МИНОБРНАУКИ РОССИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«ВОРОНЕЖСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

(ФГБОУ ВО «ВГУ»)

УТВЕРЖДАЮ

Заведующий кафедрой

функционального анализа

и операторных уравнений

Каменский М.И.

19.05.2022 г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

Б1.О.03.05 Безопасность операционных систем (операционные системы и их безопасность)

1. Код и наименование направления специальности: 10.05.04 информационно-аналитические системы безопасности

2. Профиль специализации: Информационная безопасность финансовых и экономических структур, Автоматизация информационно-аналитической деятельности

3. Квалификация выпускника: специалист по защите информации

4. Форма обучения: очная

5. Кафедра, отвечающая за реализацию дисциплины: функционального анализа и операторных уравнений

6. Составители программы: Груздев Денис Владиславович, преподаватель, математический факультет, кафедра функционального анализа и операторных уравнений .

7. Рекомендована: НМС математического факультета, протокол №0500-03 от 24.03.2022г.

8. Учебный год: 2025-2026 **Семестр:** 7

9. Цели и задачи учебной дисциплины:

Цели изучения дисциплины:

- освоение студентами принципов построения систем защиты информации в рамках операционной системы (ОС), изучение методов анализа надежности операционных систем и получения практических умений и навыков администрирования операционной системы, приводящего к надежной и безопасной работе пользователей с операционной системой и с приложениями под ее управлением.

Задачи учебной дисциплины:

- изучение принципов построения подсистем защиты в ОС различной архитектуры;

- изучение возможных средств и методов несанкционированного доступа к ресурсам ОС и получение навыков предотвращения подобных попыток;

- применение системного подхода к проблеме защиты информации в ОС;

- освоение механизмов защиты информации в ОС и потенциальных возможностей по их преодолению.

10. Место учебной дисциплины в структуре ООП:

Дисциплина Безопасность операционных систем (операционные системы и их безопасность) относится к обязательной части блока Б1.

Для изучения и освоения дисциплины нужны знания из предшествующих курсов: Информатика, Математическая логика и теория алгоритмов, Языки программирования, Технология и методы программирования.

11. Планируемые результаты обучения по дисциплине/модулю (знания, умения, навыки), соотнесенные с планируемыми результатами освоения образовательной программы (компетенциями выпускников):

Код	Название компетенции	Коды	Индикаторы	Планируемые результаты обучения
ОПК-11	Способен осуществлять синтез технологий и основных компонентов функциональной и обеспечивающей частей создаваемых информационно-аналитических систем, в том числе выбор мероприятий по защите информации	ОПК-11.3	Осуществляет меры противодействия нарушениям безопасности с использованием различных программных и аппаратных средств защиты	**знать:** основные типы современных операционных систем и оболочек, их возможности и принципы построения; основные понятий по безопасности операционных систем; требования, предъявляемые к системе защиты современных ОС; **уметь:** оценивать эффективность и надежность встроенной защиты в ОС; выявлять имеющие место проблемные места в защите ОС и использовать комплекс мero-

				приятий для обеспечения защиты; **владеть:** навыками установки и настройки современных ОС; навыками построения системной защиты современной ОС;
ОПК-13	Способен производить настройку и обслуживание компонентов обеспечивающей части информационно-аналитических систем на всех этапах жизненного цикла, встроенных средств защиты информации, восстанавливать их работоспособность при внештатных ситуациях	ОПК-13.4	Настраивает, обслуживает и восстанавливает средства защиты информации на всех этапах жизненного цикла информационно-аналитических систем	**знать:** организацию управления доступом и защиты ресурсов ОС; основные механизмы безопасности; **уметь:** администрировать встроенный функционал ОС, направленный на встроенную политику безопасности; **владеть:** навыками применения методов обеспечения безопасности ОС.
		ОПК-13.5	Способен администрировать системы управления базами данных, операционные системы и компьютерные сети	**знать:** применяемые на практике критерии и методы оценивания эффективности и надежности средств защиты используемых ОС; **уметь:** пользоваться встроенными инструментами и средствами защиты, предоставляемыми ОС; проводить анализ и оценивание встроенных в ОС механизмов защиты; **владеть:** навыками организации управления доступом и защитой ресурсов ОС; применения действующую законодательную базу в области информационной безопасности;

