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

УТВЕРЖДАЮ
Проректор по учебной и методической работе
_____/Шубаева В.Г./
«28» августа 2020 г.

ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Рабочая программа дисциплины

Направление подготовки	10.03.01 Информационная безопасность
Направленность (профиль) программы	Безопасность компьютерных систем (в экономике и управлении)
Уровень высшего образования	бакалавриат
Форма обучения	очная

Составители:
_____/д.э.н., профессор Стельмашонок Е.В.
_____/к.т.н., доцент Сухостат В.В.

Санкт-Петербург
2020

СОДЕРЖАНИЕ

1. ЦЕЛЬ И ЗАДАЧИ ДИСЦИПЛИНЫ 3
2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ 3
3. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ 3
4. ОБЪЕМ И СТРУКТУРА ДИСЦИПЛИНЫ 4
5. СОДЕРЖАНИЕ РАЗДЕЛОВ И ТЕМ ДИСЦИПЛИНЫ 5
6. ЗАНЯТИЯ СЕМИНАРСКОГО ТИПА 7
7. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ 8
7.1. Методические указания для обучающегося по освоению дисциплины 8
7.2. Организация самостоятельной работы 8
8. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ 9
9. РЕСУРСНОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ 10
9.1 Учебно-методическое и информационное обеспечение дисциплины 10
9.2. Материально-техническое обеспечение учебного процесса 11
10. ОСОБЕННОСТИ ОСВОЕНИЯ ДИСЦИПЛИНЫ ДЛЯ ИНВАЛИДОВ И ЛИЦ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ 11
11. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕЙ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ 12

1. ЦЕЛЬ И ЗАДАЧИ ДИСЦИПЛИНЫ

Цель (цели) освоения дисциплины: способствовать освоению студентами необходимого начального объема знаний в области информационной безопасности, умений и навыков использования современных программных средств защиты информации**.**

Задачи:

- определение места и роли информационной безопасности в системе национальной безопасности Российской Федерации;
- приобретение теоретических знаний в области основных направлений информационной безопасности;
- формирование умения использования современных программных средств защиты информации;
- выработка практических навыков работы пользователя для защиты данных в операционной среде;
- закрепление теоретических знаний по обработке и защите информации в среде пакетов прикладных программ универсального назначения.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Дисциплина Б1.Б. «Основы информационной безопасности» относится к базовой части дисциплин Блока 1 и является обязательной для освоения обучающимся вне зависимости от направленности (профиля) программы.

3. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ

Планируемые результаты обучения по дисциплине, соотнесенные с планируемыми результатами освоения образовательной программы представлены в таблице 3.1.

Таблица 3.1 – Планируемые результаты обучения по дисциплине, соотнесенные с планируемыми результатами освоения образовательной программы

Код и наименование компетенции выпускника	Этапы формирования компетенций	Планируемые результаты обучения/индикаторы достижения компетенций (показатели освоения компетенции)
1	2	3
ОК-5 - способностью понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики	Первый уровень (пороговый) (ОК-5)-1-	Знать: место, роль и основные проблемы обеспечения информационной безопасности в системе национальной безопасности Российской Федерации З1(ОК-5). Уметь: проявлять активную позицию в условиях информационного противоборства У1(ОК-5). Владеть: профессиональной терминологией и методами анализа специальной литературы по вопросам обеспечения информационной безопасности В1(ОК-5)

ОПК-7 - способностью определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты	Первый уровень (пороговый) (ОПК-7)-1	Знать: виды, возможные методы и пути реализации угроз информационной безопасности объекта защиты З1 (ОПК-7). Уметь: анализировать и оценивать угрозы информационной безопасности объекта защиты У1 (ОПК-7). Владеть: профессиональной терминологией и навыками изучения специальной литературы по вопросам обеспечения информационной безопасности. В1 (ОПК-7.)

4. ОБЪЕМ И СТРУКТУРА ДИСЦИПЛИНЫ

Трудоемкость дисциплины составляет 4 зачетные единицы, 144 часа, из которых 36 часов самостоятельной работы обучающегося отводится на подготовку и защиту экзамена.

