

МИНОБРНАУКИ РОССИИ

федеральное государственное бюджетное образовательное учреждение высшего образования

«Санкт-Петербургский государственный экономический университет»



**Программно-аппаратные средства защиты информации**

**Рабочая программа дисциплины**

Направление подготовки/  
Специальность

10.03.01 Информационная безопасность

Направленность (профиль) программы/  
Специализация

Безопасность компьютерных систем (в экономике и управлении)

Уровень высшего образования

Бакалавриат

Форма обучения

очная

Год набора

2023

Составитель(и):

к.физмат.н, Васильева Ирина Николаевна

Часов по учебному плану	108	<b>Виды контроля в семестрах:</b>  Зачет: семестр 5
в том числе:		
контактная работа	80	
самостоятельная работа	28	
практическая подготовка	0	
часов на контроль	0	

**Распределение часов дисциплины:**

Семестр:	5
Вид занятий	Часы
Лекционные занятия	24
Практические занятия	
Лабораторные работы	56
<b>Итого аудиторных часов</b>	<b>80</b>
Самостоятельная работа	28
Часы на контроль	0
<b>Итого академических часов</b>	<b>108</b>
<b>Общая трудоемкость в зачетных единицах</b>	<b>3</b>

Санкт-Петербург  
2023

# СОДЕРЖАНИЕ

<b>1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ .....</b>	<b>3</b>
<b>2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ .....</b>	<b>3</b>
<b>3. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ .....</b>	<b>3</b>
<b>4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ* .....</b>	<b>3</b>
<b>5. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ.....</b>	<b>7</b>
<b>5.1 Рекомендуемая литература .....</b>	<b>7</b>
<b>5.2 Перечень лицензионного и свободно распространяемого программного обеспечения, в     т.ч. отечественного производства .....</b>	<b>7</b>
<b>5.3 Перечень информационных справочных систем (ИСС) и современных     профессиональных баз данных (СПБД).....</b>	<b>8</b>
<b>6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ .....</b>	<b>8</b>
<b>7. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩЕГОСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ.....</b>	<b>10</b>
<b>8. ОСОБЕННОСТИ ОСВОЕНИЯ ДИСЦИПЛИНЫ ДЛЯ ИНВАЛИДОВ И ЛИЦ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ .....</b>	<b>11</b>
<b>ФОНД ОЦЕНОЧНЫХ СРЕДСТВ.....</b>	<b>13</b>
<b>1.1 Контрольные вопросы и задания к промежуточной аттестации .....</b>	<b>13</b>
<b>1.2 Темы письменных работ.....</b>	<b>13</b>
<b>1.3 Контрольные точки .....</b>	<b>13</b>
<b>1.4 Другие объекты оценивания .....</b>	<b>13</b>
<b>1.5 Самостоятельная работа обучающегося .....</b>	<b>13</b>
<b>1.6 Шкала оценивания результата .....</b>	<b>13</b>

## 1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

<b>Цель:</b>	Дать студентам необходимые знания в области программно-аппаратной защиты информации, умения и навыки использования программных и аппаратных средств защиты.
--------------	---

## 2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Дисциплина Б1.О Программно-аппаратные средства защиты информации относится к обязательной части Блока 1.

## 3. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ

Код и наименование компетенции выпускника	Код и наименование индикатора достижения компетенций	Планируемые результаты обучения по дисциплине
ОПК-9 - Способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности;	ОПК-9.02 - Демонстрирует необходимые знания в области программно-аппаратной защиты информации, умения и навыки использования программных и аппаратных средств защиты	<p><b>Знать:</b> нормативные требования к средствам технической защиты информации, основные возможности и функциональные подсистемы программно-аппаратных средств защиты информации; принципы работы и правила эксплуатации программно-аппаратных средств защиты информации.</p> <p><b>Уметь:</b> на основе полученных знаний самостоятельно осуществлять установку, настройку и применение программно-аппаратных средств защиты информации, исходя из условий поставленной задачи.</p> <p><b>Владеть:</b> приемами администрирования программно-аппаратных средств защиты информации, формулировки требований к встроенным и наложенным средствам защиты информации от несанкционированного доступа.</p>

