МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

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

УТВЕРЖДАЮ
Проректор по учебной работе

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Управление средствами защиты информации

Уровень образования: **высшее образование - специалитет**
Направление подготовки / специальность: **10.05.03 Информационная безопасность автоматизированных систем**
Направленность (профиль) / специализация: **Информационная безопасность автоматизированных банковских систем**
Форма обучения: **очная**
Факультет: **ФБ, Факультет безопасности**
Кафедра: **КИБЭВС, Кафедра комплексной информационной безопасности электронно-вычислительных систем**
Курс: **4**
Семестр: **7**
Учебный план набора 2020 года

Распределение рабочего времени

№	Виды учебной деятельности	7 семестр	Всего	Единицы
1	Лекции	18	18	часов
2	Лабораторные работы	36	36	часов
3	Контроль самостоятельной работы (курсовой проект / курсовая работа)	18	18	часов
4	Всего аудиторных занятий	72	72	часов
5	Самостоятельная работа	72	72	часов
6	Всего (без экзамена)	144	144	часов
7	Общая трудоемкость	144	144	часов
		4.0	4.0	З.Е.

Зачёт: 7 семестр
Курсовой проект / курсовая работа: 7 семестр

Томск

Рассмотрена и одобрена на заседании кафедры
протокол № 12 от «26» 11 2019 г.

ЛИСТ СОГЛАСОВАНИЯ

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

Разработчик:

Доцент каф. БИС _____ И. А. Рахманенко

Заведующий обеспечивающей каф. КИБЭВС _____ А. А. Шелупанов

Рабочая программа дисциплины согласована с факультетом и выпускающей кафедрой:

Декан ФБ _____ Д. В. Кручинин

Заведующий выпускающей каф. КИБЭВС _____ А. А. Шелупанов

Эксперты:

Доцент кафедры комплексной информационной безопасности электронно-вычислительных систем (КИБЭВС) _____ А. А. Конев

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

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.03.03) относится к блоку 1 (вариативная часть).

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

3. Требования к результатам освоения дисциплины

Процесс изучения дисциплины направлен на формирование следующих компетенций:

– ПК-13 способностью участвовать в проектировании средств защиты информации автоматизированной системы;

– ПК-19 способностью разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированной системы;

– ПК-26 способностью администрировать подсистему информационной безопасности автоматизированной системы;

– ПК-28 способностью управлять информационной безопасностью автоматизированной системы;

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; обеспечивать централизованное управление средствами защиты информации автоматизированных систем предприятия; администрировать подсистемы информационной безопасности автоматизированных систем.

– **владеть** навыками анализа информационной безопасности объектов и систем на 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 4.0 зачетных единицы и представлена в таблице 4.1.

Таблица 4.1 – Трудоемкость дисциплины

Виды учебной деятельности	Всего часов	Семестры
		7 семестр
Аудиторные занятия (всего)	72	72
Лекции	18	18
Лабораторные работы	36	36
Контроль самостоятельной работы (курсовой проект / курсовая работа)	18	18
Самостоятельная работа (всего)	72	72
Выполнение курсового проекта / курсовой работы	36	36
Оформление отчетов по лабораторным работам	29	29
Проработка лекционного материала	7	7
Всего (без экзамена)	144	144
Общая трудоемкость, ч	144	144
Зачетные Единицы	4.0	4.0

5. Содержание дисциплины

5.1. Разделы дисциплины и виды занятий

Разделы дисциплины и виды занятий приведены в таблице 5.1.

Таблица 5.1 – Разделы дисциплины и виды занятий

Названия разделов дисциплины	Лек., ч	Лаб. раб., ч	КП/КР, ч	Сам. раб., ч	Всего часов (без экзамена)	Формируемые компетенции
7 семестр						
1 Централизованное управление средствами защиты информации от несанкционированного доступа в локальной сети.	4	20	18	14	38	ПК-13, ПК-19, ПК-26, ПК-28
2 Централизованная инвентаризация ресурсов локальной сети. Удалённый контроль работоспособности средств защиты информации на рабочих станциях.	2	4		7	13	ПК-13, ПК-19, ПК-26, ПК-28
3 Централизованная защита от вирусов в локальной сети.	4	6		7	17	ПК-13, ПК-19, ПК-26, ПК-28
4 Централизованный учет и управление программно-аппаратными средствами защиты информации.	4	6		7	17	ПК-13, ПК-19, ПК-26, ПК-28
5 Администрирование и управление средствами защиты информации от несанкционированного доступа.	0	0		36	36	ПК-13, ПК-19, ПК-26, ПК-28
6 Анализ нормативных требований по управлению средствами защиты ин-	4	0		1	5	ПК-13, ПК-19, ПК-28