Форма промежуточной аттестации: экзамен - 1 семестр.

Распределение фонда времени по темам по очной форме обучения представлено в таблице 4.1

Таблица 4.1 – Распределение фонда времени по темам дисциплины (очная форма обучения)

Номер и наименование тем	Объем дисциплины (ак. часы)			
	Контактная работа			СРО
	ЗЛТ	ПЗ	ЛР	
1	*2*	*3*	*4*	*5*
Тема 1.1. Введение. Составляющие национальных интересов Российской Федерации в информационной сфере.	3	2		4
Тема 1.2. Понятие, сущность и актуальность защиты информации. Предмет и объект защиты информации.	4			8
Тема 1.3. Основные определения и задачи информационной безопасности. Риски и угрозы информационной безопасности	4			8
Тема 1.4. Принципы построения защищенных систем	4			8
Тема 1.5. Нормативно-правовое обеспечение информационной безопасности. Стандарты информационной безопасности.	2	4		4
Тема 2.1. Методы и технологии защиты информации. Классификация методов и средств защиты информации.	2			4
Тема 2.2. Антивирусная защита.	2			4
Тема 2.3. Системы идентификации и аутентификации. Системы разграничения доступа.	4	4		8
Тема 2.4. Стеганографические и криптографические методы	6	10		8
Тема 2.5. Технология электронной подписи	2	4		4
Тема 2.6. Методы обнаружения и блокирования угроз информационной безопасности	2			4
Тема 2.7. Методы защиты в операционных системах. Сетевые технологии защиты	5	8		8
Всего по дисциплине:	**40**	**32**		**72**

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

5. СОДЕРЖАНИЕ РАЗДЕЛОВ И ТЕМ ДИСЦИПЛИНЫ

Раздел 1. Теоретические основы информационной безопасности.

Тема 1.1. Введение. Составляющие национальных интересов Российской Федерации в информационной сфере

Предмет и задачи дисциплины. Значение и место дисциплины в подготовке бакалавров информационной безопасности. Научная и учебная взаимосвязь дисциплины «Основы информационной безопасности» с другими дисциплинами рабочего учебного плана.

Анализ нормативных источников, научной и учебной литературы. Знания и умения студентов, которые должны быть получены в результате изучения дисциплины.

Понятие и современная концепция национальной безопасности. Теоретические основы национальной политики в сфере **защиты информации**. Место **информационной безопасности** в системе национальной безопасности.

Задачи в области **обеспечения информационной безопасности** Российской Федерации. Реализация Стратегии национальной безопасности Российской Федерации до 2020.

Понятие и назначение Доктрины информационной безопасности. Интересы личности, общества и государства в **информационной сфере**. Составляющие национальных интересов в информационной сфере, пути их достижения.

Состояние **информационной безопасности** Российской Федерации и основные задачи по ее **обеспечению.** Особенности **обеспечения информационной безопасности** в различных сферах общественной жизни. Основные положения государственной политики обеспечения информационной безопасности, мероприятия по их реализации. Понятия информационной войны и информационного оружия. Проблема общемирового противодействия **угрозам информационной безопасности**.

Тема 1.2. Понятие, сущность и актуальность защиты информации. Предмет и объект защиты информации

Существующие подходы к содержательной части понятия «**защита информации**». Методологическая основа раскрытия сущности и определения понятия защиты информации. Цели защиты информации.

Понятие и назначение концепции защиты информации. Теория защиты информации как основа концепции защиты информации. Содержание концепции защиты информации, ее значение для разработки стратегии, формирования целевых программ и практических мероприятий по защите информации. **Проблема информационной безопасности** предприятия. Причины актуальности и важности **проблемы обеспечения информационной безопасности**.

Достоверная информация и ценность информации. Право собственника информации на ее использование и защиту от доступа к ней.

