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

Документ подписан электронной подписью
Сертификат: a1119608-cdff-4455-b54e-5235117c185c
Владелец: Сенченко Павел Васильевич
Действителен: с 17.09.2019 по 16.09.2024

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

УПРАВЛЕНИЕ СРЕДСТВАМИ ЗАЩИТЫ ИНФОРМАЦИИ

Уровень образования: **высшее образование - специалитет**
Направление подготовки / специальность: **10.05.02 Информационная безопасность телекоммуникационных систем**
Направленность (профиль) / специализация: **Управление безопасностью телекоммуникационных систем и сетей**
Форма обучения: **очная**
Факультет: **Факультет безопасности (ФБ)**
Кафедра: **Кафедра безопасности информационных систем (БИС)**
Курс: **4**
Семестр: **7**
Учебный план набора 2021 года

Объем дисциплины и виды учебной деятельности

Виды учебной деятельности	7 семестр	Всего	Единицы
Лекционные занятия	18	18	часов
Лабораторные занятия	36	36	часов
Самостоятельная работа	54	54	часов
Общая трудоемкость (включая промежуточную аттестацию)	108	108	часов
	3	3	з.е.

Формы промежуточной аттестация	Семестр
Зачет	7

Томск

1. Общие положения

1.1. Цели дисциплины

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

1.2. Задачи дисциплины

1. Получение знаний и умений по методам сбора и аудита событий информационной безопасности в современных средствах защиты информации.
2. Получение умений и навыков централизованного управления клиентскими модулями средств защиты информации и реагирования на угрозы безопасности.
3. Получение знаний о методах контроля работоспособности и целостности клиентских модулей средств защиты информации.
4. Изучение методов контроля и оценки установленного программного и аппаратного обеспечения на защищаемых компьютерах в локальной сети.
5. Изучение методов обеспечения и контроля антивирусной защиты рабочих станций в сети организации.

2. Место дисциплины в структуре ОПОП

Блок дисциплин: Б1. Дисциплины (модули).
Часть блока дисциплин: Обязательная часть.
Модуль дисциплин: Модуль специальности (special hard skills - SHS).
Индекс дисциплины: Б1.О.03.20.
Реализуется с применением электронного обучения, дистанционных образовательных технологий.

3. Перечень планируемых результатов обучения по дисциплине, соотнесенных с индикаторами достижения компетенций

Процесс изучения дисциплины направлен на формирование следующих компетенций в соответствии с ФГОС ВО и основной образовательной программой (таблица 3.1):
Таблица 3.1 – Компетенции и индикаторы их достижения

Компетенция	Индикаторы достижения компетенции	Планируемые результаты обучения по дисциплине
Универсальные компетенции		

УК-10. Способен принимать обоснованные экономические решения в различных областях жизнедеятельности	УК-10.1. Знает базовые принципы функционирования экономики и экономического развития общества, источники финансирования профессиональной деятельности , критерии оценки затрат и обоснованности экономических решений	Знает критерии оценки затрат и обоснованности экономических решений в рамках внедрений средств защиты информации в защищенные телекоммуникационные системы
	УК-10.2. Умеет принимать и обосновывать экономические решения в различных областях жизнедеятельности, планировать деятельность с учетом экономически оправданных затрат, направленных на достижение результата	Умеет принимать и обосновывать экономические решения в областях, связанных с проектированием защищенных телекоммуникационных систем
	УК-10.3. Владеет основами финансовой грамотности, а также навыками расчета и оценки экономической целесообразности планируемой деятельности (проекта), ее (его) финансирования из различных источников	Владеет навыками оценки экономической целесообразности внедрения средств защиты информации от несанкционированного доступа
Общепрофессиональные компетенции		

