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

Системное администрирование

Уровень образования: **высшее образование - специалитет**
Направление подготовки / специальность: **10.05.04 Информационно-аналитические системы безопасности**
Направленность (профиль) / специализация: **Информационная безопасность финансовых и экономических структур**
Форма обучения: **очная**
Факультет: **ФБ, Факультет безопасности**
Кафедра: **БИС, Кафедра безопасности информационных систем**
Курс: **4**
Семестр: **8**
Учебный план набора 2013 года

Распределение рабочего времени

№	Виды учебной деятельности	8 семестр	Всего	Единицы
1	Лекции	36	36	часов
2	Лабораторные работы	72	72	часов
3	Всего аудиторных занятий	108	108	часов
4	Самостоятельная работа	108	108	часов
5	Всего (без экзамена)	216	216	часов
6	Общая трудоемкость	216	216	часов
		6.0	6.0	З.Е.

Дифференцированный зачет: 8 семестр

Томск 2018

Рассмотрена и одобрена на заседании кафедры
протокол № 6 от « 15 » 5 2018 г.

ЛИСТ СОГЛАСОВАНИЯ

Рабочая программа дисциплины составлена с учетом требований федерального государственного образовательного стандарта высшего образования (ФГОС ВО) по направлению подготовки (специальности) 10.05.04 Информационно-аналитические системы безопасности, утвержденного 01.12.2016 года, рассмотрена и одобрена на заседании кафедры КИБЭВС «___» _____ 20__ года, протокол №_____.

Разработчики:

Преподаватель каф. КИБЭВС	_____	А. Ю. Якимук
Доцент каф. 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. БИС	_____	Р. В. Мещеряков

Эксперты:

Доцент кафедры безопасности информационных систем (БИС)	_____	О. О. Евсютин
Доцент каф. КИБЭВС	_____	К. С. Сарин

1. Цели и задачи дисциплины

1.1. Цели дисциплины

Целью преподавания дисциплины является обучение студентов принципам эксплуатации ЭВС и сетей на уровне системного администрирования.

Объектами изучения являются:

принципы системного администрирования ЭВС и сетей;

аппаратное и программное (включая операционные системы) обеспечение ЭВС с точки зрения автоматизации управления ими.

1.2. Задачи дисциплины

– получение студентами знаний о задачах и нормативно-правовом обеспечении системного администрирования;

– получение студентами умений, связанных с контролем аппаратной и программной конфигурации ЭВС;

– получение студентами знаний о методах и умений по использованию средств автоматизации работы с аппаратным и программным обеспечением ЭВС, в том числе в рамках локальной вычислительной сети

2. Место дисциплины в структуре ОПОП

Дисциплина «Системное администрирование» (Б1.В.ДВ.4.1) относится к блоку 1 (вариативная часть).

Предшествующими дисциплинами, формирующими начальные знания, являются: Безопасность операционных систем, Безопасность сетей ЭВМ, Информатика, Организация ЭВМ и вычислительных систем.

Последующими дисциплинами являются: Безопасность программного обеспечения, Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты, Преддипломная практика.

3. Требования к результатам освоения дисциплины

Процесс изучения дисциплины направлен на формирование следующих компетенций:

– ПК-6 способностью готовить научно-технические отчеты, обзоры, публикации, доклады по результатам выполненных исследований;

В результате изучения дисциплины обучающийся должен:

– **знать** основные задачи и нормативно-правовое обеспечение системного администрирования

– **уметь** осуществлять контроль аппаратной и программной конфигурации ЭВС

– **владеть** навыками обеспечения автоматизации работы с аппаратным и программным обеспечением ЭВС, в том числе в рамках локальной вычислительной сети

4. Объем дисциплины и виды учебной работы

Общая трудоемкость дисциплины составляет 6.0 зачетных единицы и представлена в таблице 4.1.