формации						
Итого за семестр	18	36	18	72	144	
Итого	18	36	18	72	144	

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
7 семестр			
1 Централизованное управление средствами защиты информации от несанкционированного доступа в локальной сети.	Принципы построения СЗИ “Secret Net”; основные механизмы защиты; аппаратные средства; конфигурирование; аудит; мониторинг и оперативное управление; полномочное управление доступом и контроль печати.	4	ПК-13, ПК-19, ПК-26, ПК-28
	Итого	4	
2 Централизованная инвентаризация ресурсов локальной сети. Удалённый контроль работоспособности средств защиты информации на рабочих станциях.	Знакомство с интерфейсом «КБ Инвентаризация»; подготовка к инспекциям; инспекции компьютеров; получение отчетов с результатами инспектирования. Удалённый контроль работоспособности средств защиты информации на рабочих станциях.	2	ПК-13, ПК-19, ПК-26, ПК-28
	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-13, ПК-19, ПК-26, ПК-28
	Итого	4	
4 Централизованный учет и управление программно-аппаратными средствами защиты информации.	Назначение «SafeNet Authentication Manager»; возможности; архитектура; настройка; управление жизненным циклом средств аутентификации; аудит использования средств аутентификации.	4	ПК-13, ПК-19, ПК-26, ПК-28
	Итого	4	
6 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-19, ПК-28
	Итого	4	

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	6
Предшествующие дисциплины						
1 Безопасность операционных систем	+	+	+	+	+	
2 Безопасность сетей ЭВМ	+	+	+		+	
3 Организационное и правовое обеспечение 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.	КСР (КП/КР)	Сам. раб.	
ПК-13	+	+	+	+	Конспект самоподготовки, Защита отчета, Отчет по лабораторной работе, Опрос на занятиях, Защита курсовых проектов / курсовых работ, Зачёт, Тест
ПК-19	+	+	+	+	Конспект самоподготовки, Защита отчета, Отчет по лабораторной работе, Опрос на занятиях, Защита курсовых проектов / курсовых работ, Зачёт, Тест
ПК-26	+	+	+	+	Конспект самоподготовки, Защита отчета, Отчет по лабораторной работе, Опрос на занятиях, Защита курсовых проектов / курсовых работ, Зачёт, Тест

ПК-28	+	+	+	+	Конспект самоподготовки, Защита отчета, Отчет по лабораторной работе, Опрос на занятиях, Защита курсовых проектов / курсовых работ, Зачёт, Тест

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
7 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.	6	ПК-13, ПК-19, ПК-26, ПК-28
	Замкнутая программная среда. Контроль целостности.	4	
	Аудит событий информационной безопасности в СЗИ от НСД Secret Net. Работа со сведениями в журнале регистрации событий. Теневое копирование	4	
	Оперативное управление защищаемыми рабочими станциями и мониторинг событий информационной безопасности	6	
	Итого	20	
2 Централизованная инвентаризация ресурсов локальной сети. Удалённый контроль работоспособности средств защиты информации на рабочих станциях.	“КБ Инвентаризация”. Проведение инспекций и учет изменений конфигурации защищаемых рабочих станций.	4	ПК-13, ПК-19, ПК-26, ПК-28
	Итого	4	
3 Централизованная защита от вирусов в локальной сети.	Управление серверами администрирования "Kaspersky Security Center"	6	ПК-13, ПК-19, ПК-26, ПК-28
	Итого	6	
4 Централизованный учет и управление программно-аппаратными средствами защиты информации.	Управление жизненным циклом средств аутентификации eToken с помощью Safenet Authentication Manager.	6	ПК-13, ПК-19, ПК-26, ПК-28
	Итого	6	
Итого за семестр		36	

