств:
Тестирование
Реферат
Контрольная работа
Экзамен

Составители: ст. преп. Пиков В.А.

Москва, 2020 год

Таблица 1

ПОКАЗАТЕЛЬ УРОВНЯ СФОРМИРОВАННОСТИ КОМПЕТЕНЦИЙ

Безопасность операционных систем					
ФГОС ВО **10.03.01 «Информационная безопасность »**					
В процессе освоения данной дисциплины студент формирует и демонстрирует следующие **профессиональные и профильно-специализированные компетенции**:					
КОМПЕТЕНЦИИ		**Перечень компонентов**	**Технология формирования компетенций**	**Форма оценочного средства**	**Степени уровней освоения компетенций**
ИНДЕКС	**ФОРМУЛИРОВКА**				
ПК - 2	способностью применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач	**знать:** • принципы построения и функционирования, примеры реализаций современных операционных систем **уметь:** • использовать средства операционных систем для обеспечения эффективного и безопасного функционирования автоматизированных систем **владеть:** • навыками установки и настройки операционных систем семейств Windows и Linux с учетом требований по обеспечению информационной безопасности.	лекция, самостоятельная работа, семинарские занятия	УО, К/Р, Т	**Базовый уровень** знает принципы построения и функционирования, примеры реализаций современных операционных систем, умеет использовать средства операционных систем для обеспечения эффективного и безопасного функционирования автоматизированных систем **Повышенный уровень** обладает навыками установки, настройки, использования операционных систем семейств Windows и Linux с учетом требований информационной безопасности, их восстановлением после сбоев

		знать • отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценки защищенности компьютерных систем **уметь:** • формулировать и настраивать политику безопасности распространенных операционных систем, а также локальных вычислительных сетей, построенных на их основе **владеть:** • навыками эксплуатации и администрирования (в части, касающейся разграничения доступа, аутентификации и аудита) баз данных, локальных компьютерных сетей, программных систем с учетом требований по обеспечению информационной безопасности	лекция, самостоятельная работа, семинарские занятия, лабораторные работы	УО, К/Р, Т,Р	**Базовый уровень** знает отечественные и зарубежные стандарты в области компьютерной безопасности и может оценить защищенность компьютерных систем, настроить политику безопасности распространенных операционных систем **Повышенный уровень** может оценить защищенность компьютерных систем, настроить политику безопасности распространенных операционных систем, владеет навыками эксплуатации и администрирования безопасного доступа, аутентификации и аудита баз данных, локальных компьютерных сетей, программных систем с учетом требований по обеспечению информационной безопасности.

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

1. Темы рефератов

«Структура подсистемы безопасности ОС и выполняемые ею функции»

1. Средства обнаружения уязвимостей в ОС Windows 7/8, Linux.
2. Уменьшение уязвимости ОС при работе в Интернет за счет использования пакетов программ VMWare, Virtual Box.
3. Организация разграничения доступа в ОС Windows7/8, Linux
4. Организация аудита стандартными средствами в ОС Windows7/8, Linux
5. Средства организации аудита сторонних разработчиков для ОС Windows 7/8, Linux
6. Антивирусные средства для ОС Windows . 7/8, Linux
7. Межсетевые экраны для ОС Windows 7/8, Linux
8. Средства аутентификации сторонних разработчиков для ОС Windows 7/8, Linux
9. Доменные групповые политики Server 2012
10. Настройка параметров безопасности в ОС Windows 7/8, Linux
11. Структура системы безопасности ОС Windows
12. Исследование уровня безопасности операционной системы Linux
13. Системный реестр Windows
14. Обзор и статистика методов, лежащих в основе атак на современные ОС

2. Тестовые вопросы по курсу «Безопасность операционных систем»

Тест 1

1 К основным функциям подсистемы защиты операционной системы относятся:

1. Идентификация, аутентификация, авторизация, управление политикой безопасности и разграничение доступа
2. Криптографические функции
3. Сетевые функции
4. Все вышеперечисленные

2 Риск – это…

1. Вероятностная оценка величины возможного ущерба, который может понести владелец информационного ресурса в результате успешно проведенной атаки
2. Фактическая оценка величины ущерба, который понес владелец информационного ресурса в результате успешно проведенной атаки
3. Действие, которое направлено на нарушение конфиденциальности, целостности и/или доступности информации, а также на нелегальное использование других ресурсов сети
4. Реализованная угроза

3. В классификацию вирусов по способу заражения входят

1. опасные
2. Файловые

3. Резидентные
4. Загрузочные
5. Файлово -загрузочные
6. Нерезидентные

4. Идентификация и аутентификации применяются для …
1. Регистрации событий безопасности
2. Выявления попыток несанкционированного доступа
3. Обеспечения целостности данных
4. Для ограничения доступа случайных и незаконных субъектов информационной
5. Системы к её объектам

5. Управление доступом, основанное на сопоставлении меток конфиденциальности информации, содержащейся в объектах (файлы, папки, рисунки) и официального раз
решения (допуска) субъекта к информации соответствующего уровня конфиденциаль
ности, называется ...
1. Мандатное
2. Принудительное
3. Статистическое
4. Дискретное

6. Файловая система
1. Не является частью ОС, а включает совокупность всех файлов на диске
2. Является частью ОС, включает все файлы на диске и системные программные средства, реализующие различные операции над файлами.
3. Не является частью ОС, а включает все файлы и наборы структур данных, ис пользуемых для управления файлами.