Таблица 4.1 – Трудоемкость дисциплины

Виды учебной деятельности	Всего часов	Семестры
		8 семестр
Аудиторные занятия (всего)	108	108
Лекции	36	36
Лабораторные работы	72	72
Самостоятельная работа (всего)	108	108
Оформление отчетов по лабораторным работам	64	64
Проработка лекционного материала	10	10

Самостоятельное изучение тем (вопросов) теоретической части курса	14	14
Написание рефератов	20	20
Всего (без экзамена)	216	216
Общая трудоемкость, ч	216	216
Зачетные Единицы	6.0	6.0

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
8 семестр					
1 Основные принципы эксплуатации ЭВС и сетей	6	0	2	8	ПК-6
2 Управление ЭВС и локальными вычислительными сетями	8	20	28	56	ПК-6
3 Эксплуатация аппаратного обеспечения ЭВС	6	12	18	36	ПК-6
4 Эксплуатация операционных систем ЭВС	10	24	28	62	ПК-6
5 Эксплуатация прикладного программного обеспечения ЭВС	6	16	32	54	ПК-6
Итого за семестр	36	72	108	216	
Итого	36	72	108	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
8 семестр			
1 Основные принципы эксплуатации ЭВС и сетей	Основные задачи системного администрирования локальной вычислительной сети. Нормативно-правовая документация в системном администрировании. Типы лицензий на программное обеспечение. Курсы повышения квалификации системных администраторов.	6	ПК-6
	Итого	6	
2 Управление ЭВС и локальными вычислительными	Методы и средства определения аппаратной и программной конфигурации ЭВС. Контроль изменений состава	8	ПК-6

сетями	аппаратного и программного обеспечения ЭВС в рамках локальной вычислительной сети. Удаленный доступ и управление ЭВС. Преимущества виртуализации операционных систем и сетевых сервисов. Методы и средства виртуализации операционных систем и программного обеспечения. Интеграция виртуальных операционных систем и программного обеспечения в локальную вычислительную сеть.		
	Итого	8	
3 Эксплуатация аппаратного обеспечения ЭВС	Методы и средства тестирования быстродействия аппаратного обеспечения ЭВС и передачи данных в локальной вычислительной сети. Методы обеспечения надежности работы ЭВС. Методы и средства контроля и диагностики состояния аппаратного обеспечения ЭВС. Резервирование аппаратного обеспечения и данных. RAID-массивы.	6	ПК-6
	Итого	6	
4 Эксплуатация операционных систем ЭВС	Методы и средства автоматизации установки и настройки операционных систем на локальных ЭВС. Средства резервирования и переноса настроек операционной системы. Методы и средства автоматизации установки и настройки операционных систем на ЭВС, входящих в локальную вычислительную сеть. Методы и средства обновления операционных систем.	10	ПК-6
	Итого	10	
5 Эксплуатация прикладного программного обеспечения ЭВС	Методы и средства автоматизации установки программного обеспечения на ЭВС, входящих в локальную вычислительную сеть. Методы резервирования и переноса настроек программного обеспечения. Методы и средства обновленияпрограммного обеспечения. Средства автоматизации резервирования и синхронизации данных в рамках локальной вычислительной сети.	6	ПК-6
	Итого	6	
Итого за семестр		36	

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 Безопасность операционных систем				+	
2 Безопасность сетей ЭВМ	+	+	+	+	+
3 Информатика	+				
4 Организация ЭВМ и вычислительных систем	+		+	+	
Последующие дисциплины					
1 Безопасность программного обеспечения					+
2 Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты	+	+	+	+	+
3 Преддипломная практика	+	+	+	+	+

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-6	+	+	+	Конспект самоподготовки, Отчет по лабораторной работе, Опрос на занятиях, Тест, Реферат, Дифференцированный зачет

6. Интерактивные методы и формы организации обучения

Не предусмотрено РУП.

