Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Нагиев Рамазан Нагиевич
Должность: Директор
Дата подписания: 30.04.2023 23:26:14
Уникальный программный ключ:
8d9b2d75432cebd5b55675845b1efd3d732286ff

МИНОБРНАУКИ РОССИИ

федеральное государственное бюджетное образовательное учреждение высшего образования
«Санкт-Петербургский государственный экономический университет»

УТВЕРЖДАЮ
Проректор по учебной и методической работе
_____ В.Г. Шубаева
«23» января 2022 г.

Управление комплексной информационной безопасностью информационных технологий

Рабочая программа дисциплины

Направление подготовки/ *Специальность* — *09.03.03 Прикладная информатика*

Направленность (профиль) программы/ *Специализация* — *Управление бизнес-процессами и проектами*

Уровень высшего образования — *Бакалавриат*

Форма обучения — *очная*

Год набора — *2022*

Составитель*(и)*:

к.физмат.н, Кияев Владимир Ильич
к.э.н, Газуль Станислав Михайлович

Часов по учебному плану	108	**Виды контроля в семестрах:**
в том числе:		
контактная работа	42	Зачет: семестр 6
самостоятельная работа	66	
практическая подготовка	0	
часов на контроль	0	

Распределение часов дисциплины:

Семестр:	6
Вид занятий	Часы
Лекционные занятия	18
Практические занятия	24
Лабораторные работы	
Итого аудиторных часов	**42**
Самостоятельная работа	66
Часы на контроль	0
Итого академических часов	**108**
Общая трудоемкость в зачетных единицах	**3**

Санкт-Петербург
2022

СОДЕРЖАНИЕ

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ 3

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ 3

3. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ 3

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ* 3

5. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ 9

5.1 Рекомендуемая литература 9

5.2 Перечень лицензионного и свободно распространяемого программного обеспечения, в т.ч. отечественного производства 10

5.3 Перечень информационных справочных систем (ИСС) и современных профессиональных баз данных (СПБД) 10

6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ 10

7. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩЕГОСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ 11

8. ОСОБЕННОСТИ ОСВОЕНИЯ ДИСЦИПЛИНЫ ДЛЯ ИНВАЛИДОВ И ЛИЦ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ 12

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ 14

1.1 Контрольные вопросы и задания к промежуточной аттестации 14

1.2 Темы письменных работ 14

1.3 Контрольные точки 14

1.4 Другие объекты оценивания 14

1.5 Самостоятельная работа обучающегося 14

1.6 Шкала оценивания результата 14

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Цель:	Заложить методически правильные основы знаний по информационной безопасности и системам защиты информации, необходимых специалистам, занимающимся вопросами проектирования, внедрения и эксплуатации корпоративных вычислительных и информационных систем (ВС/ИС), а также вопросами обеспечения комплексной безопасности таких систем.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Дисциплина Б1.В Управление комплексной информационной безопасностью информационных технологий относится к части, формируемой участниками образовательных отношений Блока 1.

3. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ

Код и наименование компетенции выпускника	**Код и наименование индикатора достижения компетенций**	**Планируемые результаты обучения по дисциплине**
ПК-6 - Способен организовывать управление ИТ-инфраструктурой и комплексной информационной безопасностью	*ПК-6.2 - Понимает информационные угрозы, использует методы для управления комплексной информационной безопасностью предприятия*	*Знать: тенденции совершенствования инструментария в области проектирования и управления комплексной информационной безопасности.* *Уметь: ставить и решать прикладные задачи по обеспечению информационной безопасности, надежности и эффективности ИС..* *Владеть: методами ИТ-управления информационной безопасностью предприятия..*

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ*

Номер и наименование тем и/или разделов/тем	**Содержание дисциплины**	**Объем дисциплины (академические часы)**			
		Контактная работа			**СРО**
		ЗЛТ	**ПЗ**	**ЛР**	
Тема 1. Предпосылки становления предметной	Обзор предпосылок становления предметной области управления информационной безопасностью.	2	2		6

