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
_____П.В. Сенченко
«23» _____12_____ 2020 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

ПРОГРАММНО-АППАРАТНЫЕ СРЕДСТВА ЗАЩИТЫ СЕТЕЙ И СИСТЕМ СВЯЗИ

Уровень образования: **высшее образование - бакалавриат**
Направление подготовки / специальность: **11.03.02 Инфокоммуникационные технологии и системы связи**
Направленность (профиль) / специализация: **Защищенные системы и сети связи**
Форма обучения: **очная**
Факультет: **Радиотехнический факультет (РТФ)**
Кафедра: **Кафедра радиоэлектроники и систем связи (РСС)**
Курс: **4**
Семестр: **7**
Учебный план набора 2021 года

Объем дисциплины и виды учебной деятельности

Виды учебной деятельности	7 семестр	Всего	Единицы
Лекционные занятия	26	26	часов
Практические занятия	18	18	часов
в т.ч. в форме практической подготовки	18	18	часов
Лабораторные занятия	16	16	часов
в т.ч. в форме практической подготовки	16	16	часов
Самостоятельная работа	48	48	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	7

Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Сенченко П.В.
Должность: Проректор по УР
Дата подписания: 23.12.2020
Уникальный программный ключ:
a1119608-cdff-4455-b54e-5235117c185c

Томск

Согласована на портале № 59936

1. Общие положения

1.1. Цели дисциплины

1. Изучение способов защиты информационных процессов в сетях с гибридной физической средой.
2. Изучение возможностей применения программно-аппаратных средств в сетях связи для повышения их защищенности.
3. Работа в компьютерных вычислительных сетях (ВС) с применением программных средств защиты и использования существующих, встроенных в архитектуру ОС, средств связи.

1.2. Задачи дисциплины

1. Изучение способов создания защищенного сетевого соединения, защищенных протоколов связи, защиты от несанкционированного доступа сообщений электронной почты, сетевых ресурсов.
2. Изучение принципов работы брандмауэров, средств предотвращения вторжений, антивирусных программ на основе использования аппаратных средств защиты.
3. Развитие навыков настройки и анализа программных средств защиты, политик безопасности, использования программных отладчиков, сетевых анализаторов.

2. Место дисциплины в структуре ОПОП

Блок дисциплин: Б1. Дисциплины (модули).
Часть блока дисциплин: Часть, формируемая участниками образовательных отношений.
Модуль дисциплин: Модуль направленности (профиля) (major).
Индекс дисциплины: Б1.В.02.14.
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		
-	-	-
Профессиональные компетенции		

Согласована на портале № 59936

ПКР-6. Способен оценивать параметры безопасности и защищать программное обеспечение и сетевые устройства администрируемой сети с помощью специальных средств управления безопасностью	ПКР-6.1. Знает архитектуру, протоколы и общие принципы функционирования аппаратных, программных и программно аппаратных средств администрируемой сети.	Владеет способами настройки протоколов передачи в компьютерных сетях, учитывает связь программных модулей с их аппаратной реализацией, использует свойства моделей доступа для организации доверительного сегмента сети, настраивает антивирусное программное обеспечение, учитывая средства защиты операционной системы, устанавливает многофакторную аутентификацию и идентификацию, использует отечественное оборудование для защиты компьютерной системы.
	ПКР-6.2. Знает основные принципы, криптографические протоколы и программные средства обеспечения информационной безопасности сетевых устройств.	Использует протоколы простой аутентификации, строгой аутентификации и протоколы доказательства с нулевым разглашением, осуществляет подпись документов различными видами цифровой подписи в том числе и при использовании совместно с токенами, применяет передачу данных защищенными протоколами в том числе с использованием технологий VPN
	ПКР-6.3. Умеет применять программные, аппаратные и программно-аппаратные средства защиты сетевых устройств от несанкционированного доступа.	Установит средства доверительной загрузки операционной системы, настроит токены для организации многофакторной аутентификации, использует системы обнаружения вторжений в компьютерную систему и анализаторы ее уязвимостей.
	ПКР-6.4. Пользоваться нормативно-технической документацией в области обеспечения информационной безопасности инфокоммуникационных систем.	Определяет наличие сертификатов ФСТЭК, ФСБ на электронное оборудование и программные комплексы, использует рекомендации, указанные в технической документации при обслуживании КС и установке программного обеспечения, выбирает рекомендованные средства доверенной загрузки операционной системы.
	ПКР-6.5. Владеет навыками и средствами установки и управления специализированными программными средствами защиты сетевых устройств администрируемой сети от несанкционированного доступа.	Устанавливает и настраивает сетевое оборудование - маршрутизаторы, коммутаторы, формирует заданную топологию компьютерной сети и ее многоуровневую IP адресацию, использует средства VPN и защищенные протоколы для работы сети, устанавливает различного рода сетевые фильтры для защиты от несанкционированного доступа.