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
8 семестр			
2 Управление ЭВС и локальными вычислительными сетями	Инвентаризация аппаратного и программного обеспечения ЭВС, входящих в локальную вычислительную сеть.	8	ПК-6
	Удаленный доступ и управление ЭВС, входящими в локальную вычислительную сеть.	6	

	Виртуализация операционных систем и программного обеспечения.	6	
	Итого	20	
3 Эксплуатация аппаратного обеспечения ЭВС	Тестирование быстродействия аппаратного обеспечения ЭВС.	6	ПК-6
	Контроль и диагностика состояния аппаратного обеспечения	6	
	Итого	12	
4 Эксплуатация операционных систем ЭВС	Автоматизация установки и настройки операционных систем на локальных ЭВС.	8	ПК-6
	Автоматизация установки и настройки операционных систем на ЭВС, входящих в локальную вычислительную сеть.	8	
	Автоматизация обновления операционных систем на ЭВС, входящих в локальную вычислительную сеть.	8	
	Итого	24	
5 Эксплуатация прикладного программного обеспечения ЭВС	Автоматизация установки и обновления программного обеспечения на ЭВС, входящих в локальную вычислительную сеть.	8	ПК-6
	Резервирование настроек программного обеспечения. Автоматизация резервирования и синхронизации данных в рамках локальной вычислительной сети	8	
	Итого	16	
Итого за семестр		72	

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
8 семестр				
1 Основные принципы эксплуатации ЭВС и сетей	Проработка лекционного материала	2	ПК-6	Опрос на занятиях
	Итого	2		
2 Управление ЭВС и локальными вычислительными сетями	Написание рефератов	10	ПК-6	Опрос на занятиях, Отчет по лабораторной работе, Реферат, Тест
	Проработка лекционного материала	2		
	Оформление отчетов по лабораторным работам	16		

	Итого	28		
3 Эксплуатация аппаратного обеспечения ЭВС	Проработка лекционного материала	2	ПК-6	Опрос на занятиях, Отчет по лабораторной работе, Тест
	Оформление отчетов по лабораторным работам	16		
	Итого	18		
4 Эксплуатация операционных систем ЭВС	Написание рефератов	10	ПК-6	Опрос на занятиях, Отчет по лабораторной работе, Реферат, Тест
	Проработка лекционного материала	2		
	Оформление отчетов по лабораторным работам	16		
	Итого	28		
5 Эксплуатация прикладного программного обеспечения ЭВС	Самостоятельное изучение тем (вопросов) теоретической части курса	14	ПК-6	Опрос на занятиях, Отчет по лабораторной работе, Тест
	Проработка лекционного материала	2		
	Оформление отчетов по лабораторным работам	16		
	Итого	32		
Итого за семестр		108		
Итого		108		

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
8 семестр				
Конспект самоподготовки	5	5	5	15
Опрос на занятиях	5	5	5	15
Отчет по лабораторной работе	10	20	20	50
Реферат		5	5	10
Тест			10	10
Итого максимум за период	20	35	45	100
Нарастающим итогом	20	55	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. Компьютерные сети: Принципы, технологии, протоколы : учебное пособие для вузов / В. Г. Олифер, Н. А. Олифер. - 3-е изд. - СПб. : Питер, 2006. - 960 с. (наличие в библиотеке ТУСУР - 92 экз.)

12.2. Дополнительная литература

1. Сетевые операционные системы : Учебник для вузов / Виктор Григорьевич Олифер, Наталия Алексеевна Олифер. - СПб. : Питер, 2002. - 538[6] с. (наличие в библиотеке ТУСУР - 49 экз.)

12.3. Учебно-методические пособия

12.3.1. Обязательные учебно-методические пособия

1. Конев А.А. Системное администрирование [Электронный ресурс]: методические указания по выполнению лабораторных работ. 2017. 136 с. — Режим доступа: http://kibevs.tusur.ru/sites/default/files/files/upload/lab_sa.pdf (дата обращения: 19.05.2018).
2. Конев А.А. Системное администрирование [Электронный ресурс]: темы рефератов и методические указания к самостоятельной работе. 2017. 3 с. — Режим доступа: http://kibevs.tusur.ru/sites/default/files/files/upload/sa_sam.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

Лаборатория безопасности сетей ЭВМ / Лаборатория криптографии в банковском деле

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

634045, Томская область, г. Томск, ул. Красноармейская, д. 146, 804 ауд.

