МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

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

УТВЕРЖДАЮ
Директор департамента образования

Документ подписан электронной подписью
Сертификат: 1c6cfa0a-52a6-4f49-aef0-5584d3fd4820
Владелец: Троян Павел Ефимович
Действителен: с 19.01.2016 по 16.09.2019

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Безопасность операционных систем

Уровень образования: **высшее образование - специалитет**
Направление подготовки / специальность: **10.05.03 Информационная безопасность автоматизированных систем**
Направленность (профиль) / специализация: **Информационная безопасность автоматизированных банковских систем**
Форма обучения: **очная**
Факультет: **ФБ, Факультет безопасности**
Кафедра: **КИБЭВС, Кафедра комплексной информационной безопасности электронно-вычислительных систем**
Курс: **2, 3**
Семестр: **4, 5**
Учебный план набора 2013 года

Распределение рабочего времени

№	Виды учебной деятельности	4 семестр	5 семестр	Всего	Единицы
1	Лекции	28	18	46	часов
2	Практические занятия	18	0	18	часов
3	Лабораторные работы	16	36	52	часов
4	Всего аудиторных занятий	62	54	116	часов
5	Из них в интерактивной форме	16	16	32	часов
6	Самостоятельная работа	46	54	100	часов
7	Всего (без экзамена)	108	108	216	часов
8	Подготовка и сдача экзамена	0	36	36	часов
9	Общая трудоемкость	108	144	252	часов
		3.0	4.0	7.0	З.Е.

Зачет: 4 семестр
Экзамен: 5 семестр

Томск 2018

Рассмотрена и одобрена на заседании кафедры
протокол № 6 от « 6 » 5 2018 г.

ЛИСТ СОГЛАСОВАНИЯ

Рабочая программа дисциплины составлена с учетом требований федерального государственного образовательного стандарта высшего образования (ФГОС ВО) по направлению подготовки (специальности) 10.05.03 Информационная безопасность автоматизированных систем, утвержденного 01.12.2016 года, рассмотрена и одобрена на заседании кафедры КИБЭВС «___» _____ 20__ года, протокол №_____.

Разработчики:

Преподаватель кафедры комплексной информационной безопасности электронно-вычислительных систем (КИБЭВС)	_____	А. Ю. Якимук
Доцент кафедры комплексной информационной безопасности электронно-вычислительных систем (КИБЭВС)	_____	А. А. Конев
Заведующий обеспечивающей каф. КИБЭВС	_____	А. А. Шелупанов

Рабочая программа дисциплины согласована с факультетом и выпускающей кафедрой:

Декан ФБ	_____	Е. М. Давыдова
Заведующий выпускающей каф. КИБЭВС	_____	А. А. Шелупанов

Эксперты:

Доцент кафедры комплексной информационной безопасности электронно-вычислительных систем (КИБЭВС)	_____	К. С. Сарин
Доцент кафедры безопасности информационных систем (БИС)	_____	О. О. Евсютин

1. Цели и задачи дисциплины

1.1. Цели дисциплины

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

- Задачи изучения дисциплины – получение студентами:
- – знаний об устройстве и принципах функционирования ОС различной архитектуры;
- – умений и навыков в области администрирования операционных систем;
- – знаний о методах несанкционированного доступа (НСД) к ресурсам ОС;
- – знаний о структуре подсистемы защиты в ОС;
- – навыков использования средств и методов защиты от НСД к ресурсам ОС.

2. Место дисциплины в структуре ОПОП

Дисциплина «Безопасность операционных систем» (Б1.Б.8) относится к блоку 1 (базовая часть).

Предшествующими дисциплинами, формирующими начальные знания, являются: Безопасность операционных систем, Информатика, Организация ЭВМ и вычислительных систем, Основы информационной безопасности, Языки программирования.

Последующими дисциплинами являются: Безопасность операционных систем, Прикладная криптография, Программно-аппаратные средства обеспечения информационной безопасности.

3. Требования к результатам освоения дисциплины

Процесс изучения дисциплины направлен на формирование следующих компетенций:

- ПК-3 способностью проводить анализ защищенности автоматизированных систем;
- ПК-14 способностью проводить контрольные проверки работоспособности применяемых программно-аппаратных, криптографических и технических средств защиты информации;
- ПК-17 способностью проводить инструментальный мониторинг защищенности информации в автоматизированной системе и выявлять каналы утечки информации;
- ПК-26 способностью администрировать подсистему информационной безопасности автоматизированной системы;

В результате изучения дисциплины обучающийся должен:

- **знать** – принципы построения и функционирования, примеры реализаций современных операционных систем; – функции операционных систем, основные концепции управления процессорами, памятью, вспомогательной памятью, устройствами; – критерии оценки эффективности и надежности средств защиты операционных систем; – принципы организации и структуру подсистем защиты операционных систем семейств UNIX и Windows.
- **уметь** – использовать средства операционных систем для обеспечения эффективного и безопасного функционирования автоматизированных систем; – оценивать эффективность и надежность защиты операционных систем; – планировать политику безопасности операционных систем.
- **владеть** – профессиональной терминологией в области информационной безопасности; – навыками работы с операционными системами семейств UNIX и Windows, восстановление операционных систем после сбоев; – навыками установки и настройки операционных систем семейств UNIX и Windows 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. Объем дисциплины и виды учебной работы

Общая трудоемкость дисциплины составляет 7.0 зачетных единицы и представлена в таблице 4.1.