12 Объем дисциплины в зачетных единицах/час.— 5/180

Форма промежуточной аттестации: экзамен

13. Трудоемкость по видам учебной работы

Вид учебной работы	Трудоемкость	
	Всего	По семестрам
		5 семестр
Аудиторные занятия	68	68

в том числе:	лекции	34	34
	практические		
	лабораторные	34	34
Самостоятельная работа		76	76
в том числе: курсовая работа (проект)			
Форма промежуточной аттестации *(экзамен – 36 час.)*		36	36
Итого:		180	180

13.1. Содержание дисциплины

№ п/п	Наименование раздела дисциплины	Содержание раздела дисциплины
1. Лекции		
1.1	Теоретические основы защиты ОС	Понятие безопасности информационных систем в нормативных документах. Классификация защищенности (международные стандарты). Обзор свойств основных классов. Политика безопасности, формальное представление политик безопасности.
1.2	Методы защиты ОС	Нарушения безопасности. Изъяны защиты. Классификация изъянов защиты по размещению в вычислительной системе. ОС как среда нарушений безопасности. Категории изъянов защиты в ОС. Понятие доверенного ПО операционных систем, ТСВ. Свойство безопасности ОС, гарантированность безопасности. Принципы разработки доверенного ПО. Структура безопасной ОС. Общие принципы построения защищенных ОС.
1.3	Модель безопасности	Модель безопасности ОС семейства Windows. Контроль доступа к объектам Windows. Типы субъектов и объектов защиты. Атрибутивная природа контроля доступа к объектам защиты. Списки и записи контроля доступа. Проверка доступа. Эффективные права доступа.
1.4	Контроль безопасности в ОС	Организация контроля безопасности в ОС Windows. Шаблоны безопасности. Анализ безопасности с помощью шаблонов. Подсистема аудита. Защита данных при хранении в ОС, EFS. Защита данных при передаче, поддержка VPN. Контроль целостности в ОС. Целостность ядра ОС. Обеспечение целостности кода. Управление учетными записями. Мандатный контроль целостности. Изоляция привилегий пользовательского интерфейса. Защищенные процессы. Изоляция нулевой сессии.

1.5	Безопасность серверных приложений	Обеспечение безопасности серверных приложений ОС. Сервер IIS, его механизмы защиты. Защита DNS. Защита RDS (протокола удалённого рабочего стола).
1.6	Безопасность UNIX-систем	Обеспечение безопасности UNIX-систем. Защита ОС на этапе загрузки. Шифрование файловых систем в ОС UNIX. Защищенные терминалы. Аутентификация в ОС, реализация в ОС UNIX. Управление учетными записями и домашними каталогами. Дискреционный контроль доступа в UNIX-системах. Биты защиты. Усиление базовой безопасности ОС UNIX. Механизмы SELinux, RSBAC, GRSecurity. Применение подключаемых модулей аутентификации PAM. Аудит и журналировние событий в UNIX-системах. Анализ журналов, управление ими и защита.
1.7	Безопасность сетевых взаимодействий	Защита сетевого взаимодействия в ОС UNIX. Фильтрация трафика. Использование прокси-серверов. Криптографическая защита сетевого взаимодействия. Технологии Open SSL, SSH.
1.8	Безопасность приложений	Обеспечение безопасности на уровне приложений. Задание конфигурации безопасности. Файлы конфигурации. Настройка безопасности сервера, модули, создание замкнутой среды выполнения. Анализ уязвимостей на примере ОС UNIX.
3. Практические работы		
3. Лабораторные работы		
3.1	Теоретические основы защиты ОС	Понятие безопасности информационных систем в нормативных документах. Классификация защищенности (международные стандарты). Обзор свойств основных классов. Политика безопасности, формальное представление политик безопасности.
3.2	Методы защиты ОС	Нарушения безопасности. Изъяны защиты. Классификация изъянов защиты по размещению в вычислительной системе. ОС как среда нарушений безопасности. Категории изъянов защиты в ОС. Понятие доверенного ПО операционных систем, ТСВ. Свойство безопасности ОС, гарантированность безопасности. Принципы разработки доверенного ПО. Структура безопасной ОС. Общие принципы построения защищенных ОС.
3.3	Модель безопасности	Модель безопасности ОС семейства Windows. Контроль доступа к объектам Windows. Типы субъектов и объектов защиты. Атрибутивная природа контроля доступа к объектам защиты. Списки и записи контроля доступа. Проверка доступа. Эффективные права доступа.
3.4	Контроль безопасности в ОС	Организация контроля безопасности в ОС Windows. Шаблоны безопасности. Анализ безопасности с помощью шаблонов. Подсистема аудита. Защита данных при