Описание имеющегося оборудования:

- Компьютеры класса не ниже GigaByte GA-F2A68HM-DS2 rev1.0 (RTL) / AMD A4-6300 / DDR-III DIMM 8Gb / SVGARadeon HD 8370D / HDD 1Tb Gb SATA-III Seagate (10 шт.);
- Обучающий стенд локальные компьютерные сети Microtik routerboard (2 шт.);
- ViPNET УМК «Безопасность сетей»;
- Коммутатор Mikrotik CRS125-24G-1S-IN (6 шт.);
- Компьютер класса не ниже i5-7400/8DDR4/SSD120G;
- Анализатор кабельных сетей MI 2016 Multi LAN 350 (3 шт.);
- Анализатор Wi-Fi сетей NETSCOUT AirCheck G2 (2 шт.);
- Сервер класса не ниже 4xE7-4809v4/512GBRE16/L9300-8i/5T6000G7;
- Маршрутизатор Cisco 891-K9 (2 шт.);
- Маршрутизатор Cisco C881-V-K9 (2 шт.);
- Маршрутизатор Check Point CPAP-SG1200R-NGFW (2 шт.);
- Комплект специализированной учебной мебели;
- Рабочее место преподавателя.

Программное обеспечение:

– Cisco Packet Tracer
– Система мониторинга Zabbix

- Kaspersky endpoint security
- Microsoft Windows 10
- XSpider
- Анализатор трафика Wireshark
- Дистрибутив Kali Linux
- Межсетевой экран ИКС Lite
- МежсетевойэкранPositive Technologies Application Firewall Education
- Система анализа защищенности сети MaxPatrol Education
- Система обнаружения вторжений Snort
- Система обнаружения вторжений Suricata
- Средство построения виртуальных частных сетей OpenVPN

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. Какой из методов контроля целостности файлов отсутствует в СЗИ от НСД?

a) Контроль содержимого

b) Контроль атрибутов

c) Контроль санкционированных изменений

d) Контроль существования

2. Для чего предназначена программа оперативного управления в СЗИ от НСД?

a) Для защиты конфиденциальной информации

b) Для идентификации и аутентификации пользователей до загрузки ОС

c) Для централизованного управления защищаемыми компьютерами

d) Для контроля вывода конфиденциальной информации

3. Назовите один из режимов работы программы оперативного управления в СЗИ от НСД?

a) Режим управления защитными механизмами

b) Режим идентификации и аутентификации пользователей

c) Режим мониторинга и оперативного управления

d) Режим аппаратной блокировки защищаемого компьютера

4. Выберите типовые задачи администратора безопасности, для выполнения которых НЕ используется программа оперативного управления СЗИ от НСД в режиме конфигурирования:

a) Редактирование структуры оперативного управления

b) Настройка параметров сбора локальных журналов

c) Контролирование состояния защищенности системы

d) Настройка параметров сетевых соединений

5. Перечислите типовые задачи администратора безопасности, для выполнения которых используется программа оперативного управления в режиме управления.

a) Контролирование и оповещение о произошедших событиях несанкционированного доступа

b) Контролирование текущего состояния защищаемых компьютеров

c) Настройка почтовой рассылки уведомлений о событиях НСД

d) Выполнение действий с защищаемыми компьютерами при возникновении угроз для безопасности системы

6. Для чего необходимо квитирование событий НСД в СЗИ от НСД?

a) Для устранения последствий НСД

b) Для предотвращения НСД в будущем

c) Для фиксации реакции администратора безопасности на событие НСД

d) Для удаления события НСД из журналов аудита

7. Какой из механизмов удаленного управления защищаемым компьютером не реализован в Kaspersky Security Center?

a) Удаленная установка приложений

b) Удаленная перезагрузка защищаемого компьютера

c) Удаленный контроль целостности информации ограниченного доступа

d) Удаленное управление настройками антивируса

8. Какие возможности управления аппаратными идентификаторами eToken НЕ предоставляют средства учета и управления программно-аппаратными СЗИ?