Таблица 4.1 – Трудоемкость дисциплины

Виды учебной деятельности	Всего часов	Семестры	
		4 семестр	5 семестр
Аудиторные занятия (всего)	116	62	54
Лекции	46	28	18
Практические занятия	18	18	0
Лабораторные работы	52	16	36
Из них в интерактивной форме	32	16	16
Самостоятельная работа (всего)	100	46	54
Оформление отчетов по лабораторным работам	52	16	36
Проработка лекционного материала	32	14	18
Подготовка к практическим занятиям, семинарам	16	16	0
Всего (без экзамена)	216	108	108
Подготовка и сдача экзамена	36	0	36
Общая трудоемкость, ч	252	108	144
Зачетные Единицы	7.0	3.0	4.0

5. Содержание дисциплины

5.1. Разделы дисциплины и виды занятий

Разделы дисциплины и виды занятий приведены в таблице 5.1.

Таблица 5.1 – Разделы дисциплины и виды занятий

Названия разделов дисциплины	Лек., ч	Прак. зан., ч	Лаб. раб., ч	Сам. раб., ч	Всего часов (без экзамена)	Формируемые компетенции
4 семестр						
1 Общая характеристика ОС	6	0	0	2	8	ПК-3
2 Управление памятью	4	4	0	6	14	ПК-3
3 Управление устройствами	4	4	0	6	14	ПК-14, ПК-3
4 Файловые системы	4	4	4	6	18	ПК-14, ПК-17, ПК-26
5 Управление процессами	4	4	4	8	20	ПК-14, ПК-17, ПК-26
6 Администрирование ОС	4	0	8	12	24	ПК-14, ПК-26
7 Контрольная работа и обсуждение ее результатов	2	2	0	6	10	ПК-3
Итого за семестр	28	18	16	46	108	
5 семестр						
8 Основные механизмы обеспечения безопасности ОС	2	0	0	2	4	ПК-3
9 Средства и методы аутентификации	4	0	8	12	24	ПК-14, ПК-26

в ОС						
10 Разграничение доступа к ресурсам ОС	6	0	16	20	42	ПК-14, ПК-17, ПК-26
11 Контроль работы подсистемы защиты	4	0	10	12	26	ПК-14, ПК-17, ПК-26
12 Контрольная работа и обсуждение ее результатов	2	0	2	8	12	ПК-3
Итого за семестр	18	0	36	54	108	
Итого	46	18	52	100	216	

5.2. Содержание разделов дисциплины (по лекциям)

Содержание разделов дисциплин (по лекциям) приведено в таблице 5.2.

Таблица 5.2 – Содержание разделов дисциплин (по лекциям)

Названия разделов	Содержание разделов дисциплины (по лекциям)	Трудоемкость, 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.	6	ПК-3
	Итого	6	
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	ПК-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	ПК-3
	Итого	4	
4 Файловые системы	Физическая организация файловых систем. Логическая организация файловых систем. Физическая организация файла. Операции с файлами. Функциональные возможности файловых систем.	4	ПК-26
	Итого	4	
5 Управление процессами	Типы программ, работа со службами. Организация динамических и статических вызовов. Процессы и потоки.	4	ПК-14, ПК-17

	Дескрипторы процесса и потока. Сохранение и восстановление процессов и потоков. Планирование потоков. Синхронизация процессов. Тупиковые ситуации. Наследование ресурсов. Межпроцессное взаимодействие.		
	Итого	4	
6 Администрирование ОС	Задачи и принципы сопровождения системного программного обеспечения. Настройка, измерение производительности и модификация ОС.	4	ПК-26
	Итого	4	
7 Контрольная работа и обсуждение ее результатов	Обсуждение результатов контрольной работы.	2	ПК-3
	Итого	2	
Итого за семестр		28	
5 семестр			
8 Основные механизмы обеспечения безопасности ОС	Типовые угрозы безопасности ресурсов ОС. Требования к безопасности ОС. Основные группы механизмов защиты ресурсов ОС.	2	ПК-3
	Итого	2	
9 Средства и методы аутентификации в ОС	Аутентификация на основе пароля. Аутентификация с использованием физического объекта. Биометрические методы аутентификации. Многофакторная аутентификация. Технология SSO.	4	ПК-14, ПК-26
	Итого	4	
10 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	ПК-14, ПК-26
	Итого	6	
11 Контроль работы подсистемы защиты	Организация и использование средств аудита. Контроль и восстановление целостности подсистемы защиты и ее параметров. Управление безопасностью ОС.	4	ПК-17, ПК-26
	Итого	4	
12 Контрольная работа и обсуждение ее результатов	Обсуждение результатов контрольной работы.	2	ПК-3
	Итого	2	

Итого за семестр		18	
Итого		46	

5.3. Разделы дисциплины и междисциплинарные связи с обеспечивающими (предыдущими) и обеспечиваемыми (последующими) дисциплинами

Разделы дисциплины и междисциплинарные связи с обеспечивающими (предыдущими) и обеспечиваемыми (последующими) дисциплинами представлены в таблице 5.3.