Уровни секретности сведений, составляющих государственную тайну. Перечень конфиденциальных сведений. Критерии, условия и принципы отнесения информации к защищаемой. Классификация конфиденциальной информации по видам тайны и степеням конфиденциальности. Пути получения информации. Методы оценки количества информации. Информация как объект права собственности. Субъекты информационных отношений по отношению к определенной информации. Полномочия, включающие право собственности. Понятие объекта защиты. Носители информации как конечные **объекты защиты**. Особенности отдельных видов носителей как **объектов защиты**.

Тема 1.3. Основные определения и задачи информационной безопасности. Риски и угрозы информационной безопасности

Понятие **безопасности автоматизированной информационной системы**. Понятие **защиты информации**. Конфиденциальность, целостность, доступность.

Субъекты, заинтересованные в обеспечении информационной безопасности. Уровни **обеспечения информационной безопасности**. Системы обеспечения информационной безопасности.

Понятие **угрозы информационной безопасности**. Основные **виды и источники угроз информационной безопасности**. Внутренние и внешние угрозы. Понятие уязвимости **информационной системы**, атаки на систему. Понятие риска.

Причины, виды, каналы утечки и искажения информации. Основные методы **реализации угроз информационной безопасности**: методы нарушения секретности, целостности и доступности информации.

Политика безопасности. Информационные риски. Управление рисками. Качественный и количественный анализ риска. Методики оценки рисков. Модель оценки рисков. Экономические последствия атак на информацию. Структура ущерба предприятия от **реализации угроз информационной безопасности.**

Тема 1.4. Принципы построения защищенных систем

Понятие **защищенной системы обработки информации.**

Задачи построения защищенных систем.

Принципы построения **защищенных автоматизированных информационных систем**. Модель многоуровневой защиты.

Тема 1.5. Нормативно-правовое обеспечение информационной безопасности. Стандарты информационной безопасности

Правовые меры защиты информации. Государственное регулирование в сфере **информационной безопасности.** Правовые режимы доступа к информации. Виды тайн. Персональные данные. Государственные регулирующие органы РФ. Компьютерные преступления.

Основные международные стандарты **информационной безопасности**. Процессы управления информационной безопасностью. Процесс управления рисками организации и его процедуры. Проблемы применения стандартов информационной безопасности.

Раздел 2. Методологические основы защиты информации

Тема 2.1. Методы и технологии защиты информации. Классификация методов и средств защиты информации

Определение методов и технологий защиты информации.

Обобщенные категории **методов защиты информации**. Организационные меры защиты информации. Технологические методы и средства защиты информации. Криптографические и правовые методы защиты информации.

Особенности защиты на разных уровнях **информационной системы**. Противодействие инсайдерской деятельности.

Тема 2.2. Антивирусная защита

Вредоносное программное обеспечение. Классификация вредоносных программ.

Понятие компьютерного вируса. Троянские программы. Основные типы компьютерных вирусов. Основные классы вредоносных программ по характеру воздействия на компьютерную систему.

Основные тенденции развития вирусных технологий. Возможные последствия вирусных атак. Методы и средства антивирусной защиты.

Тема 2.3. Системы идентификации и аутентификации. Системы разграничения доступа.

Системы идентификации и аутентификации: основные определения, типы, область применения, классификация. Парольная защита. Общие подходы к построению парольных систем. Выбор паролей. Методы взлома паролей. Методы выбора паролей.

Дискреционное и мандатное управление доступом. Уровни доступа. Ролевое управление доступом. Двухуровневое назначение прав доступа.

Тема 2.4. Стеганографические и криптографические методы

Исторические методы стеганографии. Цифровая стеганография. Определения и методы цифровой стеганографии. Стегосистема. Области применения компьютерной стеганографии.

Основы современной криптографии. Понятия и определения современной криптографии. Стойкость шифра. Стойкость алгоритмов шифрования. Классификация криптоаналитических атак. Классификация криптографических алгоритмов. Исторические шифры. Требования, предъявляемые к современным алгоритмам шифрования. Симметричные алгоритмы шифрования. Алгоритмы шифрования с открытым ключом.