ОПК-16. Способен проектировать защищенные телекоммуникационные системы и их элементы, проводить анализ проектных решений по обеспечению заданного уровня безопасности и требуемого качества обслуживания телекоммуникационных систем, разрабатывать необходимую техническую документацию с учетом действующих нормативных и методических документов, проводить подготовку исходных данных для технико-экономического обоснования соответствующих проектных решений	ОПК-16.1. Знает общие принципы проектирования систем и сетей электрической связи и принципы построения защищенных телекоммуникационных систем, номенклатуру и содержание нормативных правовых актов и нормативных методических документов, применяемых при проектировании защищенных телекоммуникационные систем	Знает принципы построения защищенных телекоммуникационных систем с учетом применения средств защиты информации от несанкционированного доступа, нормативные документы ФСТЭК, используемые при проектировании защищенных телекоммуникационные систем
	ОПК-16.2. Умеет разрабатывать необходимую техническую документацию в области проектирования защищенных телекоммуникационных систем с учетом действующих нормативных и методических документов	Умеет разрабатывать необходимую техническую документацию в области проектирования защищенных телекоммуникационных систем с учетом действующих нормативных и методических документов
	ОПК-16.3. Имеет навыки проектирования элементов защищенных телекоммуникационных систем	Имеет навыки проектирования элементов защищенных телекоммуникационных систем, включающих средства защиты информации от несанкционированного доступа
Профессиональные компетенции		
-	-	-

4. Объем дисциплины в зачетных единицах с указанием количества академических часов, выделенных на контактную работу обучающихся с преподавателем и на самостоятельную работу обучающихся

Общая трудоемкость дисциплины составляет 3 зачетных единиц, 108 академических часов.

Распределение трудоемкости дисциплины по видам учебной деятельности представлено в таблице 4.1.

Таблица 4.1 – Трудоемкость дисциплины по видам учебной деятельности

Виды учебной деятельности	Всего часов	Семестры
		7 семестр
Контактная аудиторная работа обучающихся с преподавателем, всего	54	54
Лекционные занятия	18	18
Лабораторные занятия	36	36
Самостоятельная работа обучающихся, в т.ч. контактная внеаудиторная работа обучающихся с преподавателем, всего	54	54
Подготовка к зачету	14	14
Подготовка к тестированию	10	10
Подготовка к лабораторной работе, написание отчета	30	30

Общая трудоемкость (в часах)	108	108
Общая трудоемкость (в з.е.)	3	3

5. Структура и содержание дисциплины

5.1. Разделы (темы) дисциплины и виды учебной деятельности

Структура дисциплины по разделам (темам) и видам учебной деятельности приведена в таблице 5.1.

Таблица 5.1 – Разделы (темы) дисциплины и виды учебной деятельности

Названия разделов (тем) дисциплины	Лек. зан., ч	Лаб. раб.	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	22	46	ОПК-16, УК-10
2 Централизованная инвентаризация ресурсов локальной сети. Удалённый контроль работоспособности средств защиты информации на рабочих станциях	2	4	10	16	ОПК-16, УК-10
3 Централизованная защита от вирусов в локальной сети	4	6	8	18	ОПК-16, УК-10
4 Централизованный учет и управление средствами персональной идентификации и аутентификации	4	6	8	18	ОПК-16, УК-10
5 Анализ нормативных требований по управлению средствами защиты информации	4	-	6	10	ОПК-16, УК-10
Итого за семестр	18	36	54	108	
Итого	18	36	54	108	

5.2. Содержание разделов (тем) дисциплины

Содержание разделов (тем) дисциплины (в т.ч. по лекциям) приведено в таблице 5.2.

Таблица 5.2 – Содержание разделов (тем) дисциплины (в т.ч. по лекциям)

Названия разделов (тем) дисциплины	Содержание разделов (тем) дисциплины (в т.ч. по лекциям)	Трудоемкость (лекционные занятия), ч	Формируемые компетенции
7 семестр			
1 Централизованное управление средствами защиты информации от несанкционированного доступа в локальной сети	Принципы построения СЗИ “Secret Net Studio”; основные механизмы защиты; аппаратные средства; конфигурирование; аудит; мониторинг и оперативное управление; полномочное управление доступом и контроль печати.	4	ОПК-16, УК-10
	Итого	4	