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 4 зачетных единиц, 144 академических часов. Распределение трудоемкости дисциплины по видам учебной деятельности представлено в

Согласована на портале № 59936

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	60	60
Лекционные занятия	26	26
Практические занятия	18	18
Лабораторные занятия	16	16
Самостоятельная работа обучающихся, в т.ч. контактная внеаудиторная работа обучающихся с преподавателем, всего	48	48
Подготовка к тестированию	20	20
Написание отчета по практическому занятию (семинару)	10	10
Подготовка к лабораторной работе, написание отчета	10	10
Написание отчета по лабораторной работе	8	8
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	Прак. зан., ч	Лаб. раб.	Сам. раб., ч	Всего часов (без экзамена)	Формируемые компетенции
7 семестр						
1 Архитектура программно-аппаратных средств защиты ОС. Причины возникновения сбоев в оперативной памяти, общие принципы построения систем защиты (triple functions).	2	4	-	4	10	ПКР-6
2 Основные понятия, классификация задач, решаемых программно-аппаратными средствами идентификации и аутентификации в сетях связи. Общеизвестные случаи результатов слабой защиты сетевых коммуникаций.	4	2	4	8	18	ПКР-6
3 Основные угрозы КС. История создания избирательной и полномочной политики безопасности. Понятия субъектов и объектов доступа.	4	-	-	2	6	ПКР-6
4 Виды аудита компьютерных сетей и систем связи с помощью программно-аппаратных средств, классификация событий для проведения аудита.	4	4	4	10	22	ПКР-6

Согласована на портале № 59936

5 Программно-аппаратные средства шифрования; построение аппаратных компонент криптозащиты данных. Инфраструктура управления открытыми ключами, базовые архитектуры систем управления сертификатами.	2	-	-	2	4	ПКР-6
6 Программно-аппаратные методы и средства ограничения доступа к компонентам связи в компьютерных сетях и защиты программ от несанкционированного копирования. Вирусы, их анализ, антивирусные программы.	2	-	4	6	12	ПКР-6
7 Применение смарт-карт для аппаратной защиты данных, их классификация. Аппаратные компоненты смарт-карт. Программное обеспечение для смарт-карт.	2	-	-	2	4	ПКР-6
8 Радиочастотная идентификация -пример удаленной защиты данных с помощью аппаратных средств. Классификация средств RFID, структура и функционирование систем RFID.	2	4	-	4	10	ПКР-6
9 Разрушающие программные воздействия с помощью программно-аппаратных средств. Способы использования микроконтроллеров и одноплатных микрокомпьютеров для доступа в защищенные сети связи.	2	4	4	8	18	ПКР-6
10 Способы защиты от разрушающих программных воздействий (РПВ) в компьютерных системах связи с помощью программно-аппаратных средств.	2	-	-	2	4	ПКР-6
Итого за семестр	26	18	16	48	108	
Итого	26	18	16	48	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			

Согласована на портале № 59936

1 Архитектура программно-аппаратных средств защиты ОС. Причины возникновения сбоев в оперативной памяти, общие принципы построения систем защиты (triple functions).	Предмет и задачи защиты информации в сетях и системах связи с помощью программно-аппаратных средств, ее взаимосвязь с другими дисциплинами. Краткая история развития. Актуальность защиты информации в современном мире. Причины возникновения аппаратных и программных уязвимостей, общие принципы построения систем защиты (triple functions). Понятие политики безопасности и необходимости оценки рисков, критерии, используемые для классификации уровня защищенности (безопасности) компьютерных сетей и системы связи.	2	ПКР-6
	Итого	2	
2 Основные понятия, классификация задач, решаемых программно-аппаратными средствами идентификации и аутентификации в сетях связи. Общеизвестные случаи результатов слабой защиты сетевых коммуникаций.	Основные понятия, классификация задач, решаемых программно-аппаратными средствами идентификации и аутентификации. Идентификация субъекта с помощью аппаратных средств, понятие протокола идентификации, идентифицирующая информация. Методы аутентификации: парольная схема, биометрический и token способы, многофакторная и взаимная аутентификации. Протоколы идентификации с нулевой передачей знаний.	4	ПКР-6
	Итого	4	