Тема 2.5. Технология электронной подписи

Алгоритмы электронной подписи. Хеширование. Типы криптографических хеш-функций. Защищенная цифровая подпись. Цифровые сертификаты.

Тема 2.6. Методы обнаружения и блокирования угроз информационной безопасности

Этапы процесса осуществления атаки на **информационную систему**. Классификация систем обнаружения атак. Обманные системы. Системы контроля целостности и системы анализа журналов регистрации. Системы регистрации событий**.**

Тема 2.7. Методы защиты в операционных системах. Сетевые технологии защиты

Защищенные информационные системы. Оценка безопасности операционной системы. Структура операционной системы. Инструменты настройки безопасности ОС Windows. Аутентификация пользователей Windows. Защищенная файловая система NTFS. Средства шифрования ОС Windows. Безопасное уничтожение данных. Методы защиты системных файлов в Windows. Защита работы пользователей в сети Windows.
Защита офисных документов. Технологии защиты баз данных.

Основные принципы организации сетевой защиты. Типичные угрозы безопасности и уязвимости сетевых информационных систем. Классификация способов несанкционированного доступа и жизненный цикл атак. Нападения на политику безопасности и процедуры административного управления. Нападения на постоянные и сменные компоненты системы защиты. Нападения на протоколы информационного взаимодействия. Нападения на функциональные элементы компьютерных сетей.

Способы противодействия несанкционированному сетевому и межсетевому доступу. Аутентификация пользователя локальной сети. Разграничение доступа к локальной сети. Противодействие несанкционированному межсетевому доступу. Использование межсетевых экранов (Firewall). Критерии их оценки.

Туннелирование. Технология виртуальных частных сетей. Защищенные сетевые протоколы. **Безопасность работы** в сети Интернет. Безопасная доставка e-mail сообщений.

6. ЗАНЯТИЯ СЕМИНАРСКОГО ТИПА

Таблица 6.1 – Практические занятия/Семинарские занятия/Лабораторные работы

№ темы	Тема занятия	Вид занятия/Оценочное средство
1	*2*	*3*
1.1	Определение проблем и приоритетов в области информационной безопасности	ПЗ:/Деловая игра
1.5	Учебные слушания группы по структурным составляющим обеспечения информационной безопасности	ПЗ:/Тематическая дискуссия/ Деловая игра/Отчет. Научное эссе.
2.3	Создание учетных записей пользователей. Шифрование и управление доступом к файлам и папкам на	ПЗ:/ Решение прикладных задач

	локальном компьютере	
2.4	Изучение шифра «Поворотные решетки Кардано» Анализ шифра табличной перестановки Криптоанализ шифра простой замены Криптоанализ многоалфавитных шифров (шифр Виженера) Изучение шифра RSA	ПЗ:/ Решение прикладных задач
2.5	Использование цифровой подписи проектов VBA Изучение электронной цифровой подписи Эль-Гамаля	ПЗ: / Решение прикладных задач/Отчет. Индивидуальное задание
2.7	Защита документов MS WORD Защита книг MS EXCEL Защита баз данных MS ACCESS	ПЗ: / Решение прикладных задач

* ПЗ – практические занятия, СЗ – семинарские занятия, ЛР – лабораторные работы

7. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ

7.1. Методические указания для обучающегося по освоению дисциплины

Для формирования четкого представления об объеме и характере знаний и умений, которыми надо будет овладеть по дисциплине в самом начале учебного курса обучающийся должен ознакомиться с учебно-методической документацией:

– рабочей программой дисциплины: с целями и задачами дисциплины, ее связями с другими дисциплинами образовательной программы, перечнем знаний и умений, которыми в процессе освоения дисциплины должен владеть обучающийся,

– порядком проведения текущего контроля успеваемости и промежуточной аттестации;

– графиком консультаций преподавателей кафедры.

Систематическое выполнение учебной работы на занятиях лекционных и семинарских типов, а также выполнение самостоятельной работы позволит успешно освоить дисциплину.