7. Уровень мультипрограммирования, обеспечиваемый операционной системой,
1. Тем выше, чем больше объем оперативной памяти, имеющейся в системе
2. Тем ниже, чем меньше объем дисковой и оперативной памяти системы
3. Зависит от выбранного способа управления основной памятью системы

8 По какому принципу осуществляется физическая организация и адресация файлов в файловой системе ОС UNIX
1. Осуществляется простое перечисление номеров кластеров (прямая адресация)
2 Прямой способ адресации сочетается с косвенным
3 Используется связный список кластеров

9 Что обеспечивает большую производительность компьютера
1. Создание виртуального диска
2. Кеширование накопителей и памяти
3. Увеличение числа буферов обмена операционной системы.

10 Какой подход к определению прав доступа к разделяемым ресурсам вычислитель
ной системы используется в универсальных ОС
1. Мандатный доступ

2. Избирательный доступ
3. Комбинированный мандатно-избирательный доступ

11. Ядро операционной системы
1. Имеет строго определенный размер. Обеспечивает специальные функции по об
работке запросов и загружается в память по мере необходимости
2. Является резидентной частью ОС, состоит из программ, управляющих различ
ными ресурсами ЭВМ.
3. Является транзитной частью ОС, обеспечивает обработку запросов активных процессов и интерфейс с аппаратной средой.

12 Драйвер это
1. Системный программный модуль, предназначенный для управления работой внешнего устройства
2. Системный программный модуль, предназначенный для управления работой внешнего устройства и его контроллера
3. Это программа, предназначенная для распознавания ОС нового установленного внешнего устройства

Тест 2

1. Может ли Администратор в ОС Windows безнаказанно выполнять любые операции с любыми объектами (файлами, устройствами) системы
А. Да, без каких-либо ограничений
Б. Нет, только с разрешения владельца объекта
В. Может, но владелец-пользователь объекта всегда об этом узнает

2. Основными компонентами подсистемы ввода-вывода операционной системы являются
А. Устройства ввода-вывода
Б. Драйверы, управляющие внешними устройствами
В. Драйверы устройств и файловая система

3.Байт-ориентированные драйверы в ОС Unix управляют
А. Внешними устройствами прямого доступа
Б. Не адресуемыми и не позволяющими производить операцию поиска устройствами
В. Могу управлять и теми и другими устройствами

4.Режим работы ОС с переменным числом задач предполагает
А. Отсутствие ограничений на количество задач, одновременно обрабатываемых операционной системой
Б. В ОС выполняется несколько зада. Каждой задаче выделяется несколько разделов памяти, постоянного размера
В. В системе выполняется несколько задач. Каждой задаче выделяется раздел памяти, определяемый потребностью задачи

5. Реально виртуальная вычислительная машина
А. Не существует
Б. Функционально эквивалентна реальной вычислительной системе

В. Функционально эквивалентна нескольким вычислительным системам

6. Виртуальным адресным пространством называется
А. Совокупность адресов переменных и команд, вырабатываемых транслятором, переводящим программу в машинный код
Б. Диапазон адресов оперативной памяти, занятой выполняемым процессом
В. Адресное пространство на диске, занятое программой, переведенной в машинный код

7. Файловая структура в Linux имеет
А. Централизованную структуру
Б. Децентрализованную структуру
В. Централизованную монтируемую структуру.

8. Какую модель памяти использует современные аппаратные средства.
А. Сегментная модель.
Б. Сегментно-страничная модель.
В. Динамическая модель.

9. Чем больше размер логического диска, отформатированного под FAT на жестком диске
А. Тем ниже эффективность использования диска
Б. Тем выше эффективность использования диска
В. Эффективность использования диска не зависит от порядка его разбиения на логические диски

10. Что такое эксклюзивная кэш-память
А . Это память, предполагающая перенос информации из кэша более низкого уровня в
кэш более высокого по мере заполнения первого
Б. Это память, предполагающая дублирование информации, находящейся в первом и втором кэше памяти
В. Это такая архитектура, при которой устанавливается зависимость между физическими размерами кэша первого и второго уровня

11. Достоинствами сегментного распределения виртуальной памяти является
А Возможность загрузки с диска в оперативную память и обратно больших порций необходимых данных.
Б. Облегчение механизма преобразования виртуальных адресов процесса в физические
В. Возможность задания дифференцированных прав доступа процесса к его сегментам

12. Критерием эффективности системы разделения времени является
А. Способность выдерживать заранее заданные интервалы времени между запуском программы и получением результат
Б. Эффективность работы пользователя
В. Максимальная пропускная способность системы.