2 Централизованная инвентаризация ресурсов локальной сети. Удалённый контроль работоспособности средств защиты информации на рабочих станциях	Знакомство с основными задачами инвентаризации и контроля защищаемых ресурсов; подготовка к инспекциям; инспекции компьютеров; получение отчетов с результатами инспектирования. Удалённый контроль работоспособности средств защиты информации на рабочих станциях.	2	ОПК-16, УК-10
	Итого	2	
3 Централизованная защита от вирусов в локальной сети	Управление защитными механизмами IT-инфраструктуры с помощью Kaspersky Security Center. Архитектура и типовые структуры защиты на базе Kaspersky Security Center. Управление серверами и группами администрирования. Управление клиентскими компьютерами. Работа с отчетами, статистикой.	4	ОПК-16, УК-10
	Итого	4	
4 Централизованный учет и управление средствами персональной идентификации и аутентификации	Назначение «SafeNet Authentication Manager»; возможности; архитектура; настройка; управление жизненным циклом средств аутентификации; аудит использования средств аутентификации.	4	ОПК-16, УК-10
	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	ОПК-16, УК-10
	Итого	4	
Итого за семестр		18	
Итого		18	

5.3. Практические занятия (семинары)

Не предусмотрено учебным планом

5.4. Лабораторные занятия

Наименование лабораторных работ приведено в таблице 5.4.

Таблица 5.4 – Наименование лабораторных работ

Названия разделов (тем) дисциплины	Наименование лабораторных работ	Трудоемкость, ч	Формируемые компетенции
7 семестр			
1 Централизованное управление средствами защиты информации от несанкционированного доступа в локальной сети	Secret Net Studio. Разграничение доступа к данным. Разграничение доступа к устройствам. Контроль печати конфиденциальных данных.	6	ОПК-16, УК-10
	Secret Net Studio. Замкнутая программная среда. Контроль целостности.	4	ОПК-16, УК-10
	Secret Net Studio. Аудит событий информационной безопасности в СЗИ от НСД Secret Net. Работа со сведениями в журнале регистрации событий. Теневое копирование	4	ОПК-16, УК-10
	Оперативное управление защищаемыми рабочими станциями и мониторинг событий информационной безопасности	6	ОПК-16, УК-10
	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	ОПК-16, УК-10
	Итого	4	
3 Централизованная защита от вирусов в локальной сети	Управление серверами администрирования "Kaspersky Security Center"	6	ОПК-16, УК-10
	Итого	6	
4 Централизованный учет и управление средствами персональной идентификации и аутентификации	Управление жизненным циклом средств аутентификации eToken с помощью Safenet Authentication Manager.	6	ОПК-16, УК-10
	Итого	6	
Итого за семестр		36	
Итого		36	

5.5. Курсовой проект / курсовая работа

Не предусмотрено учебным планом

5.6. Самостоятельная работа

Виды самостоятельной работы, трудоемкость и формируемые компетенции представлены в таблице 5.6.

Таблица 5.6 – Виды самостоятельной работы, трудоемкость и формируемые компетенции

