МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ СИСТЕМ
УПРАВЛЕНИЯ И РАДИОЭЛЕКТРОНИКИ»
(ТУСУР)

УТВЕРЖДАЮ
Проректор по УР
_____Сенченко П.В.
«22» _____02_____ 2023 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

БЕЗОПАСНОСТЬ ОПЕРАЦИОННЫХ СИСТЕМ

Уровень образования: **высшее образование - бакалавриат**
Направление подготовки / специальность: **10.03.01 Информационная безопасность**
Направленность (профиль) / специализация: **Безопасность автоматизированных систем**
Форма обучения: **очная**
Факультет: **Факультет безопасности (ФБ)**
Кафедра: **Кафедра комплексной информационной безопасности электронно-вычислительных систем (КИБЭВС)**
Курс: **2, 3**
Семестр: **4, 5**
Учебный план набора 2023 года

Объем дисциплины и виды учебной деятельности

Виды учебной деятельности	4 семестр	5 семестр	Всего	Единицы
Лекционные занятия	26	18	44	часов
Практические занятия	12		12	часов
Лабораторные занятия	24	40	64	часов
Самостоятельная работа	46	50	96	часов
Подготовка и сдача экзамена		36	36	часов
Общая трудоемкость (включая промежуточную аттестацию)	108	144	252	часов
	3	4	7	з.е.

Формы промежуточной аттестация	Семестр
Зачет	4
Экзамен	5

Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Сенченко П.В.
Должность: Проректор по УР
Дата подписания: 22.02.2023
Уникальный программный ключ:
a1119608-cdff-4455-b54e-5235117c185c

Томск

Согласована на портале № 72440

1. Общие положения

1.1. Цели дисциплины

1. Целью дисциплины «Безопасность операционных систем» является освоение принципов построения современных операционных систем (ОС) и принципов администрирования подсистемы защиты информации в ОС.

1.2. Задачи дисциплины

1. Получение студентами знаний об устройстве и принципах функционирования ОС различной архитектуры.
2. Получение студентами умений и навыков в области администрирования операционных систем.
3. Получение студентами знаний о методах несанкционированного доступа (НСД) к ресурсам ОС.
4. Получение студентами знаний о структуре подсистемы защиты в ОС.
5. Получение студентами навыков использования средств и методов защиты от НСД к ресурсам ОС.

2. Место дисциплины в структуре ОПОП

Блок дисциплин: Б1. Дисциплины (модули).
Часть блока дисциплин: Обязательная часть.
Модуль дисциплин: Модуль направления подготовки (special hard skills - SHS).
Индекс дисциплины: Б1.О.03.11.
Реализуется с применением электронного обучения, дистанционных образовательных технологий.

3. Перечень планируемых результатов обучения по дисциплине, соотнесенных с индикаторами достижения компетенций

Процесс изучения дисциплины направлен на формирование следующих компетенций в соответствии с ФГОС ВО и основной образовательной программой (таблица 3.1):

Таблица 3.1 – Компетенции и индикаторы их достижения

Компетенция	Индикаторы достижения компетенции	Планируемые результаты обучения по дисциплине
Универсальные компетенции		
-	-	-
Общепрофессиональные компетенции		

Согласована на портале № 72440

ОПК-2. Способен применять информационно-коммуникационные технологии, программные средства системного и прикладного назначения, в том числе отечественного производства, для решения задач профессиональной деятельности	ОПК-2.1. Знает классификацию компьютерных систем, виды информационного взаимодействия и обслуживания, основы построения информационно-вычислительных систем	Знает принципы построения и функционирования, примеры реализаций современных операционных систем.
	ОПК-2.2. Умеет проводить анализ и выбор информационных технологий, программных средств системного и прикладного назначения для решения задач профессиональной деятельности	Умеет планировать политику безопасности операционных систем.
	ОПК-2.3. Владеет навыками использования информационно-коммуникационных технологий и программных средств системного и прикладного назначения для решения задач профессиональной деятельности	Владеет навыками установки и настройки операционных систем семейств UNIX и Windows с учетом требований по обеспечению информационной безопасности.

Согласована на портале № 72440

ОПК-4.2. Способен администрировать операционные системы, системы управления базами данных, вычислительные сети	ОПК-4.2.1. Знает типовые средства, методы и протоколы идентификации, аутентификации и авторизации, а также критерии оценки эффективности и надежности средств защиты программного обеспечения автоматизированных систем	Знает принципы организации и структуру подсистем защиты операционных систем семейств UNIX и Windows.
	ОПК-4.2.2. Умеет создавать, удалять и изменять учетные записи пользователей автоматизированной системы, устанавливать и настраивать операционные системы, системы управления базами данных, компьютерные сети и программные системы с учетом требований по обеспечению защиты информации	Умеет использовать средства операционных систем для обеспечения эффективного и безопасного функционирования автоматизированных систем.
	ОПК-4.2.3. Владеет навыками установки обновлений программного обеспечения автоматизированной системы, а также навыками обнаружения и устранения неисправностей в работе системы защиты информации автоматизированной системы	Владеет навыками работы с операционными системами семейств UNIX и Windows, восстановления операционных систем после сбоев.

Согласована на портале № 72440

ОПК-4.3. Способен выполнять работы по установке, настройке, администрированию, обслуживанию и проверке работоспособности отдельных программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации автоматизированных систем	ОПК-4.3.1. Знает основные меры по защите информации в автоматизированных системах, а также содержание эксплуатационной документации автоматизированной системы	Знает основные штатные средства и средства защиты информации, применяемые для обеспечения безопасности операционных систем.
	ОПК-4.3.2. Умеет устранять выявленные уязвимости автоматизированной системы, приводящие к возникновению угроз безопасности информации, проводить анализ доступных информационных источников с целью выявления известных уязвимостей, используемых в системе защиты информации программных и программно-аппаратных средств	Умеет оценивать эффективность и надежность защиты операционных систем; восстанавливать работу операционных систем после сбоев.
	ОПК-4.3.3. Владеет навыками осуществления автономной наладки технических и программных средств системы защиты информации автоматизированной системы	Владеет 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.

Согласована на портале № 72440

ОПК-4.4. Способен осуществлять диагностику и мониторинг систем защиты автоматизированных систем	ОПК-4.4.1. Знает критерии оценки защищенности автоматизированной системы, технические средства контроля эффективности мер защиты информации	Знает критерии оценки эффективности и надежности средств защиты операционных систем.
	ОПК-4.4.2. Умеет осуществлять контроль обеспечения уровня защищенности в автоматизированных системах, контролировать события безопасности и действия пользователей автоматизированных систем, а также документировать процедуры и результаты контроля функционирования системы защиты информации автоматизированной системы	Умеет оценивать эффективность и надежность защиты операционных систем.
	ОПК-4.4.3. Владеет навыками оценки защищенности автоматизированных систем с помощью типовых программных средств	Владеет навыками проведения аудита защищенности операционных систем с помощью штатных и сторонних средств.

Согласована на портале № 72440

ОПК-9. Способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности	ОПК-9.1. Знает основные понятия криптографии и криптографические методы защиты информации	Знает функции операционных систем, основные концепции управления процессорами, памятью, вспомогательной памятью, устройствами.
	ОПК-9.2. Умеет определять наличие типовых технических каналов утечки информации, а также применять методики расчета и инструментального контроля показателей технической защиты информации на объектах информатизации	Умеет оценивать эффективность и надежность защиты операционных систем.
	ОПК-9.3. Владеет практическими навыками обоснованного выбора и использования СКЗИ при решении задач профессиональной деятельности	Владеет 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.
Профессиональные компетенции		
-	-	-

4. Объем дисциплины в зачетных единицах с указанием количества академических часов, выделенных на контактную работу обучающихся с преподавателем и на самостоятельную работу обучающихся

Общая трудоемкость дисциплины составляет 7 зачетных единиц, 252 академических часов.

