

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



УТВЕРЖДАЮ

Проректор по учебной и
методической работе

/Шубаева В.Г./


« 20 » июня 20 18 г.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ БИЗНЕС-СТРУКТУР

Рабочая программа дисциплины

Направление подготовки	42.03.01 Реклама и связи с общественностью
Направленность (профиль) программы	Реклама и связи с общественностью в бизнесе
Уровень образования	высшего бакалавриат
Форма обучения	очная

Составитель:

 к.пед.н., доцент Герасимов С.В.

Санкт-Петербург
2018

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	4
6.	ЗАНЯТИЯ СЕМИНАРСКОГО ТИПА	6
7.	МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ	7
7.1.	МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩЕГОСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ	7
7.2.	ОРГАНИЗАЦИЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ	7
8.	ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ	8
9.	РЕСУРСНОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ	9
9.1.	УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ	9
9.2.	МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ УЧЕБНОГО ПРОЦЕССА	10
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	11

1. ЦЕЛЬ И ЗАДАЧИ ДИСЦИПЛИНЫ

Цель освоения дисциплины: формирование у обучающихся комплексного понимания информационной безопасности, как нового качественного феномена в условиях функционирования постиндустриального общества, а также принципов и норм сочетания правового, технического, психофизического и этического регулирования в информационном пространстве, направленного на обеспечение баланса интересов личности, общества и государства в бизнесе посредством исполнения требований информационной безопасности.

Задачи:

- понимание обучающимися основ информационной безопасности, особенностей ее использования в средствах массовой информации, рекламы, связей с общественностью как самостоятельной отрасли и одновременно подотрасли информационного права;
- формирование целостного представления о назначении, характере, содержании и особенностях информационной безопасности, регулирующей правовые, технические, корпоративные и онтологические отношения в сфере бизнеса, рекламы и связей с общественностью;
- раскрытие системы информационной безопасности, регулирующей различные отношения в рассматриваемой области;
- ознакомление с существующей практикой информационной безопасности в масс-медийной, рекламной и PR-деятельности в сфере бизнеса;
- освоение основных технологий в сфере информационной безопасности, используемых в СМИ, рекламе и связях с общественностью;
- приобретение системных знаний о тенденциях развития информационной безопасности в России и за рубежом.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Дисциплина Б1.В.ДВ "Информационная безопасность бизнес-структур" относится к выборным дисциплинам Блока 1 и является обязательной для освоения обучающимся после их выбора.

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)
ПК-12 Способностью под контролем осуществлять профессиональные функции в области рекламы в общественных, производственных, коммерческих	Второй уровень (углубленный) (ПК-12) –2	Знать: специфику профессиональной деятельности в области рекламы в общественных, производственных, коммерческих структурах, средствах массовой информации 32(ПК-12) Уметь: правильно понимать поставленные руководителем рекламные задачи и творчески подходить к их решению У2(ПК-12). Владеть: навыками защиты информации в рамках своей профессиональной деятельности, осуществляемой в общественных, производственных, коммерческих

структурах, средствах массовой информации		структурах, средствах массовой информации В2(ПК-12).
ПК-15 Владением навыками работы в отделе рекламы, маркетинговом отделе, рекламном агентстве	Второй уровень (углубленный) (ПК-15) –2	Знать: социально-психологические особенности организации совместной деятельности в отделах по рекламе, маркетингу и в рекламном агентстве 32(ПК-15). Уметь: налаживать вертикальные и горизонтальные деловые связи в ходе выполнения профессиональных функций специалиста отдела рекламы, маркетингового отдела или сотрудника рекламного агентства У2(ПК-15). Владеть: навыками поддержания информационной безопасности работы отдела рекламы, маркетингового отдела, рекламного агентства В2(ПК-15)

4. ОБЪЕМ И СТРУКТУРА ДИСЦИПЛИНЫ

Трудоемкость дисциплины составляет 3 зачетных единиц, 108 часов.

Форма промежуточной аттестации: зачет – 6 семестр.

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

Таблица 4.1 – Распределение фонда времени по темам дисциплины

Номер и наименование тем	Объем дисциплины (ак. часы)			
	Контактная работа			СРО
	ЗЛТ	ПЗ	ЛР	
1	2	3	4	5
Тема 1. Понятие, предпосылки и процессы формирования информационной безопасности личности, общества и государства	2	4		6
Тема 2. Сущность информационного общества, его особенности тенденции развития	2	4		6
Тема 3. Информационная безопасность в системе национальной безопасности. Система информационной безопасности.	2	4		6
Тема 4. Понятие и особенности информационных рисков, опасностей и угроз	2	4		6
Тема 5. Основы доктрины информационной безопасности.	3	4		7
Тема 6. Характеристика технической и психофизической составляющих информационной безопасности	3	4		7
Тема 7. Специфика информационной безопасности в бизнесе	4	4		8
Тема 8. Особенности информационной безопасности в рекламной и PR-деятельности	4	4		8
Всего по дисциплине:	22	32		54

*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

Тема 1. Понятие, предпосылки и процессы формирования информационной безопасности личности, общества и государства.