## 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. Основные термины и определения защиты	Цели и задачи дисциплины "Программно-аппаратные средства защиты информации", ее место в структуре ОПОП. ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения», Рекомендации по стандартизации Р	2			4

информации.	50.1.056-2005 «Техническая защита информации. Основные термины и определения». Понятия защиты информации, технической защиты информации, объекта защиты информации, защищаемой информации, защищаемой информационной системы (ИС), защищаемых ресурсов ИС, техники защиты информации, средства защиты информации, системы защиты информации.				
Тема 2. Нормативные требования к средствам программно-аппаратной защиты информации.	Структура нормативных требований в сфере защиты информации. Государственные регулирующие органы в сфере технической защиты информации. Требования импортозамещения и требования безопасности. Классы информационных систем, для которых предъявляются специальные требования по защите информации. Государственные информационные системы: определение, классификация. Государственные информационные системы общего пользования: определения, классификация. Информационные системы обработки персональных данных: определение, классификация. Объекты КИИ: определение, классификация. Требования по безопасности информации ФСТЭК России. Алгоритм определения набора защитных мер информационной системы (для ГИС, ИСПДн, КИИ). Федеральный закон "О лицензировании отдельных видов деятельности". Лицензирование деятельности по технической защите конфиденциальной информации, разработке и производству средств защиты информации. Сертификация средств технической защиты информации на соответствие требованиям по безопасности информации. Классификация сертифицированных средств защиты информации по уровню контроля отсутствия недеklarированных возможностей (старая). Современные классификации по уровням доверия, профили защиты для различных видов средств защиты информации, классы защиты. Классификация комплексных средств защиты информации по РД «Средства вычислительной техники. Защита от НСД к информации. Показатели защищенности от НСД к информации». Реестр сертифицированных средств защиты информации ФСТЭК России. Реестр российского программного обеспечения. Выбор средств защиты информации для информационной системы определенного класса.	4		4	4
Тема 3. Основные угрозы безопасности информации и уязвимости информационных систем.	Понятия безопасности информации (данных), угрозы безопасности информации, источника угроз безопасности информации, уязвимости (информационной системы), модели угроз (безопасности информации), несанкционированного воздействия, компьютерной атаки. Банк данных угроз безопасности информации ФСТЭК России. Построение модели нарушителя и модели угроз. Методический документ "Методика оценки угроз безопасности информации" ФСТЭК России.	4		4	4

	<p>Порядок оценки угроз безопасности информации: исходные данные для оценки угроз, основные этапы оценки. Возможные негативные последствия реализации угроз. Возможные воздействия и объекты воздействия. Уровни архитектуры систем и сетей, на которых определяются объекты воздействия. Распределения границ при оценке угроз безопасности информации между оператором и поставщиком услуг. Типы нарушителей и их потенциал. Основные факторы возникновения угроз безопасности информации. Основные способы реализации (возникновения) угроз безопасности информации. Оценка актуальности угроз безопасности информации. ГОСТ Р 56546-2015 "Защита информации. Уязвимости информационных систем. Классификация уязвимостей информационных систем". Методы обнаружения и анализа уязвимостей. Источники информации об уязвимостях. Системы оценки уязвимостей (стандарт CVSS). Базы данных уязвимостей (CVE, NVD), база данных уязвимостей ФСТЭК России. Сканеры безопасности. Виды сканирования. Сканер безопасности ScanOval. Активные методы поиска уязвимостей, тестирование на проникновение. Виды тестирования на проникновение.</p>				
Тема 4. Средства защиты информации и подсистемы безопасности компьютерных систем.	<p>Основные виды средств защиты информации, их назначение и краткая характеристика. Идентификация, аутентификация и авторизация. Системы дискреционного и мандатного управления доступом. Средства сетевой защиты информации уровня периметра сети и уровня хоста. Средства мониторинга безопасности информации. Построение системы защиты информации. Принцип многоуровневой защиты (эшелонированной обороны). Виды архитектур систем ЗИ, принципы выбора архитектуры системы ЗИ.</p>	4		8	4
Тема 5. Комплексные средства защиты информации от несанкционированного доступа.	<p>Понятия несанкционированного доступа, защиты информации от несанкционированного доступа, средства защиты информации от несанкционированного доступа. Варианты реализации средств защиты информации от несанкционированного доступа: средствами операционной системы, наложенными средствами защиты. История развития средств защиты информации от несанкционированного доступа. Функциональные модули средств защиты информации от несанкционированного доступа. Средства идентификации, аутентификации и управления доступом. Аппаратные аутентификаторы. Средства контроля печати. Средства контроля целостности. Проблемы обеспечения целостности системного программного обеспечения. Средства контроля целостности системных объектов. Средства гарантированного уничтожения информации. Средства формирования замкнутой программной среды. Средства контроля машинных носителей информации. Средства</p>	4		20	4