Распределение трудоемкости дисциплины по видам учебной деятельности представлено в таблице 4.1.

Таблица 4.1 – Трудоемкость дисциплины по видам учебной деятельности

Виды учебной деятельности	Всего часов	Семестры	
		4 семестр	5 семестр
Контактная аудиторная работа обучающихся с преподавателем, всего	120	62	58
Лекционные занятия	44	26	18
Практические занятия	12	12	
Лабораторные занятия	64	24	40
Самостоятельная работа обучающихся, в т.ч. контактная внеаудиторная работа обучающихся с преподавателем, всего	96	46	50
Подготовка к зачету	13	13	
Подготовка к тестированию	22	12	10
Написание отчета по практическому занятию (семинару)	7	7	
Подготовка к лабораторной работе, написание отчета	52	12	40
Выполнение индивидуального задания	2	2	
Подготовка и сдача экзамена	36		36
Общая трудоемкость (в часах)	252	108	144
Общая трудоемкость (в з.е.)	7	3	4

Согласована на портале № 72440

5. Структура и содержание дисциплины

5.1. Разделы (темы) дисциплины и виды учебной деятельности

Структура дисциплины по разделам (темам) и видам учебной деятельности приведена в таблице 5.1.

Таблица 5.1 – Разделы (темы) дисциплины и виды учебной деятельности

Названия разделов (тем) дисциплины	Лек. зан., ч	Прак. зан., ч	Лаб. раб.	Сам. раб., ч	Всего часов (без экзамена)	Формируемые компетенции
4 семестр						
1 Общая характеристика ОС	4	-	-	4	8	ОПК-2, ОПК-4.2
2 Управление памятью	4	2	-	5	11	ОПК-2, ОПК-4.2, ОПК-4.3
3 Управление устройствами	4	2	-	5	11	ОПК-2, ОПК-4.2
4 Файловые системы	4	2	4	8	18	ОПК-2, ОПК-4.2
5 Управление процессами	4	2	4	7	17	ОПК-2, ОПК-4.2
6 Администрирование ОС	6	4	16	17	43	ОПК-2, ОПК-4.2, ОПК-4.3, ОПК-4.4
Итого за семестр	26	12	24	46	108	
5 семестр						
7 Основные механизмы обеспечения безопасности ОС	2	-	-	2	4	ОПК-2, ОПК-4.3, ОПК-9
8 Средства и методы аутентификации в ОС	6	-	4	6	16	ОПК-2, ОПК-4.2, ОПК-4.3, ОПК-9
9 Разграничение доступа к ресурсам ОС	6	-	24	28	58	ОПК-2, ОПК-4.2, ОПК-4.3, ОПК-4.4, ОПК-9
10 Контроль работы подсистемы защиты	4	-	12	14	30	ОПК-2, ОПК-4.2, ОПК-4.3, ОПК-4.4, ОПК-9
Итого за семестр	18	0	40	50	108	
Итого	44	12	64	96	216	

5.2. Содержание разделов (тем) дисциплины

Содержание разделов (тем) дисциплины (в т.ч. по лекциям) приведено в таблице 5.2.

Таблица 5.2 – Содержание разделов (тем) дисциплины (в т.ч. по лекциям)

Названия разделов (тем) дисциплины	Содержание разделов (тем) дисциплины (в т.ч. по лекциям)	Трудоемкость (лекционные занятия), ч	Формируемые компетенции
4 семестр			
1 Общая характеристика ОС	История развития ОС. Назначение и функции ОС и ее подсистем. Системы разделения времени, пакетной обработки, реального времени. Управление ресурсами. Структура операционной системы. Типы ядра. Интерфейс ОС с пользователями.	4	ОПК-2, ОПК-4.2
	Итого	4	

Согласована на портале № 72440

2 Управление памятью	Типы адресов. Структура виртуального адресного пространства процесса. Виртуальная память. Преобразование адресов. Методы распределения памяти. Защита памяти. Учет свободной и занятой памяти. Алгоритмы выбора вытесняемой страницы. Принципы работы кэш-памяти.	4	ОПК-2, ОПК-4.2, ОПК-4.3
	Итого	4	
3 Управление устройствами	Прерывания в ОС. Структура и функции подсистемы управления устройствами ввода-вывода. Системные сервисы ввода-вывода. Драйверы внешних устройств. Многоуровневые драйверы.	4	ОПК-2, ОПК-4.2
	Итого	4	
4 Файловые системы	Физическая организация файловых систем. Логическая организация файловых систем. Физическая организация файла. Операции с файлами. Функциональные возможности файловых систем.	4	ОПК-2, ОПК-4.2
	Итого	4	
5 Управление процессами	Типы программ, работа со службами. Организация динамических и статических вызовов. Процессы и потоки. Дескрипторы процесса и потока. Сохранение и восстановление процессов и потоков. Планирование потоков. Синхронизация процессов. Тупиковые ситуации. Наследование ресурсов. Межпроцессное взаимодействие.	4	ОПК-2, ОПК-4.2
	Итого	4	
6 Администрирование ОС	Задачи и принципы сопровождения системного программного обеспечения. Настройка, измерение производительности и модификация ОС.	6	ОПК-2, ОПК-4.2
	Итого	6	
	Итого за семестр	26	
	5 семестр		
7 Основные механизмы обеспечения безопасности ОС	Типовые угрозы безопасности ресурсов ОС. Требования к безопасности ОС. Основные группы механизмов защиты ресурсов ОС.	2	ОПК-2, ОПК-4.3, ОПК-9
	Итого	2	

Согласована на портале № 72440

8 Средства и методы аутентификации в ОС	Аутентификация на основе пароля. Аутентификация с использованием физического объекта. Биометрические методы аутентификации. Многофакторная аутентификация. Технология SSO.	6	ОПК-2, ОПК-4.3, ОПК-9
	Итого	6	
9 Разграничение доступа к ресурсам ОС	Классификация субъектов и объектов доступа. Права доступа. Методы разграничения доступа. Разграничение доступа к файловым объектам. Наследование разрешений. Разграничение доступа к устройствам. Ограничения на запуск программного обеспечения.	6	ОПК-2, ОПК-4.3, ОПК-4.4, ОПК-9
	Итого	6	
10 Контроль работы подсистемы защиты	Организация и использование средств аудита. Контроль и восстановление целостности подсистемы защиты и ее параметров. Управление безопасностью ОС.	4	ОПК-2, ОПК-4.4
	Итого	4	
Итого за семестр		18	
Итого		44	

5.3. Практические занятия (семинары)

Наименование практических занятий (семинаров) приведено в таблице 5.3.

Таблица 5.3. – Наименование практических занятий (семинаров)

Названия разделов (тем) дисциплины	Наименование практических занятий (семинаров)	Трудоемкость, ч	Формируемые компетенции
4 семестр			
2 Управление памятью	Моделирование процессов управления памятью	2	ОПК-2, ОПК-4.2
	Итого	2	
3 Управление устройствами	Моделирование процессов управления устройствами	2	ОПК-2, ОПК-4.2
	Итого	2	
4 Файловые системы	Моделирование процессов управления файлами	2	ОПК-2, ОПК-4.2
	Итого	2	
5 Управление процессами	Моделирование процессов управления процессами	2	ОПК-2, ОПК-4.2
	Итого	2	
6 Администрирование ОС	Моделирование процессов администрирования операционной системой на примере Astra Linux	4	ОПК-2, ОПК-4.2, ОПК-4.4
	Итого	4	
Итого за семестр		12	

Согласована на портале № 72440

Итого	12	

5.4. Лабораторные занятия

Наименование лабораторных работ приведено в таблице 5.4.

