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: **38.05.01 Экономическая безопасность**
Специализация: **Экономико-правовое обеспечение экономической безопасности**
Направленность (профиль): **Проектная деятельность при обеспечении экономической и информационной безопасности**
Форма обучения: **очная**
Факультет: **ФБ, Факультет безопасности**
Кафедра: **КИБЭВС, Кафедра комплексной информационной безопасности электронно-вычислительных систем**
Курс: **3**
Семестр: **5**
Учебный план набора 2016 года

Распределение рабочего времени

№	Виды учебной деятельности	5 семестр	Всего	Единицы
1	Лекции	18	18	часов
2	Лабораторные работы	32	32	часов
3	Всего аудиторных занятий	50	50	часов
4	Из них в интерактивной форме	20	20	часов
5	Самостоятельная работа	22	22	часов
6	Всего (без экзамена)	72	72	часов
7	Общая трудоемкость	72	72	часов
		2.0	2.0	З.Е.

Зачет: 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) 38.05.01 Экономическая безопасность, утвержденного 16.01.2017 года, рассмотрена и одобрена на заседании кафедры КИБЭВС «___» _____ 20__ года, протокол №_____.

Разработчики:

Преподаватель кафедры КИБЭВС	_____	А. Ю. Якимук
Доцент кафедры 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 КИБЭВС	_____	Е. Ю. Костюченко
Доцент кафедры КИБЭВС	_____	К. С. Сарин

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 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.В.ОД.1) относится к блоку 1 (вариативная часть).

Предшествующими дисциплинами, формирующими начальные знания, являются: Информатика, Операционные системы, Основы информационной безопасности.

3. Требования к результатам освоения дисциплины

Процесс изучения дисциплины направлен на формирование следующих компетенций:

– ПК-20 способностью соблюдать в профессиональной деятельности требования, установленные нормативными правовыми актами в области защиты государственной тайны и информационной безопасности, обеспечивать соблюдение режима секретности;

В результате изучения дисциплины обучающийся должен:

– **знать** − основные виды и угрозы безопасности операционных систем; − защитные механизмы и средства обеспечения безопасности операционных систем.

– **уметь** – использовать средства операционных систем для обеспечения эффективного и безопасного функционирования автоматизированных систем.

– **владеть** − профессиональной терминологией в области информационной безопасности.

4. Объем дисциплины и виды учебной работы

Общая трудоемкость дисциплины составляет 2.0 зачетных единицы и представлена в таблице 4.1.

Таблица 4.1 – Трудоемкость дисциплины

Виды учебной деятельности	Всего часов	Семестры
		5 семестр
Аудиторные занятия (всего)	50	50
Лекции	18	18
Лабораторные работы	32	32
Из них в интерактивной форме	20	20
Самостоятельная работа (всего)	22	22
Подготовка к контрольным работам	2	2
Оформление отчетов по лабораторным работам	12	12
Проработка лекционного материала	8	8
Всего (без экзамена)	72	72
Общая трудоемкость, ч	72	72
Зачетные Единицы	2.0	2.0

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	Лаб. раб., ч	Сам. раб., ч	Всего часов (без экзамена)	Формируемые компетенции
5 семестр					
1 Основные механизмы обеспечения безопасности ОС	2	0	4	6	ПК-20
2 Средства и методы аутентификации в ОС	4	8	6	18	ПК-20
3 Разграничение доступа к ресурсам ОС	6	16	6	28	ПК-20
4 Контроль работы подсистемы защиты	4	8	4	16	ПК-20
5 Контрольная работа и обсуждение ее результатов	2	0	2	4	ПК-20
Итого за семестр	18	32	22	72	
Итого	18	32	22	72	

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
5 семестр			
1 Основные механизмы обеспечения безопасности ОС	Типовые угрозы безопасности ресурсов ОС. Требования к безопасности ОС. Основные группы механизмов защиты ресурсов ОС.	2	ПК-20
	Итого	2	
2 Средства и методы аутентификации в ОС	Аутентификация на основе пароля. Аутентификация с использованием физического объекта. Биометрические методы аутентификации. Многофакторная аутентификация. Технология SSO.	4	ПК-20
	Итого	4	
3 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-20
	Итого	6	
4 Контроль работы подсистемы защиты	Организация и использование средств аудита. Контроль и восстановление целостности подсистемы защиты и ее	4	ПК-20

	параметров. Управление безопасностью ОС.		
	Итого	4	
5 Контрольная работа и обсуждение ее результатов	Обсуждение результатов контрольной работы	2	ПК-20
	Итого	2	
Итого за семестр		18	

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
Предшествующие дисциплины					
1 Информатика			+	+	
2 Операционные системы	+		+	+	
3 Основы 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.	Лаб. раб.	Сам. раб.	
ПК-20	+	+	+	Проверка контрольных работ, Отчет по лабораторной работе, Опрос на занятиях, Зачет, Тест