	<p>доверенной загрузки: назначение и виды реализации. Классификация средств доверенной загрузки в документах ФСТЭК России. Средства самозащиты, защиты от администратора ИТ-системы. Средства криптографической защиты информации. Средства аудита событий. Средство защиты информации от несанкционированного доступа Secret Net. Варианты исполнения, функциональные возможности. Архитектура домена безопасности Secret Net Studio при централизованном (сетевом) развертывании и управлении. Рекомендации по настройке для соответствия требованиям о защите информации. Шаблоны безопасности. Автономная установка Secret Net. Локальное администрирование Secret Net. Настройка механизмов защиты Secret Net, настройка аудита, настройка дополнительных модулей сетевой защиты. Средство защиты информации от несанкционированного доступа Dallas Lock. Варианты исполнения, функциональные возможности. Установка и администрирование Dallas Lock, настройка механизмов защиты, настройка аудита.</p>				
<p>Тема 6. Подсистемы безопасности ОС CH Astra Linux SE.</p>	<p>Операционная система Astra Linux, варианты исполнения, релизы, операционная система специального назначения, защищенное средство виртуализации. Подсистемы безопасности ОС специального назначения Astra Linux SE. Рекомендации по настройке для соответствия требованиям о защите информации. Модель безопасности ОС CH Astra Linux SE. Модуль PARSEC. Базовая модель дискреционного управления доступом и расширенные списки ACL. Мандатный контекст безопасности. Управление пользователями и группами. Управление доступом к объектам файловой системы. Контроль целостности объектов файловой системы. Настройка политик безопасности. Формирование замкнутой программной среды. Ограничение программной среды - режим киоска. Контроль съемных носителей информации. Подсистема аудита ОС CH Astra Linux SE.</p>	2		12	4
<p>Тема 7. Защита от разрушающих программных воздействий.</p>	<p>Понятие вредоносного программного обеспечения, признаки вредоносности. Сущность разрушающих программных воздействий. Модели взаимодействия прикладных программ и программы злоумышленника. Методы внедрения вредоносных программных средств. Основные тенденции развития вирусных технологий. Бесфайловые атаки. Методы детектирования вредоносных программ, их ограничения и преимущества. Сигнатурный, эвристический и поведенческий анализ, контроль целостности. Технологии самозащиты вредоносного программного обеспечения. Защита от разрушающих программных воздействий, необходимые и достаточные условия недопущения разрушающего воздействия. Основные компоненты средства антивирусной защиты информации, их</p>	4		8	4

	особенности, характеристики, возможности применения. Классификация средств антивирусной защиты в документах ФСТЭК России. Сложные целенаправленные атаки (АРТ-атаки). Характерные особенности АРТ-атак, этапы реализации АРТ-атак. Понятие техник, тактик и процедур нарушителей. Сложность выявления АРТ-атак. Понятие проактивной защиты. Деятельность по киберразведке Threat intelligence.				
<b>Контроль:</b>					<b>0</b>
<b>Всего по дисциплине:</b>		<b>24</b>	<b>0</b>	<b>56</b>	<b>28</b>