Таблица 5.4 – Наименование лабораторных работ

Названия разделов (тем) дисциплины	Наименование лабораторных работ	Трудоемкость, ч	Формируемые компетенции
4 семестр			
4 Файловые системы	Управление ресурсами в ОС Windows	4	ОПК-2, ОПК-4.2
	Итого	4	
5 Управление процессами	Управление системными службами и процессами в ОС Windows	4	ОПК-2, ОПК-4.2
	Итого	4	
6 Администрирование ОС	Администрирование ОС Windows	4	ОПК-2, ОПК-4.2
	Администрирование ОС Astra Linux	8	ОПК-2, ОПК-4.2
	Основные механизмы обеспечения безопасности в ОС Astra Linux	4	ОПК-2, ОПК-4.2, ОПК-4.3, ОПК-4.4
	Итого	16	
Итого за семестр		24	
5 семестр			
8 Средства и методы аутентификации в ОС	Двухфакторная аутентификация в операционных системах	4	ОПК-2, ОПК-4.2, ОПК-4.3, ОПК-9
	Итого	4	
9 Разграничение доступа к ресурсам ОС	Дискреционный механизм разграничения доступа к файловым объектам	4	ОПК-2, ОПК-4.2, ОПК-4.4
	Мандатный механизм разграничения доступа к файловым объектам	4	ОПК-2, ОПК-4.2, ОПК-4.3, ОПК-4.4
	Разграничение доступа к устройствам	4	ОПК-2, ОПК-4.2, ОПК-4.4, ОПК-9
	Разграничение доступа к запуску программного обеспечения	4	ОПК-2, ОПК-4.2, ОПК-4.4
	Разграничение доступа к ресурсам в ОС Astra Linux	8	ОПК-2, ОПК-4.2, ОПК-4.3, ОПК-4.4
	Итого	24	
10 Контроль работы подсистемы защиты	Аудит событий безопасности операционной системы	4	ОПК-2, ОПК-4.2, ОПК-4.4
	Анализ, настройка и контроль целостности параметров безопасности подсистемы защиты	4	ОПК-2, ОПК-4.2, ОПК-4.4
	Контроль работы подсистемы защиты в ОС Astra Linux	4	ОПК-2, ОПК-4.3, ОПК-4.4, ОПК-9
	Итого	12	

Согласована на портале № 72440

Итого за семестр	40	
Итого	64	

5.5. Курсовой проект / курсовая работа

Не предусмотрено учебным планом

5.6. Самостоятельная работа

Виды самостоятельной работы, трудоемкость и формируемые компетенции представлены в таблице 5.6.

Таблица 5.6. – Виды самостоятельной работы, трудоемкость и формируемые компетенции

Названия разделов (тем) дисциплины	Виды самостоятельной работы	Трудоемкость, ч	Формируемые компетенции	Формы контроля
4 семестр				
1 Общая характеристика ОС	Подготовка к зачету	2	ОПК-2, ОПК-4.2	Зачёт
	Подготовка к тестированию	2	ОПК-2, ОПК-4.2	Тестирование
	Итого	4		
2 Управление памятью	Подготовка к зачету	2	ОПК-2, ОПК-4.2	Зачёт
	Подготовка к тестированию	2	ОПК-2, ОПК-4.2	Тестирование
	Написание отчета по практическому занятию (семинару)	1	ОПК-2, ОПК-4.2	Отчет по практическому занятию (семинару)
	Итого	5		
3 Управление устройствами	Подготовка к зачету	2	ОПК-2, ОПК-4.2	Зачёт
	Подготовка к тестированию	2	ОПК-2, ОПК-4.2	Тестирование
	Написание отчета по практическому занятию (семинару)	1	ОПК-2, ОПК-4.2	Отчет по практическому занятию (семинару)
	Итого	5		
4 Файловые системы	Подготовка к зачету	2	ОПК-2, ОПК-4.2	Зачёт
	Подготовка к тестированию	2	ОПК-2, ОПК-4.2	Тестирование
	Написание отчета по практическому занятию (семинару)	2	ОПК-2, ОПК-4.2	Отчет по практическому занятию (семинару)
	Подготовка к лабораторной работе, написание отчета	2	ОПК-2, ОПК-4.2	Лабораторная работа
	Итого	8		

Согласована на портале № 72440

5 Управление процессами	Подготовка к зачету	2	ОПК-2, ОПК-4.2	Зачёт
	Подготовка к тестированию	2	ОПК-2, ОПК-4.2	Тестирование
	Написание отчета по практическому занятию (семинару)	1	ОПК-2, ОПК-4.2	Отчет по практическому занятию (семинару)
	Подготовка к лабораторной работе, написание отчета	2	ОПК-2, ОПК-4.2	Лабораторная работа
	Итого	7		
6 Администрирование ОС	Подготовка к зачету	3	ОПК-2, ОПК-4.2, ОПК-4.3, ОПК-4.4	Зачёт
	Выполнение индивидуального задания	2	ОПК-2, ОПК-4.2	Индивидуальное задание
	Подготовка к тестированию	2	ОПК-2, ОПК-4.2, ОПК-4.3, ОПК-4.4	Тестирование
	Написание отчета по практическому занятию (семинару)	2	ОПК-2, ОПК-4.2, ОПК-4.4	Отчет по практическому занятию (семинару)
	Подготовка к лабораторной работе, написание отчета	8	ОПК-2, ОПК-4.2, ОПК-4.3, ОПК-4.4	Лабораторная работа
	Итого	17		
Итого за семестр		46		
5 семестр				
7 Основные механизмы обеспечения безопасности ОС	Подготовка к тестированию	2	ОПК-2, ОПК-4.3, ОПК-9	Тестирование
	Итого	2		
8 Средства и методы аутентификации в ОС	Подготовка к тестированию	2	ОПК-2, ОПК-4.2, ОПК-4.3, ОПК-9	Тестирование
	Подготовка к лабораторной работе, написание отчета	4	ОПК-2, ОПК-4.2, ОПК-4.3, ОПК-9	Лабораторная работа
	Итого	6		

Согласована на портале № 72440

9 Разграничение доступа к ресурсам ОС	Подготовка к тестированию	4	ОПК-2, ОПК-4.2, ОПК-4.3, ОПК-4.4	Тестирование
	Подготовка к лабораторной работе, написание отчета	24	ОПК-2, ОПК-4.2, ОПК-4.3, ОПК-4.4	Лабораторная работа
	Итого	28		
10 Контроль работы подсистемы защиты	Подготовка к тестированию	2	ОПК-2, ОПК-4.3, ОПК-4.4, ОПК-9	Тестирование
	Подготовка к лабораторной работе, написание отчета	12	ОПК-2, ОПК-4.3, ОПК-4.4, ОПК-9	Лабораторная работа
	Итого	14		
Итого за семестр		50		
	Подготовка и сдача экзамена	36		Экзамен
Итого		132		

5.7. Соответствие компетенций, формируемых при изучении дисциплины, и видов учебной деятельности

Соответствие компетенций, формируемых при изучении дисциплины, и видов учебной деятельности представлено в таблице 5.7.

Таблица 5.7 – Соответствие компетенций, формируемых при изучении дисциплины, и видов занятий

Формируемые компетенции	Виды учебной деятельности				Формы контроля
	Лек. зан.	Прак. зан.	Лаб. раб.	Сам. раб.	
ОПК-2	+	+	+	+	Зачёт, Индивидуальное задание, Лабораторная работа, Отчет по практическому занятию (семинару), Тестирование, Экзамен
ОПК-4.2	+	+	+	+	Зачёт, Индивидуальное задание, Лабораторная работа, Отчет по практическому занятию (семинару), Тестирование, Экзамен
ОПК-4.3	+		+	+	Зачёт, Лабораторная работа, Тестирование, Экзамен
ОПК-4.4	+	+	+	+	Зачёт, Лабораторная работа, Отчет по практическому занятию (семинару), Тестирование, Экзамен
ОПК-9	+		+	+	Лабораторная работа, Тестирование, Экзамен

6. Рейтинговая система для оценки успеваемости обучающихся

6.1. Балльные оценки для форм контроля

Балльные оценки для форм контроля представлены в таблице 6.1.