Таблица 5.3 – Разделы дисциплины и междисциплинарные связи

Наименование дисциплин	№ разделов данной дисциплины, для которых необходимо изучение обеспечивающих и обеспечиваемых дисциплин											
	1	2	3	4	5	6	7	8	9	10	11	12
Предшествующие дисциплины												
1 Безопасность операционных систем	+	+	+	+	+	+	+	+	+	+	+	+
2 Информатика	+			+		+						
3 Организация ЭВМ и вычислительных систем		+	+	+								
4 Основы информационной безопасности								+	+	+	+	
5 Языки программирования					+							
Последующие дисциплины												
1 Безопасность операционных систем	+	+	+	+	+	+	+	+	+	+	+	+
2 Прикладная криптография				+		+			+			
3 Программно-аппаратные средства обеспечения информационной безопасности									+	+	+	

5.4. Соответствие компетенций, формируемых при изучении дисциплины, и видов занятий

Соответствие компетенций, формируемых при изучении дисциплины, и видов занятий представлено в таблице 5.4.

Таблица 5.4 – Соответствие компетенций, формируемых при изучении дисциплины, и видов занятий

Компетенции	Виды занятий				Формы контроля
	Лек.	Прак. зан.	Лаб. раб.	Сам. раб.	
ПК-3	+	+	+	+	Контрольная работа, Экзамен, Опрос на занятиях, Зачет, Отчет по практическому занятию

ПК-14	+	+	+	+	Экзамен, Отчет по лабораторной работе, Зачет, Тест, Отчет по практическому занятию
ПК-17	+		+	+	Экзамен, Отчет по лабораторной работе, Зачет, Тест, Отчет по практическому занятию
ПК-26	+		+	+	Экзамен, Отчет по лабораторной работе, Зачет, Тест, Отчет по практическому занятию

6. Интерактивные методы и формы организации обучения

Технологии интерактивного обучения при разных формах занятий приведены в таблице 6.1.

Таблица 6.1 – Технологии интерактивного обучения при разных формах занятий

Методы	Интерактивные практические занятия, ч	Интерактивные лабораторные занятия, ч	Интерактивные лекции, ч	Всего, ч
4 семестр				
IT-методы	4	4		8
Презентации с использованием интерактивной доски с обсуждением			8	8
Итого за семестр:	4	4	8	16
5 семестр				
IT-методы		10		10
Презентации с использованием мультимедиа с обсуждением			6	6
Итого за семестр:	0	10	6	16
Итого	4	14	14	32

7. Лабораторные работы

Наименование лабораторных работ приведено в таблице 7.1.

Таблица 7.1 – Наименование лабораторных работ

Названия разделов	Наименование лабораторных работ	Трудоемкость, ч	Формируемые компетенции
4 семестр			
4 Файловые системы	Управление ресурсами в ОС Windows	4	ПК-14, ПК-17, ПК-26
	Итого	4	
5 Управление процессами	Управление системными службами и процессами в ОС Windows	4	ПК-26
	Итого	4	
6	Администрирование ОС Windows	4	ПК-26

Администрирование ОС	Восстановление ОС Windows	4	
	Итого	8	
Итого за семестр		16	
5 семестр			
9 Средства и методы аутентификации в ОС	Аутентификация в операционных системах при помощи физического объекта	4	ПК-26
	Двухфакторная аутентификация в программном обеспечении на основе технологии SSO	4	
	Итого	8	
10 Разграничение доступа к ресурсам ОС	Дискреционный механизм разграничения доступа к файловым объектам	4	ПК-26
	Мандатный механизм разграничения доступа к файловым объектам	4	
	Разграничение доступа к устройствам	4	
	Разграничение доступа к запуску программного обеспечения	4	
	Итого	16	
11 Контроль работы подсистемы защиты	Аудит событий безопасности операционной системы	4	ПК-17
	Анализ, настройка и контроль целостности параметров безопасности подсистемы защиты	6	
	Итого	10	
12 Контрольная работа и обсуждение ее результатов	Обсуждение результатов контрольной работы по разделам 8-11	2	ПК-3
	Итого	2	
Итого за семестр		36	
Итого		52	

8. Практические занятия (семинары)

Наименование практических занятий (семинаров) приведено в таблице 8.1.

Таблица 8.1 – Наименование практических занятий (семинаров)

Названия разделов	Наименование практических занятий (семинаров)	Трудоемкость, ч	Формируемые компетенции
4 семестр			
2 Управление памятью	Моделирование процессов управления памятью в нотации IDEF0	4	ПК-3
	Итого	4	
3 Управление устройствами	Моделирование процессов управления устройствами в нотации IDEF0	4	ПК-14
	Итого	4	
4 Файловые системы	Моделирование процессов управления	4	ПК-14

	файлами в нотации IDEF0		
	Итого	4	
5 Управление процессами	Моделирование процессов управления процессами в нотации IDEF0	4	ПК-14
	Итого	4	
7 Контрольная работа и обсуждение ее результатов	Проведение контрольной работы по разделам 1-6	2	ПК-3
	Итого	2	
Итого за семестр		18	
Итого		18	

9. Самостоятельная работа

Виды самостоятельной работы, трудоемкость и формируемые компетенции представлены в таблице 9.1.

