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.

МЕЖДУНАРОДНЫЕ И РОССИЙСКИЕ НОРМАТИВНЫЕ АКТЫ И СТАНДАРТЫ ПО 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

Составитель(и):
_____/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 9
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 основных принципов и методов, применяемых при защите информации в компьютерных системах объектов информатизации, создаваемых и эксплуатируемых в различных сферах народного хозяйства.

Задачи:

- приобретение теоретических знаний в области нормативно-правовой базы по защите информации в компьютерных системах;
- формирование умения применять современные отечественные и зарубежные стандарты по защите информации;
- выработка практических навыков использования стандартов для защиты информации в конкретных компьютерных системах;
- выработка практических навыков построения защищенных информационных технологий;
- формирование умения организовывать работу по внедрению нормативно-правовой базы по защите информации на предприятии.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Дисциплина Б1.В «Международные и российские нормативные акты и стандарты по информационной безопасности» относится к вариативной части дисциплин Блока 1, и является обязательной для освоения обучающимся после выбора обучающимся 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)
ПК-9- способностью осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности	Третий уровень (продвинутый) (ПК-9) –3	Знать: основные нормативно-правовые, нормативно-методические документы и стандарты в области информационной безопасности и защиты информации. З3(ПК-9) Уметь: ранжировать требования различных нормативно-правовых актов и стандартов по частным вопросам защиты информации У3 (ПК-9) Владеть: навыками пользования профессиональной терминологии, изложенной в руководящих документах регуляторов в области защиты информации. В3(ПК-9)
ПК-10 - способностью проводить анализ информационной безопасности объектов и систем на соответствие требованиям	Второй уровень (углубленный) (ПК-10) –2	Знать современное состояние, классификацию и тенденции развития нормативно-правовой базы информационной безопасности. З2(ПК-10) Уметь: планировать работу по внедрению

стандартов в области информационной безопасности		требований нормативно-правовой базы по защите информации на предприятии У2 (ПК-10) Владеть навыками постановки прикладных задач защиты информации в терминах нормативно-методических документов в области информационной безопасности. В2(ПК-10)
ПК-15 - способностью организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	Второй уровень (углубленный) (ПК-15) –2	Знать: Нормативно-правовые акты по защите информации ограниченного доступа. З2(ПК-15) Уметь: Определять типы угроз безопасности персональных данных, актуальных для информационной системы. У2 (ПК-15) Владеть: Навыками определения уровня защищенности персональных данных при их обработке в информационной системе. В2(ПК-15)

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 – 7 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*
Раздел 1. Общие вопросы нормативной базы в области ЗИ РФ				
Тема 1.1. Основные нормативно-правовые акты и методические документы в области ЗИ	2	4		6
Тема 1.2. Нормативно-правовые акты по вопросам ЗИ ограниченного доступа.	2			6
Тема 1.3. Нормативно-правовые акты по вопросам безопасности информационных систем персональных данных (ИСПДн).	2	4		6
Раздел 2. Нормативно-правовые акты по вопросам ИБ и ЗИ в РФ				
Тема 2.1. Информационные сообщения регуляторов в области ЗИ.	2			6
Тема 2.2. Нормативно-правовые акты по вопросам безопасности информации в ключевых системах информационных инфраструктурах и АСУ производственными и технологическими процессами.	2			6
Тема 2.3. Нормативно-правовые акты по вопросам безопасности информации в государственных ИС и ИС общего пользования.	2			6

Тема 2.4. Нормативно-правовые акты по вопросам электронной подписи и криптографической ЗИ	2			6
Тема 2.5. Организационно-распорядительные документы по вопросам информационной безопасности и ЗИ.	2	4		6
Раздел 3. Национальные и международные стандарты в области ИБ				
Тема 3.1. Государственные стандарты РФ по вопросам ИБ и ЗИ.	2	10		6
Тема 3.2. Рекомендации МСЭ	2	10		6
Тема 3.3. Стандарты ISO/IEC. Британская серия BS 7799	2	6		6
Тема 3.4 Стандарты ведущих западных стран (Германия, США)	2	10		6
Всего по дисциплине:	**24**	**48**		**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. Общие вопросы нормативной базы в области ЗИ РФ

Тема 1.1. Основные нормативно-правовые акты и методические документы в области защиты информации.