Согласована на портале № 59936

3 Основные угрозы КС. История создания избирательной и полномочной политики безопасности. Понятия субъектов и объектов доступа.	Классификация субъектов и объектов доступа. Основные аппаратные подходы к защите данных от НСД. Абстрактные модели доступа. Программно-аппаратное шифрование, контроль доступа и разграничение доступа. Иерархический принцип доступа к файлу. Аппаратная защита сетевого файлового ресурса. Программная фиксация доступа к файлам. Дискреционная (разграничительная) модель управления доступом. Способы программно-аппаратной фиксации факта доступа. Надежность систем ограничения доступа. Мандатная (представительная) модель управления доступом. Программная реализации мандатной модели доступа.	4	ПКР-6
	Итого	4	
4 Виды аудита компьютерных сетей и систем связи с помощью программно-аппаратных средств, классификация событий для проведения аудита.	Виды аудита компьютерных систем связи с помощью программно-аппаратных средств. Контроль целостности данных, использование цифровой подписи с защитой аппаратными средствами. Программные системы предотвращения и обнаружения вторжений, локальные и беспроводные.	4	ПКР-6
	Итого	4	

Согласована на портале № 59936

5 Программно-аппаратные средства шифрования; построение аппаратных компонент криптозащиты данных. Инфраструктура управления открытыми ключами, базовые архитектуры систем управления сертификатами.	Генерация ключей программно-аппаратными средствами. Ключи для симметричных и несимметричных алгоритмов. Эфемерный ключ. Программно-аппаратные средства шифрования в реальном времени, построение аппаратных компонент криптозащиты данных. Угрозы криптографическим ключам. Повреждение ключей. Защита алгоритма шифрования. Принцип чувствительной области и принцип главного ключа, необходимые и достаточные функции аппаратного средства криптозащиты систем связи.	2	ПКР-6
	Итого	2	
6 Программно-аппаратные методы и средства ограничения доступа к компонентам связи в компьютерных сетях и защиты программ от несанкционированного копирования. Вирусы, их анализ, антивирусные программы.	Программно-аппаратные методы и средства ограничения доступа к компонентам ЭВМ, защиты программ от несанкционированного копирования. Программные и технические средства защиты информации в системах связи. Встроенная аппаратная защита программ от излучения. Устаревшие технические средства защиты. Программная защита от отладки, защита от дизассемблирования, защита от трассировки по аппаратным прерываниям процессорных процедур. Применение обфускации, протекторов и упаковщиков для усиления защиты системы связи. Методы, затрудняющие считывание скопированной информации. Основные функции средств защиты от копирования. Аппаратные приемы противодействия динамическим способам снятия защиты программ от копирования.	2	ПКР-6
	Итого	2	

Согласована на портале № 59936

7 Применение смарт-карт для аппаратной защиты данных, их классификация. Аппаратные компоненты смарт-карт. Программное обеспечение для смарт-карт.	Аппаратные компоненты смарт-карт. Программное обеспечение для смарт-карт. Контактные и бесконтактные смарт – карты с соответствующими интерфейсами ISO – 7816, USB (RuToken, eToken), ISO/ IEC 14443.. Интеллектуальные карты. Жизненный цикл смарт-карт. Выпускаемые серийно интегральные схемы смарт-карт. Инфраструктура поддержки смарт-карт. Проблемы безопасности смарт-карт. Классификация атак на смарт-карты.	2	ПКР-6
	Итого	2	
8 Радиочастотная идентификация -пример удаленной защиты данных с помощью аппаратных средств. Классификация средств RFID, структура и функционирование систем RFID.	Базовые принципы радиочастотной идентификации. Структура и функционирование систем RFID. Удаленная передача данных в системах RFID, способы кодирования. Считыватели и транспондеры, электронные и программные компоненты систем RFID, стандартизация. Примеры применения: идентификация товаров, транспортных средств, иммобилайзерные системы, идентификация животных.	2	ПКР-6
	Итого	2	
9 Разрушающие программные воздействия с помощью программно-аппаратных средств. Способы использования микроконтроллеров и одноплатных микрокомпьютеров для доступа в защищенные сети связи.	Компьютерные вирусы, как особый класс разрушающих программных воздействий. Развитие программно-аппаратной вирусной базы и тенденции формирования новых типов вирусов, поддерживаемых аппаратным способом. Способы заражения локальных компьютеров с помощью микроконтроллеров и одноплатных компьютеров. Программные черви и закладки. Программно-аппаратные средства противодействия компьютерным вирусам и их состояние в современных условиях.	2	ПКР-6
	Итого	2	

Согласована на портале № 59936

10 Способы защиты от разрушающих программных воздействий (РПВ) в компьютерных системах связи с помощью программно-аппаратных средств.	Программно-аппаратная защита от разрушающих программных воздействий (РПВ). Проблема восстановления аппаратных настроек операционной системы после воздействия РПВ и применения средств противодействия в системах связи.	2	ПКР-6
	Итого	2	
Итого за семестр		26	
Итого		26	

5.3. Практические занятия (семинары)

Наименование практических занятий (семинаров) приведено в таблице 5.3.