		хранении в ОС, EFS. Защита данных при передаче, поддержка VPN. Контроль целостности в ОС. Целостность ядра ОС. Обеспечение целостности кода. Управление учетными записями. Мандатный контроль целостности. Изоляция привилегий пользовательского интерфейса. Защищенные процессы. Изоляция нулевой сессии.
3.5	Безопасность серверных приложений	Обеспечение безопасности серверных приложений ОС. Сервер IIS, его механизмы защиты. Защита DNS. Защита RDS (протокола удалённого рабочего стола).
3.6	Безопасность UNIX-систем	Обеспечение безопасности UNIX-систем. Защита ОС на этапе загрузки. Шифрование файловых систем в ОС UNIX. Защищенные терминалы. Аутентификация в ОС, реализация в ОС UNIX. Управление учетными записями и домашними каталогами. Дискреционный контроль доступа в UNIX-системах. Биты защиты. Усиление базовой безопасности ОС UNIX. Механизмы SELinux, RSBAC, GRSecurity. Применение подключаемых модулей аутентификации PAM. Аудит и журналировние событий в UNIX-системах. Анализ журналов, управление ими и защита.
3.7	Безопасность сетевых взаимодействий	Защита сетевого взаимодействия в ОС UNIX. Фильтрация трафика. Использование прокси-серверов. Криптографическая защита сетевого взаимодействия. Технологии Open SSL, SSH.
3.8	Безопасность приложений	Обеспечение безопасности на уровне приложений. Задание конфигурации безопасности. Файлы конфигурации. Настройка безопасности сервера, модули, создание замкнутой среды выполнения. Анализ уязвимостей на примере ОС UNIX.

13.2. Темы (разделы) дисциплины и виды занятий

№ п/п	Наименование раздела дисциплины	Виды занятий (часов)			
		Лекции	Лабораторные	Самостоятельная работа	Всего
1	Теоретические основы защиты ОС	4	2	4	10
2	Методы защиты ОС	4	4	6	14
3	Модель безопасности	4	4	8	16
4	Контроль безопасности в ОС	4	6	10	20
5	Безопасность серверных приложений	4	4	10	18
6	Безопасность UNIX-систем	6	6	18	30
7	Безопасность сетевых взаимодействий	4	4	6	14
8	Безопасность приложений	4	4	14	22
	Итого	34	34	76	144

14. Методические указания для обучающихся по освоению дисциплины

В процессе преподавания дисциплины используются такие виды учебной работы, как лекции, лабораторные занятия, а также различные виды самостоятельной работы обучающихся. На лекциях рассказывается теоретический материал, на лабораторных занятиях решаются примеры по теоретическому материалу, прочитанному на лекциях.

При изучении курса «Безопасность операционных систем (операционные системы и их безопасность)» обучающимся следует внимательно слушать и конспектировать материал, излагаемый на аудиторных занятиях. Для его понимания и качественного усвоения рекомендуется следующая последовательность действий.