Возникновение и развитие научных взглядов на проблему информационной безопасности. Исторические, политологические, социологические, юридические предпосылки и аспекты возникновения, формирования и развития информационной безопасности. Социологическая парадигма информационной безопасности. Научно-

техническая революция, которая значительно раздвинула границы совершенствования социума и индивида и, наконец, оказала сильнейшее воздействие на социальное и информационное становление общества и личности. Процессы глобализации как одна из предпосылок явления информационной безопасности. Основные процессы формирования информационной безопасности. Информационная безопасность все чаще становится объективной необходимостью в обычной жизнедеятельности социума.

Тема 2. Сущность информационного общества, его особенности тенденции развития.

Сущность, принципы и содержание информационного общества, место и роль постиндустриального социума в современном развитии человеческой цивилизации. Социологический анализ информационного общества, способность и проблематика социальной адаптации в данном обществе, исследование этой социальной адаптации как объективного механизма функционирования современного информационного общества. Закономерности и особенности функционирования системы информационной безопасности в рамках существующего информационного общества, необходимость и приоритетность социально-технологического подхода в управлении процессами формирования информационной безопасности в российском социуме. Понятие, сущность, конститутивные принципы организации информационного общества. Тенденции и перспективы его развития. Особенности формирования российского информационного общества. Характеристика трансформации российского социума в современных демократических условиях. Основные политические, экономические и социальные позиции нынешнего российского общества, его степень готовности к условиям функционирования в глобальном информационном сообществе.

Тема 3. Информационная безопасность в системе национальной безопасности. Система информационной безопасности.

Современное геополитическое и социально-экономическое положение России предопределяет особую актуальность защиты ее интересов и обеспечения национальной безопасности. Национальная безопасность представляет собой наиважнейшую составляющую системы безопасности и самым тесным образом переплетена с экономическим, политическим, социальным и духовно-нравственным развитием государства. Позиции и взгляды на определение и суть национальной безопасности России. национальная безопасность как совокупность всех видов безопасности, обеспечивающих в своих форматах физическую, материальную, духовную и социальную защиту личности, общества и государства. Элементы национальной безопасности. Информационная безопасность как новый элемент в системе национальной безопасности. Задачи информационной безопасности в Стратегии национальной безопасности Российской Федерации до 2020 года. Информационная безопасность и социальная безопасность.

Тема 4. Понятие и особенности информационных рисков, опасностей и угроз.

Глобальный и внешний характер информационных рисков, опасностей и угроз. Их сущность и классификация. Характеристика основных глобальных проблем. Стратегия выживания человека на основе решения глобальных проблем современности. Особенность глобальных информационных угроз и др. заключается в том, что их источники не направлены на конкретного субъекта информационного мирового пространства, т.е. не проецируются на личность и общество определенного государства, но охватывают их в совокупности. Иначе говоря, глобальные информационные риски, опасности и угрозы носят обезличенный характер и касаются всех, но понятие все – не имеет конкретного адресата. Информационный риск как понятие представляет собой возникновение ситуации, характеризующейся неопределенностью результата, учитывающей вероятное или обязательное наличие неблагоприятных последствий. Информационная опасность как совокупность вероятных или реально действующих факторов, процессов и явлений, которые могут оказать деструктивное воздействие на

объекты и субъекты, подвергающиеся опасному посягательству. Информационная угроза как намерение реализовать вероятную опасность. Внутренние источники и причины информационных опасностей и угроз. Понятие инсайдерской угрозы.

Тема 5. Основы доктрины информационной безопасности.

Концепция информационной безопасности, изложенная в Доктрине информационной безопасности. Социально-политические и экономические факторы принятия Доктрины информационной безопасности. Анализ основных положений Доктрины информационной безопасности. Окинавская хартия, как фактор признания Россией глобального характера актуальности информационной безопасности. Характеристика технико-технологической составляющей в Доктрине информационной безопасности. Психофизические составляющие в Доктрине информационной безопасности. Анализ социального характера Доктрины информационной безопасности. Проблематика и недостатки в Доктрине информационной безопасности.

Тема 6. Характеристика технической и психофизической составляющих информационной безопасности.