Таблица 9.1 – Виды самостоятельной работы, трудоемкость и формируемые компетенции

Названия разделов	Виды самостоятельной работы	Трудоемкость, ч	Формируемые компетенции	Формы контроля
4 семестр				
1 Общая характеристика ОС	Проработка лекционного материала	2	ПК-3	Зачет
	Итого	2		
2 Управление памятью	Подготовка к практическим занятиям, семинарам	4	ПК-3	Зачет, Отчет по практическому занятию
	Проработка лекционного материала	2		
	Итого	6		
3 Управление устройствами	Подготовка к практическим занятиям, семинарам	4	ПК-14, ПК-3	Зачет, Отчет по практическому занятию
	Проработка лекционного материала	2		
	Итого	6		
4 Файловые системы	Проработка лекционного материала	2	ПК-26, ПК-14, ПК-17	Зачет, Отчет по лабораторной работе, Тест
	Оформление отчетов по лабораторным работам	4		
	Итого	6		
5 Управление процессами	Подготовка к практическим занятиям, семинарам	2	ПК-17, ПК-14, ПК-26	Зачет, Отчет по лабораторной работе, Отчет по практическому занятию, Тест
	Проработка лекционного материала	2		
	Оформление отчетов	4		

	по лабораторным работам			
	Итого	8		
6 Администрирование ОС	Подготовка к практическим занятиям, семинарам	2	ПК-26, ПК-14	Зачет, Отчет по лабораторной работе, Отчет по практическому занятию, Тест
	Проработка лекционного материала	2		
	Оформление отчетов по лабораторным работам	4		
	Оформление отчетов по лабораторным работам	4		
	Итого	12		
7 Контрольная работа и обсуждение ее результатов	Подготовка к практическим занятиям, семинарам	4	ПК-3	Контрольная работа, Опрос на занятиях
	Проработка лекционного материала	2		
	Итого	6		
Итого за семестр		46		
5 семестр				
8 Основные механизмы обеспечения безопасности ОС	Проработка лекционного материала	2	ПК-3	Экзамен
	Итого	2		
9 Средства и методы аутентификации в ОС	Проработка лекционного материала	4	ПК-26	Отчет по лабораторной работе, Тест, Экзамен
	Оформление отчетов по лабораторным работам	4		
	Оформление отчетов по лабораторным работам	4		
	Итого	12		
10 Разграничение доступа к ресурсам ОС	Проработка лекционного материала	4	ПК-26, ПК-17	Отчет по лабораторной работе, Тест, Экзамен
	Оформление отчетов по лабораторным работам	4		
	Оформление отчетов по лабораторным работам	4		
	Оформление отчетов по лабораторным	4		

	работам			
	Оформление отчетов по лабораторным работам	4		
	Итого	20		
11 Контроль работы подсистемы защиты	Проработка лекционного материала	2	ПК-26, ПК-14, ПК-17	Отчет по лабораторной работе, Тест, Экзамен
	Оформление отчетов по лабораторным работам	4		
	Оформление отчетов по лабораторным работам	6		
	Итого	12		
12 Контрольная работа и обсуждение ее результатов	Проработка лекционного материала	6	ПК-3	Контрольная работа, Опрос на занятиях
	Оформление отчетов по лабораторным работам	2		
	Итого	8		
Итого за семестр		54		
	Подготовка и сдача экзамена	36		Экзамен
Итого		136		

10. Курсовой проект / курсовая работа

Не предусмотрено РУП.

11. Рейтинговая система для оценки успеваемости обучающихся

11.1. Балльные оценки для элементов контроля

Таблица 11.1 – Балльные оценки для элементов контроля

Элементы учебной деятельности	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				
Зачет			30	30
Контрольная работа			10	10
Опрос на занятиях	4	6	6	16
Отчет по лабораторной работе		8	8	16
Отчет по практическому занятию	6	6	6	18
Тест			10	10
Итого максимум за период	10	20	70	100

Нарастающим итогом	10	30	100	100
5 семестр				
Контрольная работа			12	12
Опрос на занятиях	6	4	4	14
Отчет по лабораторной работе	16	8	10	34
Тест			10	10
Итого максимум за период	22	12	36	70
Экзамен				30
Нарастающим итогом	22	34	70	100

11.2. Пересчет баллов в оценки за контрольные точки

Пересчет баллов в оценки за контрольные точки представлен в таблице 11.2.