Названия разделов (тем) дисциплины	Виды самостоятельной работы	Трудоемкость, ч	Формируемые компетенции	Формы контроля
7 семестр				
1 Централизованное управление средствами защиты информации от несанкционированного доступа в локальной сети	Подготовка к зачету	4	ОПК-16, УК-10	Зачёт
	Подготовка к тестированию	2	ОПК-16, УК-10	Тестирование
	Подготовка к лабораторной работе, написание отчета	16	ОПК-16, УК-10	Лабораторная работа
	Итого	22		
2 Централизованная инвентаризация ресурсов локальной сети. Удалённый контроль работоспособности средств защиты информации на рабочих станциях	Подготовка к зачету	2	ОПК-16, УК-10	Зачёт
	Подготовка к тестированию	2	ОПК-16, УК-10	Тестирование
	Подготовка к лабораторной работе, написание отчета	6	ОПК-16, УК-10	Лабораторная работа
	Итого	10		
3 Централизованная защита от вирусов в локальной сети	Подготовка к зачету	2	ОПК-16, УК-10	Зачёт
	Подготовка к тестированию	2	ОПК-16, УК-10	Тестирование
	Подготовка к лабораторной работе, написание отчета	4	ОПК-16, УК-10	Лабораторная работа
	Итого	8		
4 Централизованный учет и управление средствами персональной идентификации и аутентификации	Подготовка к зачету	2	ОПК-16, УК-10	Зачёт
	Подготовка к тестированию	2	ОПК-16, УК-10	Тестирование
	Подготовка к лабораторной работе, написание отчета	4	ОПК-16, УК-10	Лабораторная работа
	Итого	8		
5 Анализ нормативных требований по управлению средствами защиты информации	Подготовка к зачету	4	ОПК-16, УК-10	Зачёт
	Подготовка к тестированию	2	ОПК-16, УК-10	Тестирование
	Итого	6		
Итого за семестр		54		
Итого		54		

5.7. Соответствие компетенций, формируемых при изучении дисциплины, и видов учебной деятельности

Соответствие компетенций, формируемых при изучении дисциплины, и видов учебной деятельности представлено в таблице 5.7.

Таблица 5.7 – Соответствие компетенций, формируемых при изучении дисциплины, и видов занятий

Формируемые компетенции	Виды учебной деятельности			Формы контроля
	Лек. зан.	Лаб. раб.	Сам. раб.	
ОПК-16	+	+	+	Зачёт, Лабораторная работа, Тестирование
УК-10	+	+	+	Зачёт, Лабораторная работа, Тестирование

6. Рейтинговая система для оценки успеваемости обучающихся

6.1. Балльные оценки для форм контроля

Балльные оценки для форм контроля представлены в таблице 6.1.

Таблица 6.1 – Балльные оценки

Формы контроля	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	0	0	30	30
Лабораторная работа	20	20	20	60
Тестирование	0	0	10	10
Итого максимум за период	20	20	60	100
Нарастающим итогом	20	40	100	100

6.2. Пересчет баллов в оценки за текущий контроль

Пересчет баллов в оценки за текущий контроль представлен в таблице 6.2.

Таблица 6.2 – Пересчет баллов в оценки за текущий контроль

Баллы на дату текущего контроля	Оценка
≥ 90% от максимальной суммы баллов на дату ТК	5
От 70% до 89% от максимальной суммы баллов на дату ТК	4
От 60% до 69% от максимальной суммы баллов на дату ТК	3
< 60% от максимальной суммы баллов на дату ТК	2

6.3. Пересчет суммы баллов в традиционную и международную оценку

Пересчет суммы баллов в традиционную и международную оценку представлен в таблице 6.3.

Таблица 6.3 – Пересчет суммы баллов в традиционную и международную оценку

Оценка	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)

7. Учебно-методическое и информационное обеспечение дисциплины

7.1. Основная литература

1. Девянин, П. Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками : учебное пособие / П. Н. Девянин. — 2-е изд., испр. и доп. — Москва : Горячая линия-Телеком, 2017. — 338 с. [Электронный ресурс]: — Режим доступа: https://e.lanbook.com/book/111049.

7.2. Дополнительная литература

1. Фомин, Д. В. Информационная безопасность и защита информации: специализированные аттестованные программные и программно-аппаратные средства : методические указания / Д. В. Фомин. — Благовещенск : АмГУ, 2017. — 240 с. [Электронный ресурс]: — Режим доступа: https://e.lanbook.com/book/156494.
2. Ермакова, А. Ю. Методы и средства защиты компьютерной информации : учебное пособие / А. Ю. Ермакова. — Москва : РТУ МИРЭА, 2020. — 223 с. [Электронный ресурс]: — Режим доступа: https://e.lanbook.com/book/163844.

7.3. Учебно-методические пособия

7.3.1. 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.
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.
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.

7.3.2. 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.