Организационно-технические методы обеспечения информационной безопасности Российской Федерации. Глобальная компьютеризация. Развитие современных информационно-коммуникационных систем и технологий. Проблемы хакерства. Проблема электронных вирусов. Проблема технических сбоев. Проблема нерегулируемого и неконтролируемого роста информационных потоков, усиление негативного информационного воздействия на психику и онтологию субъекта. Проблема подмены эмпирического познания мира информационно-коммуникационными технологиями. Характеристика инсайдерских угроз. Проблемы государственного управления процессом подготовки кадров в области обеспечения информационной безопасности. Проблемы кадрового обеспечения информационной безопасности. Характеристика основных социальных технологий, определяющих эффективность информационной безопасности личности, общества, организации и государства.

Тема 7. Специфика информационной безопасности в бизнесе.

Анализ современного информационного продукта, производимого СМИ. Типология бизнеса. Бизнес как фактор информационной опасности и угрозы. Деструктивная роль негативной информации СМИ на бизнес-структуры. Тактические СМИ как информационная угроза. Информационные войны как угроза информационной и социальной (и национальной) безопасности. Бизнес-структура как субъект информационной безопасности. Информационные риски, опасности и угрозы в производственном коллективе и профессиональной деятельности. Инсайдерство.

Тема 8. Особенности информационной безопасности в рекламной и PR-деятельности.

Рекламная и PR-деятельность как субъекты информационной безопасности. Специфика информационных рисков, опасностей и угроз в рекламной и PR-деятельности. Рекламный продукт и PR-продукт как потенциальный источник информационной опасности или угрозы. Правовая и этическая ответственность за свою деятельность. Рекламный и PR-отделы как субъекты информационной безопасности. Инсайдерский фактор. Производственный фактор. Социальные технологии, позволяющие обеспечивать информационную безопасность коллектива.

6. ЗАНЯТИЯ СЕМИНАРСКОГО ТИПА

Таблица 6.1 – Практические занятия/ Семинарские занятия / Лабораторные работы

№ темы	Тема занятия	Вид занятия/ Оценочное средство
1	2	3
1	Характеристика процессов формирования информационной	ПЗ: Доклад-

	безопасности.	сообщение
2	Глобальное информационное общество: особенности и преимущества	ПЗ: Доклад-сообщение
3	Понятие системы обеспечения информационной безопасности	ПЗ: Доклад-сообщение
4	Субъекты системы обеспечения информационной безопасности	ПЗ: Контрольная работа 1
5	Характеристика технических и психофизических информационных опасностей и угроз	ПЗ: Доклад-сообщение
6	Современные информационные войны	ПЗ: Доклад-сообщение
7	Социальные технологии обеспечения информационной безопасности в бизнесе	ПЗ: Доклад-сообщение
8	Подготовка рекламного и PR-продукта с учетом информационной безопасности	ПЗ: Контрольная работа 2

*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 обратиться 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.

Электронный учебно-методический комплекс дисциплины наименование дисциплины размещен в СДО «Moodle» на сайте СПбГЭУ de.unecon.ru/

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
1-8	Подготовка к практическим занятиям по дисциплине.
1-8	Выполнение заданий по темам дисциплины
1-4	Подготовка к контрольной точке №1 «Контрольная работа 1»
5-8	Подготовка к контрольной точке №2 «Контрольная работа 2»

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

Методические рекомендации включают в себя все виды самостоятельной работы, предусмотренные для успешного освоения дисциплины.

8. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

В преподавании дисциплины используются разнообразные образовательные технологии как традиционные, так и с применением активных и интерактивных методов обучения.

Активные и интерактивные методы обучения:

- лекция-дискуссия (тема №1);
- проблемная лекция (тема № 7,8);
- аналитические доклады (тема №1-8);

В процессе изучения дисциплины используются следующие активные методы обучения:

Лекция-дискуссия. Дискуссия – это взаимодействие преподавателя и учащегося, свободный обмен мнениями, идеями и взглядами по исследуемому вопросу. Это оживляет учебный процесс, активизирует познавательную деятельность аудитории и, что очень важно, позволяет преподавателю управлять коллективным мнением группы, использовать его в целях убеждения, преодоления негативных установок и ошибочных мнений некоторых обучаемых. Эффект достигается только при правильном подборе вопросов для дискуссии и умелом, целенаправленном управлении ею. Так же можно предложить слушателям проанализировать и обсудить конкретные ситуации, материал.

По ходу лекции-дискуссии преподаватель приводит отдельные примеры в виде ситуаций или кратко сформулированных проблем и предлагает студентам коротко обсудить, затем краткий анализ, выводы и лекция продолжается.

Положительным в дискуссии является, то, что обучаемые согласятся с точкой зрения преподавателя с большой охотой, скорее в ходе дискуссии, нежели во время беседы, когда преподаватель лишь указывает на необходимость принять его позицию по обсуждаемому вопросу.