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 лабораторные занятия, ч	Интерактивные лекции, ч	Всего, ч
5 семестр			
IT-методы	4		4
IT-методы	10		10
Презентации с использованием мультимедиа с обсуждением		6	6
Итого за семестр:	14	6	20
Итого	14	6	20

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
5 семестр			
2 Средства и методы аутентификации в ОС	Аутентификация в операционных системах при помощи физического объекта	4	ПК-20
	Двухфакторная аутентификация в программном обеспечении на основе технологии SSO	4	
	Итого	8	
3 Разграничение доступа к ресурсам ОС	Дискреционный механизм разграничения доступа к файловым объектам	4	ПК-20
	Мандатный механизм разграничения доступа к файловым объектам	4	
	Разграничение доступа к устройствам	4	
	Разграничение доступа к запуску программного обеспечения	4	
	Итого	16	
4 Контроль работы подсистемы защиты	Аудит событий безопасности операционной системы	4	ПК-20
	Анализ, настройка и контроль целостности параметров безопасности подсистемы защиты	4	
	Итого	8	
Итого за семестр		32	

8. Практические занятия (семинары)

Не предусмотрено РУП.

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
5 семестр				
1 Основные механизмы обеспечения безопасности ОС	Проработка лекционного материала	2	ПК-20	Зачет, Отчет по лабораторной работе, Тест
	Оформление отчетов по лабораторным работам	2		
	Итого	4		
2 Средства и методы аутентификации в ОС	Проработка лекционного материала	2	ПК-20	Зачет, Отчет по лабораторной работе, Тест
	Оформление отчетов по лабораторным работам	4		

	Итого	6		
3 Разграничение доступа к ресурсам ОС	Проработка лекционного материала	2	ПК-20	Зачет, Отчет по лабораторной работе, Тест
	Оформление отчетов по лабораторным работам	4		
	Итого	6		
4 Контроль работы подсистемы защиты	Проработка лекционного материала	2	ПК-20	Зачет, Отчет по лабораторной работе, Тест
	Оформление отчетов по лабораторным работам	2		
	Итого	4		
5 Контрольная работа и обсуждение ее результатов	Подготовка к контрольным работам	2	ПК-20	Проверка контрольных работ, Тест
	Итого	2		
Итого за семестр		22		
Итого		22		

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
5 семестр				
Зачет			30	30
Опрос на занятиях	2	2	2	6
Отчет по лабораторной работе	12	16	16	44
Проверка контрольных работ			10	10
Тест			10	10
Итого максимум за период	14	18	68	100
Нарастающим итогом	14	32	100	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. 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).

2. 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 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.);
- Компьютеры: DEPO Neos DF226/ i3-7100/ DDR4 8G/ Жесткий диск 500G/ мышь/ клавиатура/ монитор (6шт.);
- Комплект специализированной учебной мебели;
- Рабочее место преподавателя.

Программное обеспечение:

– Microsoft Windows 10
– VirtualBox

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

DeviceLock
Process Explorer
JaCarta SecurLogon
Adobe Photoshop

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

Пароль
Физический объект
Биометрия
Все применяются

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

exFAT

UDF

NTFS

FAT32

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

Идентификатор продукта

Идентификатор производителя

Страна изготовитель

Серийный номер

5. 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

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

Реестр

Командная строка

Административные шаблоны

Настройки приложения

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

Домен

Логин

Пин-код

Пароль

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

Дискреционная модель

Мандатная модель

Ролевая модель

Применяются все перечисленные модели

9. 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

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. 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

12. Какое действие не фиксируется при аудите системных событий?

Запуск элементов системы безопасности

Отключение элементов системы безопасности
Присвоение привилегий пользователю
Изменение системного времени
13. 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
14. Какие типы объектов не могут подвергаться фиксации при аудите доступа к объектам?
Файл
Каталог
Учетная запись
Ключ реестра
15. 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
16. 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
17. 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
18. 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
19. Какого типа журнала аудита в DeviceLock не существует?
Журнал событий
Журнал событий и DeviceLock
Журнал теневого копирования
Журнал DeviceLock
20. Какой тип аудита в DeviceLock фиксирует все попытки доступа, которые были заблокированы?
Аудит успеха
Аудит разрешений
Аудит запрета
Аудит отказа

14.1.2. Темы контрольных работ

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.

14.1.3. Зачёт

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.

14.1.4. Темы опросов на занятиях

Типовые угрозы безопасности ресурсов ОС. Требования к безопасности ОС. Основные группы механизмов защиты ресурсов ОС.

Аутентификация на основе пароля. Аутентификация с использованием физического объекта. Биометрические методы аутентификации. Многофакторная аутентификация. Технология SSO.

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.

Организация и использование средств аудита. Контроль и восстановление целостности подсистемы защиты и ее параметров. Управление безопасностью ОС.

14.1.5. Темы лабораторных работ

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.