13. В каких вычислительных системах не ограничена возможность наращивания числа процессоров

А. В мультипроцессорных системах с симметричной архитектурой
Б. В кластерных системах
В. В системах с симметрично – мультипроцессированным способом организации вы числительного процесса

14. Как называется состояние потока, когда он имеет все необходимые для выполнения ресурсы, в том числе и ресурс центрального процессора.
А. Состояние выполнения.
Б. Состояние готовности
В. Заблокированное состояние ожидания

15. При вытесняющем мультипрограммировании
А. Механизм планирования потоков распределен между операционной системой и прикладными программами
Б. Функции планирования потоков целиком сосредоточены в операционной системе
В. Разработчик приложений сам проектирует алгоритм планирования потоков своего приложения

16. В современных операционных системах механизм планировании потоков
А. Основан на приоритетах обслуживания
Б. Основан на концепции квантования
В. Алгоритм планирования основан на использовании приоритетов и концепции квантования

17. Дисковые квоты используются
А. Для обеспечения безопасности доступа к данным диска
Б. Для контроля расходования дискового пространства пользователем
В. Для контроля расходования дискового пространства и обеспечения безопасности до
ступа к данным пользователем

18. Файл «подкачки» наиболее эффективно расположить…
А. На виртуальном диске
Б. В непрерывной области оперативной памяти
В. На жестком диске

19. Системный реестр WINDOWS это:
А. База данных, содержащая наибольшую информацию, обеспечивающую функционирование вычислительной системы.
Б. Это отчет о произошедших в системе сбоях
В. Это таблица распределения оперативной памяти между активными в данный момент процессами.

20. Аутентификация, которая обеспечивает защиту только от несанкционированных действий
А.В системах, где нарушитель не может во время сеанса работы прочитать аутентифи кационную информацию, называется …
Б. Статической
В. Устойчивой
Г. Постоянной
Д. Переменной

.

3.Варианты контрольных работ

3.1 Контрольная работа на тему «Управление доступом»

1 Угрозы безопасности ОС
2. Контроль доступа к файлам в ОС Windows7/8, Linux

3.2 Контрольная работа на тему «Управление памятью»

1. Понятие виртуального адресного пространства
2. Алгоритмы распределения памяти
3. Используя средства ОС, определить объем физической, виртуальной памяти, величину файла подкачки и его размещение в компьютере м

4.1.Контрольные вопросы к экзамену по дисциплине (6 семестр)

1. Общая характеристика операционных систем.
2. Назначение и возможности систем клона UNIX.
3. Системы группы Windows.
4. Интерфейс ОС с пользователями.
5. Диалоговые и пакетные интерфейсы.
6. Функции ОС.
7. Принципиальная организация ядра ОС
8. Концепция виртуального ресурса и виртуальной вычислительной машины
9. Факторы, влияющие на структуру и функции ОС.
10. Логическая организация файловой системы.
11. Типы файлов. Монтирование файловой структуры.
12. Логическая организация файла
13. Физическая организация и адресация файла
14. Схема адресации файлов систем S5 и UFS
15. Физическая организация FAT
16. Физическая организация файловой систем S5 и UFS
17. Физическая организация NTFS
18. Контроль доступа к файлам в ОС Unix
19. Контроль доступа к файлам в ОС Windows
20. Задачи ОС по управлению файлами и устройствами
21. Многослойная модель ввода-вывода
22. Функции ОС по управлению памятью
23. Типы адресов
24. Алгоритмы распределения памяти без использования внешней памяти
25. Страничная виртуальная память
26. Сегментная виртуальная память
27. Странично-сегментная виртуальная память
28. Кэш-память
29. Виртуальный диск.
30. Сохранение и восстановление процессов.
31. Организация управления доступом и защиты ресурсов ОС.
32. Основные механизмы безопасности: средства и методы аутентификации в ОС
33. Модели разграничения доступа.

34. Организация и использование средств аудита.
35. Администрирование ОС: задачи и принципы сопровождения системного программного обеспечения.
36. Генерация, настройка, измерение производительности и модификация систем.
37. Управление безопасностью ОС.
38. Основные стандарты ОС.
39. Механизмы аудита в ОС.
40. Журналирование служб и приложений.
41. Механизмы контроля доступа к ресурсам.
42. Аутентификация в операционных системах.
43. Службы доменных имен,
44. Распределение адресов и DHCP.
45. Установка и настройки серверных операционных систем.
46. Серверные операционные системы. Добавление ролей. Доменные службы.
47. Создание и управление инфраструктурой на основе виртуальных машин.
48. Платформы для виртуализации на основе Windows HyperV.
49. Наложенные средства защиты операционных систем и интеграция их в инфраструктуру ОС.
50. Файловые системы ОС Windows и Linux восстановление удаленных файлов.

4.2. Пример экзаменационного билета

1. Классификация средств защиты информации от НСД по РД ФСТЭК
2. Использование библиотеки windows.h для создания приложений
3. Настройте политику разграничения доступа для папки temp в linux так чтобы root не имел к ней доступа.