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
_____ П. Е. Троян
«___» _____ 20__ г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Управление средствами защиты информации

Уровень образования: **высшее образование - бакалавриат**
Направление подготовки / специальность: **10.03.01 Информационная безопасность**
Направленность (профиль) / специализация: **Безопасность автоматизированных систем**
Форма обучения: **очная**
Факультет: **ФБ, Факультет безопасности**
Кафедра: **КИБЭВС, Кафедра комплексной информационной безопасности электронно-вычислительных систем**
Курс: **3, 4**
Семестр: **6, 7**
Учебный план набора 2014 года

Распределение рабочего времени

№	Виды учебной деятельности	6 семестр	7 семестр	Всего	Единицы
1	Лекции	18	0	18	часов
2	Лабораторные работы	28	0	28	часов
3	Контроль самостоятельной работы (курсовой проект / курсовая работа)	0	18	18	часов
4	Всего аудиторных занятий	46	18	64	часов
5	Из них в интерактивной форме	14	0	14	часов
6	Самостоятельная работа	26	18	44	часов
7	Всего (без экзамена)	72	36	108	часов
8	Общая трудоемкость	72	36	108	часов
		2.0	1.0	3.0	З.Е.

Зачет: 6 семестр
Курсовой проект / курсовая работа: 7 семестр

Томск 2018

Согласована на портале № 47314

Рассмотрена и одобрена на заседании кафедры
протокол № от «___» _____ 20__ г.

ЛИСТ СОГЛАСОВАНИЯ

Рабочая программа дисциплины составлена с учетом требований федерального государственного образовательного стандарта высшего образования (ФГОС ВО) по направлению подготовки (специальности) 10.03.01 Информационная безопасность, утвержденного 01.12.2016 года, рассмотрена и одобрена на заседании кафедры КИБЭВС «___» _____ 20__ года, протокол №_____.

Разработчики:

Доцент каф. БИС	_____	И. А. Рахманенко
Доцент каф. КИБЭВС	_____	К. С. Сарин

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 безопасности информационных систем (БИС)	_____	О. О. Евсютин
Доцент каф. КИБЭВС	_____	А. А. Конев

Согласована на портале № 47314

1. Цели и задачи дисциплины

1.1. Цели дисциплины

Целью преподавания дисциплины является освоение методов управления программными средствами защиты информации, реализованными на основе клиент-серверной технологии.

1.2. Задачи дисциплины

– Получение знаний и умений по методам сбора и аудита событий информационной безопасности в современных средствах защиты информации;

– Получение умений и навыков централизованного управления клиентскими модулями и реагирования на угрозы безопасности;

– Получение знаний о методах контроля работоспособности и целостности клиентских модулей средств защиты информации;

– Изучение методов контроля и оценки установленного программного и аппаратного обеспечения на защищаемых компьютерах в локальной сети;

– Изучение методов обеспечения и контроля антивирусной защиты рабочих станций в сети организации.

2. Место дисциплины в структуре ОПОП

Дисциплина «Управление средствами защиты информации» (Б1.В.ОД.8) относится к блоку 1 (вариативная часть).

Предшествующими дисциплинами, формирующими начальные знания, являются: Безопасность операционных систем, Безопасность сетей ЭВМ, Организационное и правовое обеспечение информационной безопасности, Управление средствами защиты информации.

Последующими дисциплинами являются: Программно-аппаратные средства защиты информации, Управление средствами защиты информации.

3. Требования к результатам освоения дисциплины

Процесс изучения дисциплины направлен на формирование следующих компетенций:

– ПК-1 способностью выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации;

– ПК-10 способностью проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности;

– ПК-15 способностью организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю;

– ПК-6 способностью принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации;

– ПК-13 способностью принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации;

В результате изучения дисциплины обучающийся должен:

– **знать** принципы организации информационных систем в соответствии с требованиями по защите информации; возможности и назначение современных средств защиты информации от несанкционированного доступа.

– **уметь** выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных средств защиты информации; организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю; эффективно использовать различные методы и средства защиты информации для компьютерных сетей; администрировать подсистемы информационной безопасности автоматизированных систем.