a) Обновление содержимого eToken

b) Обслуживание запросов на разблокировку eToken

c) Извлечение ключей шифрования из памяти eToken

d) Самостоятельная регистрация eToken пользователем на отдельном WEB-сайте

9. Какой из вариантов ответа не относится к возможностям централизованного аудита событий, связанных с информационной безопасностью в локальной сети организации с помощью программы оперативного управления СЗИ от НСД?

a) Контролирование состояния защищенности системы

b) Определение обстоятельств, которые привели к изменению состояния защищенности системы или к НСД

c) Настройка конфигурационных параметров серверов безопасности и агентов

d) Выявление причин произошедших изменений состояния защищенности системы

10. Какой из вариантов ответов не используется для оперативного извещения администратора безопасности о событиях несанкционированного доступа в программе оперативного управления СЗИ от НСД?

a) Визуальное отображение НСД на диаграмме управления

b) Письмо на электронную почту администратору безопасности

c) Уведомление на телефон администратора безопасности по SMS

d) Звуковое уведомление в программе оперативного управления при возникновении НСД

11. Механизм замкнутой программной среды в СЗИ от НСД позволяет удовлетворить следующим мерам защиты информации в государственных информационных системах:

a) Выявление, анализ уязвимостей информационной системы и оперативное устранение вновь выявленных уязвимостей

b) Блокирование сеанса доступа в информационную систему после установленного времени бездействия (неактивности) пользователя или по его запросу

c) Управление запуском (обращениями) компонентов программного обеспечения, в том числе определение запускаемых компонентов, настройка параметров запуска компонентов, контроль

за запуском компонентов программного обеспечения

d) Защита архивных файлов, параметров настройки средств защиты информации и программного обеспечения и иных данных, не подлежащих изменению в процессе обработки информации

12. Для реализации меры защиты информации в государственных информационных системах «Контроль использования интерфейсов ввода (вывода) информации на машинные носители

информации» в СЗИ от НСД следует использовать следующую подсистему:

a) Модуль входа

b) Подсистема контроля целостности

c) Подсистема разграничения доступа к устройствам

d) Замкнутая программная среда

13. Какую из мер защиты информации в государственных информационных системах не позволяет реализовать СЗИ от НСД?

a) Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа

b) Управление запуском (обращениями) компонентов программного обеспечения, в том числе определение запускаемых компонентов, настройка параметров запуска компонентов, контроль

за запуском компонентов программного обеспечения

c) Реализация антивирусной защиты

d) Управление доступом к машинным носителям информации

14. Для реализации меры защиты информации в государственных информационных системах «Мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них» в СЗИ от НСД следует использовать следующую подсистему:

a) Подсистема контроля целостности

b) Подсистема разграничения доступа к устройствам

c) Подсистема оперативного управления

d) Замкнутая программная среда

15. Для чего предназначен механизм контроля подключения и изменения устройств в СЗИ от НСД?