7.4. Современные профессиональные базы данных и информационные справочные системы

1. При изучении дисциплины рекомендуется обращаться к современным базам данных, информационно-справочным и поисковым системам, к которым у ТУСУРа открыт доступ: https://lib.tusur.ru/ru/resursy/bazy-dannyh.
2. 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.

8. Материально-техническое и программное обеспечение дисциплины

8.1. 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 достаточным количеством посадочных мест для учебной группы, оборудованная доской и стандартной учебной мебелью. Имеются мультимедийное оборудование и учебно-наглядные пособия, обеспечивающие тематические иллюстрации по лекционным разделам дисциплины.

8.2. Материально-техническое и программное обеспечение для лабораторных работ

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:

- Интерактивная доска IQBoard DVT TN100;
- Проектор Optoma EH400;
- Веб-камера Logitech C920s;
- Усилитель Roxton AA-60M;
- Потолочный громкоговоритель Roxton PA-20T;
- Аппаратные средства аутентификации пользователя "eToken Pro";
- Программно-аппаратный комплекс защиты информации: ПАК ViPNet Coordinator HW100 C 4.x, ПАК ViPNet Coordinator HW1000 4.x;
- Устройства чтения смарт-карт и радиометок: адаптер компьютерный для считывания и передачи в ПК серийных номеров бесконтактных идентификаторов IronLogic Z-2 USB;
- Магнитно-маркерная доска;
- Комплект специализированной учебной мебели;
- Рабочее место преподавателя.

Программное обеспечение:

- Kaspersky endpoint security;
- Microsoft Windows 10;
- VirtualBox;
- Аппаратно-программные средства управления доступом к данным, шифрования: DallasLock;

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:

- Интерактивная доска TraceBoard TS-408L;
- Проектор ViewSonic PJD5154 DLP;
- Комплект специализированной учебной мебели;
- Рабочее место преподавателя.

Программное обеспечение:

- Kaspersky endpoint security;
- KasperskySecurityCenter;
- Microsoft Windows 10;
- VirtualBox;

8.3. 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.

Описание имеющегося оборудования:

- учебная мебель;
- компьютеры;

- компьютеры подключены к сети «Интернет» и обеспечивают доступ в электронную информационно-образовательную среду ТУСУРа.

Перечень программного обеспечения:

- Microsoft Windows;
- OpenOffice;
- Kaspersky Endpoint Security 10 для Windows;
- 7-Zip;
- Google Chrome.

8.4. 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 зрения** 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.

9. Оценочные материалы и методические рекомендации по организации изучения дисциплины

9.1. Содержание оценочных материалов для текущего контроля и промежуточной аттестации

Для оценки степени сформированности и уровня освоения закрепленных за дисциплиной компетенций используются оценочные материалы, представленные в таблице 9.1.

Таблица 9.1 – Формы контроля и оценочные материалы

Названия разделов (тем) дисциплины	Формируемые компетенции	Формы контроля	Оценочные материалы (ОМ)
1 Централизованное управление средствами защиты информации от несанкционированного доступа в локальной сети	ОПК-16, УК-10	Зачёт	Перечень вопросов для зачета
		Лабораторная работа	Темы лабораторных работ
		Тестирование	Примерный перечень тестовых заданий
2 Централизованная инвентаризация ресурсов локальной сети. Удалённый контроль работоспособности средств защиты информации на рабочих станциях	ОПК-16, УК-10	Зачёт	Перечень вопросов для зачета
		Лабораторная работа	Темы лабораторных работ
		Тестирование	Примерный перечень тестовых заданий

3 Централизованная защита от вирусов в локальной сети	ОПК-16, УК-10	Зачёт	Перечень вопросов для зачета
		Лабораторная работа	Темы лабораторных работ
		Тестирование	Примерный перечень тестовых заданий
4 Централизованный учет и управление средствами персональной идентификации и аутентификации	ОПК-16, УК-10	Зачёт	Перечень вопросов для зачета
		Лабораторная работа	Темы лабораторных работ
		Тестирование	Примерный перечень тестовых заданий
5 Анализ нормативных требований по управлению средствами защиты информации	ОПК-16, УК-10	Зачёт	Перечень вопросов для зачета
		Тестирование	Примерный перечень тестовых заданий

Шкала оценки сформированности отдельных планируемых результатов обучения по дисциплине приведена в таблице 9.2.