области комплексной информационной безопасности.					
Тема 2. Ключевые вопросы формирования системы информационной безопасности.	Ключевые вопросы комплексной информационной безопасности (ИБ). Анализ феномена расширения области информационных угроз с развитием информационных технологий. Экономическая и информационная безопасность предприятия.	1	2		4
Тема 3. Концепция информационной безопасности Российской Федерации. Разработка корпоративной концепции информационной безопасности компании.	Развитие информационной составляющей бизнес-среды и вопросы её безопасности. Национальная политика и доктрина информационной безопасности. Уровни реализации ИБ и концепция ИБ Российской Федерации. Внешние и внутренние системные информационные угрозы. Общая инфраструктура глобальной ИБ и общая инфраструктура глобальной ИБ. Национальные интересы РФ в информационной сфере и угрозы их безопасности Концепция информационной безопасности Российской Федерации. Концептуальное видение проблемы информационной защищенности компании. Бизнес-модель компании и модель ИБ. Содержание и объекты Концепции информационной безопасности организации. Базовые правила реализации ИБ в современной компании.	1	2		6
Тема 4. Правовые аспекты информационной безопасности. Законодательство в сфере информационной безопасности.	Введение понятий информационного права. Информация: правовая и неправовая. Особенности информации в юридическом аспекте. Принципы и система информационного права. Российское и зарубежное законодательство в области информационной безопасности.	1	1		4
Тема 5. Виды защищаемой информации. Модель угроз и модель информационной безопасности.	Информационное поле и информационный контур компании. Ключевые вопросы информационной безопасности современного предприятия. Содержание поля информационной безопасности. Общая классификация охраняемой информации. Закон РФ о коммерческой тайне, процедура реализации и управления процессом «Коммерческая тайна компании». Категории и виды угроз ИБ, ключевые области процесса анализа угроз. Ключевые области процесса анализа угроз, модель возможных угроз и основные классы методов защиты данных и информации. Типичное соотношение	1	1		6

	внутренних ИТ-угроз и распространенные пути утечки данных. Алгоритм анализа и оценки угроз, внутренние системные угрозы, пользователь ИТ, как источник угрозы. Инфраструктурные и внешние угрозы, реальные пути осуществления угроз. Концептуальная модель защиты от угроз и алгоритм формирования процесса управления информационной безопасностью. Содержание модели информационной безопасности, адаптивная модель на базе нейронных сетей с использованием нейро-нечеткого классификатора. Структура модели защиты информационных ресурсов и схема программно-аппаратного анализа на основе профилактического сканирования информационного поля компании. Формирование процесса оценки защищенности информационной среды.				
Тема 6. Защищенная информационная система. Программа информационной безопасности.	Колебание уровня информационной безопасности компании. Концептуальные требования защищенности корпоративной информационной системы. Модель анализа безопасности информационной системы при отсутствии злоумышленных угроз. Определение защищенности ИС, необходимое и достаточное условие безопасности ИС. Концепция гарантированности безопасности ИС. Методология анализа защищенности информационной системы. Модели системы защиты с частичным и полным перекрытием. Понятие и уровни ответственности в информационной сфере. Программа информационной безопасности компании. Мероприятия по выполнению программы ИБ: аспекты, процедуры и контроль выполнения.	1	1		4
Тема 7. Организационно-распорядительные документы в сфере информационной безопасности. Политика информационной безопасности.	Значимость организационно-нормативных документов компании в управлении безопасностью в ИТ-сфере. Иерархия организационно-нормативных документов и уровень базовых документов в иерархии. Концепция информационной безопасности компании и сферы её приложения концепции. Политика ИБ как базовая основа процесса управления информационной безопасностью в компании. Системные требования к разработке общей политики ИБ, суть стратегического фактора ИБ. Уровни реализации политики безопасности. Правила разработки и реализации политики ИБ, взаимосвязь и детализация частных политик ИБ. Жизненный цикл политики ИБ, спиральная модель ЖЦ политики ИБ. Примеры неадекватной	1	1		4