Таблица 5.3 – Наименование практических занятий (семинаров)

Названия разделов (тем) дисциплины	Наименование практических занятий (семинаров)	Трудоемкость, ч	Формируемые компетенции
7 семестр			
1 Архитектура программно-аппаратных средств защиты ОС. Причины возникновения сбоев в оперативной памяти, общие принципы построения систем защиты (triple functions).	Антивирусное ПО - Comodo	4	ПКР-6
	Итого	4	
2 Основные понятия, классификация задач, решаемых программно-аппаратными средствами идентификации и аутентификации в сетях связи. Общеизвестные случаи результатов слабой защиты сетевых коммуникаций.	Формирование защищенной компьютерной сети для использования персональных данных в отделе кадров предприятия.	2	ПКР-6
	Итого	2	
4 Виды аудита компьютерных сетей и систем связи с помощью программно-аппаратных средств, классификация событий для проведения аудита.	Поиск аппаратных уязвимостей в операционной системе	4	ПКР-6
	Итого	4	
8 Радиочастотная идентификация - пример удаленной защиты данных с помощью аппаратных средств. Классификация средств RFID, структура и функционирование систем RFID.	Процедура чипирования, технические параметры.	4	ПКР-6
	Итого	4	
9 Разрушающие программные воздействия с помощью программно-аппаратных средств. Способы использования микроконтроллеров и одноплатных микрокомпьютеров для доступа в защищенные сети связи.	Микрокомпьютеры — характеристики и работа в сети.	4	ПКР-6
	Итого	4	
Итого за семестр		18	

Согласована на портале № 59936

Итого	18	

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			
2 Основные понятия, классификация задач, решаемых программно-аппаратными средствами идентификации и аутентификации в сетях связи. Общеизвестные случаи результатов слабой защиты сетевых коммуникаций.	Дизассемблирование программных модулей.	4	ПКР-6
	Итого	4	
4 Виды аудита компьютерных сетей и систем связи с помощью программно-аппаратных средств, классификация событий для проведения аудита.	Анализ сетевого соединения	4	ПКР-6
	Итого	4	
6 Программно-аппаратные методы и средства ограничения доступа к компонентам связи в компьютерных сетях и защиты программ от несанкционированного копирования. Вирусы, их анализ, антивирусные программы.	Изучение вирусной программы.	4	ПКР-6
	Итого	4	
9 Разрушающие программные воздействия с помощью программно-аппаратных средств. Способы использования микроконтроллеров и одноплатных микрокомпьютеров для доступа в защищенные сети связи.	Операционная система маршрутизатора Cisco	4	ПКР-6
	Итого	4	
Итого за семестр		16	
Итого		16	

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				

Согласована на портале № 59936

1 Архитектура программно-аппаратных средств защиты ОС. Причины возникновения сбоев в оперативной памяти, общие принципы построения систем защиты (triple functions).	Подготовка к тестированию	2	ПКР-6	Тестирование
	Написание отчета по практическому занятию (семинару)	2	ПКР-6	Отчет по практическому занятию (семинару)
	Итого	4		
2 Основные понятия, классификация задач, решаемых программно-аппаратными средствами идентификации и аутентификации в сетях связи. Общеизвестные случаи результатов слабой защиты сетевых коммуникаций.	Подготовка к тестированию	2	ПКР-6	Тестирование
	Подготовка к лабораторной работе, написание отчета	2	ПКР-6	Лабораторная работа
	Написание отчета по лабораторной работе	2	ПКР-6	Отчет по лабораторной работе
	Написание отчета по практическому занятию (семинару)	2	ПКР-6	Отчет по практическому занятию (семинару)
	Итого	8		
3 Основные угрозы КС. История создания избирательной и полномочной политики безопасности. Понятия субъектов и объектов доступа.	Подготовка к тестированию	2	ПКР-6	Тестирование
	Итого	2		
4 Виды аудита компьютерных сетей и систем связи с помощью программно-аппаратных средств, классификация событий для проведения аудита.	Подготовка к тестированию	2	ПКР-6	Тестирование
	Написание отчета по практическому занятию (семинару)	2	ПКР-6	Отчет по практическому занятию (семинару)
	Подготовка к лабораторной работе, написание отчета	4	ПКР-6	Лабораторная работа
	Написание отчета по лабораторной работе	2	ПКР-6	Отчет по лабораторной работе
	Итого	10		