Конституция Российской Федерации. Доктрина информационной безопасности Российской Федерации. Стратегия развития информационного общества в Российской Федерации. Стратегия национальной безопасности Российской Федерации до 2020 года. Федеральные законы РФ: «О безопасности», «Об информации, информационных технологиях и о защите и информации», «О техническом регулировании», «О коммерческой тайне», «О связи».

Тема 1.2. Нормативно-правовые акты по вопросам ЗИ ограниченного доступа

Федеральный закон РФ «О лицензировании отдельных видов деятельности». Федеральный закон РФ «О государственной тайне». Указ Президента РФ «Об утверждении Перечня сведений конфиденциального характера». Положение о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти. Административные регламенты ФСТЭК.

Тема 1.3. Нормативно-правовые акты по вопросам безопасности информационных систем персональных данных (ИСПДн)

Федеральный закон РФ «О персональных данных». Постановление Правительства РФ «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных». Положение об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации. Постановление Правительства РФ «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных». Базовая модель угроз безопасности персональных данных. Методика определения актуальных угроз безопасности персональных данных. Приказ ФСТЭК «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

Раздел 2. Нормативно-правовые акты по вопросам ИБ и ЗИ в РФ

Тема 2.1. Информационные сообщения регуляторов в области ЗИ.

Информационное сообщение ФСТЭК России «Об особенностях защиты персональных данных при их обработке в информационных системах персональных данных и сертификации средств защиты информации, предназначенных для защиты персональных данных». Разъяснение Роскомнадзора России по вопросам отнесения фото- и видео-изображения, дактилоскопических данных и иной информации к биометрическим

персональным данным и особенности их обработки. Информационное сообщение ФСТЭК России «По вопросам защиты информации и обеспечения безопасности персональных данных при их обработке в информационных системах в связи с изданием приказов ФСТЭК России № 17 от 11 февраля 2013 г. и № 21 от 18 февраля 2013 г.»

Тема 2.2. Нормативно-правовые акты по вопросам безопасности информации в ключевых системах информационных инфраструктурах и АСУ производственными и технологическими процессами

Рекомендации по обеспечению безопасности информации в ключевых системах информационной инфраструктуры. Основные направления государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры Российской Федерации. Приказ ФСТЭК России «Об утверждении Требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды».

Тема 2.3. Нормативно-правовые акты по вопросам безопасности информации в ГИС и ИС общего пользования.

Приказ Минкомсвязи РФ «Об утверждении Требований по обеспечению целостности, устойчивости функционирования и безопасности информационных систем общего пользования». Приказ ФСБ РФ и ФСТЭК России «Об утверждении требований о защите информации, содержащейся в информационных системах общего пользования. Приказ ФСТЭК России «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах». Меры защиты информации в государственных информационных системах: методический документ ФСТЭК России. Приказ Минкомсвязи РФ «Об утверждении Технических требований к взаимодействию информационных систем в единой системе межведомственного электронного взаимодействия».

Тема 2.4. Нормативно-правовые акты по вопросам электронной подписи и криптографической ЗИ

Федеральный закон РФ «Об электронной подписи». Положение о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005). Требования к форме квалифицированного сертификата ключа проверки электронной подписи. Требования к средствам электронной подписи и требований к средствам удостоверяющего центра.

Тема 2.5. Организационно-распорядительные документы по вопросам информационной безопасности и ЗИ.

Положение о ФСТЭК России. Положения о лицензировании деятельности по технической защите конфиденциальной информации, разработке и производству средств защиты конфиденциальной информации. Положение о сертификации средств защиты информации. Положение по аттестации объектов информатизации по требованиям безопасности информации. Руководящие документы Гостехкомиссии и ФСТЭК России. Методические документы ФСТЭК России.