	политики безопасности и следствий, к которым приводят такие политики, общее резюме по неудачным политикам ИБ. Корпоративные стандарты ИБ и организационно-распорядительные документы.				
Тема 8. Управление информационными рисками.	Влияние рисков на достижение стратегических целей компании. Взаимосвязь процессов управления бизнесом и управления экономической и информационной безопасностью в компании. Влияние ИТ-рисков на базовые показатели деятельности компании. Области применения риск-менеджмента в сфере ИТ. Определение понятия «ИТ-риск», неопределенность как источник риска. Классификация рисков, ИТ-риски и риски программной инженерии. Специфика информационных рисков. Место управления рисками в системе управления ИБ. Общая схема менеджмента ИТ-рисков, базовые компоненты системы управления рисками. Системные действия и практические шаги по управлению рисками. Формирование процесса управления ИТ-рисками, содержание итерационного процесса управления, входы и выходы этапов процесса управления рисками. Процесс принятия решения по результатам анализа рисков. Соотношение «уровень ИТ-риска – уровень защиты», основные способы отработки рисков. Методики и программные продукты для оценки рисков. Оценка экономической эффективности системы управления рисками.	2	2		4
Тема 9. Стандартизация в сфере информационной безопасности.	Определение стандарта, уровни представления стандартов. Приоритетные направления разработки стандартов в сфере информатизации, роль стандартов информационной безопасности. Содержание этапов стандартизации, объекты стандартизации в открытой информационной системе. Хронология стандартизации в сфере информационной безопасности. «Оранжевая книга», «Критерии оценки доверенных компьютерных систем», «Радужная серия», Европейские критерии безопасности ИТ». «Федеральные критерии безопасности ИТ», «Руководящие документы Гостехкомиссии РФ», критерии адекватности средств защиты, структура профиля защиты. Функциональные требования к доверенному вычислительному ядру ИС, требования к технологии разработки ИС с учетом требований ИБ. Британский стандарт BS 7799 (ISO/IEC 17799:2000). Единые критерии оценки безопасности	2	2		4

	информационных технологий, структура профиля защиты ИТ-продукта, иерархия и классы функциональных требований. Сравнение стандартов ИТ-безопасности, развитие семейства стандартов ISO 270.				
Тема 10. Математические модели систем и процессов защиты информации: концепции, требования, методы реализации.	Место математических моделей в реализации защиты информации. Математические модели процессов и систем защиты информации (СЗИ). Общие требования к модели СЗИ, этапы построения модели СЗИ результаты практического моделирования. Декомпозиция модели СЗИ, контроль параметров состояния СЗИ (метрики моделей), пример модели процесса защиты. Адаптивная модель СЗИ на базе нейронных сетей, построение «хромосомы» степени угрозы и соответствующего уровня защищенности в нейросети с нечеткими связями. Объективные сложности построения моделей. Методы экспертных оценок.	1	2		4
Тема 11. Сервисы для обеспечения информационной безопасности и защиты от инсайдеров.	Сервисы ИБ как реализация модели системы защиты информации. Архитектурная безопасность, схема распределенного документооборота с возможностью «обхода» СЗИ головного офиса предприятия. Феномен инсайдера в проблеме реализации ИБ, общие характеристики инсайдеров, статистический портрет инсайдера. Стандартный набор сервисов ИБ: идентификация / аутентификация пользователя, управление доступом, пример реализации контроля доступа. Механизмы целостности и контроля защищенности данных и сообщений, пример комплексного программного решения, включающего защиту от инсайдеров.	1	2		4
Тема 12. Криптографические методы защиты информации.	Схема предприятия с распределенной информационной инфраструктурой. Базовые моменты для организации управления ИБ распределенного предприятия. Криптографические методы защиты информации. Шифрование данных и информации, виды практического шифрования, процедура шифрования информации. Требования к криптографическим СЗИ. Базовые разделы криптографии, схемы криптосистемы с закрытым и открытым ключами, шифрование на базе хэш-функций. Применение блочных алгоритмов шифрования. Управление криптографическими ключами. Стандарты шифрования в России. Электронная цифровая подпись, схема системы ЭЦП на базе алгоритма шифрования RSA.	1	2		4