Согласована на портале № 59936

5 Программно-аппаратные средства шифрования; построение аппаратных компонент криптозащиты данных. Инфраструктура управления открытыми ключами, базовые архитектуры систем управления сертификатами.	Подготовка к тестированию	2	ПКР-6	Тестирование
	Итого	2		
6 Программно-аппаратные методы и средства ограничения доступа к компонентам связи в компьютерных сетях и защиты программ от несанкционированного копирования. Вирусы, их анализ, антивирусные программы.	Подготовка к тестированию	2	ПКР-6	Тестирование
	Подготовка к лабораторной работе, написание отчета	2	ПКР-6	Лабораторная работа
	Написание отчета по лабораторной работе	2	ПКР-6	Отчет по лабораторной работе
	Итого	6		
7 Применение смарт-карт для аппаратной защиты данных, их классификация. Аппаратные компоненты смарт-карт. Программное обеспечение для смарт-карт.	Подготовка к тестированию	2	ПКР-6	Тестирование
	Итого	2		
8 Радиочастотная идентификация -пример удаленной защиты данных с помощью аппаратных средств. Классификация средств RFID, структура и функционирование систем RFID.	Подготовка к тестированию	2	ПКР-6	Тестирование
	Написание отчета по практическому занятию (семинару)	2	ПКР-6	Отчет по практическому занятию (семинару)
	Итого	4		
9 Разрушающие программные воздействия с помощью программно-аппаратных средств. Способы использования микроконтроллеров и одноплатных микрокомпьютеров для доступа в защищенные сети связи.	Подготовка к тестированию	2	ПКР-6	Тестирование
	Написание отчета по практическому занятию (семинару)	2	ПКР-6	Отчет по практическому занятию (семинару)
	Подготовка к лабораторной работе, написание отчета	2	ПКР-6	Лабораторная работа
	Написание отчета по лабораторной работе	2	ПКР-6	Отчет по лабораторной работе
	Итого	8		

Согласована на портале № 59936

10 Способы защиты от разрушающих программных воздействий (РПВ) в компьютерных системах связи с помощью программно-аппаратных средств.	Подготовка к тестированию	2	ПКР-6	Тестирование
	Итого	2		
Итого за семестр		48		
	Подготовка и сдача экзамена	36		Экзамен
Итого		84		

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.	Прак. зан.	Лаб. раб.	Сам. раб.	
ПКР-6	+	+	+	+	Лабораторная работа, Тестирование, Экзамен, Отчет по лабораторной работе, Отчет по практическому занятию (семинару)

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				
Лабораторная работа	5	5	10	20
Тестирование	5	5	10	20
Отчет по лабораторной работе	5	5	5	15
Отчет по практическому занятию (семинару)	5	5	5	15
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

Согласована на портале № 59936

≥ 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. Системы контроля и управления доступом. (Серия «Обеспечение безопасности объектов»; Выпуск 2). / В.А. Ворона, В.А. Тихонов. — М. : Горячая линия-Телеком, 2013. — 272 с. [Электронный ресурс]: — Режим доступа: http://e.lanbook.com/book/5135.

2. Величко, В.В. Телекоммуникационные системы и сети: В 3 томах. Том 3. - Мультисервисные сети : учебное пособие / В.В. Величко, Е.А. Субботин, В.П. Шувалов, А.Ф. Ярославцев ; под ред. Шувалова В.П. Москва : Горячая линия-Телеком, 2015. — 592 с. [Электронный ресурс]: — Режим доступа: https://e.lanbook.com/book/64092.

7.2. Дополнительная литература

1. Т.В. Вахний, С.Ю. Кузьмин. Разработка аппаратно-программного средства защиты от уязвимости badusb. — // Математические структуры и моделирование. — 2016. — № 2. — С. 116-125. [Электронный ресурс]: — Режим доступа: http://e.lanbook.com/journal/issue/298339.

2. Аутентификация. Теория и практика обеспечения безопасного доступа к информационным ресурсам. / А.А. Афанасьев, Л.Т. Веденьев, А.А. Воронцов, Э.Р. Газизова. — М. : Горячая линия-Телеком, 2012. — 550 с. [Электронный ресурс]: — Режим доступа: http://e.lanbook.com/book/5114.

3. Башмаков, А.В. Выбор оптимального подхода к построению защищенных беспроводных локальных сетей.// Вестник государственного университета морского и речного флота имени адмирала С. О. Макарова. — 2015. — № 1. — С. 222-228. [Электронный ресурс]: — Режим доступа: http://e.lanbook.com/journal/issue/296034.

7.3. Учебно-методические пособия

7.3.1. Обязательные учебно-методические пособия

1. Сети связи и системы коммутации: Руководство к практическим занятиям / В. М. Винокуров - 2012. 41 с. [Электронный ресурс]: — Режим доступа: https://edu.tusur.ru/publications/1517.