Таблица 6.1 – Балльные оценки

Согласована на портале № 72440

Формы контроля	Максимальный балл на 1-ую КТ с начала семестра	Максимальный балл за период между 1КТ и 2КТ	Максимальный балл за период между 2КТ и на конец семестра	Всего за семестр
4 семестр				
Зачёт	0	0	30	30
Индивидуальное задание	0	0	10	10
Лабораторная работа	5	10	10	25
Тестирование	0	0	10	10
Отчет по практическому занятию (семинару)	5	10	10	25
Итого максимум за период	10	20	70	100
Нарастающим итогом	10	30	100	100
5 семестр				
Лабораторная работа	15	15	20	50
Тестирование	0	0	20	20
Экзамен				30
Итого максимум за период	15	15	40	100
Нарастающим итогом	15	30	70	100

6.2. Пересчет баллов в оценки за текущий контроль

Пересчет баллов в оценки за текущий контроль представлен в таблице 6.2.

Таблица 6.2 – Пересчет баллов в оценки за текущий контроль

Баллы на дату текущего контроля	Оценка
≥ 90% от максимальной суммы баллов на дату ТК	5
От 70% до 89% от максимальной суммы баллов на дату ТК	4
От 60% до 69% от максимальной суммы баллов на дату ТК	3
< 60% от максимальной суммы баллов на дату ТК	2

6.3. Пересчет суммы баллов в традиционную и международную оценку

Пересчет суммы баллов в традиционную и международную оценку представлен в таблице 6.3.

Таблица 6.3 – Пересчет суммы баллов в традиционную и международную оценку

Оценка	Итоговая сумма баллов, учитывает успешно сданный экзамен	Оценка (ECTS)
5 (отлично) (зачтено)	90 – 100	A (отлично)
4 (хорошо) (зачтено)	85 – 89	B (очень хорошо)
	75 – 84	C (хорошо)
	70 – 74	D (удовлетворительно)
3 (удовлетворительно) (зачтено)	65 – 69	
	60 – 64	E (посредственно)
2 (неудовлетворительно) (не зачтено)	Ниже 60 баллов	F (неудовлетворительно)

7. Учебно-методическое и информационное обеспечение дисциплины

7.1. Основная литература

1. Раводин О.М., Раводин В.О. Безопасность операционных систем: Учебное пособие. – 2-е изд., перераб. и доп. – Томск: В-Спектр, 2006. – 226 с. (наличие в библиотеке ТУСУР - 80 экз.).

Согласована на портале № 72440

2. Проскурин, В.Г. Защита в операционных системах [Электронный ресурс] : учеб. пособие — Электрон. дан. — Москва : Горячая линия-Телеком, 2014. — 192 с. [Электронный ресурс]: — Режим доступа: https://e.lanbook.com/book/63241.

3. Мартемьянов, Ю.Ф. Операционные системы. Концепции построения и обеспечения безопасности [Электронный ресурс] : учеб. пособие / Ю.Ф. Мартемьянов, А.В. Яковлев, А.В. Яковлев. — Электрон. дан. — Москва : Горячая линия-Телеком, 2011. — 332 с. [Электронный ресурс]: — Режим доступа: https://e.lanbook.com/book/5176.

7.2. Дополнительная литература

1. Беленькая, М.Н. Администрирование в информационных системах [Электронный ресурс] : учеб. пособие / М.Н. Беленькая, С.Т. Малиновский, Н.В. Яковенко. — Электрон. дан. — Москва : Горячая линия-Телеком, 2011. — 400 с. [Электронный ресурс]: — Режим доступа: https://e.lanbook.com/book/5117.

7.3. Учебно-методические пособия

7.3.1. Обязательные учебно-методические пособия

1. Конев А.А., Якимук А.Ю. Безопасность операционных систем: лабораторный практикум. Ч. 1. – Томск: В-Спектр, 2017. – 118 с. [Электронный ресурс]: — Режим доступа: https://disk.fb.tusur.ru/bos_/laboratory_work_1.pdf.

2. Конев А.А., Якимук А.Ю. Безопасность операционных систем: лабораторный практикум. Ч. 2. – Томск: В-Спектр, 2017. – 132 с. [Электронный ресурс]: — Режим доступа: https://disk.fb.tusur.ru/bos_/laboratory_work_2.pdf.

3. Конев А.А., Якимук А.Ю. Безопасность операционных систем: методические указания по выполнению практических работ. – Томск: В-Спектр, 2017. [Электронный ресурс]: — Режим доступа: https://disk.fb.tusur.ru/bos_/practice.pdf.

4. Конев А.А., Якимук А.Ю. Безопасность операционных систем: практикум для самостоятельной работы. – Томск: В-Спектр, 2017. [Электронный ресурс]: — Режим доступа: https://disk.fb.tusur.ru/bos_/independent_work.pdf.

7.3.2. Учебно-методические пособия для лиц с ограниченными возможностями здоровья и инвалидов

Учебно-методические материалы для самостоятельной и аудиторной работы обучающихся из числа лиц с ограниченными возможностями здоровья и инвалидов предоставляются в формах, адаптированных к ограничениям их здоровья и восприятия информации.

Для лиц с нарушениями зрения:

– в форме электронного документа;

– в печатной форме увеличенным шрифтом.

Для лиц с нарушениями слуха:

– в форме электронного документа;

– в печатной форме.

Для лиц с нарушениями опорно-двигательного аппарата:

– в форме электронного документа;

– в печатной форме.

7.4. Современные профессиональные базы данных и информационные справочные системы

1. При изучении дисциплины рекомендуется обращаться к современным базам данных, информационно-справочным и поисковым системам, к которым у ТУСУРа открыт доступ: https://lib.tusur.ru/ru/resursy/bazy-dannyh.

8. Материально-техническое и программное обеспечение дисциплины

8.1. Материально-техническое и программное обеспечение для лекционных занятий

Для проведения занятий лекционного типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации используется учебная аудитория с достаточным количеством посадочных мест для учебной группы, оборудованная доской и стандартной учебной

Согласована на портале № 72440

мебелью. Имеются мультимедийное оборудование и учебно-наглядные пособия, обеспечивающие тематические иллюстрации по лекционным разделам дисциплины.

8.2. Материально-техническое и программное обеспечение для практических занятий

Аудитория Интернет-технологий и информационно-аналитической деятельности: учебная аудитория для проведения занятий лекционного типа, учебная аудитория для проведения занятий практического типа, учебная аудитория для проведения занятий лабораторного типа; 634045, Томская область, г. Томск, ул. Красноармейская, д. 146, 402 ауд.

Описание имеющегося оборудования:

- Интерактивная доска IQBoard DVT TN100;
- Проектор Optoma EH400;
- Веб-камера Logitech C920s;
- Акустическая система Yamaha;
- Комплект беспроводных микрофонов Clevermic;
- Магнитно-маркерная доска;
- Комплект специализированной учебной мебели;
- Рабочее место преподавателя.

Программное обеспечение:

- Microsoft Windows 10;
- VirtualBox;

8.3. Материально-техническое и программное обеспечение для лабораторных работ

Аудитория Интернет-технологий и информационно-аналитической деятельности: учебная аудитория для проведения занятий лекционного типа, учебная аудитория для проведения занятий практического типа, учебная аудитория для проведения занятий лабораторного типа; 634045, Томская область, г. Томск, ул. Красноармейская, д. 146, 402 ауд.

Описание имеющегося оборудования:

- Интерактивная доска IQBoard DVT TN100;
- Проектор Optoma EH400;
- Веб-камера Logitech C920s;
- Акустическая система Yamaha;
- Комплект беспроводных микрофонов Clevermic;
- Магнитно-маркерная доска;
- Комплект специализированной учебной мебели;
- Рабочее место преподавателя.