Данный метод позволяет преподавателю видеть, насколько эффективно слушатели используют полученные знания в ходе дискуссии. Отрицательное же то, что обучаемые

могут неправильно определять для себя область изучения или не уметь успешно обсуждать возникающие проблемы. Поэтому в целом занятие может оказаться запутанным. Слушатели в этом случае могут укрепиться в собственном мнении, а не изменить его. Выбор вопросов для активизации учащихся и темы для обсуждения, составляется самим преподавателем в зависимости от конкретных дидактических задач, которые преподаватель ставит перед собой для данной аудитории.

Проблемная лекция. В отличие от информационной лекции, на которой студенты получают интерпретированную преподавателем информацию, на проблемной лекции, новый теоретический материал подается как неизвестное, которое необходимо открыть, решивши проблемную ситуацию. Задача педагога заключается в необходимости прогнозировать проблемную стратегию обучения, обеспечить участие студентов в анализе возникшего противоречия, привлекать их к решению проблемных ситуаций, учить выдвигать оригинальные пути их решения, учить анализировать полученную новую информацию в свете известных теорий, выдвигать гипотезы и использовать различные методы для их решения. На проблемной лекции привлечение студентов к активной деятельности осуществляется преподавателем с помощью создания проблемных ситуаций.

Доклад - выступление, содержащее научную информацию. Оптимальное время доклада — 5-10 минут. Докладчик коротко излагает историю вопроса и информирует слушателей о том, какой материал был использован при подготовке доклада. Основная часть доклада содержит рассуждения автора, касающиеся избранной проблемы, изложение собственной точки зрения, которую докладчик обосновывает, используя различные способы доказательств: приводит аналогичные примеры, цитирует высказывания видных ученых, общественных деятелей, ставит вопросы, использует примеры из жизненного опыта слушателей. В заключительной части обобщается сказанное, формулируются выводы и предложения

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
1. Васильева, И.Н. Управление информационной безопасностью : учебное пособие / И.Н.Васильева ; М-во образования и науки Рос. Федерации, С.-Петерб. гос. экон. ун-т, Каф. вычисл. систем и программирования.— Санкт-Петербург : Изд-во СПбГЭУ, 2014.— 82 с. : ил., табл. — Сведения доступны также по Интернету: opac.unecon.ru	Основная	58	ЭБ OPAC.UN ECON.RU
2. Андреевский, И.Л. Управление ИТ-сервисами и контентом : учебное пособие / И.Л.Андреевский, Х.И.Аминов ; М-во образования и науки Рос. Федерации, С.-Петерб. гос. экон. ун-т, Каф. информ. систем в экономике.— Санкт-Петербург : Изд-во СПбГЭУ, 2014. — 103 с. : ил., табл. — Сведения доступны также по Интернету: opac.unecon.ru	Основная	55	ЭБ OPAC.UN ECON.RU

3. Майорова, Е.В. Защита и обработка конфиденциальных документов : учебное пособие / Е.В.Майорова ; Министерство образования и науки Российской Федерации, Санкт-Петербургский гос. экономический ун-т, Кафедра вычислительных систем и программирования.— Санкт-Петербург : Изд-во СПбГЭУ, 2016.— 79 с. : табл. — Сведения доступны также по Интернету: opac.unicon.ru	Основная	55	ЭБ OPAC.UNECON.RU
4. Барабанова, М.И. Информационные технологии: открытые системы, сети, безопасность в системах и сетях : учебное пособие / М.И.Барабанова, В.И.Кияев ; М.-во образования и науки Рос. Федерации, С.-Петерб. гос. экон. ун-т, Каф. информатики.— 2-е изд., испр. и доп. — Санкт-Петербург : Изд-во СПбГЭУ, 2013.— 262 с. : ил. — Сведения доступны также по Интернету: opac.unicon.ru	Дополнительная	13	ЭБ OPAC.UNECON.RU
5. Бугорский, В.Н. Экономика защиты информации : учебное пособие / В.Н.Бугорский, Е.В.Степашонок, О.Д.Мердина ; М.-во образования и науки Рос. Федерации, С.-Петерб. гос. экон. ун-т, Каф. вычисл. систем и программирования.— Санкт-Петербург : Изд-во СПбГЭУ, 2015.— 120 с. : ил., табл. — Сведения доступны также по Интернету: opac.unicon.ru	Дополнительная	25	ЭБ OPAC.UNECON.RU
6. Морозов, С.К. Физические основы защиты информации : учебное пособие / С.К.Морозов ; Министерство образования и науки Российской Федерации, Санкт-Петербургский гос. экономический ун-т.— Санкт-Петербург : Изд-во СПбГЭУ, 2015.— 79 с. : ил., табл. — Сведения доступны также по Интернету: opac.unicon.ru	Дополнительная	35	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 eLIBRARY – 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.unicon.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

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).