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.

ЗАЩИТА ИНФОРМАЦИОННЫХ СИСТЕМ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

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:
_____/к.т.н., доцент Солодянников А.В.
_____/ст. преподаватель Полегенько А.М.

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 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 10
11. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕЙ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ 11

1. ЦЕЛЬ И ЗАДАЧИ ДИСЦИПЛИНЫ

Цель дисциплины: изучение студентами организации защиты персональных данных, а также технологии построения системы защиты информационных систем персональных данных.

Задачи:

- приобретение знаний в области информационной безопасности в части определения категорий персональных данных, прав субъектов и операторов персональных данных, типовых моделей угроз безопасности, принципов и условий обработки и хранения персональных данных, организационных и технических мер безопасности при хранении персональных данных на носителях, мероприятий по защите персональных данных при их обработке в информационных системах, структуры государственной системы контроля и надзора за обеспечением безопасности персональных данных, руководящих, методических и нормативных документов;
- формирование умения классифицировать информационные системы безопасности персональных данных, формировать перечень актуальных угроз безопасности персональных данных, оптимизировать систему защиты персональных данных;
- овладение навыками работы с нормативно-правовыми актами, методами и средствами выявления угроз безопасности информационным системам обработки персональных данных, методами формирования требований по защите информации.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Дисциплина Б1.В.ДВ. «Защита информационных систем обработки персональных данных» относится к выборным дисциплинам Блока 1 и является обязательной для освоения обучающимися 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-2 – способностью применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования	Второй уровень (углубленный) (ПК-2) –2	Знать: основные инструментальные средства, организационные и технические меры безопасности при обработке и хранении данных в информационных системах. З2(ПК-2) Уметь: выбирать и использовать инструментальные средства для хранения и обработки данных в информационных системах. У2 (ПК-2) Владеть: методами и средствами выявления угроз безопасности информационным системам обработки персональных данных. В2 (ПК-2)

для решения профессиональных задач		
ПК-4 – способностью участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты	Второй уровень (углубленный) (ПК-4) –2	Декомпозиция II Знать: средства поддержания конфиденциальности, целостности и доступности информации, технологии организации защиты данных в информационных системах. З2 (II)(ПК-4) Уметь: организовать защиту данных в информационных системах; проводить анализ и оценивание механизмов защиты; осваивать и внедрять новые методы и средства защиты данных У2(II) (ПК-4) Владеть: основными принципами и приемами совместного применения средств защиты в информационных системах обработки персональных данных. В2 (II)(ПК-4)

4. ОБЪЕМ И СТРУКТУРА ДИСЦИПЛИНЫ

Трудоемкость дисциплины составляет 3 зачетные единицы, 108 часов.
Форма промежуточной аттестации: зачет- 8 семестр.
Распределение фонда времени по темам дисциплины 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. Объекты и субъекты защиты персональных данных				
Введение	1			
1.1. Нормативно-правовое обеспечение защиты персональных данных	2			4
1.2. Система государственного контроля и надзора за обеспечением безопасности персональных данных	1			4
1.3. Обязанности и ответственность операторов персональных данных	1			4
1.4. Описание информационных систем персональных данных	2			4
1.5. Классификация информационных систем персональных данных	1			4
Раздел 2. Организация защиты информационных систем персональных данных и реализация системы защиты персональных данных				
2.1. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах	1			6
2.2. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах	1		6	6
2.3. Мероприятия по защите персональных данных при их обработке в информационных системах	1			6
2.4. Порядок применения криптографических средств для	1		8	6

защиты персональных данных				
2.5. Оптимизация системы защиты персональных данных	2		8	5
2.6. Организационные и технические меры безопасности при хранение персональных данных на носителях	2		8	5
2.7. Документальное обеспечение деятельности оператора персональных данных	2			6
Всего по дисциплине:	**18**		**30**	**60**

*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

ВВЕДЕНИЕ

Предмет, цели, задачи и содержание курса защиты информационных систем обработки персональных данных. Роль и место курса в подготовке специалистов по организации и технологии защиты информации в государственных и коммерческих структурах. Базовые знания, необходимые для изучения курса. Рекомендуемые учебные пособия.

РАЗДЕЛ 1. ОБЪЕКТЫ И СУБЪЕКТЫ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

1.1. Нормативно-правовое обеспечение защиты персональных данных

Основные нормативно-правовые акты в области защиты персональных данных. Требования ФЗ «О персональных данных». Понятийный аппарат. Обеспечение конфиденциальности персональных данных. Специальные категории персональных данных. Право субъекта персональных данных на доступ к своим персональным данным. Принципы обработки и хранения персональных данных. Условия обработки персональных данных: согласие субъекта на обработку, обрабатываемые без уведомления персональных данных. Особенности обработки персональных данных в государственных или муниципальных информационных системах персональных данных.