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
7 семестр				
1 Централизованное управление средствами защиты информации от несанкционированного доступа в локальной сети.	Проработка лекционного материала	3	ПК-13, ПК-19, ПК-26, ПК-28	Зачёт, Защита отчета, Конспект самоподготовки, Отчет по лабораторной работе, Тест
	Оформление отчетов по лабораторным работам	11		
	Итого	14		
2 Централизованная инвентаризация ресурсов локальной сети. Удалённый контроль работоспособности средств защиты информации на рабочих станциях.	Проработка лекционного материала	1	ПК-13, ПК-19, ПК-26, ПК-28	Зачёт, Защита отчета, Конспект самоподготовки, Опрос на занятиях, Отчет по лабораторной работе, Тест
	Оформление отчетов по лабораторным работам	6		
	Итого	7		
3 Централизованная защита от вирусов в локальной сети.	Проработка лекционного материала	1	ПК-13, ПК-19, ПК-26, ПК-28	Зачёт, Защита отчета, Конспект самоподготовки, Отчет по лабораторной работе, Тест
	Оформление отчетов по лабораторным работам	6		
	Итого	7		
4 Централизованный учет и управление программно-аппаратными средствами защиты информации.	Проработка лекционного материала	1	ПК-13, ПК-19, ПК-26, ПК-28	Зачёт, Защита отчета, Конспект самоподготовки, Отчет по лабораторной работе, Тест
	Оформление отчетов по лабораторным работам	6		
	Итого	7		
5 Администрирование и управление средствами защиты информации от несанкционированного доступа.	Выполнение курсового проекта / курсовой работы	36	ПК-13, ПК-19, ПК-26, ПК-28	Защита курсовых проектов / курсовых работ, Тест
	Итого	36		

6 Анализ нормативных требований по управлению средствами защиты информации	Проработка лекционного материала	1	ПК-13, ПК-19	Зачёт, Конспект самоподготовки, Тест
	Итого	1		
Итого за семестр		72		
Итого		72		

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 Secret Net”. 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-13, ПК-19, ПК-26, ПК-28
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 Secret Net". Курсовая работа выполняется по вариантам. При желании студента возможна замена на другое СЗИ от НСД.

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
7 семестр				
Зачёт			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

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]: учебное пособие / П. Н. Девянин. — 2-е изд., испр. и доп. — Москва : Горячая линия-Телеком, 2017. — 338 с. — Режим доступа: https://e.lanbook.com/book/111049 (дата обращения: 14.03.2021).

12.2. Дополнительная литература

1. Фомин, Д. В. Информационная безопасность и защита информации [Электронный ресурс]: специализированные аттестованные программные и программно-аппаратные средства : методические указания / Д. В. Фомин. — Благовещенск : АмГУ, 2017. — 240 с. — Режим доступа: https://e.lanbook.com/book/156494 (дата обращения: 14.03.2021).

2. Ермакова, А. Ю. Методы и средства защиты компьютерной информации [Электронный ресурс]: учебное пособие / А. Ю. Ермакова. — Москва : РТУ МИРЭА, 2020. — 223 с. — Режим доступа: https://e.lanbook.com/book/163844 (дата обращения: 14.03.2021).

12.3. Учебно-методические пособия

12.3.1. Обязательные учебно-методические пособия

1. Лабораторный практикум по дисциплине “Управление средствами защиты информации” / Рахманенко И.А. - 2021. - 103 с. [Электронный ресурс]: — Режим доступа: https://disk.fb.tusur.ru/information_security_management/laboratory_work.pdf (дата обращения:

14.03.2021).

2. Методические указания по выполнения курсовой работы по дисциплине "Управление средствами защиты информации" для студентов специальностей 10.03.01, 10.05.02, 10.05.03 / Рахманенко И.А. - 2019. - 7 с. [Электронный ресурс]: — Режим доступа: https://disk.fb.tusur.ru/information_security_management/course_work.pdf (дата обращения: 14.03.2021).