2. Изучение сетевого протокола TCP/IP: Методические указания к лабораторным работам / Е. Ю. Агеев - 2012. 16 с. [Электронный ресурс]: — Режим доступа: https://edu.tusur.ru/publications/2040.

Согласована на портале № 59936

3. Основы компьютерных сетевых технологий: Методические рекомендации к организации самостоятельной работы / Е. Ю. Агеев - 2012. 12 с. [Электронный ресурс]: — Режим доступа: https://edu.tusur.ru/publications/1657.

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 практических занятий

Учебная лаборатория "Компьютерной радиоэлектроники": учебная аудитория для проведения занятий практического типа, учебная аудитория для проведения занятий лабораторного типа; 634034, Томская область, г. Томск, Вершинина улица, д. 47, 412 ауд.

Описание имеющегося оборудования:
- Доска магнитно-маркерная;
- Компьютер Core 2 (11 шт.);
- Телевизор Samsung;
- Комплект специализированной учебной мебели;
- Рабочее место преподавателя.

Программное обеспечение:
- 7-Zip;
- Adobe Acrobat Reader;
- Google Chrome;
- LibreOffice;
- Microsoft Windows 8;
- PDF-XChange Viewer;
- PDFCreator;

8.3. Материально-техническое и программное обеспечение для лабораторных работ

Учебная лаборатория радиоэлектроники / Лаборатория ГПО: учебная аудитория для проведения занятий практического типа, учебная аудитория для проведения занятий

Согласована на портале № 59936

лабораторного типа; 634034, Томская область, г. Томск, Вершинина улица, д. 47, 407 ауд.

Описание имеющегося оборудования:

- Доска магнитно-маркерная;
- Коммутатор D-Link Switch 24 port;
- Компьютеры класса не ниже ПЭВМ INTEL Celeron D336 2.8ГГц. (12 шт.);
- Вольтметр В3-38 (7 шт.);
- Генератор сигналов специальной формы АКИП ГСС-120 (2 шт.);
- Кронштейн PTS-4002;
- Осциллограф EZ Digital DS-1150C (3 шт.);
- Осциллограф С1-72 (4 шт.);
- Телевизор плазменный Samsung;
- Цифровой генератор сигналов РСС-80 (4 шт.);
- Цифровой осциллограф GDS-810C (3 шт.);
- Автоматизированное лабораторное место по схемотехнике и радиоавтоматике (7 шт.);
- Комплект специализированной учебной мебели;
- Рабочее место преподавателя.

Программное обеспечение:

- 7-Zip;
- Adobe Acrobat Reader;
- Far Manager;
- Google Chrome;
- LibreOffice;
- PDF-XChange Viewer;
- PDFCreator;

8.4. 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.

8.5. 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,

Согласована на портале № 59936

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 Архитектура программно-аппаратных средств защиты ОС. Причины возникновения сбоев в оперативной памяти, общие принципы построения систем защиты (triple functions).	ПКР-6	Тестирование	Примерный перечень тестовых заданий
		Экзамен	Перечень экзаменационных вопросов
		Отчет по практическому занятию (семинару)	Темы практических занятий
2 Основные понятия, классификация задач, решаемых программно-аппаратными средствами идентификации и аутентификации в сетях связи. Общеизвестные случаи результатов слабой защиты сетевых коммуникаций.	ПКР-6	Лабораторная работа	Темы лабораторных работ
		Тестирование	Примерный перечень тестовых заданий
		Экзамен	Перечень экзаменационных вопросов
		Отчет по лабораторной работе	Темы лабораторных работ
		Отчет по практическому занятию (семинару)	Темы практических занятий
3 Основные угрозы КС. История создания избирательной и полномочной политики безопасности. Понятия субъектов и объектов доступа.	ПКР-6	Тестирование	Примерный перечень тестовых заданий
		Экзамен	Перечень экзаменационных вопросов