– **владеть** навыками анализа информационной безопасности объектов и систем на

Согласована на портале № 47314

соответствие требованиям стандартов в области информационной безопасности; навыками выявления и уничтожения компьютерных вирусов; методами и средствами выявления угроз безопасности автоматизированным системам.

4. Объем дисциплины и виды учебной работы

Общая трудоемкость дисциплины составляет 3.0 зачетных единицы и представлена в таблице 4.1.

Таблица 4.1 – Трудоемкость дисциплины

Виды учебной деятельности	Всего часов	Семестры	
		6 семестр	7 семестр
Аудиторные занятия (всего)	64	46	18
Лекции	18	18	0
Лабораторные работы	28	28	0
Контроль самостоятельной работы (курсовой проект / курсовая работа)	18	0	18
Из них в интерактивной форме	14	14	0
Самостоятельная работа (всего)	44	26	18
Выполнение курсового проекта / курсовой работы	18	0	18
Оформление отчетов по лабораторным работам	21	21	0
Проработка лекционного материала	5	5	0
Всего (без экзамена)	108	72	36
Общая трудоемкость, ч	108	72	36
Зачетные Единицы	3.0	2.0	1.0

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	КП/КР, ч	Сам. раб., ч	Всего часов (без экзамена)	Формируемые компетенции
6 семестр						
1 Централизованное управление средствами защиты информации от несанкционированного доступа в локальной сети.	4	16	0	13	33	ПК-1, ПК-6, ПК-15
2 Централизованная инвентаризация ресурсов локальной сети. Удалённый контроль работоспособности средств защиты информации на рабочих станциях.	2	4	0	4	10	ПК-1, ПК-15
3 Централизованная защита от вирусов в локальной сети.	4	4	0	4	12	ПК-1, ПК-15
4 Централизованный учет и	4	4	0	4	12	ПК-1, ПК-15

Согласована на портале № 47314

управление программно-аппаратными средствами защиты информации.						
5 Анализ нормативных требований по управлению средствами защиты информации	4	0	0	1	5	ПК-10, ПК-13, ПК-15
Итого за семестр	18	28	0	26	72	
7 семестр						
6 Администрирование и управление средствами защиты информации от несанкционированного доступа.	0	0	18	18	18	ПК-1, ПК-6, ПК-10, ПК-15, ПК-13
Итого за семестр	0	0	18	18	36	
Итого	18	28	18	44	108	

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
6 семестр			
1 Централизованное управление средствами защиты информации от несанкционированного доступа в локальной сети.	Принципы построения средств защиты информации; основные механизмы защиты; аппаратные средства; конфигурирование; аудит; мониторинг и оперативное управление; полномочное управление доступом и контроль печати.	4	ПК-6, ПК-15
	Итого	4	
2 Централизованная инвентаризация ресурсов локальной сети. Удалённый контроль работоспособности средств защиты информации на рабочих станциях.	Основы проведения инвентаризации ресурсов в локальной сети; подготовка к инспекциям; инспекции компьютеров; получение отчетов с результатами инспектирования. Удалённый контроль работоспособности средств защиты информации на рабочих станциях.	2	ПК-15
	Итого	2	
3 Централизованная защита от вирусов в локальной сети.	Управление серверами администрирования; управление группами администрирования; управление клиентскими компьютерами; работа с отчетами, статистикой.	4	ПК-15
	Итого	4	
4 Централизованный учет и управление программно-аппаратными средствами защиты информации.	Назначение средств учета и управления аппаратными идентификаторами и носителями ключевой информации; возможности; архитектура; настройка; управление жизненным циклом средств аутентификации; аудит использования средств аутентификации.	4	ПК-15

Согласована на портале № 47314

	Итого	4	
5 Анализ нормативных требований по управлению средствами защиты информации	Анализ нормативных требований по управлению средствами защиты информации. Анализ нормативных требований Федеральной службы по техническому и экспортному контролю (ФСТЭК) при обеспечении мер безопасности персональных данных, в государственных информационных системах. Анализ требований безопасности к автоматизированным системам управления технологическими процессами.	4	ПК-10, ПК-13, ПК-15
	Итого	4	
Итого за семестр		18	
Итого		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	6
Предшествующие дисциплины						
1 Безопасность операционных систем	+	+	+	+		+
2 Безопасность сетей ЭВМ	+	+	+			+
3 Организационное и правовое обеспечение информационной безопасности					+	
4 Управление средствами защиты информации	+	+	+	+	+	+
Последующие дисциплины						
1 Программно-аппаратные средства защиты информации	+		+	+	+	+
2 Управление средствами защиты информации	+	+	+	+	+	+

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.	КСР (КП/КР)	Сам. раб.	