Таблица 11.2 – Пересчет баллов в оценки за контрольные точки

Баллы на дату контрольной точки	Оценка
≥ 90% от максимальной суммы баллов на дату КТ	5
От 70% до 89% от максимальной суммы баллов на дату КТ	4
От 60% до 69% от максимальной суммы баллов на дату КТ	3
< 60% от максимальной суммы баллов на дату КТ	2

11.3. Пересчет суммы баллов в традиционную и международную оценку

Пересчет суммы баллов в традиционную и международную оценку представлен в таблице 11.3.

Таблица 11.3 – Пересчет суммы баллов в традиционную и международную оценку

Оценка (ГОС)	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)

12. Учебно-методическое и информационное обеспечение дисциплины

12.1. 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.)

2. Проскурин, В.Г. Защита в операционных системах [Электронный ресурс] [Электронный ресурс]: учеб. пособие — Электрон. дан. — Москва : Горячая линия-Телеком, 2014. — 192 с. — Режим доступа: https://e.lanbook.com/book/63241 (дата обращения: 19.05.2018).

3. Мартемьянов, Ю.Ф. Операционные системы. Концепции построения и обеспечения безопасности [Электронный ресурс] [Электронный ресурс]: учеб. пособие / Ю.Ф. Мартемьянов, А.В.

Яковлев, А.В. Яковлев. — Электрон. дан. — Москва : Горячая линия-Телеком, 2011. — 332 с. — Режим доступа: https://e.lanbook.com/book/5176 (дата обращения: 19.05.2018).

12.2. Дополнительная литература

1. Беленькая, М.Н. Администрирование в информационных системах [Электронный ресурс] [Электронный ресурс]: учеб. пособие / М.Н. Беленькая, С.Т. Малиновский, Н.В. Яковенко. — Электрон. дан. — Москва : Горячая линия-Телеком, 2011. — 400 с. — Режим доступа: https://e.lanbook.com/book/5117 (дата обращения: 19.05.2018).

12.3. Учебно-методические пособия

12.3.1. Обязательные учебно-методические пособия

1. Конев А.А., Якимук А.Ю. Безопасность операционных систем [Электронный ресурс]: лабораторный практикум. Ч. 1. – Томск: В-Спектр, 2017. – 118 с. — Режим доступа: http://kibevs.tusur.ru/sites/default/files/files/upload/bezopasnost_operatsionnykh_sistem_-_1.pdf (дата обращения: 19.05.2018).
2. Конев А.А., Якимук А.Ю. Безопасность операционных систем [Электронный ресурс]: лабораторный практикум. Ч. 2. – Томск: В-Спектр, 2017. – 132 с. — Режим доступа: http://kibevs.tusur.ru/sites/default/files/files/upload/bos2-lab.pdf (дата обращения: 19.05.2018).
3. Конев А.А., Якимук А.Ю. Безопасность операционных систем [Электронный ресурс]: методические указания по выполнению практических работ. – Томск: В-Спектр, 2017. — Режим доступа: http://kibevs.tusur.ru/sites/default/files/files/upload/bos-pract.pdf (дата обращения: 19.05.2018).
4. Конев А.А., Якимук А.Ю. Безопасность операционных систем [Электронный ресурс]: практикум для самостоятельной работы. – Томск: В-Спектр, 2017. — Режим доступа: http://kibevs.tusur.ru/sites/default/files/files/upload/bos-samrab.pdf (дата обращения: 19.05.2018).

12.3.2. 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.

12.4. Профессиональные базы данных и информационные справочные системы

1. http://www.elibrary.ru - научная электронная библиотека;
2. http://www.edu.ru - веб-сайт системы федеральных образовательных порталов;
3. http://edu.fb.tusur.ru/ - образовательный портал факультета безопасности;
4. https://fstec.ru/ - Федеральная служба по техническому и экспортному контролю.

12.5. Периодические издания

1. Информация и безопасность [Электронный ресурс]: научный журнал. - Воронеж : ВГТУ . - Журнал выходит с 1998 г. — Режим доступа: https://elibrary.ru/title_about.asp?id=8748 (дата обращения: 19.05.2018).

13. Материально-техническое обеспечение дисциплины и требуемое программное обеспечение

13.1. Общие требования к материально-техническому и программному обеспечению дисциплины

13.1.1. 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 количеством посадочных мест не менее 22-24, оборудованная доской и стандартной учебной мебелью. Имеются демонстрационное оборудование и учебно-наглядные пособия, обеспечивающие тематические иллюстрации по лекционным разделам дисциплины.

13.1.2. Материально-техническое и программное обеспечение для практических занятий

Учебная аудитория

учебная аудитория для проведения занятий практического типа

634045, Томская область, г. Томск, ул. Красноармейская, д. 146, 403 ауд.

Описание имеющегося оборудования:

- Комплект специализированной учебной мебели;
- Рабочее место преподавателя.

Программное обеспечение не требуется.

13.1.3. 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:

- Экран раздвижной;
- Мультимедийный проектор View Sonic PJD5154 DLP;
- Компьютеры AMD A8-5600K/ ASUS A88XM-A/ DDR3 4 Gb/ WD5000AAKX 500 Gb (15 шт.);
- Комплект специализированной учебной мебели;
- Рабочее место преподавателя.