Программное обеспечение:

- Microsoft Windows 10;
- VirtualBox;

8.4. Материально-техническое и программное обеспечение для самостоятельной работы

Для самостоятельной работы используются учебные аудитории (компьютерные классы), расположенные по адресам:

- 634050, Томская область, г. Томск, Ленина проспект, д. 40, 233 ауд.;
- 634045, Томская область, г. Томск, ул. Красноармейская, д. 146, 209 ауд.;
- 634034, Томская область, г. Томск, Вершинина улица, д. 47, 126 ауд.;
- 634034, Томская область, г. Томск, Вершинина улица, д. 74, 207 ауд.

Описание имеющегося оборудования:

- учебная мебель;
- компьютеры;
- компьютеры подключены к сети «Интернет» и обеспечивают доступ в электронную информационно-образовательную среду ТУСУРа.

Перечень программного обеспечения:

- Microsoft Windows;
- OpenOffice;

Согласована на портале № 72440

- Kaspersky Endpoint Security 10 для Windows;
- 7-Zip;
- Google Chrome.

8.5. Материально-техническое обеспечение дисциплины для лиц с ограниченными возможностями здоровья и инвалидов

Освоение дисциплины лицами с ограниченными возможностями здоровья и инвалидами осуществляется с использованием средств обучения общего и специального назначения.

При занятиях с обучающимися с **нарушениями слуха** предусмотрено использование звукоусиливающей аппаратуры, мультимедийных средств и других технических средств приема/передачи учебной информации в доступных формах, мобильной системы преподавания для обучающихся с инвалидностью, портативной индукционной системы. Учебная аудитория, в которой занимаются обучающиеся с нарушением слуха, оборудована компьютерной техникой, аудиотехникой, видеотехникой, электронной доской, мультимедийной системой.

При занятиях с обучающимися с **нарушениями зрения** предусмотрено использование в лекционных и учебных аудиториях возможности просмотра удаленных объектов (например, текста на доске или слайда на экране) при помощи видеоувеличителей для комфортного просмотра.

При занятиях с обучающимися с **нарушениями опорно-двигательного аппарата** используются альтернативные устройства ввода информации и другие технические средства приема/передачи учебной информации в доступных формах, мобильной системы обучения для людей с инвалидностью.

9. Оценочные материалы и методические рекомендации по организации изучения дисциплины

9.1. Содержание оценочных материалов для текущего контроля и промежуточной аттестации

Для оценки степени сформированности и уровня освоения закрепленных за дисциплиной компетенций используются оценочные материалы, представленные в таблице 9.1.

Таблица 9.1 – Формы контроля и оценочные материалы

Названия разделов (тем) дисциплины	Формируемые компетенции	Формы контроля	Оценочные материалы (ОМ)
1 Общая характеристика ОС	ОПК-2, ОПК-4.2	Зачёт	Перечень вопросов для зачета
		Тестирование	Примерный перечень тестовых заданий
2 Управление памятью	ОПК-2, ОПК-4.2, ОПК-4.3	Зачёт	Перечень вопросов для зачета
		Тестирование	Примерный перечень тестовых заданий
		Отчет по практическому занятию (семинару)	Темы практических занятий
3 Управление устройствами	ОПК-2, ОПК-4.2	Зачёт	Перечень вопросов для зачета
		Тестирование	Примерный перечень тестовых заданий
		Отчет по практическому занятию (семинару)	Темы практических занятий

Согласована на портале № 72440

4 Файловые системы	ОПК-2, ОПК-4.2	Зачёт	Перечень вопросов для зачета
		Лабораторная работа	Темы лабораторных работ
		Тестирование	Примерный перечень тестовых заданий
		Отчет по практическому занятию (семинару)	Темы практических занятий
5 Управление процессами	ОПК-2, ОПК-4.2	Зачёт	Перечень вопросов для зачета
		Лабораторная работа	Темы лабораторных работ
		Тестирование	Примерный перечень тестовых заданий
		Отчет по практическому занятию (семинару)	Темы практических занятий
6 Администрирование ОС	ОПК-2, ОПК-4.2, ОПК-4.3, ОПК-4.4	Зачёт	Перечень вопросов для зачета
		Индивидуальное задание	Примерный перечень вариантов индивидуальных заданий
		Лабораторная работа	Темы лабораторных работ
		Тестирование	Примерный перечень тестовых заданий
		Отчет по практическому занятию (семинару)	Темы практических занятий
7 Основные механизмы обеспечения безопасности ОС	ОПК-2, ОПК-4.3, ОПК-9	Тестирование	Примерный перечень тестовых заданий
		Экзамен	Перечень экзаменационных вопросов
8 Средства и методы аутентификации в ОС	ОПК-2, ОПК-4.2, ОПК-4.3, ОПК-9	Лабораторная работа	Темы лабораторных работ
		Тестирование	Примерный перечень тестовых заданий
		Экзамен	Перечень экзаменационных вопросов
9 Разграничение доступа к ресурсам ОС	ОПК-2, ОПК-4.2, ОПК-4.3, ОПК-4.4, ОПК-9	Лабораторная работа	Темы лабораторных работ
		Тестирование	Примерный перечень тестовых заданий
		Экзамен	Перечень экзаменационных вопросов

Согласована на портале № 72440

10 Контроль работы подсистемы защиты	ОПК-2, ОПК-4.2, ОПК-4.3, ОПК-4.4, ОПК-9	Лабораторная работа	Темы лабораторных работ
		Тестирование	Примерный перечень тестовых заданий
		Экзамен	Перечень экзаменационных вопросов

Шкала оценки сформированности отдельных планируемых результатов обучения по дисциплине приведена в таблице 9.2.

Таблица 9.2 – Шкала оценки сформированности планируемых результатов обучения по дисциплине

Оценка	Баллы за ОМ	Формулировка требований к степени сформированности планируемых результатов обучения		
		знать	уметь	владеть
2 (неудовлетворительно)	< 60% от максимальной суммы баллов	отсутствие знаний или фрагментарные знания	отсутствие умений или частично освоенное умение	отсутствие навыков или фрагментарные применение навыков
3 (удовлетворительно)	от 60% до 69% от максимальной суммы баллов	общие, но не структурированные знания	в целом успешно, но не систематически осуществляемое умение	в целом успешное, но не систематическое применение навыков
4 (хорошо)	от 70% до 89% от максимальной суммы баллов	сформированные, но содержащие отдельные проблемы знания	в целом успешное, но содержащие отдельные пробелы умение	в целом успешное, но содержащие отдельные пробелы применение навыков
5 (отлично)	≥ 90% от максимальной суммы баллов	сформированные систематические знания	сформированное умение	успешное и систематическое применение навыков

Шкала комплексной оценки сформированности компетенций приведена в таблице 9.3.

Таблица 9.3 – Шкала комплексной оценки сформированности компетенций

Оценка	Формулировка требований к степени компетенции
2 (неудовлетворительно)	Не имеет необходимых представлений о проверяемом материале или Знать на уровне **ориентирования**, представлений. Обучающийся знает основные признаки или термины изучаемого элемента содержания, их отнесенность к определенной науке, отрасли или объектам, узнает в текстах, изображениях или схемах и знает, к каким источникам нужно обращаться для более детального его усвоения.
3 (удовлетворительно)	Знать и уметь на **репродуктивном** уровне. Обучающихся знает изученный элемент содержания репродуктивно: произвольно воспроизводит свои знания устно, письменно или в демонстрируемых действиях.

Согласована на портале № 72440

4 (хорошо)	Знать, уметь, владеть на **аналитическом** уровне. Зная на репродуктивном уровне, указывать на особенности и взаимосвязи изученных объектов, на их достоинства, ограничения, историю и перспективы развития и особенности для разных объектов усвоения.
5 (отлично)	Знать, уметь, владеть на **системном** уровне. Обучающийся знает изученный элемент содержания системно, произвольно и доказательно воспроизводит свои знания устно, письменно или в демонстрируемых действиях, учитывая и указывая связи и зависимости между этим элементом и другими элементами содержания дисциплины, его значимость в содержании дисциплины.