Согласована на портале № 47314

ПК-1		+	+	+	Защита отчета, Отчет по лабораторной работе, Защита курсовых проектов / курсовых работ, Тест
ПК-6	+	+	+	+	Защита отчета, Отчет по лабораторной работе, Защита курсовых проектов / курсовых работ, Тест
ПК-10	+		+	+	Конспект самоподготовки, Защита курсовых проектов / курсовых работ, Зачет, Тест
ПК-13	+		+	+	Конспект самоподготовки, Защита отчета, Отчет по лабораторной работе, Опрос на занятиях, Защита курсовых проектов / курсовых работ, Зачет, Тест
ПК-15	+	+	+	+	Конспект самоподготовки, Защита отчета, Отчет по лабораторной работе, Опрос на занятиях, Защита курсовых проектов / курсовых работ, 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
6 семестр			
Презентации с использованием слайдов с обсуждением		6	6
Case-study (метод конкретных ситуаций)	4		4
Решение ситуационных задач	4		4
Итого за семестр:	8	6	14
7 семестр			
Итого за семестр:	0	0	0
Итого	8	6	14

7. Лабораторные работы

Наименование лабораторных работ приведено в таблице 7.1.

Согласована на портале № 47314

Таблица 7.1 – Наименование лабораторных работ

Названия разделов	Наименование лабораторных работ	Трудоемкость, ч	Формируемые компетенции
6 семестр			
1 Централизованное управление средствами защиты информации от несанкционированного доступа в локальной сети.	Разграничение доступа к данным. Разграничение доступа к устройствам. Контроль печати конфиденциальных данных.	4	ПК-1, ПК-6, ПК-15
	Замкнутая программная среда. Контроль целостности.	4	
	Аудит событий информационной безопасности СЗИ от НСД. Работа со сведениями в журнале регистрации событий. Теневое копирование.	4	
	Оперативное управление защищаемыми рабочими станциями и мониторинг событий информационной безопасности	4	
	Итого	16	
2 Централизованная инвентаризация ресурсов локальной сети. Удалённый контроль работоспособности средств защиты информации на рабочих станциях.	Централизованная инвентаризация ресурсов локальной сети. Проведение инспекций и учет изменений конфигурации защищаемых рабочих станций.	4	ПК-1, ПК-15
	Итого	4	
3 Централизованная защита от вирусов в локальной сети.	Управление серверами администрирования Kaspersky Security Center. Централизованная настройка средства антивирусной защиты Kaspersky Endpoint Security. Аудит событий и дополнительные возможности.	4	ПК-1, ПК-15
	Итого	4	
4 Централизованный учет и управление программно-аппаратными средствами защиты информации.	Управление жизненным циклом средств аутентификации аппаратных идентификаторов с помощью средств централизованного учета и управления программно-аппаратными средствами защиты информации.	4	ПК-1, ПК-15
	Итого	4	
Итого за семестр		28	
Итого		28	

8. Практические занятия (семинары)

Не предусмотрено РУП.

9. Самостоятельная работа

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

Согласована на портале № 47314

Таблица 9.1 – Виды самостоятельной работы, трудоемкость и формируемые компетенции