a) Для слежения за неизменностью содержимого ресурсов компьютера

b) Для ограничения использования ПО на компьютере

c) Для обнаружения и реагирования на изменения аппаратной конфигурации компьютера
d) Для централизованного управления защищаемыми компьютерами
16. Для чего предназначен механизм контроля целостности (КЦ) в СЗИ от НСД?
a) Для ограничения использования ПО на компьютере
b) Для обнаружения и реагирования на изменения аппаратной конфигурации компьютера
c) Для централизованного управления защищаемыми компьютерами
d) Для слежения за неизменностью содержимого ресурсов компьютера
17. Для чего предназначен механизм замкнутой программной среды в СЗИ от НСД?
a) Для обнаружения и реагирования на изменения аппаратной конфигурации компьютера
b) Для централизованного управления защищаемыми компьютерами
c) Для слежения за неизменностью содержимого ресурсов компьютера
d) Для ограничения использования ПО на компьютере
18. Назовите режимы для замкнутой программной среды в СЗИ от НСД?
a) Конфиденциальный и секретный
b) Эталонный и полномочный
c) Мягкий и жесткий
d) Дискреционный и мандатный
19. Какая из защитных функций НЕ относится к Kaspersky Security Center?
a) Удаленное управление антивирусными средствами защиты
b) Учет установленного программного обеспечения и поиск в них уязвимостей
c) Разграничение доступа пользователей к информации ограниченного доступа
d) Аудит событий информационной безопасности, происходящих на защищаемых компьютерах в сети организации
20. Какие из перечисленных защитных механизмов в СЗИ от НСД НЕ используются для обеспечения защиты информации ограниченного доступа?
a) Контроль целостности
b) Разграничение доступа к устройствам
c) Идентификация и аутентификация пользователей
d) Полномочное разграничение доступа
21. Согласно приказу ФСТЭК России от 11 февраля 2013 г. N 17 об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, какое из действий НЕ относится к выявлению инцидентов
информационной безопасности и реагированию на них?
a) Определение лиц, ответственных за выявление инцидентов
b) Анализ инцидентов, в том числе определение источников и причин возникновения инцидентов, а также оценка их последствий
c) Определение лиц, которым разрешены действия по внесению изменений в базовую конфигурацию информационной системы и ее системы защиты информации
d) Планирование и принятие мер по предотвращению повторного возникновения инцидентов
22. Согласно приказу ФСТЭК России от 11 февраля 2013 г. N 17 об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, какое из действий относится к контролю (мониторингу) за
обеспечением уровня защищенности информации, содержащейся в информационной системе?
a) Анализ инцидентов, в том числе определение источников и причин возникновения инцидентов, а также оценка их последствий
b) Определение параметров настройки программного обеспечения, включая программное
обеспечение средств защиты информации, состава и конфигурации технических средств и программного обеспечения до внесения изменений в базовую конфигурацию информационной системы и ее системы защиты информации
c) Анализ и оценка функционирования системы защиты информации информационной

системы, включая выявление, анализ и устранение недостатков в функционировании системы защиты информации информационной системы

d) Управление средствами защиты информации в информационной системе, в том числе параметрами настройки программного обеспечения

23. Согласно приказу ФСТЭК России от 11 февраля 2013 г. N 17 об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, к мерам по ограничению программной среды относится высказывание:

a) Должны обеспечивать управление правами и привилегиями субъектов доступа, разграничение доступа субъектов доступа к объектам доступа на основе совокупности установленных в информационной системе правил разграничения доступа, а также обеспечивать контроль соблюдения

этих правил

b) Должны обеспечивать сбор, запись, хранение и защиту информации о событиях безопасности в информационной системе, а также возможность просмотра и анализа информации о таких

событиях и реагирование на них

c) Должны обеспечивать установку и (или) запуск только разрешенного к использованию в

информационной системе программного обеспечения или исключать возможность установки и

(или) запуска запрещенного к использованию в информационной системе программного обеспечения

d) Должны обеспечивать обнаружение в информационной системе компьютерных программ

либо иной компьютерной информации, предназначенной для несанкционированного уничтожения,

блокирования, модификации, копирования компьютерной информации или нейтрализации средств

защиты информации, а также реагирование на обнаружение этих программ и информации

24. Для чего предназначено теневое копирование в СЗИ от НСД?

a) Для накопления информации о событиях, регистрируемых на компьютере средствами системы защиты

b) Для контроля и оповещения о произошедших событиях несанкционированного доступа

c) Для перемещения дубликатов (копий) данных, выводимых на отчуждаемые носители информации

d) Неправильный ответ

25. Для каких устройств НЕ осуществляется теневое копирование в СЗИ от НСД?

a) Принтеры

b) USB-носители

c) Сетевые карты

d) CD-приводы

26. С какой целью может использоваться Kaspersky Security Center в государственных информационных системах?

a) Защита конфиденциальной информации, в том числе персональных данных, а также сведений составляющих государственную и коммерческую тайну

b) Управление жизненным циклом аппаратных аутентификаторов

c) Сбор, обработка и систематизация информации о программном и аппаратном обеспечении, установленном на компьютерах и серверах в локальной вычислительной сети

d) Централизованное решение основных задач по управлению и обслуживанию системы защиты сети организации

14.1.2. Темы опросов на занятиях

Преимущества виртуализации операционных систем и сетевых сервисов

Методы и средства обновления операционных систем

14.1.3. Темы рефератов

Средства удаленного доступа и управления ЭВС в UNIX-подобных операционных системах.