9.1.1. Примерный перечень тестовых заданий

1. Какое из перечисленных программных средств может применяться для обеспечения двухфакторной аутентификации в операционной системе?
   а) DeviceLock
   б) Process Explorer
   в) JaCarta SecurLogon
   г) Adobe Photoshop
2. Какой фактор аутентификации не применяется в eToken, но встречается в некоторых моделях JaCarta?
   а) Пароль
   в) Физический объект
   б) Биометрия
   г) Все применяются
3. Какая файловая система должна быть на диске, к ресурсам которого необходимо присвоить категорию конфиденциальности в Secret Net?
   а) exFAT
   б) UDF
   в) NTFS
   г) FAT32
4. Какой из параметров не учитывается при внесении устройства в белый список в DeviceLock?
   а) Идентификатор продукта
   б) Идентификатор производителя
   в) Страна изготовитель
   г) Серийный номер
5. Под каким уровнем конфиденциальности необходимо войти в систему администратору, чтобы Secret Net позволила ему изменять параметры операционной системы?
   а) Высший (строго конфиденциально)
   б) Средний (конфиденциально)
   в) Низший (не конфиденциально)
   г) Администратору можно проводить настройки под любым уровнем
6. С помощью чего можно настроить доступность функционала таких приложений как eToken PKI Client для пользователей?
   а) Реестр
   б) Командная строка
   в) Административные шаблоны
   г) Настройки приложения
7. Какая информация не содержится в профиле, создаваемом на eToken для входа в операционную систему?
   а) Домен
   б) Логин
   в) Пин-код
   г) Пароль
8. Какая из моделей разграничения доступа не применяется в Secret Net?

Согласована на портале № 72440

а) Дискреционная модель
б) Мандатная модель
в) Ролевая модель
г) Применяются все перечисленные модели

9. Какую возможность предоставляет использование технологии SSO?
   а) Развитие и продвижение сайта
   б) Безопасное подключение к web-ресурсам
   в) Автоматическая аутентификация в приложениях при подключенном eToken
   г) Передача электронной почты в сети
10. Каким образом предоставить полный доступ для любой клавиатуры, подключенной к системе с установленным запретом доступа к usb-портам в DeviceLock?
    а) Внести клавиатуру в белый список как Unique Device
    б) Внести клавиатуру в белый список как Device Model
    в) Отключить управление доступом к USB HID в настройках безопасности программы
    г) Любой из перечисленных вариантов
11. Какую оснастку необходимо добавить в консоль управления, чтобы провести анализ безопасности операционной системы?
    а) Монитор IP-безопасности
    б) Системный монитор
    в) Анализ и настройка безопасности
    г) Редактор объектов групповой политики
12. Какое действие не фиксируется при аудите системных событий?
    а) Запуск элементов системы безопасности
    б) Отключение элементов системы безопасности
    в) Присвоение привилегий пользователю
    г) Изменение системного времени
13. Какие права предоставляются пользователю при мандатном разграничении доступа в случае, если уровень конфиденциальности файла ниже уровня сеанса пользователя?
    а) Запись
    б) Смена владельца
    в) Чтение
    г) Изменение разрешений
14. Какие события не фиксируются при аудите управления учетными записями?
    а) Создание учетной записи для пользователя
    б) Изменение пароля пользователя
    в) Назначение прав пользователю
    г) Внесение учетной записи в группу
15. Какой вариант развития событий невозможен в случае, если размер журнала событий превысит максимально допустимы?
    а) Будут затираться старые события по мере необходимости
    б) Будет требоваться очищение журнала вручную администратором
    в) Будет прекращен аудит событий
    г) Будет происходить архивация журнала
16. Какой группы настроек нет в шаблоне безопасности?
    а) Файловая система
    б) Системные службы
    в) Политика паролей
    г) Политики учетных записей
17. Что из нижеперечисленного является группой настроек в шаблоне безопасности?
    а) Отладка программ
    б) Создание файла подкачки
    в) Локальные политики
    г) Архивация файлов и каталогов
18. Какого типа результатов анализа параметров безопасности операционной системы не существует?
    а) Элемент определен в базе и в системе, значения совпадают
    б) Элемент определен в базе и в системе, значения не совпадают

Согласована на портале № 72440

в) Элемент отсутствует в базе и в системе
г) Элемент не анализировался

19. Какие типы объектов не могут подвергаться фиксации при аудите доступа к объектам?
    а) Файл
    б) Каталог
    в) Учетная запись
    г) Ключ реестра
20. Какие данные фиксируются при аудите изменения политики
    а) Изменение системного времени
    б) Запуск элементов системы безопасности
    в) Назначение прав пользователя
    г) Отключение элементов системы безопасности
21. В результате какого действия программа, запрещенная правилом хеша, будет запущена?
    а) Программу перенесли в другую папку
    б) Программу переименовали
    в) Программу изменили или заменили на другую версию
    г) Программу разрешили правилом сертификата
22. С помощью какого правила в политике ограниченного использования программ можно запретить запуск любых приложений от одного производителя?
    а) Правилом пути
    б) Правилом хеша
    в) Правилом сертификата
    г) Правилом зон интернета
23. Принцип работы какого разрешения характеризуется возможностью создавать файлы, но невозможностью их изменять или удалять?
    а) Чтение
    б) Чтение и выполнение
    в) Запись
    г) Список содержимого папки
24. Отсутствие настройки по какому параметру может привести к бесполезности параметра «Требовать неповторяемости паролей»?
    а) Максимальный срок действия пароля
    б) Минимальная длина пароля
    в) Минимальный срок действия пароля
    г) Пароль должен отвечать требованиям сложности
25. Чем обусловлено требование неповторяемости паролей?
    а) Пароль не должен повторять логин пользователя
    б) У всех пользователей должны быть разные пароли
    в) Пароль должен отличаться от нескольких предыдущих
    г) В пароле не должно быть одинаковых сегментов
26. Какой из следующих типов архивации позволяет заархивировать те файлы и папки, которые были изменены с момента последней архивации, и при этом не сбросить атрибут «архивный» с этих файлов?
    а) Копирующий
    б) Добавочный
    в) Разностный
    г) Ежедневный
27. Какого права доступа не существует для принтеров?
    а) Управление принтером
    б) Управление документами
    в) Управление печатью
    г) Печать
28. Какая из перечисленных возможностей доступна администратору eToken?
    а) Инициализация eToken
    б) Присвоение имени eToken
    в) Задать новый PIN-код eToken, если пользователь забыл его
    г) Просмотр содержимого eToken

Согласована на портале № 72440

29. Какого типа журнала аудита в DeviceLock не существует?
    а) Журнал событий
    б) Журнал событий и DeviceLock
    в) Журнал теневого копирования
    г) Журнал DeviceLock
30. Какой тип аудита в DeviceLock фиксирует все попытки доступа, которые были заблокированы?
    а) Аудит успеха
    б) Аудит разрешений
    в) Аудит запрета
    г) Аудит отказа