Согласована на портале № 59936

4 Виды аудита компьютерных сетей и систем связи с помощью программно-аппаратных средств, классификация событий для проведения аудита.	ПКР-6	Лабораторная работа	Темы лабораторных работ
		Тестирование	Примерный перечень тестовых заданий
		Экзамен	Перечень экзаменационных вопросов
		Отчет по лабораторной работе	Темы лабораторных работ
		Отчет по практическому занятию (семинару)	Темы практических занятий
5 Программно-аппаратные средства шифрования; построение аппаратных компонент криптозащиты данных. Инфраструктура управления открытыми ключами, базовые архитектуры систем управления сертификатами.	ПКР-6	Тестирование	Примерный перечень тестовых заданий
		Экзамен	Перечень экзаменационных вопросов
6 Программно-аппаратные методы и средства ограничения доступа к компонентам связи в компьютерных сетях и защиты программ от несанкционированного копирования. Вирусы, их анализ, антивирусные программы.	ПКР-6	Лабораторная работа	Темы лабораторных работ
		Тестирование	Примерный перечень тестовых заданий
		Экзамен	Перечень экзаменационных вопросов
		Отчет по лабораторной работе	Темы лабораторных работ
7 Применение смарт-карт для аппаратной защиты данных, их классификация. Аппаратные компоненты смарт-карт. Программное обеспечение для смарт-карт.	ПКР-6	Тестирование	Примерный перечень тестовых заданий
		Экзамен	Перечень экзаменационных вопросов
8 Радиочастотная идентификация -пример удаленной защиты данных с помощью аппаратных средств. Классификация средств RFID, структура и функционирование систем RFID.	ПКР-6	Тестирование	Примерный перечень тестовых заданий
		Экзамен	Перечень экзаменационных вопросов
		Отчет по практическому занятию (семинару)	Темы практических занятий

Согласована на портале № 59936

9 Разрушающие программные воздействия с помощью программно-аппаратных средств. Способы использования микроконтроллеров и одноплатных микрокомпьютеров для доступа в защищенные сети связи.	ПКР-6	Лабораторная работа	Темы лабораторных работ
		Тестирование	Примерный перечень тестовых заданий
		Экзамен	Перечень экзаменационных вопросов
		Отчет по лабораторной работе	Темы лабораторных работ
		Отчет по практическому занятию (семинару)	Темы практических занятий
10 Способы защиты от разрушающих программных воздействий (РПВ) в компьютерных системах связи с помощью программно-аппаратных средств.	ПКР-6	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

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

Согласована на портале № 59936

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. Надо ли защищать следующих субъектов - пользователей, обслуживающий персонал (уборщица в компьютерном зале, настройщик компьютеров и пр.)?
   а) Надо защищать всех перечисленных.
   б) Надо защищать всех, кроме уборщиц - они ничего не понимают.
   в) Надо защищать всех, кроме уборщиц и ремонтников.
   г) Только открытую (не секретная часть)
2. Что понимается под системой защиты КС?
   а)Под системой защиты информации в КС понимается единый комплекс правовых норм, организационных мер, технических, программных и криптографических средств, обеспечивающий защищенность информации в КС в соответствии с принятой политикой безопасности.
   б)Под системой защиты информации в КС понимаются методы и средства организационной защиты информации -организационно-технические и организационно-правовые мероприятия, проводимые в процессе создания и эксплуатации КС для обеспечения защиты информации. Эти мероприятия должны проводиться при строительстве или ремонте помещений, в которых будет размещаться КС; проектировании системы, монтаже и наладке ее технических и программных средств; испытаниях и проверке работоспособности КС. На этом уровне защиты информации рассматриваются международные договоры, подзаконные акты государства, государственные стандарты и локальные нормативные акты конкретной организации.
   в) Это комплексное мероприятие.
   г) Это системное мероприятие.
3. Что является объектом защиты информации?
   а) Объектом защиты является АСОД
   б) Объектом защиты является КС
   в) Объектом защиты является только винчестер с записанной на нем информацией.
   г) Компьютер
4. Суть метода манипуляции с кодом программы при защите программ от копирования:
   а) Изменение защищаемой программы
   б) «Привязка» программы к винчестеру