Поддержка RAID-массивов в UNIX-подобных операционных системах

Средства обновления операционных систем в UNIX-подобных операционных системах

14.1.4. Вопросы на самоподготовку

Контроль изменений состава аппаратного и программного обеспечения ЭВС в рамках локальной вычислительной сети UNIX

Средства резервирования и переноса настроек операционной системы UNIX

14.1.5. Вопросы дифференцированного зачета

1. Классификация задач системного администрирования локальной вычислительной сети.
2. Основные нормативные документы, использующиеся в системном администрировании.
3. Типы лицензий на программное обеспечение.
4. Основные направления повышения квалификации системных администраторов.
5. Методы определения аппаратной и программной конфигурации ЭВС.
6. Возможности средств инвентаризации аппаратной и программной конфигурации ЭВС.
7. Способы контроля изменений состава аппаратного и программного обеспечения ЭВС в рамках локальной вычислительной сети.
8. Методы и средства автоматизации контроля работоспособности узлов локальной вычислительной сети.
9. Методы удаленного доступа и управления ЭВС.
10. Программные средства удаленного доступа и управления ЭВС.
11. Программно-аппаратные средства удаленного доступа и управления ЭВС.
12. Методы и средства виртуализации операционных систем и сетевых сервисов. Преимущества и недостатки использования виртуализации в локальной вычислительной сети.
13. Методы и средства тестирования быстродействия аппаратного обеспечения ЭВС.
14. Методы и средства тестирования передачи данных в локальной вычислительной сети.
15. Методы и средства контроля и диагностики состояния аппаратного обеспечения ЭВС.
16. Резервирование аппаратного обеспечения и данных.
17. RAID-массивы. Варианты реализации. Преимущества и недостатки.
18. Методы и средства автоматизации установки и настройки операционных систем на локальных ЭВС и ЭВС, входящих в локальную вычислительную сеть.
19. Технология и средства клонирования операционных систем.
20. Технология и средства создания образа операционной системы.
21. Технология WDS.
22. Встроенные в операционные системы семейства Windows средства резервирования и переноса настроек операционной системы.
23. Сторонние для операционных систем семейства Windows средства резервирования и переноса настроек операционной системы.
24. Методы и средства обновления операционных систем.
25. Возможности WSUS.
26. Методы и средства автоматизации установки программного обеспечения на ЭВС, входящих в локальную вычислительную сеть.
27. Возможности ActiveDirectory в установке программного обеспечения в рамках локальной вычислительной сети
28. Методы резервирования и переноса настроек программного обеспечения.
29. Методы и средства обновления программного обеспечения.
30. Средства автоматизации резервирования и синхронизации данных в рамках локальной вычислительной сети.

14.1.6. Темы лабораторных работ

Инвентаризация аппаратного и программного обеспечения ЭВС, входящих в локальную вычислительную сеть.

Удаленный доступ и управление ЭВС, входящими в локальную вычислительную сеть.

Виртуализация операционных систем и программного обеспечения.

Тестирование быстродействия аппаратного обеспечения ЭВС.

Контроль и диагностика состояния аппаратного обеспечения

Автоматизация установки и настройки операционных систем на локальных ЭВС.

Автоматизация установки и настройки операционных систем на ЭВС, входящих в локальную вычислительную сеть.

Автоматизация обновления операционных систем на ЭВС, входящих в локальную вычислительную сеть.

Автоматизация установки и обновления программного обеспечения на ЭВС, входящих в локальную вычислительную сеть.

Резервирование настроек программного обеспечения. Автоматизация резервирования и синхронизации данных в рамках локальной вычислительной сети

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.