Программное обеспечение:

– Microsoft Windows 10
– VirtualBox

Лаборатория программно-аппаратных средств обеспечения информационной безопасности

учебная аудитория для проведения занятий практического типа, учебная аудитория для проведения занятий лабораторного типа

634045, Томская область, г. Томск, ул. Красноармейская, д. 146, 405 ауд. Описание имеющегося оборудования:

- Компьютеры класса не ниже M/B ASUSTeK S-775 P5B i965 / Core 2 Duo E6300 / DDR-II DIMM 2048 Mb / Sapphire PCI-E Radeon 256 Mb / 160 Gb Seagate (15 шт.);
- Комплект специализированной учебной мебели;
- Рабочее место преподавателя.
- Аппаратные средства аутентификации пользователя «eToken Pro»

Программное обеспечение:

– Microsoft Windows 7 Pro
– VirtualBox
– Антивирусный программный комплекс: Kaspersky endpoint security

13.1.4. 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, 201 ауд.;
- 634034, Томская область, г. Томск, Вершинина улица, д. 47, 126 ауд.;

- 634034, Томская область, г. Томск, Вершинина улица, д. 74, 207 ауд.

Состав оборудования:
- учебная мебель;
- компьютеры класса не ниже ПЭВМ INTEL Celeron D336 2.8ГГц. - 5 шт.;
- компьютеры подключены к сети «Интернет» и обеспечивают доступ в электронную информационно-образовательную среду университета.

Перечень программного обеспечения:
- Microsoft Windows;
- OpenOffice;
- Kaspersky Endpoint Security 10 для Windows;
- 7-Zip;
- Google Chrome.

13.2. 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 зрениями** 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.

14. Оценочные материалы и методические рекомендации по организации изучения дисциплины

14.1. Содержание оценочных материалов и методические рекомендации

Для оценки степени сформированности и уровня освоения закрепленных за дисциплиной компетенций используются оценочные материалы в составе:

14.1.1. Тестовые задания

1. Какая информация не содержится в профиле, создаваемом на eToken для входа в операционную систему?

Домен
Логин
Пин-код
Пароль

2. Какая из моделей разграничения доступа не применяется в Secret Net?

Дискреционная модель
Мандатная модель
Ролевая модель
Применяются все перечисленные модели

3. Какую возможность предоставляет использование технологии SSO?

Развитие и продвижение сайта
Безопасное подключение к web-ресурсам
Автоматическая аутентификация в приложениях при подключенном eToken

Передача электронной почты в сети

4. Какой тип аудита в DeviceLock фиксирует все попытки доступа, которые были заблокированы?

Аудит успеха

Аудит разрешений

Аудит запрета

Аудит отказа

5. Какой из параметров не учитывается при внесении устройства в белый список в DeviceLock?

Идентификатор продукта

Идентификатор производителя

Страна изготовитель

Серийный номер

6. Отсутствие настройки по какому параметру может привести к бесполезности параметра «Требовать неповторяемости паролей»?

Максимальный срок действия пароля

Минимальная длина пароля

Минимальный срок действия пароля

Пароль должен отвечать требованиям сложности

7. Чем обусловлено требование неповторяемости паролей?

Пароль не должен повторять логин пользователя

У всех пользователей должны быть разные пароли

Пароль должен отличаться от нескольких предыдущих

В пароле не должно быть одинаковых сегментов

8. Под каким уровнем конфиденциальности необходимо войти в систему администратору, чтобы Secret Net позволила ему изменять параметры операционной системы?

Высший (строго конфиденциально)

Средний (конфиденциально)

Низший (не конфиденциально)

Администратору можно проводить настройки под любым уровнем

9. С помощью чего можно настроить доступность функционала таких приложений как eToken PKI Client для пользователей?

Реестр

Командная строка

Административные шаблоны

Настройки приложения

10. Каким образом предоставить полный доступ для любой клавиатуры, подключенной к системе с установленным запретом доступа к usb-портам в DeviceLock?

Внести клавиатуру в белый список как Unique Device

Внести клавиатуру в белый список как Device Model

Отключить управление доступом к USB HID в настройках безопасности программы

Любой из перечисленных вариантов

11. В результате какого действия программа, запрещенная правилом хеша, будет запущена?

Программу перенесли в другую папку

Программу переименовали

Программу изменили или заменили на другую версию

Программу разрешили правилом сертификата

12. С помощью какого правила в политике ограниченного использования программ можно запретить запуск любых приложений от одного производителя?

Правилом пути

Правилом хеша

Правилом сертификата

Правилом зон интернета

13. Принцип работы какого разрешения характеризуется возможностью создавать файлы, но

невозможностью их изменять или удалять?

Чтение

Чтение и выполнение

Запись

Список содержимого папки

14. Какие права предоставляются пользователю при мандатном разграничении доступа в случае, если уровень конфиденциальности файла ниже уровня сеанса пользователя?

Запись

Смена владельца

Чтение

Изменение разрешений

15. Какую оснастку необходимо добавить в консоль управления, чтобы провести анализ безопасности операционной системы?

Монитор IP-безопасности

Системный монитор

Анализ и настройка безопасности

Редактор объектов групповой политики

16. Какое действие не фиксируется при аудите системных событий?