1. После каждой лекции студентам рекомендуется подробно разобрать прочитанный теоретический материал, выучить все определения и формулировки теорем, разобрать примеры, решенные на лекции. Перед следующей лекций обязательно повторить материал предыдущей лекции.

2. Перед лабораторным занятием обязательно повторить лекционный материал. После практического занятия еще раз разобрать решенные на этом занятии примеры, после чего приступить к выполнению домашнего задания. Если при решении примеров, заданных на дом, возникнут вопросы, обязательно задать на следующем практическом занятии или в присутственный час преподавателю.

3. При подготовке к лабораторным занятиям повторить основные понятия по темам, изучить примеры. Решая задачи, предварительно понять, какой теоретический материал нужно использовать. Наметить план решения, попробовать на его основе решить практические задачи.

4. Выбрать время для работы с литературой по дисциплине в библиотеке: каждый вторник с 15:00 до 18:00

Самостоятельная учебная деятельность студентов по дисциплине «**Безопасность операционных систем**» предполагает изучение рекомендуемой преподавателем литературы по вопросам лекционных и практических занятий (приведены выше), самостоятельное освоение понятийного аппарата и подготовку к текущим аттестациям (**выполнению практических заданий**) (примеры см. ниже).

Вопросы лекционных и практических занятий обсуждаются на занятиях в виде устного опроса – индивидуального и фронтального. При подготовке к лекционным и практическим занятиям, обучающимся важно помнить, что их задача, отвечая на основные вопросы плана занятия и дополнительные вопросы преподавателя, показать свои знания и кругозор, умение логически построить

ответ, владение математическим аппаратом и иные коммуникативные навыки, умение отстаивать свою профессиональную позицию. В ходе устного опроса выявляются детали, которые по каким-то причинам оказались недостаточно осмысленными студентами в ходе учебных занятий. Тем самым опрос выполняет важнейшие обучающую, развивающую и корректирующую функции, позволяет студентам учесть недоработки и избежать их при подготовке к промежуточным аттестациям.

Все выполняемые студентами самостоятельно задания (выполнение контрольной работы и практических заданий) подлежат последующей проверке преподавателем. Результаты текущих аттестаций учитываются преподавателем при проведении промежуточной аттестации (**7 семестр – экзамен**).

15. Перечень основной и дополнительной литературы, ресурсов интернет, необходимых для освоения дисциплины

а) основная литература:

№ п/п	Источник
1	*Таненбаум, Эндрю. Современные операционные системы = Modern Operating Systems / Э. Таненбаум ; [пер. с англ. Н. Вильчинского, А. Лашкевича] .— 3-е изд. — СПб. [и др.] : Питер, 2010 .— 1115 с. : ил., табл. — (Классика Computer Science) .— Библиогр.: с.1108-1115 .— ISBN 978-5-49807-306-4.*

б) дополнительная литература:

№ п/п	Источник
2	*Хоглунд, Г. Руткиты. Внедрение в ядро Windows = Rootkits. Subverting the Windovs Kernel : пер. с англ. / Г. Хоглунд, Дж. Батлер .— СПб [и др.] : Питер, 2007 .— 284 с. — Алф. указ.: с.277-284 .— ISBN 978-5-469-01409-6.*
3	*Безбогов, Александр Александрович. Безопасность операционных систем : [учебное пособие для студ. вузов, обуч. по специальности 090105 "Комплекс. обеспечение информ. безопасности автоматизир. систем"] / А.А. Безбогов, А.В. Яковлев, Ю.Ф. Мартемьянов .— М. : Гелеос АРВ, 2008 .— 319 с. : ил., табл. — Библиогр.: с.308-310 .— ISBN 978-5-85438-181-9.*
4	*Таненбаум, Эндрю. Современные операционные системы / Э. Таненбаум ; Пер. с англ. А. Леонтьева .— 2-е изд. — СПб. : Питер, 2002 .— 1037 с. : ил., табл. — (Классика Computer Science) .— ISBN 5-318-00299-4.*
5	*Проскурин, Вадим Геннадьевич. Защита в операционных системах : Программ.-аппарат. средства обеспечения информ. безопасности :Учеб. пособие для студ. вузов по специальностям "Защищ. телекоммуникац. системы", "Орг. и технология защиты информ.", "Комплекс. обеспечение информ. безопасности автоматизир. / В. Г. Проскурин, С. В. Крутов, И. В. Мацкевич .— М. : Радио и связь, 2000 .— 164,[2] с. : ил., табл. — ISBN 5-256-01414-5 : 48.60.*
6	*Боmm, Эд. Безопасность Windows : Windows XP и Windows 2000 / Э. Боmm, К. Зихерт ; Пер. с англ. Д. Жукова и др. — СПб. : Питер, 2003 .— 681 с. : ил. — (Эффективная работа) .— Парал. тит. л. англ. — ISBN 5-8046-0116-4.*