Раздел 3. Национальные и международные стандарты в области ИБ

Тема 3.1. Государственные стандарты РФ по вопросам ИБ и ЗИ.

Серия ГОСТ Р 5****: основные термины и определения; защита от НСД; факторы, воздействующие на информацию; обеспечение безопасности сетей; требования к средствам защиты информации и системам в защищенном исполнении; испытания технических и программных средств; методы и средства обеспечения безопасности; менеджмент информационной безопасности; архитектура информационной безопасности.

Серия ГОСТ Р ИСО/МЭК «Информационная технология. Методы и средства обеспечения безопасности».

Тема 3.2. Рекомендации Международного союза электропередачи данных МСЭ

X-серия «Сети передачи данных, взаимосвязь открытых систем и безопасность»: информационная и сетевая безопасность (общие аспекты безопасности, сетевая безопасность, менеджмент безопасности, архитектура безопасности); безопасность приложений и сервисов (безопасность ЛВС, мобильная безопасность, web-безопасность, протоколы безопасности; безопасность сенсорных сетей); кибербезопасность (программные закладки, борьба со спамом, идентификация и аутентификация, техника защиты от сетевых атак); безопасность облачных вычислений.

Тема 3.3. Стандарты ISO/IEC. Британская серия BS 7799

Стандарт IEC 31010:2009 Ed.1.0 «Менеджмент риска. Методы оценки риска». Стандарт ISO/IEC 27002 «Информационные технологии. Механизмы защиты. Свод правил по управлению информационной безопасностью». BS 7799-1 «Практические правила управления информационной безопасностью». BS 7799-2 «Управление информационной безопасностью. Требования к системам управления информационной безопасностью».

Тема 3.4. Стандарты ведущих западных стран (Германия, США)

Немецкий стандарт «Руководство по обеспечению безопасности ИТ для базового уровня защищенности». Стандарты США серии FIPS: 199:2003 «Стандарт для категорирования безопасности информации и Федеральных информационных систем»; 200:2004 «Минимальные меры обеспечения безопасности для Федеральных информационных систем»; 140-3:2001 «Требования безопасности для криптографических модулей». Стандарты США серии NIST: SP 800-30:2002 «Руководство по управлению риском для систем информационной технологии»; SP 800-39:2010 «Управление риском информационной безопасности»; SP 800-5:2006 «Руководящие указания по управлению безопасностью для Федеральных информационных систем»; SP 800-53A:2010 «Руководство по оценке мер управления безопасностью для Федеральных информационных систем».

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 современном состоянии, классификации и тенденциях развития нормативно-правовой базы по информационной безопасности	ПЗ: Деловая (ролевая) игра
1.1.	Сравнительный анализ различных стандартов в области защиты информационных технологий с точки зрения эффективности достижения цели построения защищенных информационных систем.	ПЗ: Тематическая дискуссия / Отчет
1.3.	Анализ особенностей и проведение классификации информационных систем ИсПДн в организации	ПЗ: Деловая (ролевая) игра/
1.3	Базовая модель угроз безопасности персональных данных. Методика определения актуальных угроз безопасности персональных данных.	ПЗ: Деловая (ролевая) игра
2.5	Организационно-распорядительные документы по вопросам информационной безопасности и ЗИ	ПЗ: Деловая (ролевая) игра/ Отчет/Научное Эссе/Презентация
3.1	Анализ рисков для информационной системы предприятия (организации).	ПЗ: Решение прикладных задач