Названия разделов	Виды самостоятельной работы	Трудоемкость, ч	Формируемые компетенции	Формы контроля
6 семестр				
1 Централизованное управление средствами защиты информации от несанкционированного доступа в локальной сети.	Проработка лекционного материала	1	ПК-15, ПК-6, ПК-1	Зачет, Защита отчета, Конспект самоподготовки, Отчет по лабораторной работе, Тест
	Оформление отчетов по лабораторным работам	12		
	Итого	13		
2 Централизованная инвентаризация ресурсов локальной сети. Удалённый контроль работоспособности средств защиты информации на рабочих станциях.	Проработка лекционного материала	1	ПК-15, ПК-1	Зачет, Защита отчета, Конспект самоподготовки, Опрос на занятиях, Отчет по лабораторной работе, Тест
	Оформление отчетов по лабораторным работам	3		
	Итого	4		
3 Централизованная защита от вирусов в локальной сети.	Проработка лекционного материала	1	ПК-15, ПК-1	Зачет, Защита отчета, Конспект самоподготовки, Отчет по лабораторной работе, Тест
	Оформление отчетов по лабораторным работам	3		
	Итого	4		
4 Централизованный учет и управление программно-аппаратными средствами защиты информации.	Проработка лекционного материала	1	ПК-15, ПК-1	Зачет, Защита отчета, Конспект самоподготовки, Отчет по лабораторной работе, Тест
	Оформление отчетов по лабораторным работам	3		
	Итого	4		
5 Анализ нормативных требований по управлению средствами защиты информации	Проработка лекционного материала	1	ПК-10, ПК-13, ПК-15	Зачет, Конспект самоподготовки, Тест
	Итого	1		
Итого за семестр		26		
7 семестр				
6 Администрирование и управление средствами защиты информации от несанкционированного доступа.	Выполнение курсового проекта / курсовой работы	18	ПК-1, ПК-6, ПК-10, ПК-13, ПК-15	Защита курсовых проектов / курсовых работ, Тест
	Итого	18		

Согласована на портале № 47314

Итого за семестр	18		
Итого	44		

10. Курсовой проект / курсовая работа

Трудоемкость аудиторных занятий и формируемые компетенции в рамках выполнения курсового проекта / курсовой работы представлены таблице 10.1.

Таблица 10.1 – Трудоемкость аудиторных занятий и формируемые компетенции в рамках выполнения курсового проекта / курсовой работы

Наименование аудиторных занятий	Трудоемкость, ч	Формируемые компетенции
7 семестр		
Выполнение курсовой работы на тему “Администрирование и управление СЗИ от НСД”. Совместно с руководителем возможен выбор другой темы курсовой работы, однако необходимым является условие применения в рамках курсовой работы средства защиты информации от несанкционированного доступа в локальной сети с применением выданных преподавателем виртуальных машин и выполнение требований задания по варианту.	18	ПК-1, ПК-6, ПК-10, ПК-13, ПК-15
Итого за семестр	18	

10.1. Темы курсовых проектов / курсовых работ

Примерная тематика курсовых проектов / курсовых работ:

– Тема курсовой работы: "Администрирование и управление СЗИ от НСД". Курсовая работа выполняется по вариантам.

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
6 семестр				
Зачет			20	20
Защита отчета	15	15	15	45
Конспект самоподготовки		5	5	10
Отчет по лабораторной работе	5	5	5	15
Тест			10	10
Итого максимум за период	20	25	55	100
Нарастающим итогом	20	45	100	100
7 семестр				
Защита курсовых проектов / курсовых работ			100	100

Согласована на портале № 47314

Итого максимум за период			100	100
Нарастающим итогом	0	0	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. Девянин, П.Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками [Электронный ресурс] [Электронный ресурс]: учеб. пособие — Электрон. дан. — Москва : Горячая линия-Телеком, 2013. — 338 с. — Режим доступа: https://e.lanbook.com/book/63235. — Загл. с экрана. — Режим доступа: https://e.lanbook.com/book/63235 (дата обращения: 12.06.2018).

12.2. Дополнительная литература

1. Комплексная защита информации в корпоративных системах [Электронный ресурс]: учеб. пособие / В.Ф. Шаньгин. — М. : ИД «ФОРУМ» : ИНФРА-М, 2018. — 592 с. — (Высшее образование: Бакалавриат). — Режим доступа: http://znanium.com/catalog/product/937502 (дата обращения: 12.06.2018).

2. Программно-аппаратная защита информации [Электронный ресурс]: Учебное пособие / П.Б. Хорев. - 2-е изд., испр. и доп. - М.: Форум: НИЦ ИНФРА-М, 2015. - 352 с.: ил.; 60x90 1/16. - (Высшее образование). (переплет) ISBN 978-5-00091-004-7. — Режим доступа: http://znanium.com/catalog/product/489084 (дата обращения: 12.06.2018).