9.1.2. Перечень экзаменационных вопросов

1. Операционная система как расширенная виртуальная машина и как система управления ресурсами. Описание, решаемые задачи.
2. Типы ресурсов вычислительной системы и особенности управления ими.
3. Критерии эффективности работы операционных систем и классификация операционных систем на основе этих критериев.
4. Функциональные подсистемы операционной системы. Основные задачи, решаемые каждой из подсистем.
5. Типы ядра операционной системы. Описание и особенности каждого типа.
6. Подсистема управления памятью. Типы адресов. Виртуальное адресное пространство и его структура. Разделяемая и неразделяемая память.
7. Виртуальная память. Определение, принципы работы, решаемые задачи.
8. Учёт использования памяти. Описание способов учёта.
9. Страничное распределение памяти. Принцип работы, преобразование адресов.
10. Сегментное распределение памяти. Принцип работы, преобразование адресов.
11. Сегментно-страничное распределение памяти. Принцип работы, преобразование адресов.
12. Рабочий набор, его использование для выбора вытесняемой страницы.
13. Кэширование данных. Принципы работы. Согласование данных при кэшировании.
14. Типы и механизм прерываний. Обработчики прерываний. Приоритезация и маскирование прерываний.
15. Структура и функции подсистемы ввода-вывода. Принципы работы диспетчера ввода-вывода и диспетчера Plug’n’Play.
16. Особенности многоуровневого представления драйверов и работы с ними.
17. Логическая структура файловой системы. Атрибуты файлов и способы их хранения.
18. Физическая структура файловой системы. Кластер. Функции главной загрузочной записи.
19. Физическая организация файла с использованием перечня номеров кластеров и экстентов.
20. Дисковые квоты. Резервное копирование.
21. Физическая структура и особенности FAT и NTFS.
22. Физическая структура и особенности s5 и ufs.
23. Организация статических и динамических вызовов в операционной системе.
24. Понятие процесса и потока. Различия в использовании процессов и потоков. Контекст процесса.
25. Создание и уничтожение процессов и потоков. Дескрипторы процессов и потоков.
26. Планирование потоков. Стратегии и дисциплины планирования. Состояния потока.
27. Алгоритмы планирования потоков, основанные на квантовании.
28. Алгоритмы планирования потоков, основанные на приоритетах.
29. Смешанные алгоритмы планирования потоков.
30. Наследование ресурсов. Преимущества и недостатки различных вариантов наследования.
31. Способы межпроцессного обмена сообщениями. Принципы работы именованных и неименованных каналов. Принципы работы сигналов.
32. Синхронизация процессов и потоков. Решаемые задачи. Используемые средства. Критические области.
33. Семафоры, мьютексы.
34. Тупиковые ситуации. Определение, условия возникновения. Стратегии, используемые относительно взаимоблокировок.

Согласована на портале № 72440

35. Измерение и контроль производительности операционных систем.
36. Реестр. Чтение и изменение реестра. Логическая структура реестра. Назначение основных разделов. Физическая структура реестра.
37. Основные группы механизмов защиты операционных систем; основные функции этих механизмов.
38. Процедуры идентификации, аутентификации, авторизации. Определение, принцип действия.
39. Функции аутентификации по контролю доступа при работе с ОС и при настройке ОС.
40. Факторы аутентификации – определение, типы, примеры. Многофакторная аутентификация – определение, примеры.
41. Аутентификация с использованием паролей. Принцип действия, варианты реализации, недостатки.
42. Угрозы преодоления парольной защиты. Требования к паролям для увеличения их стойкости.
43. Аутентификация при помощи физического объекта. Принцип действия, варианты реализации, недостатки.
44. Технология однократного входа (SSO – Single Sign-on). Принцип действия, преимущества и недостатки. Применение физического объекта в технологии SSO.
45. Аутентификация при помощи биометрических систем. Принцип действия, варианты реализации, недостатки.
46. Методы биометрической аутентификации.
47. Принципы дискреционного управления доступом. Преимущества и недостатки дискреционной модели.
48. Реализация дискреционного механизма управления доступом в Windows и UNIX системах.
49. Принципы мандатного управления доступом. Преимущества и недостатки мандатной модели.
50. Основные права доступа к файловым объектам в ОС Windows.
51. Владелец файла и его возможности. Подходы к назначению владельца файла.
52. Классификация субъектов и объектов доступа.
53. Правила наследования прав доступа к иерархическим объектам в ОС Windows. Приоритеты правил наследования.
54. Способы обеспечения замкнутости программной среды. Достоинства и недостатки этих методов.
55. Уровни безопасности и правила политики ограниченного использования программ в ОС Windows. Приоритеты использования правил.
56. Способы разграничения доступа к устройствам. Типы прав доступа к устройствам.
57. Белый список устройств и способы его применения.
58. Аудит в операционных системах. Задачи аудита.
59. События, подвергаемые аудиту в ОС Windows. Данные, фиксируемые при аудите.
60. Задачи, решаемые с использованием оснастки «Анализ и настройка безопасности» в Windows

9.1.3. Перечень вопросов для зачета

1. История развития операционных систем. Факторы, влиявшие на развитие операционных систем на различных этапах их развития.
2. Общий подход к структуре операционных систем.
3. Операционная система как расширенная виртуальная машина и как система управления ресурсами. Описание, решаемые задачи.
4. Типы ресурсов вычислительной системы и особенности управления ими.
5. Классификация операционных систем в зависимости от особенностей управления процессорами.
6. Критерии эффективности работы операционных систем и классификация операционных систем на основе этих критериев.
7. Функциональные подсистемы операционной системы. Основные задачи, решаемые каждой из подсистем.
8. Многослойная структура ядра операционной системы. Основные особенности различных

Согласована на портале № 72440

уровней.
9. Типы ядра операционной системы. Описание и особенности каждого типа.
10. Подсистема управления памятью. Решаемые задачи. Типы адресов. Виртуальное адресное пространство и его структура. Разделяемая и неразделяемая память.
11. Виртуальная память. Определение, принципы работы, решаемые задачи.
12. Учёт использования памяти. Описание способов учёта.
13. Классификация алгоритмов распределения памяти. Описание разрывного и неразрывного распределения.
14. Страничное распределение памяти. Принцип работы, преобразование адресов.
15. Сегментное распределение памяти. Принцип работы, преобразование адресов.
16. Сегментно-страничное распределение памяти. Принцип работы, преобразование адресов.
17. Алгоритмы выбора страницы, вытесняемой во внешнюю память.
18. Рабочий набор, его использование для выбора вытесняемой страницы.
19. Кэширование данных. Принципы работы. Согласование данных при кэшировании.
20. Типы и механизм прерываний. Обработчики прерываний.
21. Приоритезация и маскирование прерываний.
22. Диспетчер прерываний. Назначение и принципы работы. Уровни прерываний.
23. Подсистема ввода-вывода. Решаемые задачи. Функции контроллеров ввода-вывода.
24. Структура и функции подсистемы ввода-вывода. Принципы работы диспетчера ввода-вывода и диспетчера Plug’n’Play.
25. Последовательность обработки операционной системой запроса на ввод-вывод.
26. Драйверы. Типы и структура. Работа с драйверами.
27. Особенности многоуровневого представления драйверов и работы с ними.
28. Файловая система. Решаемые задачи, принципы организации.
29. Логическая структура файловой системы. Каталоги. Операции с каталогами.
30. Физическая структура файловой системы. Кластер. Функции главной загрузочной записи.
31. Файлы. Их имена, типы. Атрибуты файлов и способы их хранения.
32. Способы физической организации файла. Их преимущества и недостатки.
33. Физическая организация файла с использованием перечня номеров кластеров и экстентов.
34. Дисковые квоты.
35. Резервное копирование.
36. Шифрование в NTFS.
37. Протоколирование. Структура журнала. Алгоритм восстановления данных.
38. Физическая структура и особенности FAT.
39. Физическая структура и особенности s5 и ufs.
40. Физическая структура и особенности NTFS.
41. Типы программ. Представление образа исполняемой программы в виртуальном адресном пространстве процесса.
42. Организация статических и динамических вызовов в операционной системе.
43. Понятие процесса и потока. Различия в использовании процессов и потоков. Контекст процесса.
44. Создание и уничтожение процессов и потоков. Дескрипторы процессов и потоков.
45. Планирование потоков. Стратегии и дисциплины планирования. Состояния потока.
46. Вытесняющие и невытесняющие алгоритмы планирования. Определение, отличия.
47. Алгоритмы планирования, основанные на квантовании.
48. Алгоритмы планирования, основанные на приоритетах.
49. Смешанные алгоритмы планирования.
50. Наследование ресурсов. Преимущества и недостатки различных вариантов наследования.
51. Способы межпроцессного обмена сообщениями. Принципы работы именованных и неименованных каналов.
52. Способы межпроцессного обмена сообщениями. Принципы работы сигналов.
53. Синхронизация процессов и потоков. Решаемые задачи. Используемые средства.
54. Требования к совместной работе потоков. Критические области.
55. Семафоры, мьютексы.
56. Тупиковые ситуации. Определение, условия возникновения.
57. Стратегии, используемые относительно взаимоблокировок. Алгоритмы обнаружения взаимоблокировок.