Запуск элементов системы безопасности

Отключение элементов системы безопасности

Присвоение привилегий пользователю

Изменение системного времени

17. Какие события не фиксируются при аудите управления учетными записями?

Создание учетной записи для пользователя

Изменение пароля пользователя

Назначение прав пользователю

Внесение учетной записи в группу

18. Какой вариант развития событий невозможен в случае, если размер журнала событий превысит максимально допустимы?

Будут затираться старые события по мере необходимости

Будет требоваться очищение журнала вручную администратором

Будет прекращен аудит событий

Будет происходить архивация журнала

19. Какой группы настроек нет в шаблоне безопасности?

Файловая система

Системные службы

Политика паролей

Политики учетных записей

20. Какого типа результатов анализа параметров безопасности операционной системы не существует?

Элемент определен в базе и в системе, значения совпадают

Элемент определен в базе и в системе, значения не совпадают

Элемент отсутствует в базе и в системе

Элемент не анализировался

21. Какие типы объектов не могут подвергаться фиксации при аудите доступа к объектам?

Файл

Каталог

Учетная запись

Ключ реестра

22. Какие данные фиксируются при аудите изменения политики

Изменение системного времени

Запуск элементов системы безопасности

Назначение прав пользователя

Отключение элементов системы безопасности

23. Какое из перечисленных программных средств может применяться для обеспечения двухфакторной аутентификации в операционной системе?

DeviceLock

Process Explorer

JaCarta SecurLogon

Adobe Photoshop

24. Какой фактор аутентификации не применяется в eToken, но встречается в некоторых моделях JaCarta?

Пароль

Физический объект

Биометрия

Все применяются

25. Какая файловая система должна быть на диске, к ресурсам которого необходимо присвоить категорию конфиденциальности в Secret Net?

exFAT

UDF

NTFS

FAT32

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?

Копирующий

Добавочный

Разностный

Ежедневный

27. Какого права доступа не существует для принтеров?

Управление принтером

Управление документами

Управление печатью

Печать

28. Какая из перечисленных возможностей доступна администратору eToken?

Инициализация eToken

Присвоение имени eToken

Задать новый PIN-код eToken, если пользователь забыл его

Просмотр содержимого eToken

29. Какого типа журнала аудита в DeviceLock не существует?

Журнал событий

Журнал событий и DeviceLock

Журнал теневого копирования

Журнал DeviceLock

30. Что из нижеперечисленного является группой настроек в шаблоне безопасности?

Отладка программ

Создание файла подкачки

Локальные политики

Архивация файлов и каталогов

14.1.2. Экзаменационные вопросы

1. Классификация угроз по способу их осуществления. Классификация объектов угроз.

2. Основные группы механизмов защиты операционных систем; основные функции этих механизмов.

3. Процедуры идентификации, аутентификации, авторизации. Определение, принцип действия.

4. Функции аутентификации по контролю доступа при работе с ОС.

5. Функции аутентификации по контролю доступа при настройке ОС

6. Факторы аутентификации – определение, типы, примеры. Многофакторная

аутентификация – определение, примеры.

7. Аутентификация с использованием паролей. Принцип действия, варианты реализации, недостатки.

8. Угрозы преодоления парольной защиты. Требования к паролям для увеличения их стойкости.

9. Технология однократного входа (SSO – Single Sign-on). Принцип действия, преимущества и недостатки.

10. Аутентификация при помощи физического объекта. Принцип действия, варианты реализации, недостатки.

11. Использование одноразовых паролей для аутентификации при помощи физического объекта.

12. Аутентификация в программном обеспечении при помощи физического объекта.

13. Аутентификация при помощи биометрических систем. Принцип действия, варианты реализации, недостатки.

14. Методы биометрической аутентификации.

15. Задачи механизмов управления доступом.

16. Принципы дискреционного управления доступом. Преимущества и недостатки дискреционной модели.

17. Реализация дискреционного механизма управления доступом в UNIX-системах.

18. Реализация дискреционного механизма управления доступом в Windows-системах.

19. Принципы мандатного управления доступом. Преимущества и недостатки мандатной модели.

20. Совместное использование дискреционного и мандатного механизмов. Преимущества совместного использования.

21. Основные права доступа к файловым объектам в ОС Windows.

22. Дополнительные права доступа к файловым объектам в ОС Windows.

23. Владелец файла и его возможности. Подходы к назначению владельца файла.

24. Классификация субъектов доступа.

25. Классификация объектов доступа.

26. Задачи разграничения доступа к иерархическим объектам. Назначение меток безопасности для иерархических объектов доступа.

27. Правила наследования прав доступа к иерархическим объектам в ОС Windows. Приоритеты правил наследования.

28. Права доступа к элементам реестра и принтерам в ОС Windows.

29. Особенности разграничения доступа при учёте процессов.

30. Способы обеспечения замкнутости программной среды. Достоинства и недостатки этих методов.

31. Уровни безопасности и правила политики ограниченного использования программ в ОС Windows. Приоритеты использования правил.