12.3. Учебно-методические пособия

12.3.1. Обязательные учебно-методические пособия

1. Лабораторный практикум по дисциплине “Управление средствами защиты информации”

Согласована на портале № 47314

/ Рахманенко И.А. - 2017. - 83 с. [Электронный ресурс]: — Режим доступа: http://kibevs.tusur.ru/sites/default/files/upload/work_progs/gia/uszi_lab.pdf (дата обращения: 12.06.2018).

2. Методические указания для выполнения курсовой работы по дисциплине "Управление средствами защиты информации" / Рахманенко И.А. - 2016. - 6 с. [Электронный ресурс]: — Режим доступа: http://kibevs.tusur.ru/sites/default/files/upload/work_progs/gia/uszi_course.pdf (дата обращения: 12.06.2018).

3. Методические указания для выполнения самостоятельной и индивидуальной работы по дисциплине "Управление средствами защиты информации" / Рахманенко И.А. - 2017. - 3 с. [Электронный ресурс]: — Режим доступа: http://kibevs.tusur.ru/sites/default/files/upload/work_progs/gia/uszi_sam.pdf (дата обращения: 12.06.2018).

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. Государственный реестр сертифицированных средств защиты информации: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty-po-sertifikatsii/153-sistema-sertifikatsii/591-gosudarstvennyj-reestr-sertifitsirovannykh-sredstv-zashchity-informatsii-n-ross-ru-0001-01bi00

2. Информационно-поисковые системы Google; Wikipedia.

3. Информационные, справочные и нормативные базы данных https://lib.tusur.ru/ru/resursy/bazy-dannyh

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 моделирования, проектирования и эксплуатации информационных и аналитических систем

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

634045, Томская область, г. Томск, ул. Красноармейская, д. 146, 407 ауд.

Согласована на портале № 47314

Описание имеющегося оборудования:

- Компьютеры класса не ниже: плата Gigabyte GA-H55M-S2mATX/ Intel Original Soc-1156 Core i3 3.06 GHz/ DDR III Kingston CL9 (2 шт.) по 2048 Mb/ SATA-II 250Gb Hitachi / 1024 Mb GeForse GT240 PCI-E (6 шт.);
- Комплект специализированной учебной мебели;
- Рабочее место преподавателя.

Программное обеспечение:

- Kaspersky endpoint security
- KasperskySecurityCenter
- Microsoft Windows 7 Pro
- 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.

Согласована на портале № 47314

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

Согласована на портале № 47314

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

Согласована на портале № 47314

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

Согласована на портале № 47314

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

1. Основные функции средств централизованной инвентаризации ресурсов локальной сети.
2. Что такое Kaspersky Security Center?
3. Какие основные функции в Kaspersky Security Center?
4. Как получить информацию о конкретном компьютере в сети?
5. Что такое паспорт компьютера?
6. Перечислите типовые задачи администратора безопасности, для выполнения которых используется программа оперативного управления в режиме управления.
7. Какой формат данных используется в журналах СЗИ от НСД?
8. Для каких устройств реализован механизм контроля подключения и изменения?
9. Какие есть режимы для замкнутой программной среды?
10. Перечислите типовые задачи администратора безопасности, для выполнения которых используется программа оперативного управления в режиме конфигурирования.

Согласована на портале № 47314

11. Для чего нужны отчёты о результатах инспектирования? Какие группы отчётов предлагаются средствами централизованной инвентаризации ресурсов локальной сети?

12. Что такое «Сервер администрирования»?

13. Что такое «Удаленная установка» и как ей пользоваться?