Согласована на портале № 72440

58. Средства настройки операционных систем семейства Windows NT.
59. Измерение и контроль производительности операционных систем.
60. Реестр. Чтение и изменение реестра. Логическая структура реестра. Назначение основных разделов. Физическая структура реестра.

9.1.4. Темы практических занятий

1. Моделирование процессов управления памятью
2. Моделирование процессов управления устройствами
3. Моделирование процессов управления файлами
4. Моделирование процессов управления процессами
5. Моделирование процессов администрирования операционной системой на примере Astra Linux

9.1.5. Темы лабораторных работ

1. Управление ресурсами в ОС Windows
2. Управление системными службами и процессами в ОС Windows
3. Администрирование ОС Windows
4. Администрирование ОС Astra Linux
5. Основные механизмы обеспечения безопасности в ОС Astra Linux
6. Двухфакторная аутентификация в операционных системах
7. Дискреционный механизм разграничения доступа к файловым объектам
8. Мандатный механизм разграничения доступа к файловым объектам
9. Разграничение доступа к устройствам
10. Разграничение доступа к запуску программного обеспечения
11. Разграничение доступа к ресурсам в ОС Astra Linux
12. Аудит событий безопасности операционной системы
13. Анализ, настройка и контроль целостности параметров безопасности подсистемы защиты
14. Контроль работы подсистемы защиты в ОС Astra Linux

9.1.6. Примерный перечень вариантов индивидуальных заданий

1. Восстановление работоспособности ОС Windows: восстановление реестра
2. Восстановление работоспособности ОС Windows: восстановление файла boot.ini
3. Восстановление работоспособности ОС Windows: восстановление MBR
4. Восстановление работоспособности ОС Windows: восстановление доступа при утере пароля
5. Восстановление работоспособности ОС Windows: штатные средства восстановления

9.2. Методические рекомендации

Учебный материал излагается в форме, предполагающей самостоятельное мышление студентов, самообразование. При этом самостоятельная работа студентов играет решающую роль в ходе всего учебного процесса.

Начать изучение дисциплины необходимо со знакомства с рабочей программой, списком учебно-методического и программного обеспечения. Самостоятельная работа студента включает работу с учебными материалами, выполнение контрольных мероприятий, предусмотренных учебным планом.

В процессе изучения дисциплины для лучшего освоения материала необходимо регулярно обращаться к рекомендуемой литературе и источникам, указанным в учебных материалах; пользоваться через кабинет студента на сайте Университета образовательными ресурсами электронно-библиотечной системы, а также общедоступными интернет-порталами, содержащими научно-популярные и специализированные материалы, посвященные различным аспектам учебной дисциплины.

При самостоятельном изучении тем следуйте рекомендациям:

– чтение или просмотр материала осуществляйте со скоростью, достаточной для индивидуального понимания и освоения материала, выделяя основные идеи; на основании изученного составить тезисы. Освоив материал, попытаться соотнести теорию с примерами из практики;

Согласована на портале № 72440

– если в тексте встречаются незнакомые или малознакомые термины, следует выяснить их значение для понимания дальнейшего материала;

– осмысливайте прочитанное и изученное, отвечайте на предложенные вопросы.

Студенты могут получать индивидуальные консультации, в т.ч. с использованием средств телекоммуникации.

По дисциплине могут проводиться дополнительные занятия, в т.ч. в форме вебинаров. Расписание вебинаров и записи вебинаров публикуются в электронном курсе / электронном журнале по дисциплине.

9.3. Требования к оценочным материалам для лиц с ограниченными возможностями здоровья и инвалидов

Для лиц с ограниченными возможностями здоровья и инвалидов предусмотрены дополнительные оценочные материалы, перечень которых указан в таблице 9.4.

Таблица 9.4 – Дополнительные материалы оценивания для лиц с ограниченными возможностями здоровья и инвалидов

Категории обучающихся	Виды дополнительных оценочных материалов	Формы контроля и оценки результатов обучения
С нарушениями слуха	Тесты, письменные самостоятельные работы, вопросы к зачету, контрольные работы	Преимущественно письменная проверка
С нарушениями зрения	Собеседование по вопросам к зачету, опрос по терминам	Преимущественно устная проверка (индивидуально)
С нарушениями опорно-двигательного аппарата	Решение дистанционных тестов, контрольные работы, письменные самостоятельные работы, вопросы к зачету	Преимущественно дистанционными методами
С ограничениями по общемедицинским показаниям	Тесты, письменные самостоятельные работы, вопросы к зачету, контрольные работы, устные ответы	Преимущественно проверка методами, определяющимися исходя из состояния обучающегося на момент проверки

9.4. Методические рекомендации по оценочным материалам для лиц с ограниченными возможностями здоровья и инвалидов

Для лиц с ограниченными возможностями здоровья и инвалидов предусматривается доступная форма предоставления заданий оценочных средств, а именно:

– в печатной форме;

– в печатной форме с увеличенным шрифтом;

– в форме электронного документа;

– методом чтения ассистентом задания вслух;

– предоставление задания с использованием сурдоперевода.

Лицам с ограниченными возможностями здоровья и инвалидам увеличивается время на подготовку ответов на контрольные вопросы. Для таких обучающихся предусматривается доступная форма предоставления ответов на задания, а именно:

– письменно на бумаге;

– набор ответов на компьютере;

– набор ответов с использованием услуг ассистента;

– представление ответов устно.

Процедура оценивания результатов обучения лиц с ограниченными возможностями здоровья и инвалидов по дисциплине предусматривает предоставление информации в формах, адаптированных к ограничениям их здоровья и восприятия информации:

Для лиц с нарушениями зрения:

– в форме электронного документа;

– в печатной форме увеличенным шрифтом.

Согласована на портале № 72440

Для лиц с нарушениями слуха:
– в форме электронного документа;
– в печатной форме.
Для лиц с нарушениями опорно-двигательного аппарата:
– в форме электронного документа;
– в печатной форме.

При необходимости для лиц с ограниченными возможностями здоровья и инвалидов процедура оценивания результатов обучения может проводиться в несколько этапов.

Согласована на портале № 72440

ЛИСТ СОГЛАСОВАНИЯ

Рассмотрена и одобрена на заседании кафедры КИБЭВС
протокол № 1 от «24» 1 2023 г.

СОГЛАСОВАНО:

Должность	Инициалы, фамилия	Подпись
Заведующий выпускающей каф. КИБЭВС	А.А. Шелупанов	Согласовано, c53e145e-8b20-45aa-9347-a5e4dbb90e8d
Заведующий обеспечивающей каф. КИБЭВС	А.А. Шелупанов	Согласовано, c53e145e-8b20-45aa-9347-a5e4dbb90e8d
И.О. начальника учебного управления	И.А. Лариошина	Согласовано, c3195437-a02f-4972-a7c6-ab6ee1f21e73

ЭКСПЕРТЫ:

Доцент, каф. КИБЭВС	А.А. Конев	Согласовано, 81687a04-85ce-4835-9e1e-9934a6085fdd
Доцент, каф. КИБЭВС	А.Ю. Якимук	Согласовано, 4ffdf265-fb78-4863-b293-f03438cb07cc

РАЗРАБОТАНО:

Доцент, каф. КИБЭВС	А.Ю. Якимук	Разработано, 4ffdf265-fb78-4863-b293-f03438cb07cc
Доцент, каф. КИБЭВС	А.А. Конев	Разработано, 81687a04-85ce-4835-9e1e-9934a6085fdd

Согласована на портале № 72440