32. Способы разграничения доступа к устройствам. Типы прав доступа к устройствам.

33. Белый список устройств и способы его применения.

34. Аудит в операционных системах. Задачи аудита.

35. События, подвергаемые аудиту в ОС Windows.

36. Данные о событии, которые могут фиксироваться при ведении аудита.

37. Пассивный и активный аудит. Методы, используемые в системах активного аудита.

38. Ресурсы и параметры работы системы, целостность которых можно контролировать. Этапы контроля целостности.

39. Состав шаблона безопасности в ОС Windows.

40. Задачи, решаемые с использованием оснастки «Анализ и настройка безопасности» в Windows.

14.1.3. Темы опросов на занятиях

Расскажите про правила политики ограниченного использования программ?

Назовите основные группы механизмов защиты операционных систем?

Какие основные функции у этих механизмов?

Какие существуют методы биометрической аутентификации?

14.1.4. Зачёт

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 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.

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.

14.1.5. Темы контрольных работ

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 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.

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.

1. Классификация угроз по способу их осуществления. Классификация объектов угроз.

2. Основные группы механизмов защиты операционных систем; основные функции этих механизмов.

3. Процедуры идентификации, аутентификации, авторизации. Определение, принцип действия.

4. Функции аутентификации по контролю доступа при работе с ОС.

5. Функции аутентификации по контролю доступа при настройке ОС

6. Факторы аутентификации – определение, типы, примеры. Многофакторная аутентификация – определение, примеры.

7. Аутентификация с использованием паролей. Принцип действия, варианты реализации, недостатки.

8. Угрозы преодоления парольной защиты. Требования к паролям для увеличения их стойкости.

9. Технология однократного входа (SSO – Single Sign-on). Принцип действия, преимущества и недостатки.

10. Аутентификация при помощи физического объекта. Принцип действия, варианты реализации, недостатки.

11. Использование одноразовых паролей для аутентификации при помощи физического объекта.

12. Аутентификация в программном обеспечении при помощи физического объекта.

13. Аутентификация при помощи биометрических систем. Принцип действия, варианты реализации, недостатки.

14. Методы биометрической аутентификации.

15. Задачи механизмов управления доступом.

16. Принципы дискреционного управления доступом. Преимущества и недостатки дискреционной модели.

17. Реализация дискреционного механизма управления доступом в UNIX-системах.

18. Реализация дискреционного механизма управления доступом в Windows-системах.

19. Принципы мандатного управления доступом. Преимущества и недостатки мандатной модели.

20. Совместное использование дискреционного и мандатного механизмов. Преимущества совместного использования.

21. Основные права доступа к файловым объектам в ОС Windows.

22. Дополнительные права доступа к файловым объектам в ОС Windows.

23. Владелец файла и его возможности. Подходы к назначению владельца файла.

24. Классификация субъектов доступа.

25. Классификация объектов доступа.

26. Угрозы преодоления политики разграничения доступа к ресурсам.

27. Задачи разграничения доступа к иерархическим объектам. Назначение меток безопасности для иерархических объектов доступа.

28. Правила наследования прав доступа к иерархическим объектам в ОС Windows. Приоритеты правил наследования.

29. Права доступа к элементам реестра и принтерам в ОС Windows.

30. Особенности разграничения доступа при учёте процессов.

31. Способы обеспечения замкнутости программной среды. Достоинства и недостатки этих методов.

32. Уровни безопасности и правила политики ограниченного использования программ в ОС Windows. Приоритеты использования правил.

33. Способы разграничения доступа к устройствам. Типы прав доступа к устройствам.

34. Белый список устройств и способы его применения.

35. Аудит в операционных системах. Задачи аудита.

36. События, подвергаемые аудиту в ОС Windows.

37. Данные о событии, которые могут фиксироваться при ведении аудита.

38. Пассивный и активный аудит. Методы, используемые в системах активного аудита.

39. Состав шаблона безопасности в ОС Windows.

40. Задачи, решаемые с использованием оснастки «Анализ и настройка безопасности» в Windows.

14.1.6. Вопросы для подготовки к практическим занятиям, семинарам

Моделирование процессов управления процессами в нотации IDEF0

Моделирование процессов управления файлами в нотации IDEF0

Моделирование процессов управления памятью в нотации IDEF0

Моделирование процессов управления устройствами в нотации IDEF0

14.1.7. Темы лабораторных работ

Управление ресурсами в ОС Windows

Управление системными службами и процессами в ОС Windows

Администрирование ОС Windows
Восстановление ОС Windows
Аутентификация в операционных системах при помощи физического объекта
Двухфакторная аутентификация в программном обеспечении на основе технологии SSO
Дискреционный механизм разграничения доступа к файловым объектам
Мандатный механизм разграничения доступа к файловым объектам
Разграничение доступа к устройствам
Разграничение доступа к запуску программного обеспечения
Аудит событий безопасности операционной системы
Анализ, настройка и контроль целостности параметров безопасности подсистемы защиты

14.2. 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 14.

Таблица 14 – 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 исходя из состояния обучающегося на момент проверки

14.3. 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.

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.