в) информационные электронно-образовательные ресурсы**:**

№ п/п	Источник
7	*Лекции по безопасности ОС http://nick-yk.narod.ru/doc/system.htm*
8	*http://www.lib.vsu.ru - электронный каталог ЗНБ ВГУ*

16. Перечень учебно-методического обеспечения для самостоятельной работы

№ п/п	Источник
1	*Таненбаум, Эндрю. Современные операционные системы = Modern Operating Systems / Э. Таненбаум ; [пер. с англ. Н. Вильчинского, А. Лашкевича] .— 3-е изд. — СПб. [и др.] : Питер, 2010 .— 1115 с. : ил., табл. — (Классика Computer Science) .— Библиогр.: с.1108-1115 .— ISBN 978-5-49807-306-4.*
2	*Положение об организации самостоятельной работы обучающихся в Воронежском государственном университете*

17. Образовательные технологии, используемые при реализации учебной дисциплины, включая дистанционные образовательные технологии (ДОТ, электронное обучение (ЭО), смешанное обучение):

Дисциплина может реализовываться с применением электронного обучения и дистанционных образовательных технологий. При проведении занятий в дистанционной форме используются технические и информационные ресурсы Образовательного портала "Электронный университет ВГУ" (https://edu.vsu.ru), базирующегося на системе дистанционного обучения Moodle, развернутой в университете, а также другие доступные ресурсы в сети Интернет.

Перечень необходимого программного обеспечения : операционная система Windows , Linux, браузер Mozilla Firefox, Opera или Internet Expolorer, Denwer, PHP, MySQL, Экран, ноутбук.

18. Материально-техническое обеспечение дисциплины:

Проектор, ноутбук, экран. Для проведения лекционных и практических занятий используются аудитории, соответствующие действующим санитарно-техническим нормам и противопожарным правилам.

Для самостоятельной работы используется класс с компьютерной техникой, оснащенный необходимым программным обеспечением, электронными учебными пособиями и законодательно - правовой и нормативной поисковой системой, имеющий выход в глобальную сеть.

19. Оценочные средства для проведения текущей и промежуточной аттестаций

Порядок оценки освоения обучающимися учебного материала определяется содержанием следующих разделов дисциплины:

№ п/п	Наименование раздела дисциплины (модуля)	Компетенция(и)	Индикатор(ы) достижения компетенции	Оценочные средства