1.2. Система государственного контроля и надзора за обеспечением безопасности персональных данных

Федеральные органы, уполномоченные в области обеспечения безопасности персональных данных –регуляторы. Сфера деятельности регуляторов. О Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций. О Федеральной службе технического и экспортного контроля. О Федеральной службе безопасности. Методические документы регуляторов. Типы, основание, порядок, сроки и содержание поверок.

1.3. Обязанности и ответственность операторов персональных данных

Обязанности операторов персональных данных: уведомление об обработке персональных данных, по устранению нарушений, при достижении целей обработки, при отзыве согласия субъекта. Ответственность оператора в области защиты персональных данных: гражданская, уголовная, административная, дисциплинарная.

1.4. Описание информационных систем персональных данных

Понятие информационной системы персональных данных. Условий создания и использования персональных данных: состав персональных данных и цель их обработки; технология обработки; субъекты, создающие и потребляющие персональных данных; правила доступа; используемые объекты. Формы представления персональных данных: акустическая (речевая) информация; видовая информация; информация в виде сигналов; информация в виде логических структур. Техническая структура информационной системы персональных данных: технические средства, используемые каналы связи, программные средства. Информационные потоки, циркулирующие в информационной системе персональных данных. Граничное телекоммуникационное оборудование и

виртуальные локальные сети. Характеристик безопасности персональных данных: конфиденциальность, целостность и доступность.

1.5. Классификация информационных систем персональных данных

Типовые и специальные информационные системы персональных данных. Организационная структура информационной системы персональных данных: автономные рабочие места, локальные информационные системы, распределенные информационные системы. Однопользовательские и многопользовательские информационные системы персональных данных. Информационные системы персональных данных с разграничением и без разграничения прав доступа. Классификационные признаки типовых информационных систем персональных данных: категория обрабатываемых данных, объем обрабатываемых данных, характеристики безопасности персональных данных с учетом подключений к Интернету, режима обработки персональных данных, режима разграничения прав доступа пользователей, местонахождения технических средств. Таблица классификации типовой информационной системы персональных данных.

РАЗДЕЛ 2. ОРГАНИЗАЦИЯ ЗАЩИТЫ ИНФОРМАЦИОННЫХ СИСТЕМ ПЕРСОНАЛЬНЫХ ДАННЫХ И РЕАЛИЗАЦИЯ СИСТЕМЫ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

2.1. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах

Классификация угроз безопасности персональных данных. Анализ и характеристики угроз возможной утечки информации по техническим каналам. Анализ и характеристики угроз несанкционированного доступа к информации в информационной системе персональных данных, включая характеристики источников угроз несанкционированного доступа, характеристики уязвимостей системного и прикладного программного обеспечения, характеристики угроз безопасности персональных данных, реализуемых с использованием протоколов межсетевого взаимодействия и программно-математических воздействий, характеристики нетрадиционных информационных каналов и результатов несанкционированного или случайного доступа. Типовые модели угроз безопасности персональных данных, обрабатываемых в информационных системах (автоматизированных рабочих местах, локальных и распределенных информационных системах), не имеющих и имеющих подключение к сетям связи общего пользования и (или) сетям международного информационного обмена.

2.2. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах

Формирование перечня источников угроз персональным данным: формирование перечня уязвимых звеньев информационной системы методом экспертного опроса, формирование перечня уязвимых звеньев информационной системы путем анализа результатов сетевого сканирования, формирование перечня возможных технических каналов утечки информации. Определение условий существования в информационной системе угроз безопасности информации. Составление полного перечня угроз. Формирование перечня актуальных угроз безопасности персональным данным.

2.3. Мероприятия по защите персональных данных при их обработке в информационных системах

Правовые меры защиты: распределение полномочий между субъектами; нормативно-правовой контроль использования персональных данных; назначение ответственного за защиту информации, содержащей персональных данных; правовая регламентация порядка сбора, использования, предоставления и уничтожения персональных данных. Организационно-административные меры защиты: формирование системы управления персональных данных; регламентация деятельности персонала по использованию персональных данных; регламентация порядка взаимодействия пользователей и администраторов информационных систем персональных данных;

контроль над деятельностью персонала. Технические меры защиты от НСД в информационных системах персональных данных различного класса: защита от вредоносных программ и средства защиты от вторжений; идентификация и аутентификация пользователей; разграничение и контроль доступа к персональных данных; обеспечение целостности персональных данных; регистрация событий безопасности; защита каналов передачи персональных данных

2.4. Порядок применения криптографических средств для защиты персональных данных

Установка и ввод в эксплуатацию криптосредств. Проверка готовности криптосредств к использованию. Обучение лиц работе с криптосредствами. Поэкземплярный учет используемых криптосредств. Учет лиц, допущенных к работе с криптосредствами. