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 УР
_____Сенченко П.В.
«18» _____02_____ 2022 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

АДМИНИСТРИРОВАНИЕ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ

Уровень образования: **высшее образование - магистратура**
Направление подготовки / специальность: **10.04.01 Информационная безопасность**
Направленность (профиль) / специализация: **Информационная безопасность объектов критической информационной инфраструктуры**
Форма обучения: **очная**
Факультет: **Факультет безопасности (ФБ)**
Кафедра: **Кафедра комплексной информационной безопасности электронно-вычислительных систем (КИБЭВС)**
Курс: **1**
Семестр: **1**
Учебный план набора 2023 года

Объем дисциплины и виды учебной деятельности

Виды учебной деятельности	1 семестр	Всего	Единицы
Лекционные занятия	18	18	часов
Лабораторные занятия	36	36	часов
Самостоятельная работа	54	54	часов
Подготовка и сдача экзамена	36	36	часов
Общая трудоемкость (включая промежуточную аттестацию)	144	144	часов
	4	4	з.е.

Формы промежуточной аттестация	Семестр
Экзамен	1

Томск

Согласована на портале № 63968

1. Общие положения

1.1. Цели дисциплины

1. Освоение методов 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 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 направления подготовки (hard skills – HS).
Индекс дисциплины: Б1.О.2.1.
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		
-	-	-
Общепрофессиональные компетенции		

Согласована на портале № 63968

ОПК-1. Способен обосновывать требования к системе обеспечения информационной безопасности и разрабатывать проект технического задания на ее создание;	ОПК-1.1. Знает меры (организационные, технические) и технологии обеспечения информационной безопасности	Знает организационные и технические меры, применяемые при администрировании средств защиты информации объектов критической информационной инфраструктуры
	ОПК-1.2. Знает уязвимости систем и угрозы информационной безопасности	Знает методы выявления уязвимостей систем и угрозы информационной безопасности объектов критической информационной инфраструктуры.
	ОПК-1.3. Знает нормативную базу и ГОСТы, регламентирующие процесс разработки технических заданий на создание систем обеспечения информационной безопасности объектов	Знает нормативную базу и ГОСТы, регламентирующие процесс разработки технических заданий на создание средств защиты информации объектов критической информационной инфраструктуры.
	ОПК-1.4. Умеет обосновывать требования к процессам и технологиям обеспечения информационной безопасности	Умеет обосновывать требования к процессам и технологиям обеспечения информационной безопасности объектов критической информационной инфраструктуры
	ОПК-1.5. Умеет осуществлять выбор подсистем, реализующих технологии обеспечения информационной безопасности	Умеет осуществлять выбор средств защиты информации объектов критической информационной инфраструктуры.
	ОПК-1.6. Умеет обосновывать требования к мерам обеспечения информационной безопасности	Умеет обосновывать требования к мерам обеспечения информационной безопасности объектов критической информационной инфраструктуры
	ОПК-1.7. Умеет разрабатывать техническое задание на создание подсистемы обеспечения информационной безопасности	Умеет разрабатывать техническое задание на создание средств защиты информации объектов критической информационной инфраструктуры.
	ОПК-1.8. Знает отечественные и зарубежные стандарты в области обеспечения информационной безопасности	Знает отечественные и зарубежные стандарты в области обеспечения информационной безопасности объектов критической информационной инфраструктуры
	ОПК-1.9. Знает нормативную и правовую базу в области обеспечения информационной безопасности, нормативные методические документы ФСБ России, ФСТЭК России и иных регуляторов в области обеспечения информационной безопасности	Знает нормативную и правовую базу в области обеспечения информационной безопасности объектов критической информационной инфраструктуры
	ОПК-1.10. Знает основы управления рисками информационной безопасности	Знает основы управления рисками информационной безопасности объектов критической информационной инфраструктуры
	ОПК-1.11. Умеет оценивать риски информационной безопасности	Умеет оценивать риски информационной безопасности объектов критической информационной инфраструктуры

Согласована на портале № 63968

ОПК-5. Способен проводить научные исследования, включая экспериментальные, обрабатывать результаты исследований, оформлять научно-технические отчеты, обзоры, готовить по результатам выполненных исследований научные доклады и статьи	ОПК-5.1. Знает теоретические и экспериментальные методы и средства научных исследований	Знает методы и средства научных исследований в области обеспечения информационной безопасности объектов критической информационной инфраструктуры.
	ОПК-5.2. Знает методы обработки результатов исследований	Знает методы проверки получаемых результатов исследования по обеспечению безопасности объектов критической информационной инфраструктуры.
	ОПК-5.3. Знает методику проведения патентных исследований	Знает методику проведения патентного поиска по тематике исследования и способен оформить его результаты в формате краткого аналитического отчета.
	ОПК-5.4. Знает правила и стандарты разработки отчетной документации, требования ГОСТов на оформление научно-технической документации	Знает правила и стандарты разработки отчетной документации по объектам критической информационной инфраструктуры, требования ГОСТов на оформление научно-технической документации.
	ОПК-5.5. Умеет составлять отчеты о проведенных научных исследованиях, в том числе на иностранном языке	Умеет составлять отчеты о проведенных научных исследованиях в области безопасности объектов критической информационной инфраструктуры, в том числе на иностранном языке.
	ОПК-5.6. Умеет оформлять результаты научных исследований в виде научно-технические отчетов, обзоров, научных докладов и статей	Умеет оформлять результаты научных исследований в области безопасности объектов критической информационной инфраструктуры в виде научно-технические отчетов, обзоров, научных докладов и статей.
	ОПК-5.7. Умеет представлять результаты научно-исследовательской деятельности в виде презентаций, устных докладов, вести научные дискуссии, в том числе на иностранном языке	Умеет представлять результаты научно-исследовательской деятельности в области безопасности объектов критической информационной инфраструктуры в виде презентаций, устных докладов, вести научные дискуссии, в том числе на иностранном языке
Профессиональные компетенции		

Согласована на портале № 63968

ПК-1. Способен обеспечивать анализ, проектирование, разработку, функционирование, эксплуатацию систем информационной безопасности объектов критической информационной инфраструктуры и ее частей;	ПК-1.1. Знает общие принципы проектирования систем информационной безопасности объектов критической информационной инфраструктуры и ее частей, принципы построения систем информационной безопасности объектов критической информационной инфраструктуры и ее частей, состав технико-экономического обоснования проектируемых систем информационной безопасности объектов критической информационной инфраструктуры и ее частей;	Знает общие принципы проектирования средств защиты информации объектов критической информационной инфраструктуры
	ПК-1.2. Умеет разрабатывать необходимую техническую документацию в области проектирования систем информационной безопасности объектов критической информационной инфраструктуры и ее частей с учетом действующих нормативных и методических документов, проводить подготовку исходных данных для технико-экономического обоснования проектируемых систем информационной безопасности объектов критической информационной инфраструктуры и ее частей	Умеет разрабатывать необходимую техническую документацию по администрированию средств защиты информации объектов критической информационной инфраструктуры
	ПК-1.3. Владеет навыками проектирования элементов систем информационной безопасности объектов критической информационной инфраструктуры	Владеет навыками проектирования элементов средств защиты информации объектов критической информационной инфраструктуры

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

Согласована на портале № 63968

и на самостоятельную работу обучающихся

Общая трудоемкость дисциплины составляет 4 зачетных единиц, 144 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
		1 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 тестированию	10	10
Подготовка к лабораторной работе, написание отчета	26	26
Написание конспекта самоподготовки	18	18
Подготовка и сдача экзамена	36	36
Общая трудоемкость (в часах)	144	144
Общая трудоемкость (в з.е.)	4	4

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
1 семестр					
1 Централизованное управление средствами защиты информации от несанкционированного доступа в локальной сети	4	20	16	40	ОПК-1, ОПК-5, ПК-1
2 Централизованная инвентаризация ресурсов локальной сети. Удалённый контроль работоспособности средств защиты информации на рабочих станциях	2	4	9	15	ОПК-1, ОПК-5, ПК-1
3 Централизованная защита от вирусов в локальной сети	4	6	12	22	ОПК-1, ОПК-5, ПК-1
4 Централизованный учет и управление программно-аппаратными средствами защиты информации	4	6	12	22	ОПК-1, ОПК-5, ПК-1
5 Анализ нормативных требований по управлению средствами защиты информации	4	-	5	9	ОПК-1, ОПК-5, ПК-1
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)

Согласована на портале № 63968

Названия разделов (тем) дисциплины	Содержание разделов (тем) дисциплины (в т.ч. по лекциям)	Трудоемкость (лекционные занятия), ч	Формируемые компетенции
1 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	ОПК-1, ОПК-5, ПК-1
	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	ОПК-1, ОПК-5, ПК-1
	Итого	2	
3 Централизованная защита от вирусов в локальной сети	Управление серверами администрирования; управление группами администрирования; управление клиентскими компьютерами; работа с отчетами, статистикой.	4	ОПК-1, ОПК-5, ПК-1
	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	ОПК-1, ОПК-5, ПК-1
	Итого	4	

Согласована на портале № 63968

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-1, ОПК-5, ПК-1
	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
1 семестр			
1 Централизованное управление средствами защиты информации от несанкционированного доступа в локальной сети	Разграничение доступа к устройствам.	6	ОПК-1, ОПК-5, ПК-1
	Замкнутая программная среда. Контроль целостности	4	ОПК-1, ОПК-5, ПК-1
	Работа со сведениями в журнале регистрации событий. Теневое копирование	4	ОПК-1, ОПК-5, ПК-1
	Оперативное управление защищаемыми рабочими станциями и мониторинг событий информационной безопасности	6	ОПК-1, ОПК-5, ПК-1
	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-1, ОПК-5, ПК-1
	Итого	4	

Согласована на портале № 63968

3 Централизованная защита от вирусов в локальной сети	Управление серверами администрирования "Kaspersky Security Center"	6	ОПК-1, ОПК-5, ПК-1
	Итого	6	
4 Централизованный учет и управление программно-аппаратными средствами защиты информации	Управление жизненным циклом средств аутентификации eToken с помощью Safenet Authentication Manager.	6	ОПК-1, ОПК-5, ПК-1
	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
1 семестр				
1 Централизованное управление средствами защиты информации от несанкционированного доступа в локальной сети	Подготовка к тестированию	2	ОПК-1, ОПК-5, ПК-1	Тестирование
	Подготовка к лабораторной работе, написание отчета	10	ОПК-1, ОПК-5, ПК-1	Лабораторная работа
	Написание конспекта самоподготовки	4	ОПК-1, ОПК-5, ПК-1	Конспект самоподготовки
	Итого	16		
2 Централизованная инвентаризация ресурсов локальной сети. Удалённый контроль работоспособности средств защиты информации на рабочих станциях	Подготовка к тестированию	2	ОПК-1, ОПК-5, ПК-1	Тестирование
	Подготовка к лабораторной работе, написание отчета	4	ОПК-1, ОПК-5, ПК-1	Лабораторная работа
	Написание конспекта самоподготовки	3	ОПК-1, ОПК-5, ПК-1	Конспект самоподготовки
	Итого	9		

Согласована на портале № 63968

3 Централизованная защита от вирусов в локальной сети	Подготовка к тестированию	2	ОПК-1, ОПК-5, ПК-1	Тестирование
	Подготовка к лабораторной работе, написание отчета	6	ОПК-1, ОПК-5, ПК-1	Лабораторная работа
	Написание конспекта самоподготовки	4	ОПК-1, ОПК-5, ПК-1	Конспект самоподготовки
	Итого	12		
4 Централизованный учет и управление программно-аппаратными средствами защиты информации	Подготовка к тестированию	2	ОПК-1, ОПК-5, ПК-1	Тестирование
	Подготовка к лабораторной работе, написание отчета	6	ОПК-1, ОПК-5, ПК-1	Лабораторная работа
	Написание конспекта самоподготовки	4	ОПК-1, ОПК-5, ПК-1	Конспект самоподготовки
	Итого	12		
5 Анализ нормативных требований по управлению средствами защиты информации	Подготовка к тестированию	2	ОПК-1, ОПК-5, ПК-1	Тестирование
	Написание конспекта самоподготовки	3	ОПК-1, ОПК-5, ПК-1	Конспект самоподготовки
	Итого	5		
Итого за семестр		54		
	Подготовка и сдача экзамена	36		Экзамен
Итого		90		

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-1	+	+	+	Конспект самоподготовки, Лабораторная работа, Тестирование, Экзамен
ОПК-5	+	+	+	Конспект самоподготовки, Лабораторная работа, Тестирование, Экзамен
ПК-1	+	+	+	Конспект самоподготовки, Лабораторная работа, Тестирование, Экзамен

6. Рейтинговая система для оценки успеваемости обучающихся

6.1. Балльные оценки для форм контроля

Согласована на портале № 63968

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
1 семестр				
Конспект самоподготовки	5	5	5	15
Лабораторная работа	15	15	15	45
Тестирование	0	0	10	10
Экзамен				30
Итого максимум за период	20	20	30	100
Нарастающим итогом	20	40	70	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. Мошак, Н. Н. Защищенные информационные системы : учебное пособие / Н. Н. Мошак, Л. К. Птицына. — Санкт-Петербург : СПбГУТ им. М.А. Бонч-Бруевича, 2020. — 216 с. [Электронный ресурс]: — Режим доступа: https://e.lanbook.com/book/180099.

2. Маршаков, Д. В. Программно-аппаратные средства защиты информации : учебное пособие / Д. В. Маршаков, Д. В. Фатхи. — Ростов-на-Дону : Донской ГТУ, 2021. — 228 с. — ISBN 978-5-7890-1878-1. [Электронный ресурс]: — Режим доступа: https://e.lanbook.com/book/237770.

7.2. Дополнительная литература

Согласована на портале № 63968

1. Основы информационной безопасности : учебное пособие / Е. Б. Белов, В. П. Лось, Р. В. Мещеряков, А. А. Шелупанов. — Москва : Горячая линия-Телеком, 2011. — 558 с. — ISBN 5-93517-292-5. [Электронный ресурс]: — Режим доступа: https://e.lanbook.com/book/111016.

7.3. Учебно-методические пособия

7.3.1. Обязательные учебно-методические пособия

1. Рахманенко, И.А. Администрирование средств защиты информации: Учебно-методическое пособие/ И. А. Рахманенко, А.Ю. Якимук. — Томск: ТУСУР, 2022. — 166 с. [Электронный ресурс]: — Режим доступа: https://edu.tusur.ru/publications/9988.

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.

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;

Согласована на портале № 63968

- Магнитно-маркерная доска;
- Комплект специализированной учебной мебели;
- Рабочее место преподавателя.

Программное обеспечение:
- 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, 209 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)

Согласована на портале № 63968

1 Централизованное управление средствами защиты информации от несанкционированного доступа в локальной сети	ОПК-1, ОПК-5, ПК-1	Конспект самоподготовки	Примерный перечень тем для конспектов самоподготовки
		Лабораторная работа	Темы лабораторных работ
		Тестирование	Примерный перечень тестовых заданий
		Экзамен	Перечень экзаменационных вопросов
2 Централизованная инвентаризация ресурсов локальной сети. Удалённый контроль работоспособности средств защиты информации на рабочих станциях	ОПК-1, ОПК-5, ПК-1	Конспект самоподготовки	Примерный перечень тем для конспектов самоподготовки
		Лабораторная работа	Темы лабораторных работ
		Тестирование	Примерный перечень тестовых заданий
		Экзамен	Перечень экзаменационных вопросов
3 Централизованная защита от вирусов в локальной сети	ОПК-1, ОПК-5, ПК-1	Конспект самоподготовки	Примерный перечень тем для конспектов самоподготовки
		Лабораторная работа	Темы лабораторных работ
		Тестирование	Примерный перечень тестовых заданий
		Экзамен	Перечень экзаменационных вопросов
4 Централизованный учет и управление программно-аппаратными средствами защиты информации	ОПК-1, ОПК-5, ПК-1	Конспект самоподготовки	Примерный перечень тем для конспектов самоподготовки
		Лабораторная работа	Темы лабораторных работ
		Тестирование	Примерный перечень тестовых заданий
		Экзамен	Перечень экзаменационных вопросов
5 Анализ нормативных требований по управлению средствами защиты информации	ОПК-1, ОПК-5, ПК-1	Конспект самоподготовки	Примерный перечень тем для конспектов самоподготовки
		Тестирование	Примерный перечень тестовых заданий
		Экзамен	Перечень экзаменационных вопросов

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

Согласована на портале № 63968

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

Согласована на портале № 63968

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

Согласована на портале № 63968

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

Согласована на портале № 63968

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

Согласована на портале № 63968

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 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

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

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»

Согласована на портале № 63968

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

9.1.2. Перечень экзаменационных вопросов

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?

Согласована на портале № 63968

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. Примерный перечень тем для конспектов самоподготовки

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 несанкционированного доступа в локальной сети.
7. Централизованный учет и управление программно-аппаратными средствами защиты информации.

9.1.4. Темы лабораторных работ

1. Разграничение доступа к устройствам.
2. Замкнутая программная среда. Контроль целостности
3. 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

Согласована на портале № 63968

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

Согласована на портале № 63968

процедура оценивания результатов обучения может проводиться в несколько этапов.

ЛИСТ СОГЛАСОВАНИЯ

Рассмотрена и одобрена на заседании кафедры КИБЭВС
протокол № 1 от «25» 1 2022 г.

СОГЛАСОВАНО:

Должность	Инициалы, фамилия	Подпись
Заведующий выпускающей каф. КИБЭВС	А.А. Шелупанов	Согласовано, c53e145e-8b20-45aa-9347-a5e4dbb90e8d
Заведующий обеспечивающей каф. КИБЭВС	А.А. Шелупанов	Согласовано, c53e145e-8b20-45aa-9347-a5e4dbb90e8d
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	Е.Ю. Костюченко	Согласовано, c6235dfe-234a-4234-88f9-e1597aac6463

РАЗРАБОТАНО:

Доцент, каф. КИБЭВС	А.Ю. Якимук	Разработано, 4ffdf265-fb78-4863-b293-f03438cb07cc
Доцент, каф. БИС	И.А. Рахманенко	Разработано, 438e5305-e83a-40ae-b333-7c84f2fc4661

Согласована на портале № 63968