1.	Теоретические основы защиты ОС	ОПК-11, ОПК-13	ОПК-11.3; ОПК-13.4; ОПК-13.5	Домашнее задание, контрольная работа
2.	Методы защиты ОС	ОПК-11, ОПК-13	ОПК-11.3; ОПК-13.4; ОПК-13.5	Домашнее задание, контрольная работа
3.	Модель безопасности	ОПК-11, ОПК-13	ОПК-11.3; ОПК-13.4; ОПК-13.5	Домашнее задание, контрольная работа
4.	Контроль безопасности в ОС	ОПК-11, ОПК-13	ОПК-11.3; ОПК-13.4; ОПК-13.5	Домашнее задание, контрольная работа
5.	Безопасность серверных приложений	ОПК-11, ОПК-13	ОПК-11.3; ОПК-13.4; ОПК-13.5	Домашнее задание, контрольная работа
6.	Безопасность UNIX-систем	ОПК-11, ОПК-13	ОПК-11.3; ОПК-13.4; ОПК-13.5	Домашнее задание, контрольная работа
7.	Безопасность сетевых взаимодействий	ОПК-11, ОПК-13	ОПК-11.3; ОПК-13.4; ОПК-13.5	Домашнее задание, контрольная работа
8.	Безопасность приложений	ОПК-11, ОПК-13	ОПК-11.3; ОПК-13.4; ОПК-13.5	Домашнее задание, контрольная работа
Промежуточная аттестация форма контроля - экзамен				Перечень вопросов к экзамену

20 Типовые оценочные средства и методические материалы, определяющие процедуры оценивания

20.1 Текущий контроль успеваемости Контроль успеваемости по дисциплине осуществляется с помощью следующих оценочных средств: домашнее задание, контрольная работа, презентация.

Перечень практических заданий

Тема: «Угрозы безопасности клиентским операционным системам»

Задание. По представленному описанию компании определить угрозы безопасности клиентским ОС, выбрать клиентские ОС, отвечающие интересам компании и описать процесс организации их защиты. По результатам выполнения задания подготовьте отчет.

Вопросы

1. Какие существуют основные типы угроз безопасности ОС? Обоснуйте ответ.

2. Какие механизмы защиты ОС Вы знаете?

3. В чем заключается разница защитных механизмов клиентских ОС семейства Windows и Linux? Обоснуйте ответ.

Пример контрольного задания (вариант задания)

Контрольная работа
по дисциплине «Безопасность операционных систем»
Вариант №___

Составьте алгоритм и напишите программу, обеспечивающую взаимоисключения с помощью семафора.

Текущий контроль представляет собой проверку усвоения учебного материала теоретического и практического характера, регулярно осуществляемую на занятиях.

В ходе контрольной работы обучающемуся выдается КИМ с практическим перечнем заданий и предлагается решить данные задания. В ходе выполнения заданий можно пользоваться методичкой, нельзя пользоваться интернетом, ограничение по времени – 90 минут.

20.2 Промежуточная аттестация Промежуточная аттестация по дисциплине осуществляется с помощью следующих оценочных средств:

Собеседование по билетам к зачету

Собеседование по экзаменационным билетам

Перечень вопросов к экзамену:

1. Понятие защищенной информационной системы.
2. Свойства защищенной ОС.
3. Безопасность информационных систем в нормативных документах.
4. Классификация защищенности ОС по международным стандартам.
5. Политика безопасности, формальное представление политик.
6. Классификация изъянов защиты.
7. Категории изъянов защиты в ОС.
8. Понятие доверенного ПО.
9. Свойство безопасности ОС.
10. Модель безопасности ОС семейства Windows.
11. Контроль доступа к объектам Windows.
12. Проверка доступа. Эффективные права доступа.
13. Шаблоны безопасности.
14. Подсистема аудита ОС Windows.
15. Шифрованная файловая система EFS.
16. Защита данных при передаче. VPN.
17. Контроль целостности в ОС Windows Vista.
18. Механизмы защиты уровня ядра в ОС Windows Vista.

19. Обеспечение безопасности серверных приложений ОС.
20. Сервер IIS. Механизмы защиты.
21. Защита службы DNS.
22. Защита службы RDS.
23. Защита ОС UNIX на этапе загрузки.
24. Шифрование файловых систем в ОС UNIX.
25. Защищенные терминалы.
26. Аутентификация в ОС, реализация в ОС UNIX.
27. Дискреционный контроль доступа в UNIX-системах.
28. Усиление базовой безопасности ОС UNIX.
29. Применение подключаемых модулей аутентификации PAM.
30. Аудит и журналировние событий в UNIX-системах.
31. Фильтрация трафика.
32. Криптографическая защита сетевого взаимодействия.
33. Обеспечение безопасности на уровне приложений.
34. Настройка безопасности сервера Apache.
35. Создание замкнутой среды выполнения.
36. Анализ уязвимостей на примере ОС UNIX.

Владение понятийным аппаратом данной области науки (теоретическими основами дисциплины), способность иллюстрировать ответ примерами, фактами, применять теоретические знания для решения практических задач в области информатики

Промежуточная аттестация, как правило, осуществляется в конце семестра. Результаты текущей аттестации обучающегося по решению кафедры могут быть учтены при проведении промежуточной аттестации. При несогласии студента, ему дается возможность пройти промежуточную аттестацию (без учета его текущих аттестаций) на общих основаниях.

При проведении экзамена учитываются результаты контрольных работ.

Для оценивания результатов обучения на экзамене (зачете с оценкой) используется 4-балльная шала: «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

Критерии оценивания компетенций	Уровень сформированности компетенций	Шкала оценок
Обучающийся в полной мере владеет понятийным аппаратом данной области науки (теоретическими основами дисциплины), способен иллюстрировать ответ примерами, фактами применять теоретические знания для решения практических задач	*Повышенный уровень*	*Отлично*
Обучающийся владеет понятийным аппаратом данной области науки (теоретическими основами дисциплины), способен иллюстрировать ответ примерами, фактами, допускает ошибки при решении практических задачи или способен применять теоретические знания для решения практических задач в области информатики, но допускает неточности при применении понятийного аппарата данной	*Базовый уровень*	*Хорошо*

области науки, но отвечает на дополнительные вопросы		
Обучающийся владеет частично теоретическими основами дисциплины, фрагментарно способен иллюстрировать ответ примерами, фактами, не отвечает на дополнительные вопросы *Не умеет применять теоретические знания для решения практических задач*	*Пороговый уровень*	*Удовлетворительно*
Ответ на контрольно-измерительный материал не соответствует любым трем(четырем) из перечисленных показателей. Обучающийся демонстрирует отрывочные, фрагментарные знания, допускает грубые ошибки	–	*Неудовлетворительно*

20.3 Фонд оценочных средств сформированности компетенций студентов, рекомендуемый для проведения диагностических работ

Закрытый

1. Что такое «Операционная система»? Выберите, какой вариант соответствует этому определению:

1. совокупность специальным образом организованных данных, хранимых в памяти вычислительной системы и отображающих состояние объектов и их взаимосвязей в рассматриваемой предметной области.
2. совокупность взаимосвязанных и согласованно действующих ЭВМ или процессоров и других устройств, обеспечивающих автоматизацию процессов приема, обработки и выдачи информации потребителям.
3. комплекс языковых, математических и программных средств, предназначенных для централизованного создания и ведения и совместного использования БД многими пользователями.
4. подсистема, предназначенная для централизованного хранения информации о структурах данных, взаимосвязях файлов базы данных друг с другом, типах данных и форматах их представления, принадлежности данных пользователям, кодах защиты и разграничения доступа и т.д.
5. комплекс управляющих и обрабатывающих программ, который, с одной стороны, выступает как интерфейс между аппаратурой компьютера и пользователем с его задачами, а с другой – предназначен для наиболее эффективного использования ресурсов вычислительной системы и организации надежных вычислений.

Правильный ответ: 5.

Закрытый

2. Какую функцию НЕ выполняет операционная система:

1. прием и исполнение программных запросов на запуск, приостановку, остановку других программ;
2. распределение памяти, организация виртуальной памяти;

3. управление транзакциями;
4. идентификация всех программ и данных;
5. обслуживание всех операций ввода-вывода.

Правильный ответ: 3.

Решение: Управление транзакциями – это функция СУБД, а не операционной системы

Открытый

3. Как называется выполняемая в операционной системе **программа**, с которой связывается ее адресное пространство, содержащее саму программу, данные к ней, ее стек, а также включающая текущие значения счетчика команд, регистров, переменных?