В процессе освоения дисциплины обучающимся следует:

– слушать, конспектировать излагаемый преподавателем материал;

– ставить, обсуждать актуальные проблемы курса, быть активным на занятиях;

– задавать преподавателю уточняющие вопросы с целью уяснения теоретических положений;

– выполнять задания практических занятий полностью и установленные сроки.

При затруднениях в восприятии материала следует обратиться к основным литературным источникам. Если разобраться в материале не удалось, то обратится к лектору (по графику его консультаций) или к преподавателю на занятиях семинарского типа.

Обучающимся, пропустившим занятия (независимо от причин), не имеющим письменного решения задач или не подготовившимся к данному занятию, рекомендуется не позже чем в 2 - недельный срок явиться на консультацию к преподавателю и отчитаться по теме.

7.2. Организация самостоятельной работы

Под самостоятельной работой обучающихся понимается планируемая работа обучающихся, направленная на формирование указанных компетенций, выполняемая во внеаудиторное время по заданию и при методическом руководстве преподавателя, без его непосредственного участия.

Методическое обеспечение самостоятельной работы при наличии обучающихся лиц с ограниченными возможностями представляется в формах, адаптированных к ограничениям их здоровья.

Виды самостоятельной работы по дисциплине представлены в таблице 7.2.1.

Таблица 7.2.1 – Организация самостоятельной работы обучающегося

№ темы	Вид самостоятельной работы
1	*2*
1.1	Подготовка к экзамену.
1.2	Подготовка к экзамену.
1.3	Подготовка к экзамену.
1.4	Подготовка к экзамену.
1.5	Подготовка к выполнению контрольной точки 1. Подготовка к экзамену.
2.1	Подготовка к экзамену.
2.2	Подготовка к экзамену.
2.3	Подготовка к экзамену.
2.4	Подготовка к экзамену.
2.5	Подготовка к выполнению контрольной точки 2. Подготовка к экзамену.
2.6	Подготовка к экзамену.
2.7	Подготовка к экзамену.

Каждый вид СРО, указанный в таблице 7.2.1 обеспечен методическими материалами.

8. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

В преподавании дисциплины «*Основы информационной безопасности*» используются разнообразные образовательные технологии как традиционные, так и с применением активных и интерактивных методов обучения.

Активные и интерактивные методы обучения:

– проблемная лекция (тема 1.1);
– тематическая дискуссия (тема 1.5);
– деловая (ролевая) игра (тема 1.1; 1.5).

Тематическая дискуссия: обсуждения темы (спорного или проблемного характера) в учебной группе.

Проблемная лекция: преподаватель ставит вопрос или формулирует проблемную задачу и показывает варианты ответов или способов решения, а студенты наблюдают за поиском и определяют свое отношение к полученному материалу.

Деловая (ролевая) игра: имитационный игровой метод обучения, характеризующийся следующими основными признаками:

- наличие проблемы или задачи в сфере профессиональной деятельности и распределение ролей между участниками их решения (например, с помощью метода разыгрывания ролей может быть имитировано производственное совещание);
- взаимодействие участников игрового занятия, обычно посредством проведения дискуссии;
- ввод преподавателем в процессе занятия корректирующих условий;
- оценка результатов обсуждения и подведение итогов преподавателем.

Ролевые игры отличаются от деловых игр «локальностью» и меньшей сложностью решаемых проблем, задач профессиональной деятельности, акцентом на ролевых

функциях участников в игровой деятельности и оценке её результатов. Общая цель игрового коллектива (учебной группы), как правило, отсутствует. Цели и задачи участников связаны с наилучшим (адекватным, полным, корректным и т.д.) выполнением ролевых функций. Продолжительность ролевой игры может составлять от 0,5 до 4 часов учебного времени.

К интерактивным методам обучения относится выполнение групповых и индивидуальных заданий на ПК в ходе практических занятий и самостоятельной работы по темам 1.1, 1.5, 2.5.

Выполнение индивидуальных заданий на ПК предполагает выполнение индивидуальных заданий по предотвращению несанкционированного доступа к компьютерным ресурсам и защите программных средств, по специфической защите информации в локальных и глобальных компьютерных сетях (как правило, организационной формой таких занятий являются практические занятия).

9. РЕСУРСНОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

9.1 Учебно-методическое и информационное обеспечение дисциплины

Таблица 9.1.1 – Учебно-методическое обеспечение дисциплины

Библиографическое описание издания (автор, заглавие, вид, место и год издания, кол. стр.)	**Основная/ дополнительная литература**	**Книгообеспеченность**	
		Кол-во. экз. в библ. СПбГЭУ	**Электронные ресурсы**
Сухостат В.В. Основы информационной безопасности: учебное пособие / В.В.Сухостат, И.Н.Васильева .— Санкт-Петербург : Изд-во СПбГЭУ, 2019 .— 103 с. — Сведения доступны также по Интернету: opac.unecon.ru .	основная	35	ЭБ OPAC.UNECON.RU
Нестеров, С. А. Информационная безопасность: учебник и практикум. — Электрон. дан. — Москва: Юрайт, 2019. — 321 с.	основная	–	ЭБС Юрайт
Васильева И.Н. Информационные технологии и защита информации: учебное пособие / И.Н. Васильева, Е.В. Стельмашонок.— Санкт-Петербург: Изд-во СПбГИЭУ, 2011.— 271 с. — Сведения доступны также по Интернету: opac.unecon.ru.	дополнительная	71	ЭБ OPAC.UNECON.RU
Основы информационной безопасности : методические указания к выполнению лабораторных работ в среде Windows XP, MS Office 2010 для студентов всех форм обучения направления подготовки 090900 Информационная безопасность, квалификация - бакалавр. Файл 4498.doc. /Сост.: И.Н Васильева.— СПб : СПбГИЭУ, 2012.	дополнительная	–	ЭБ OPAC.UNECON.RU
Основы информационной безопасности : методические указания к практическим занятиям для студентов всех форм обучения направления подготовки 090900 Информационная безопасность, квалификация - бакалавр. Файл 4508.doc./Сост.: Е.В. Стельмашонок, Д.Ю. Федоров.— СПб : СПбГИЭУ, 2012	дополнительная	–	ЭБ OPAC.UNECON.RU

Таблица 9.1.2 – Перечень современных профессиональных баз данных (СПБД)

№	Наименование СПБД
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

Таблица 9.1.3 – Перечень информационных справочных систем (ИСС)

№	Наименование ИСС
1	Справочная правовая система КонсультантПлюс (инсталлированный ресурс СПбГЭУ или www.consultant.ru)
2	Справочная правовая система «ГАРАНТ» (инсталлированный ресурс СПбГЭУ или www.garant.ru)
3	Информационно-справочная система «Кодекс» (инсталлированный ресурс СПбГЭУ или www.kodeks.ru)
4	Электронная библиотечная система BOOK.ru - www.book.ru
5	Электронная библиотечная система ЭБС ЮРАЙТ – www.urait.ru
6	Электронно-библиотечная система ЗНАНИУМ (ZNANIUM) – www.znanium.com
7	Электронная библиотека СПбГЭУ– opac.unecon.ru

9.2. Материально-техническое обеспечение учебного процесса

Для реализации данной дисциплины имеются специальные помещения для проведения занятий лекционного типа, занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, а также помещения для самостоятельной работы.

Таблица 9.2.1 – Перечень программного обеспечения (ПО)

№ п/п	Наименование ПО
1	Microsoft Windows Professional (КОНТРАКТ № 244/20 «26» июня 2020 г
2	Microsoft Office Professional (КОНТРАКТ № 244/20 «26» июня 2020 г)
3	7-Zip (freeware)

10. 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.

Образование обучающихся с ограниченными возможностями здоровья может быть организовано как совместно с другими обучающимися, так и в отдельных группах или в отдельных организациях.

11. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕЙ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

Фонд оценочных средств для проведения аттестации уровня сформированности компетенций, обучающихся по дисциплине, оформляется отдельным документом и является приложением к рабочей программе дисциплины (модуля).