14.1.3. Зачёт

1. Для чего предназначен механизм контроля подключения и изменения устройств?
2. Для каких устройств реализован механизм контроля подключения и изменения?
3. Для чего предназначен механизм контроля целостности (КЦ)?
4. Для чего предназначен механизм замкнутой программной среды?
5. Перечислите и поясните методы контроля целостности.
6. Какие есть режимы для замкнутой программной среды? В чем заключаются их отличия?
7. Для чего нужен журнал событий?
8. Какой формат данных используется в журналах СЗИ от НСД?
9. Приведите и поясните несколько категорий регистрации событий.
10. Кто может работать с журналом?
11. Для чего нужно теневое копирование?
12. Для каких устройств может осуществляться теневое копирование?
13. Для чего предназначена программа оперативного управления СЗИ от НСД?
14. Какие режимы работы имеет программа оперативного управления СЗИ от НСД?
15. Перечислите типовые задачи администратора безопасности, для выполнения которых используется программа оперативного управления в режиме конфигурирования.
16. Перечислите типовые задачи администратора безопасности, для выполнения которых используется программа оперативного управления в режиме управления.
17. В какой последовательности применяются параметры групповых политик?
18. Для чего необходимо квитирование событий НСД?
19. Какие виды отчетов можно построить с помощью программы ОУ?
20. В каких случаях необходимо изменение сетевых настроек?
21. Перечислите функции сервера администрирования Kaspersky Security Center.
22. Для чего необходим паспорт компьютера в средствах централизованной инвентаризации ресурсов локальной сети?
23. Назовите основные задачи, возникающие при управлении жизненным циклом устройств аутентификации.

14.1.4. Вопросы на самоподготовку

1. СЗИ от НСД – архитектура.
2. СЗИ от НСД- Защитные механизмы.
3. СЗИ от НСД - Оперативное управление.
4. Централизованная инвентаризация ресурсов локальной сети .
5. Централизованная защита от вирусов в локальной сети.
6. Централизованное управление средствами защиты от несанкционированного доступа в локальной сети.
7. Централизованный учет и управление программно-аппаратными средствами защиты информации.

14.1.5. Темы лабораторных работ

Централизованная инвентаризация ресурсов локальной сети. Проведение инспекций и учет изменений конфигурации защищаемых рабочих станций.

Управление серверами администрирования Kaspersky Security Center. Централизованная настройка средства антивирусной защиты Kaspersky Endpoint Security. Аудит событий и дополнительные возможности.

Разграничение доступа к данным. Разграничение доступа к устройствам. Контроль печати конфиденциальных данных.

Замкнутая программная среда. Контроль целостности.

Аудит событий информационной безопасности СЗИ от НСД. Работа со сведениями в журнале регистрации событий. Теневое копирование.

Согласована на портале № 47314

Оперативное управление защищаемыми рабочими станциями и мониторинг событий информационной безопасности

Управление жизненным циклом средств аутентификации аппаратных идентификаторов с помощью средств централизованного учета и управления программно-аппаратными средствами защиты информации.

14.1.6. Темы курсовых проектов / курсовых работ

Выполнение курсовой работы на тему “Администрирование и управление СЗИ от НСД”. Совместно с руководителем возможен выбор другой темы курсовой работы, однако необходимым является условие применения в рамках курсовой работы средства защиты информации от несанкционированного доступа в локальной сети с применением выданных преподавателем виртуальных машин и выполнение требований задания по варианту.

Рассмотрим задание, которое необходимо выполнить в рамках выполнения курсовой работы:

1. В соответствии с вариантом, определить информацию, обрабатываемую в автоматизированных системах организации. Определить угрозы, а также информацию, нуждающуюся в защите.
2. Объединить виртуальные машины, выданные преподавателем в домен.
3. Произвести установку серверной и клиентских частей СЗИ от НСД на виртуальные машины.
4. Произвести настройку подсистем СЗИ от НСД в соответствии с вариантом (создать каталоги и файлы на виртуальных машинах, которые бы соответствовали

данной информации). Сюда входит настройка, а также объяснение причин, в соответствии с которыми были настроены данные подсистемы:

– Политик СЗИ от НСД.
– Разграничение доступа к устройствам.
– Задание мандатного или дискреционного метода управления доступом.
– Настройка замкнутой программной среды (обязательна для нечетных вариантов).
– Настройка контроля целостности данных (обязательна для четных вариантов).
– Настройка затирания данных.
– Настройка контроля печати.

5. Подготовить пояснительную записку, содержащую описание выполненных работ, а также выводы по всей работе.

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.

Согласована на портале № 47314

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.

Согласована на портале № 47314