3. Методические указания к самостоятельной и индивидуальной работе по дисциплине "Управление средствами защиты информации" / Рахманенко И.А. - 2021. - 6 с. [Электронный ресурс]: — Режим доступа: https://disk.fb.tusur.ru/information_security_management/independent_work.pdf (дата обращения: 14.03.2021).

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.

Описание имеющегося оборудования:

- Моноблок Asus V222GAK-BA021D: IntelJ5005/ DDR44G / 500Gb/ WiFi / мышь/ клавиатура (10шт.);

- Комплект специализированной учебной мебели;

- Рабочее место преподавателя.

Программное обеспечение:

– Kaspersky endpoint security
– KasperskySecurityCenter
– Microsoft Windows 10
– VirtualBox

Лаборатория программно-аппаратных средств обеспечения информационной безопасности

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

634045, Томская область, г. Томск, ул. Красноармейская, д. 146, 405 ауд.

Описание имеющегося оборудования:

- Моноблок: Asus V222GAK-BA021D: Intel J5005/ DDR4 4G/ 500Gb/ WiFi / мышь/ клавиатура (30шт.);

- Компьютер: DEPO Neos DF226/ i3-7100/ DDR4 8G/ Жесткий диск 500G/ мышь/ клавиатура/ монитор;

- Аппаратные средства аутентификации пользователя «eToken Pro»;

- Программно-аппаратный комплекс защиты информации: ПАК ViPNet Coordinator HW100 C 4.x, ПАК ViPNet Coordinator HW1000 4.x, ПАК Аккорд;

Стенды для изучения проводных и беспроводных компьютерных сетей, включающие:

- абоненские устройства: компьютеры SuperMicro;

- коммутаторы: Mikrotik CRS125-24G-1S-IN; Mikrotik RouterBoard 1100;

- маршрутизаторы: Cisco 891-K9, Cisco C881-V-K9, Check Point CPAP-SG1200R-NGFW;

- средства анализа сетевого трафика и углубленной проверки сетевых пакетов: анализатор трафика Wireshark, дистрибутив Kali Linux;

- межсетевые экраны: ИКС Lite, Positive Technologies Application Firewall Education, CISCO ASA 5505, МЭ в составе маршрутизатора Check Point CPAP-SG1200R-NGFW;

- системы обнаружения компьютерных атак: Snort, Suricata, СОВ в составе маршрутизатора Check Point CPAP-SG1200R-NGFW;

- точки доступа: D-link dwl3600ap;

- системы защиты от утечки данных: Контур информационной безопасности SearchInform;

- средства мониторинга состояния автоматизированных систем: система мониторинга Zabbix;

- средства сканирования защищенности компьютерных сетей: сканер безопасности Xspider Education, система анализа защищенности сети MaxPatrol Education.

Устройства чтения смарт-карт и радиометок: Адаптер компьютерный для считывания и передачи в ПК серийных номеров бесконтактных идентификаторов IronLogic Z-2 USB;

- Комплект специализированной учебной мебели;

- Рабочее место преподавателя.

Программное обеспечение:

– Kaspersky endpoint security
– 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. Какой из методов контроля целостности файлов отсутствует в СЗИ от НСД Secret Net?
a) Контроль содержимого
b) Контроль атрибутов
c) Контроль санкционированных изменений
d) Контроль существования
2. Для чего предназначена программа оперативного управления Secret Net?
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 Secret Net?
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 Secret Net 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 системе Secret Net?

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 предоставляет Safenet Authentication Manager?

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 Secret Net?

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 Secret Net

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 Secret Net 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 системе Secret Net 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 Secret Net?

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 системе Secret Net следует использовать следующую подсистему:

a) Подсистема контроля целостности

b) Подсистема разграничения доступа к устройствам

c) Подсистема оперативного управления

d) Замкнутая программная среда

15. Какое из программных средств позволяет реализовать следующую меру защиты информации в государственных информационных системах: «Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов»?

a) Код Безопасности: Инвентаризация

b) Secret Net

c) SafeNet Authentication Manager

d) Kaspersky Security Center

16. Для чего предназначен механизм контроля подключения и изменения устройств в СЗИ от НСД Secret Net?