Тема 13. Защита информационной инфраструктуры от атак. Антивирусные средства защиты.	Содержание поля информационной безопасности компании, угрозы проникновения, ранжирование ИТ-угроз. Взлом защиты информационной инфраструктуры и вирусная опасность. Руткиты, ботнеты, виды атак с использованием ботнета, пример фишинг-атаки, рассылка спама, опасность блогерных страниц. Компьютерные вирусы: классификация, формы организации вирусных атак, виды вредоносного программного обеспечения. Классические компьютерные вирусы, сетевые черви (Computer Worms), троянские программы, хакерские утилиты. Факторы уязвимости вычислительных и информационных систем для внедрения вредоносных программ. Признаки появления вируса. Юридические средства борьбы с закладками, взломами и вирусами. Концептуальные положения корпоративной организации защиты от взломов и вирусной опасности, общие требования к антивирусной защите и правила для пользователей. Российские и зарубежные базовые антивирусные пакеты.	1	2		6
Тема 14. Комплексная защита информационной инфраструктуры и ресурсов. Оценка эффективности СЗИ.	Распределенная ВС/ИС, построенная на Интернет-технологиях. Базовая особенность сетевых распределенных информационных структур, общие угрозы в распределенной среде. Рекомендуемые средства защиты информации в государственных органах, состав средств защиты. Четырехуровневая модель защиты распределенной системы. Схема фильтрации трафика между защищенной корпоративной и открытой сетями. Службы и протоколы системы безопасности, которые могут иметь уязвимости. Технологии межсетевых экранов: классификация и функциональные возможности. Пример политики безопасности при обмене между корпоративной и открытой сетями. Комплекс «маршрутизатор-файервол» при подключении к Internet. Организация защиты с помощью технологии виртуальных частных сетей (VPN), способы реализации VPN-каналов. Технология защиты с использованием токенов, российские интеллектуальные карты. Биометрические средства контроля доступа, методы распознавания по изображению лица. Формирование интегральной системы ИБ, схема организации интегральной защиты информационной инфраструктуры и ресурсов,	2	2		6

	состав средств интегральной защиты. Оценка экономической эффективности интегральной системы ИБ. Развитие методов интегральной защиты.				
Контроль:					**0**
Всего по дисциплине:		**18**	**24**	**0**	**66**

*ЗЛТ – занятия лекционного типа, ПЗ – все виды занятий семинарского типа, кроме лабораторных работ, ЛР – лабораторные работы, СРО – самостоятельная работа обучающегося

5. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

5.1 Рекомендуемая литература

Библиографическое описание издания (автор, заглавие, вид, место и год издания, кол. стр.)	**Электронные ресурсы**
Барабанова, Марина Ивановна Открытые системы и сети. Комплексная безопасность в системах и сетях современного предприятия : учебник / М.И.Барабанова, В.И.Кияев, А.В.Саитов ; под ред. В.И.Кияева ; М-во науки и высш. образования Рос. Федерации, С.-Петерб. гос. экон. ун-т, Каф. информатика Электрон. текстовые дан. (1 файл : 302 МБ)Санкт-Петербург : Изд-во СПбГЭУ, 2019Загл. с титул. экрана Имеется печ. аналог Авторизованный доступ по паролю Библиогр.: 27 назв.	https://opac.unecon.ru/elibrar ... 20%D1%81%D0%B5%D1%82%D0%B8.pdf
Кияев, Владимир Ильич Комплексная информационная безопасность в управлении современным предприятием : учебное пособие / В.И.Кияев, А.В.Саидов ; Министерство образования и науки Российской Федерации, Санкт-Петербургский гос. экономический ун-т, Кафедра информатики Электрон. текстовые дан. (1 файл : 15,4 МБ)Санкт-Петербург : Изд-во СПбГЭУ, 2016Загл. с титул. экрана Имеется печ. аналог Авторизованный доступ по паролю Библиогр.: 15 назв.ЭБ OPAC.UNECON.RU	https://opac.unecon.ru/elibrar ... BE%D0%BD%D0%BD%D0%B0%D1%8F.pdf
Газуль, С. М. Управление разработкой, стандартизацией и качеством программных средств и информационных технологий : учебное пособие / С. М. Газуль, В. И. Кияев. – Санкт-Петербург : Санкт-Петербургский государственный экономический университет, 2021. – 406 с. – ISBN 978-5-7310-5630-4. – EDN PHMKML.	https://lib.unecon.ru/pwb/deta ... %5C19013655%5Cfin_work%5C31278
Газуль, Станислав Михайлович Операционные системы: основы конфигурирования серверной информационной инфраструктуры : учебное пособие / С.М.Газуль ; М-во науки и высш. образования Рос. Федерации, С.-Петерб. гос. экон. ун-т, Каф. информатики Санкт-Петербург : Изд-во	https://opac.unecon.ru/elibrar ... D1%82%D0%B5%D0%BC%D1%8B_20.pdf

СПбГЭУ, 20201 файл (2,83 МБ)Загл. с титул. экрана Имеется печ. аналог Авторизованный доступ по паролю Текст (визуальный) : электронный Библиогр.: 17 назв.ЭБ OPAC.UNECON.RU	