3.1	Построение модели угроз безопасности ИС предприятия	ПЗ: Решение прикладных задач
3.1	Анализ национальных стандартов в области ИБ РФ	ПЗ: Решение ПЗ: прикладных задач
3.1	Анализ стандартов серии 27000по менеджменту ИБ	ПЗ: Решение прикладных задач
3.1	Анализ комплекса стандартов по ИБ Банка России (ИББС)	ПЗ: Решение прикладных задач/ Тест
3.2	Порядок сертификации средств защиты информации для разработчика СЗИ.	ПЗ: Решение прикладных задач
3.2	Порядок сертификации защищенных информационных систем.	ПЗ: Решение прикладных задач
3.2	Порядок лицензирования в области создания средств защиты информации для руководителя предприятия (организации) – соискателя лицензии	ПЗ: Решение прикладных задач
3.2	Порядок лицензирования в области создания информации и защищенных информационных систем для руководителя предприятия (организации) – соискателя лицензии	ПЗ: Решение прикладных задач
3.2	Анализ нового поколения нормативных документов ФСТЭК России	ПЗ: Решение прикладных задач
3.3	Анализ применения серии стандартов/ISO/IEC в российских нормативных актах в области ИБ	ПЗ: Решение прикладных задач
3.3	Анализ применения серии стандартов BS 7799 в области ИБ РФ	ПЗ: Решение прикладных задач
3.3	Разработка профиля защиты для компьютерной системы предприятия (организации)	ПЗ: Решение прикладных задач
3.3	Построение политики безопасности для компьютерной системы предприятия (организации	ПЗ: Решение прикладных задач
3.4	Анализ немецкого стандарта «Руководство по обеспечению безопасности ИТ для базового уровня защищенности».и особенности применения его в области ИБ РФ	ПЗ: Решение прикладных задач
3.4	Анализ стандартов США серии FIPS.и особенности применения их в области ИБ РФ	ПЗ: Решение прикладных задач
3.4	Анализ стандартов США серии SP для Федеральных информационных систем и особенности применения их в области ИБ РФ	ПЗ: Решение прикладных задач
3.4	Разработка алгоритма проведения аттестационных испытаний компьютерных систем в защищенном исполнении	ПЗ: Решение прикладных задач
3.4	ПЗ: Проведение аттестационных испытаний компьютерных систем в защищенном исполнении и выдача «Аттестата соответствия».	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.
2.1	Подготовка к экзамену.
2.2	Подготовка к экзамену.
2.3	Подготовка к экзамену.
2.4	Подготовка к экзамену.
2.5	Подготовка к контрольной точке №1. Подготовка к экзамену.
3.1	Подготовка к контрольной точке №2. Подготовка к экзамену.
3.2	Подготовка к экзамену
3.3	Подготовка к экзамену.
3.4	Подготовка к экзамену.

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

8. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

В преподавании дисциплины «*Международные и российские нормативные акты и стандарты по информационной безопасности*» используются разнообразные образовательные технологии как традиционные, так и с применением активных и интерактивных методов обучения.

Активные и интерактивные методы обучения:

– проблемная лекция (1.1);
– тематическая дискуссия (тема 1.2)
– деловая (ролевая) игра (тема 1.1.)

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, 2.5, 3.1, 3.2, 3.3, 3.4.

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**
Солодянников А. В. Международные и российские акты и стандарты по информационной безопасности : учебное пособие .— Санкт-Петербург : Изд-во СПбГЭУ, 2017 .— 87 с. — Сведения доступны также по Интернету: opac.unecon.ru .	основная	25	ЭБ OPAC.UNECON.RU
Солодянников А.В. Комплексная система защиты объектов информатизации : учебное пособие .— Санкт-Петербург : Изд-во СПбГЭУ, 2017 .— 91 с. — Сведения доступны также по Интернету: opac.unecon.ru .	Основная	25	ЭБ OPAC.UNECON.RU

Васильева И.Н. Информационные технологии и защита информации: учебное пособие /И.Н. Васильева, Е.В. Стельмашонок.- СПб.: СПбГИЭУ, 2011. — 271 с. – Сведения доступны также по Интернету: opac.unecon.ru	дополнительная	71	ЭБ OPAC.UNECON.RU
Нормативная база, российские и международные стандарты по информационной безопасности : методические указания к выполнению практических занятий для студентов очной формы обучения направления подготовки 090900 Информационная безопасность, квалификация - бакалавр. Файл 11795.doc / Сост.: А.П.Кондратюк .— 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).