Таблица 9.2 – Шкала оценки сформированности планируемых результатов обучения по дисциплине

Оценка	Баллы за ОМ	Формулировка требований к степени сформированности планируемых результатов обучения		
		знать	уметь	владеть
2 (неудовлетворительно)	< 60% от максимальной суммы баллов	отсутствие знаний или фрагментарные знания	отсутствие умений или частично освоенное умение	отсутствие навыков или фрагментарные применение навыков
3 (удовлетворительно)	от 60% до 69% от максимальной суммы баллов	общие, но не структурированные знания	в целом успешно, но не систематически осуществляемое умение	в целом успешное, но не систематическое применение навыков
4 (хорошо)	от 70% до 89% от максимальной суммы баллов	сформированные, но содержащие отдельные проблемы знания	в целом успешное, но содержащие отдельные пробелы умение	в целом успешное, но содержащие отдельные пробелы применение навыков
5 (отлично)	≥ 90% от максимальной суммы баллов	сформированные систематические знания	сформированное умение	успешное и систематическое применение навыков

Шкала комплексной оценки сформированности компетенций приведена в таблице 9.3.

Таблица 9.3 – Шкала комплексной оценки сформированности компетенций

Оценка	Формулировка требований к степени компетенции

2 (неудовлетворительно)	Не имеет необходимых представлений о проверяемом материале или Знать на уровне **ориентирования**, представлений. Обучающийся знает основные признаки или термины изучаемого элемента содержания, их отнесенность к определенной науке, отрасли или объектам, узнает в текстах, изображениях или схемах и знает, к каким источникам нужно обращаться для более детального его усвоения.
3 (удовлетворительно)	Знать и уметь на **репродуктивном** уровне. Обучающихся знает изученный элемент содержания репродуктивно: произвольно воспроизводит свои знания устно, письменно или в демонстрируемых действиях.
4 (хорошо)	Знать, уметь, владеть на **аналитическом** уровне. Зная на репродуктивном уровне, указывать на особенности и взаимосвязи изученных объектов, на их достоинства, ограничения, историю и перспективы развития и особенности для разных объектов усвоения.
5 (отлично)	Знать, уметь, владеть на **системном** уровне. Обучающийся знает изученный элемент содержания системно, произвольно и доказательно воспроизводит свои знания устно, письменно или в демонстрируемых действиях, учитывая и указывая связи и зависимости между этим элементом и другими элементами содержания дисциплины, его значимость в содержании дисциплины.

9.1.1. Примерный перечень тестовых заданий

1. Какой из методов контроля целостности файлов отсутствует в СЗИ от НСД Secret Net Studio?
   a) Контроль содержимого
   b) Контроль атрибутов
   c) Контроль санкционированных изменений
   d) Контроль существования
2. Для чего предназначена программа оперативного управления Secret Net Studio?
   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. Какие типовые задачи администратора безопасности Secret Net Studio НЕ относятся к настройке параметров системы защиты?
   a) Редактирование структуры оперативного управления
   b) Настройка параметров сбора локальных журналов
   c) Контролирование состояния защищенности системы
   d) Настройка параметров сетевых соединений
4. Какие типовые задачи администратора безопасности Secret Net Studio НЕ относятся к мониторингу и управлению системой защиты?
   a) Контролирование и оповещение о произошедших событиях несанкционированного доступа
   b) Контролирование текущего состояния защищаемых компьютеров
   c) Настройка почтовой рассылки уведомлений о тревогах
   d) Выполнение действий с защищаемыми компьютерами при возникновении угроз для безопасности системы
5. Для чего необходимо квитирование тревог в системе Secret Net Studio?
   a) Для устранения последствий тревоги
   b) Для предотвращения тревог в будущем
   c) Для фиксации реакции администратора безопасности на тревогу
   d) Для удаления тревоги из журналов аудита
6. 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