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

17. Для чего предназначен механизм контроля целостности (КЦ) в СЗИ от НСД Secret Net?

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

18. Для чего предназначен механизм замкнутой программной среды в СЗИ от НСД Secret Net?

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

19. Назовите режимы для замкнутой программной среды в СЗИ от НСД Secret Net?

a) Конфиденциальный и секретный

b) Эталонный и полномочный

c) Мягкий и жесткий

d) Дискреционный и мандатный

20. 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

21. Какие из перечисленных защитных механизмов Secret Net 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

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 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

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, 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

24. 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 обеспече-

ния

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

25. Для чего предназначено теневое копирование в СЗИ от НСД Secret Net?

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

26. Для каких устройств НЕ осуществляется теневое копирование в СЗИ от НСД Secret Net?

a) Принтеры

b) USB-носители

c) Сетевые карты

d) CD-приводы

27. Назовите аппаратное средство защиты, НЕ применяемое совместно с СЗИ от НСД Secret Net:

a) Аппаратные идентификаторы «eToken»

b) Программно-аппаратный комплекс «Соболь»

c) Программно-аппаратный комплекс «Аккорд»

d) Плата «Secret Net Card»

28. С какой целью может использоваться Safenet Authentication Manager в государственных информационных системах?

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

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

c) Управление жизненным циклом аппаратных аутентификаторов

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

29. 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

30. Какое из программных средств позволяет реализовать следующую меру защиты информации в государственных информационных системах: «Уничтожение (стирание) информации на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контроль уничтожения (стирания)»?

a) Код Безопасности: Инвентаризация

b) SafeNet Authentication Manager

c) Secret Net

d) Kaspersky Security Center

14.1.2. Темы опросов на занятиях

1. Основные функции системы КБИ.
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. Для чего предназначен сайт SAM Self Service Center?

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

8. Какой формат данных используется в журнале Secret Net?

9. Для каких устройств реализован механизм контроля подключения и изменения?

10. Какие есть режимы для замкнутой программной среды?

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

12. Для чего предназначен сайт SAM Rescue Center?

13. Для чего нужны отчёты о результатах инспектирования? Какие группы отчётов предлагаются системой КБИ?

14. Что такое «Сервер администрирования»?

15. 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 журнале Secret Net?

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 Secret Net?

14. Какие режимы работы имеет программа оперативного управления Secret Net?

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 системе КБ: Инвентаризация?

23. Назовите основные задачи, возникающие при управлении жизненным циклом устройств аутентификации.

14.1.4. Вопросы на самоподготовку

1. Secret Net – архитектура.

2. Secret Net - Защитные механизмы.

3. Secret Net - Программа оперативного управления.

4. Централизованная инвентаризация ресурсов локальной сети .

5. Централизованная защита от вирусов в локальной сети.

6. Централизованное управление средствами защиты от несанкционирован-ного доступа в локальной сети.

7. Централизованный учет и управление программно-аппаратными средства-ми защиты информации.

14.1.5. Темы лабораторных работ

“КБ Инвентаризация”. Проведение инспекций и учет изменений конфигурации защищае-

мых рабочих станций.

Управление серверами администрирования "Kaspersky Security Center"

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

Замкнутая программная среда. Контроль целостности.

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

Оперативное управление защищаемыми рабочими станциями и мониторинг событий информационной безопасности

Управление жизненным циклом средств аутентификации eToken с помощью Safenet Authentication Manager.

14.1.6. Темы курсовых проектов / курсовых работ

Выполнение курсовой работы на тему “Администрирование и управление СЗИ от НСД Secret Net”. 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. Скачать демо-версию СЗИ от НСД Secret Net и требуемую документацию.

4. Произвести установку серверной и клиентских частей Secret Net на виртуальные машины.

5. Произвести настройку подсистем Secret Net 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 Secret Net.

– 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.

6. 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.

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	Решение дистанционных тестов,	Преимущественно дистанционными

опорно-двигательного аппарата	контрольные работы, письменные самостоятельные работы, вопросы к зачету	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.