\*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
1. Хорев, П. Б. Программно-аппаратная защита информации : учебное пособие / П.Б. Хорев. — 3-е изд., испр. и доп. — Электрон. дан. — Москва : ИНФРА-М, 2020. — 327 с.	<a href="https://znanium.com/catalog/document?id=364477">https://znanium.com/catalog/document?id=364477</a>
2. Внуков, А. А. Защита информации : учебное пособие для вузов / А. А. Внуков. — 3-е изд., перераб. и доп. — Электрон. дан. — Москва : Издательство Юрайт, 2020. — 161 с.	<a href="https://urait.ru/book/zaschita-informacii-490277">https://urait.ru/book/zaschita-informacii-490277</a>

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

- 7-Zip
- Dallas Lock 8.0-K (СЗИ НСД, СКН, МЭ, СОВ)
- Dallas Lock Linux (СЗИ НСД)
- Debian
- Oracle VM VirtualBox
- ОС Альт образование 10
- LibreOffice
- Dallas Lock 8.0-C (СЗИ НСД, СКН, МЭ, СОВ)
- Docker Community Edition (CE)
- Сервер безопасности для Dallas Lock 8.0-C
- Сервер безопасности для Dallas Lock 8.0-K
- Модули защиты диска и шифрования контейнеров средства защиты

информации Secret Net Studio 8

- Модули защиты от НСД и контроля устройств средства защиты информации Secret Net Studio 8
- Модуль персонального межсетевого экрана средства защиты информации Secret Net Studio 8
- Комплект "Постоянная защита" Средства защиты информации Secret Net LSP
- Astra Linux Special Edition уровень защищенности «Максимальный» («Смоленск»)

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

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

## **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
<p>Ауд. 2057 лаборатория Инженерно-технической защиты, лаборатория Программно-аппаратной защиты. Специализированная мебель и оборудование: Учебная мебель на 30 посадочных мест (Парта двухместная – 11 шт., стол – 8 шт., стулья- 30 шт.); 2 рабочих места преподавателя (2 стола, 2 стула); стол – 1 шт.; трибуна для выступлений – 1 шт.; шкаф для документов – 1 шт.; стенды настенные пробковые – 2 шт.; шкаф настенный со стеклянными створками – 4 шт.; доска для маркеров двухсторонняя – 1 шт.; персональный компьютер IBM PC-совместимый (i5-3470/RAM 8Gb/HDD 500Gb/Win7pro) – 7 шт.; персональный компьютер IBM PC-совместимый (i3-2100/RAM 8Gb/HDD 500Gb/Win7pro) – 8 шт.; коммутатор Cisco для организации локальной сети лаборатории с подключением к сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду организации – 1 шт.; шкаф серверный 42U – 1 шт.; шкаф телекоммуникационный 20U – 1 шт.; проектор NEC ME-401X – 1 шт.; экран для проектора Screen Media Goldview 244*244MW настенный – 1шт.; акустическая система марка Microlab модель Pro2– 1 шт.; коммутатор консольный Trend Net ТК-803R – 1 шт.; разветвитель видеосигнала Aten VS-92A – 1 шт.; лабораторный стенд НПП «Учтех-Профи» «ОЭ-МР» – 1 шт.; лабораторный стенд НПП «Учтех-Профи» «ОЦТ-МР» – 1 шт.; лабораторный стенд НПП «Учтех-Профи» «ФОЭ-НР» – 1 комплект; комплект плакатов НПП «Учтех-Профи» – 1 шт.; генератор акустического шума ЛГШ-301 АО «Лаборатория ППШ» – 1 шт.; виброгенератор ЛГШ-403 в комплекте с вибропреобразователями ЛВП-2о, ЛВП-2Т АО «Лаборатория ППШ» – 1 шт.; фильтр сетевой однофазный ЛФС-10-1Ф АО «Лаборатория ППШ» – 1 шт.; генератор шума по цепям электропит., заземл. и ПЭМИ ЛГШ-503 АО «Лаборатория ППШ» – 1 шт.; устройство защиты телефонных линий Гранит-8 абонентское АО «Лаборатория ППШ» – 1 шт.; сервер HP-DL – 5 шт.; Коммутатор Cisco Small Business SF302-08 – 4 шт.; Коммутатор Cisco 2950 – 3 шт.; Коммутатор Cisco 3560 – 1 шт.; Беспроводной маршрутизатор TP-Link TL - WR941 ND; Электронные ключи Guardant – 16 шт.; огнетушитель ОУ-5 – 1 шт.; огнетушитель ОП-4(3)-BCE – 1 шт. Наборы демонстрационного оборудования и учебно-наглядных пособий: мультимедийные приложения к лекционным курсам и практическим занятиям, интерактивные учебно-наглядные пособия.</p>	<p>191023, г. Санкт-Петербург, ул. Канал Грибоедова, 30/32, литер «А», «Б», «Р»</p>
<p>Ауд. 2021 Лаборатория "Лабораторный комплекс" Специализированная мебель и оборудование: Учебная мебель на 22 посадочных места (22 компьютерных стола, черных кресел 22шт.) Учебная мебель на 42 посадочных мест (парт 21 шт.) рабочее место преподавателя (компьютерный стол 1шт.)доска, меловая 3-х секционная 1шт., доска маркерная на колесиках 1 ш., часы 1 шт., кафедра</p>	<p>191023, г. Санкт-Петербург, ул. Канал Грибоедова, 30/32, литер «А», «Б», «Р»</p>