5.2 Перечень лицензионного и свободно распространяемого программного обеспечения, в т.ч. отечественного производства

- 7-Zip
- Microsoft Office Professional
- Microsoft Windows Professional
- Debian
- Альт Линукс
- Python

5.3 Перечень информационных справочных систем (ИСС) и современных профессиональных баз данных (СПБД)

№	Наименование СПБД/ ИСС
1.	Электронная библиотека Grebennikon.ru – www.grebennikon.ru
2.	Научная электронная библиотека eLIBRARRY – www.elibrary.ru
3.	Научная электронная библиотека КиберЛеника – www.cyberleninka.ru
4.	База данных ПОЛПРЕД Справочники – www.polpred.com
5.	База данных OECD Books, Papers & Statistics на платформе OECD iLibrary www.oecd-ilibrary.org
6.	Справочная правовая система КонсультантПлюс (инсталлированный ресурс СПбГЭУ или www.consultant.ru)
7.	Справочная правовая система «ГАРАНТ» (инсталлированный ресурс СПбГЭУ или www.garant.ru)
8.	Информационно-справочная система «Кодекс» (инсталлированный ресурс СПбГЭУ или www.kodeks.ru)
9.	Электронная библиотечная система BOOK.ru - www.book.ru
10.	Электронная библиотечная система ЭБС ЮРАЙТ – www.urait.ru
11.	Электронно-библиотечная система ЗНАНИУМ (ZNANIUM) – www.znanium.com
12.	Электронная библиотека СПбГЭУ– opac.unecon.ru

6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Для реализации данной дисциплины имеются специальные помещения для проведения занятий лекционного типа, занятий семинарского типа, курсового проектирования (выполнения курсовых работ) групповых и

индивидуальных консультаций, текущего контроля и промежуточной аттестации, а также помещения для самостоятельной работы.

Помещения оснащены оборудованием и техническими средствами обучения.

Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой с возможностью подключения к сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду университета.

Наименование учебных аудиторий, перечень	**Адрес (местоположение) учебных аудиторий**

Лабораторные работы по дисциплине проводятся в лаборатории «*наименование лаборатории*».

«*Наименование лаборатории*»

Вид учебных занятий	**Адрес, № аудитории**	**Лабораторное оборудование**
Лабораторные работы	*192007; г. Санкт-Петербург, ул. Прилукская, д. 3, аудитория № 102*	

Занятия по дисциплине проводятся в _____ *(указывается наименование специального помещения согласно ФГОС).*

«*Наименование специального помещения*»

Вид учебных занятий	**Адрес, № аудитории**	**Оснащенность специального помещения**
Занятия семинарского типа	*192007; г. Санкт-Петербург, ул. Прилукская, д. 3, аудитория № 110*	

7. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩЕГОСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Приступая к изучению дисциплины, обучающемуся необходимо ознакомиться со следующими документами:

– учебно-методической документацией;

– локальными нормативными актами, регламентирующими основные вопросы организации и осуществления образовательной

деятельности, в том числе регламентирующие порядок проведения текущего контроля успеваемости и промежуточной аттестации обучающихся;

– графиком консультаций сотрудников профессорско-преподавательского состава.

Уровень и глубина освоения дисциплины определяются активной и систематической работой обучающихся на лекционных занятиях, занятиях семинарского типа, выполнением самостоятельной работы, в том числе в части выделения наиболее значимых и актуальных проблем для дальнейшего изучения. Особым условием качественного освоения дисциплины является эффективная организация труда, позволяющая распределить учебную нагрузку равномерно в соответствии с графиком учебного процесса.

При подготовке к учебным занятиям обучающимся предоставляется возможность посещения консультаций сотрудников профессорско-преподавательского состава СПбГЭУ согласно расписанию, установленному в графике консультаций.

Аудиторная и внеаудиторная работа обучающихся должна быть направлена на формирование:

- фундаментальных основ мировоззрения обучающихся и естественнонаучного познания;
- базисных знаний, соответствующих направлению подготовки и заявленной профессиональной области, формирующих целевую и профессиональную основу для подготовки кадров;
- профессиональных компетенций ориентированных на удовлетворение потребностей рынка труда;
- индивидуальной траектории посредством освоения уникального набора профессиональных компетенций дополняющих компетентностную модель обучающегося, за счет ориентации на конкретные профессиональные специализированные области знаний, определяемые представителями рынка труда;
- метанавыков обучающихся, таких как: командная работа и лидерство, анализ данных, цифровые навыки, разработка и реализация проектов, межкультурное взаимодействие.

8. ОСОБЕННОСТИ ОСВОЕНИЯ ДИСЦИПЛИНЫ ДЛЯ ИНВАЛИДОВ И ЛИЦ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ

Обучение обучающихся с ограниченными возможностями здоровья при необходимости осуществляется на основе адаптированной рабочей программы с использованием специальных методов обучения и дидактических материалов, составленных с учетом особенностей психофизического развития, индивидуальных возможностей и состояния здоровья таких обучающихся (обучающегося).

В целях освоения учебной программы дисциплины инвалидами и лицами с ограниченными возможностями здоровья Университет обеспечивает:

– для инвалидов и лиц с ограниченными возможностями здоровья по зрению: размещение в доступных для обучающихся, являющихся слепыми или слабовидящими, местах и в адаптированной форме справочной информации о расписании учебных занятий; присутствие ассистента, оказывающего обучающемуся необходимую помощь; выпуск альтернативных форматов методических материалов (крупный шрифт или аудиофайлы);

– для инвалидов и лиц с ограниченными возможностями здоровья по слуху: надлежащими звуковыми средствами воспроизведение информации;

– для инвалидов и лиц с ограниченными возможностями здоровья, имеющих нарушения опорно-двигательного аппарата: возможность беспрепятственного доступа обучающихся в учебные помещения, туалетные комнаты и другие помещения кафедры, а также пребывание в указанных помещениях.

Обучающиеся из числа инвалидов и лиц с ОВЗ обеспечены печатными и (или) электронными образовательными ресурсами в формах, адаптированных к ограничениям их здоровья. Образование обучающихся с ограниченными возможностями здоровья может быть организовано как совместно с другими обучающимися, так и в отдельных группах или в отдельных организациях.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

1.1 Контрольные вопросы и задания к промежуточной аттестации

1.2 Темы письменных работ

Рабочей программой дисциплины не предусмотрено.

1.3 Контрольные точки

Номер контрольной точки	Тип контрольной точки	Способ проведения	Номера тем
1	*Контрольная работа*	*с помощью технических средств и информационных систем*	*1-7*
2	*Эссе*	*с помощью технических средств и информационных систем*	*8-14*
3	*Текущий контроль*	*с помощью технических средств и информационных систем*	*1-14*

1.4 Другие объекты оценивания

Наименования объекта оценивания	Способ проведения	Номера тем

1.5 Самостоятельная работа обучающегося

Наименования самостоятельной работы	Номера тем
Выполнение домашних заданий	*1-14*
Подготовка к лекционным и практическим занятиям	*1-14*

1.6 Шкала оценивания результата

Шкалы оценивания и процедуры оценивания результатов обучения **по дисциплине** регламентируются Положением о текущем контроле успеваемости и промежуточной аттестации обучающихся по программам высшего образования и Положением о балльно-рейтинговой системе.

Для оценки сформированности результатов обучения по дисциплине используется **балльно-рейтинговая система успеваемости обучающихся**:

Формой итогового контроля по дисциплине является зачет, итоговый результат формируется в соответствии со шкалой, приведенной ниже в таблице:

Баллы	Оценка
<55	Незачет
>=55	Зачет

Шкала оценивания результата

2 (балл до 54)	Демонстрирует непонимание проблемы. Многие требования, предъявляемые к заданию не выполнены. Демонстрируется первичное восприятие материала. Работа незакончена и /или это плагиат.
3 (балл 55-69)	Демонстрирует частичное понимание проблемы. Большинство требований, предъявляемых, к заданию выполнены. Владение элементами заданного материала. В основном выполненный материал понятен и носит целостный характер.
4 (балл 70-84)	Демонстрирует значительное понимание проблемы обозначенной дисциплиной. Все требования, предъявляемые к заданию выполнены. Содержание выполненных заданий раскрыто и рассмотрено с разных точек зрения.
5 (балл 85-100)	Демонстрирует полное понимание проблемы. Все требования, предъявляемые к заданию выполнены. Продемонстрировано уверенное владение материалом дисциплины. Выполненные задания носят целостных характер, выполнены в полном объеме, структурированы, представлены различные точки зрения, продемонстрирован творческий подход.