Правильный ответ: процесс.

Решение: Одним из основных понятий, связанных с операционными системами, является процесс - выполняемая программа, включая текущие значения счетчика команд, регистров и переменных. С каждым процессом связывается его адресное пространство, содержащее саму программу, данные к ней и ее стек. Все функционирующее на компьютере программное обеспечение, включая и операционную систему, можно представить набором процессов.

Закрытый

4. Выберите правильный ответ. Принудительная передача управления от выполняемой программы к системе, происходящая при возникновении определенного события есть:

1. Форматирование
2. Прерывание
3. Кеширование
4. Администрирование
5. Буферизация

Правильный ответ: 2.

Решение: Прерывание — это принудительная передача управления от выполняемой программы к системе (а через нее — к соответствующей программе обработки прерывания), происходящая при возникновении определенного события.

Закрытый

5. Выберите правильный ответ. Как называется такая организацию ввода/вывода, при которой данные не передаются непосредственно с устройства в заданную

область памяти (или из области памяти на устройство), а предварительно направляются во вспомогательную область памяти:

1. Форматирование
2. Прерывание
3. Сохранение контекста процессора
4. Администрирование
5. Буферизация

Правильный ответ: 5.

Решение: Буферизацию можно определить как такую организацию ввода/вывода, при которой данные не передаются непосредственно с устройства в заданную область памяти (или из области памяти на устройство), а предварительно направляются во вспомогательную область памяти, называемую буфером

Открытый

6. Напишите команду, которая изменяет **разрешения доступа** к файлу. Под доступом имеется в виду классическая триада: чтение r, изменение w и запуск x.

Правильный ответ: chmod.

Открытый

6. 7. Напишите команду, которая содержимое файла file1 «помещает» в файл file2

Правильный ответ 1: cp file1 file2

Правильный ответ 2: cat <file1 >file2

Правильный ответ 2: cat <file1>file2

Открытый

13 - 8. Напишите команду, которая для файла file1 устанавливает права на выполнение для всех категорий пользователей (для хозяина, для группы, для всех остальных)

Правильный ответ 1: chmod a+x file1

Правильный ответ 2: chmod ugo+x file1

Правильный ответ 2: chmod 777 file1

Закрытый

9. Выберите, с помощью какой команды возможно вывести первые пять строк файла file1:

1. tail -5 file1
2. head -5 file1
3. cat -5 file1
4. sed -n '5p;5q' file1

Правильный ответ: 2.

Решение: Команда head выводит первые строки файла. Количество выведенных строк задается с помощью после знака «-».

Открытый

15 10. Напишите команду, которая календарь на 2023 год «помещает» в файл file1, причем неделя должна начинаться с понедельника, а не с воскресенья:

Правильный ответ: cal -m 2023 >file1

Правильный ответ: cal -m 2023>file1

Решение: Команда cal выводит календарь на заданный год. Ключ «-m» указывает на то, что каждая неделя должна начинаться с понедельника. Знак «>» указывает на то, чтобы вывод был направлен не на экран, а в файл file1.

Критерии и шкалы оценивания заданий ФОС:

1) Задания закрытого типа (выбор одного варианта ответа, верно/неверно):

- 1 балл – указан верный ответ;
- 0 баллов – указан неверный ответ.

2) Задания закрытого типа (множественный выбор):

- 2 балла – указаны все верные ответы;
- 0 баллов — указан хотя бы один неверный ответ.

3) Задания закрытого типа (на соответствие):

- 2 балла – все соответствия определены верно;
- 0 баллов – хотя бы одно сопоставление определено неверно.

4) Задания открытого типа (короткий текст):

- 2 балла – указан верный ответ;
- 0 баллов – указан неверный ответ.

5) Задания открытого типа (число):

- 2 балла – указан верный ответ;
- 0 баллов – указан неверный ответ.

Задания раздела 20.3 рекомендуются к использованию при проведении диагностических работ с целью оценки остаточных результатов освоения данной дисциплины (знаний, умений, навыков).