7. 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
8. 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 Studio?
   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
9. Какой из вариантов ответов НЕ используется для оперативного извещения администратора безопасности о тревогах в программе оперативного управления Secret Net Studio?
   a) Визуальное отображение тревоги 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 тревоги
10. Каким мерам защиты информации в государственных информационных системах позволяет удовлетворить механизм замкнутой программной среды Secret Net Studio?
    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
11. Какую подсистему в системе Secret Net Studio следует использовать для реализации меры защиты информации в государственных информационных системах «Контроль использования интерфейсов ввода (вывода) информации на машинные носители информации»?
    a) Модуль входа
    b) Подсистема контроля целостности
    c) Подсистема разграничения доступа к устройствам
    d) Замкнутая программная среда
12. Какую из мер защиты информации в государственных информационных системах не позволяет реализовать СЗИ от НСД Secret Net Studio?
    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) Защита информации, обрабатываемой техническими средствами, от ее утечки по техническим каналам
    d) Управление доступом к машинным носителям информации

13. Какую подсистему в системе Secret Net Studio следует использовать для реализации меры защиты информации в государственных информационных системах «Мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них»?
    a) Подсистема контроля целостности
    b) Подсистема разграничения доступа к устройствам
    c) Подсистема оперативного управления
    d) Замкнутая программная среда
14. 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 Studio
    c) SafeNet Authentication Manager
    d) Kaspersky Security Center
15. Для чего предназначен механизм контроля подключения и изменения устройств в СЗИ от НСД Secret Net Studio?
    a) Для слежения за неизменностью содержимого ресурсов компьютера
    b) Для ограничения использования ПО на компьютере
    c) Для обнаружения и реагирования на изменения аппаратной конфигурации компьютера
    d) Для централизованного управления защищаемыми компьютерами
16. Для чего предназначен механизм контроля целостности (КЦ) в СЗИ от НСД Secret Net Studio?
    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 Secret Net Studio?
    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. Какие режимы для замкнутой программной среды существуют в СЗИ от НСД Secret Net Studio?
    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. Какой из перечисленных защитных механизмов Secret Net Studio НЕ используется для обеспечения защиты информации ограниченного доступа?
    a) Контроль целостности
    b) Разграничение доступа к устройствам
    c) Идентификация и аутентификация пользователей
    d) Полномочное разграничение доступа
21. Согласно приказу ФСТЭК России от 11 февраля 2013 г. N 17 об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, какое из действий НЕ относится к

выявлению инцидентов информационной безопасности и реагированию на них?

a) Определение лиц, ответственных за выявление инцидентов

b) Анализ инцидентов, в том числе определение источников и причин возникновения инцидентов, а также оценка их последствий

c) Определение лиц, которым разрешены действия по внесению изменений в базовую конфигурацию информационной системы и ее системы защиты информации

d) Планирование и принятие мер по предотвращению повторного возникновения инцидентов

22. Согласно приказу ФСТЭК России от 11 февраля 2013 г. N 17 об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, какое из действий относится к контролю (мониторингу) за обеспечением уровня защищенности информации, содержащейся в информационной системе?

a) Анализ инцидентов, в том числе определение источников и причин возникновения инцидентов, а также оценка их последствий

b) Определение параметров настройки программного обеспечения, включая программное обеспечение средств защиты информации, состава и конфигурации технических средств и программного обеспечения до внесения изменений в базовую конфигурацию информационной системы и ее системы защиты информации

c) Анализ и оценка функционирования системы защиты информации информационной системы, включая выявление, анализ и устранение недостатков в функционировании системы защиты информации информационной системы

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

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

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 Secret Net Studio?