Согласована на портале № 59936

в) Включение в тело программы «пустых модулей»
г) Переадресация

5. Антивирус Касперского вносит изменения в файлы при их лечении от вирусов. Можно ли его действия классифицировать по ст. 272 УК РФ?
   а)Эта статья не относится к работе антивируса никаким образом.
   б) Эти действия не подвергаются классификации, поскольку направлены на защиту программного обеспечения.
   в) Несомненно можно классифицировать - видоизменение программного кода всегда нарушает не только авторские права, но и в какой-то мере, алгоритм работы программы, что может повлечь за собой неконтролируемые последствия.
   г) Нельзя
6. Ассиметричные ключи содержат:
   а) Закрытую и открытую части
   б) Только закрытую (секретную часть)
   в) Зашифрованную часть
   г) Только открытую (не секретная часть)
7. В классификацию методов аутентификации по используемым средствам входят:
   а) Секретная информация - логин. Уникальный предмет - жетон, карточка. Биометрические параметры - характеристики организма.
   б) Секретная информация - пароль. Уникальный предмет - жетон, карточка. Биометрические параметры - характеристики организма. Информация ассоциированная с пользователем - координаты.
   в) Секретная информация - пароль. Биометрические параметры - характеристики организма. Информация ассоциированная с пользователем - координаты, жетон, карточка.
   г) Рисунок дна глаза и радужки
8. Задачи, решаемые инфраструктурой открытых ключей:
   а) Установление доверия, именование субъектов, обеспечение связи имени субъекта и пары ключей
   б) Именование субъектов, обеспечение связи имени субъекта и пары ключей
   в) Обеспечение связи имени субъекта и пары ключей
   г) Шифрование данных
9. Какие функции выполняет идентификация:
   а) Установление подлинности и определение полномочий субъекта, контролирование установленных полномочий субъекта во время сеанса, регистрация действий
   б) Установление подлинности субъекта, контролирование установленных полномочий субъекта во время сеанса, регистрация действий
   в) Установление подлинности и определение полномочий субъекта, контролирование установленных полномочий субъекта во время сеанса
   г) Поиск субъекта в базе данных
10. Когда теряется доверие к цепочке сертификатов открытых ключей:
    а) При потере доверия к начальному звену
    б) При потере доверия к последнему звену
    в) При разрыве среднего звена
    г) При добавлении нового звена

9.1.2. Перечень экзаменационных вопросов

1. Предмет и задачи защиты информации в сетях и системах связи с помощью программно-аппаратных средств
2. Причины возникновения аппаратных и программных уязвимостей, общие принципы построения систем защиты (triple functions).
3. Основные понятия, классификация задач, решаемых программно- аппаратными средствами идентификации и аутентификации.
4. Идентификация субъекта с помощью аппаратных средств, понятие протокола идентификации, идентифицирующая информация. Методы аутентификации: парольная схема, биометрический и token способы, многофакторная и взаимная аутентификации.
5. Генерация ключей программно-аппаратными средствами. Ключи для симметричных и

Согласована на портале № 59936

несимметричных алгоритмов. Эфемерный ключ.
6. Программно-аппаратные средства шифрования в реальном времени, построение аппаратных компонент криптозащиты данных. Угрозы криптографическим ключам.
7. Аппаратные компоненты смарт-карт. Программное обеспечение для смарт-карт.
8. Компьютерные вирусы, как особый класс разрушающих программных воздействий. Развитие программно-аппаратной вирусной базы и тенденции формирования новых типов вирусов, поддерживаемых аппаратным способом.
9. Способы заражения локальных компьютеров с помощью микроконтроллеров и одноплатных компьютеров. Программные черви и закладки.
10. Программно-аппаратные средства противодействия компьютерным вирусам и их состояние в современных условиях.
11. Программно-аппаратная защита от разрушающих программных воздействий (РПВ).
12. Проблема восстановления аппаратных настроек операционной системы после воздействия РПВ и применения средств противодействия в системах связи.

9.1.3. Темы практических занятий

1. Антивирусное ПО - Comodo
2. Формирование защищенной компьютерной сети для использования персональных данных в отделе кадров предприятия.
3. Поиск аппаратных уязвимостей в операционной системе
4. Процедура чипирования, технические параметры.
5. Микрокомпьютеры — характеристики и работа в сети.

9.1.4. Темы лабораторных работ

1. Дизассемблирование программных модулей.
2. Анализ сетевого соединения
3. Изучение вирусной программы.
4. Операционная система маршрутизатора Cisco

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.

Согласована на портале № 59936

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.

Согласована на портале № 59936

ЛИСТ СОГЛАСОВАНИЯ

Рассмотрена и одобрена на заседании кафедры РСС
протокол № 4 от «18» 12 2020 г.

СОГЛАСОВАНО:

Должность	Инициалы, фамилия	Подпись
Заведующий выпускающей каф. РСС	А.В. Фатеев	Согласовано, 595be322-a579-4ae5-8d93-e5f4ee9ceb7d
Заведующий обеспечивающей каф. РСС	А.В. Фатеев	Согласовано, 595be322-a579-4ae5-8d93-e5f4ee9ceb7d
Начальник учебного управления	Е.В. Саврук	Согласовано, fa63922b-1fce-4a6a-845d-9ce7670b004c

ЭКСПЕРТЫ:

Старший преподаватель, каф. РСС	Ю.В. Зеленецкая	Согласовано, 1f099a64-e28d-4307-a5f6-d9d92630e045
Заведующий кафедрой, каф. РСС	А.В. Фатеев	Согласовано, 595be322-a579-4ae5-8d93-e5f4ee9ceb7d

РАЗРАБОТАНО:

Доцент, каф. РСС	Н.Д. Хатьков	Разработано, d2c7ff40-c164-4c72-a8d4-afaab77e97bd

Согласована на портале № 59936