1шт., стол 1шт., тумбочка 1шт., стул из 4шт., вешалка стойка 2шт., жалюзи 3шт. Компьютер i5-8400/8GB/500GB_SSD/Viewsonic VA2410-mh - 23 шт., Установка демонстрационных учебных фильмов - 1 шт., Компьютер в комплектации системный блок Intel pentium x2 g3250 клавиатура+мышь L (жесткий диск500gb,монитор philips 21.5') - 1 шт. Наборы демонстрационного оборудования и учебно-наглядных пособий: мультимедийные приложения к лекционным курсам и практическим занятиям, интерактивные учебно-наглядные пособия.	
Ауд. 2061 Учебная аудитория (для проведения занятий лекционного типа и занятий семинарского типа, курсового проектирования (выполнения курсовых работ), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации), оборудована мультимедийным комплексом.Специализированная мебель и оборудование: Учебная мебель на 80 посадочных мест, рабочее место преподавателя, стол - 1 шт., доска меловая (3-х секционная) - 1 шт., кафедра - 1 шт., стульев - 2 шт. Переносной мультимедийный комплект: Ноутбук HP 250 G6 1WY58EA, Мультимедийный проектор LG PF1500G. Наборы демонстрационного оборудования и учебно-наглядных пособий: мультимедийные приложения к лекционным курсам и практическим занятиям, интерактивные учебно-наглядные пособия.	191023, г. Санкт-Петербург, ул. Канал Грибоедова, 30/32, литер «А», «Б», «Р»

## 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**

Рабочей программой дисциплины не предусмотрено.

### **1.2 Темы письменных работ**

Рабочей программой дисциплины не предусмотрено.

### **1.3 Контрольные точки**

<b>Номер контрольной точки</b>	<b>Тип контрольной точки</b>	<b>Способ проведения</b>	<b>Номера тем</b>
1	Информационно-аналитическая работа	с помощью технических средств и информационных систем	1-4,7
2	Индивидуальное задание	с помощью технических средств и информационных систем	5-6
3	Текущий контроль	с помощью технических средств и информационных систем	1-7

### **1.4 Другие объекты оценивания**

Рабочей программой дисциплины не предусмотрено.

### **1.5 Самостоятельная работа обучающегося**

<b>Наименования самостоятельной работы</b>	<b>Номера тем</b>
Подготовка к лекционным и практическим занятиям	1-7
Работа с аналитическими базами данных, нормативными документами, справочной литературой	1-4

### **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. Продemonстрировано уверенное владение материалом дисциплины. Выполненные задания носят целостных характер, выполнены в полном объеме, структурированы, представлены различные точки зрения, продемонстрирован творческий подход.