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 Secret Net Studio?

a) Принтеры

b) USB-носители

c) Сетевые карты

d) CD-приводы

26. Какое аппаратное средство защиты НЕ применяется совместно с СЗИ от НСД Secret Net Studio?
    a) Аппаратные идентификаторы «eToken»
    b) Программно-аппаратный комплекс «Соболь»
    c) Программно-аппаратный комплекс «Аккорд»
    d) Плата «Secret Net Card»
27. 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
28. 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
29. 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 Studio
    d) Kaspersky Security Center

9.1.2. Перечень вопросов для зачета

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.

9.1.3. Темы лабораторных работ

1. Secret Net Studio. Разграничение доступа к данным. Разграничение доступа к устройствам. Контроль печати конфиденциальных данных.
2. Secret Net Studio. Замкнутая программная среда. Контроль целостности.
3. Secret Net Studio. 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
5. “КБ Инвентаризация”. Проведение инспекций и учет изменений конфигурации защищаемых рабочих станций.
6. Управление серверами администрирования "Kaspersky Security Center"
7. Управление жизненным циклом средств аутентификации eToken с помощью Safenet Authentication Manager.

9.2. Методические рекомендации

Учебный материал излагается в форме, предполагающей самостоятельное мышление студентов, самообразование. При этом самостоятельная работа студентов играет решающую роль в ходе всего учебного процесса.

Начать изучение дисциплины необходимо со знакомства с рабочей программой, списком учебно-методического и программного обеспечения. Самостоятельная работа студента включает работу с учебными материалами, выполнение контрольных мероприятий, предусмотренных учебным планом.

В процессе изучения дисциплины для лучшего освоения материала необходимо регулярно обращаться к рекомендуемой литературе и источникам, указанным в учебных материалах; пользоваться через кабинет студента на сайте Университета образовательными ресурсами электронно-библиотечной системы, а также общедоступными интернет-порталами, содержащими научно-популярные и специализированные материалы, посвященные различным аспектам учебной дисциплины.

При самостоятельном изучении тем следуйте рекомендациям:

– чтение или просмотр материала осуществляйте со скоростью, достаточной для индивидуального понимания и освоения материала, выделяя основные идеи; на основании изученного составить тезисы. Освоив материал, попытаться соотнести теорию с примерами из практики;

– если в тексте встречаются незнакомые или малознакомые термины, следует выяснить их значение для понимания дальнейшего материала;

– осмысливайте прочитанное и изученное, отвечайте на предложенные вопросы.

Студенты могут получать индивидуальные консультации, в т.ч. с использованием средств телекоммуникации.

По дисциплине могут проводиться дополнительные занятия, в т.ч. в форме вебинаров. Расписание вебинаров и записи вебинаров публикуются в электронном курсе / электронном журнале по дисциплине.

9.3. 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 9.2.

Таблица 9.2 – 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, определяющимися исходя из состояния обучающегося на момент проверки

9.4. 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.

ЛИСТ СОГЛАСОВАНИЯ

Рассмотрена и одобрена на заседании кафедры БИС
протокол № 11 от «14» 12 2020 г.

СОГЛАСОВАНО:

Должность	Инициалы, фамилия	Подпись
Заведующий выпускающей каф. БИС	Е.Ю. Костюченко	Согласовано, c6235dfe-234a-4234-88f9-e1597aac6463
Заведующий обеспечивающей каф. БИС	Е.Ю. Костюченко	Согласовано, c6235dfe-234a-4234-88f9-e1597aac6463
Начальник учебного управления	Е.В. Саврук	Согласовано, fa63922b-1fce-4a6a-845d-9ce7670b004c

ЭКСПЕРТЫ:

Доцент, каф. КИБЭВС	А.А. Конев	Согласовано, 81687a04-85ce-4835-9e1e-9934a6085fdd
Доцент, каф. КИБЭВС	К.С. Сарин	Согласовано, 68c81ca0-0954-467a-8d01-f93a0d553669

РАЗРАБОТАНО:

Доцент, каф. БИС	И.А. Рахманенко	Разработано, 438e5305-e83a-40ae-b333-7c84f2fc4661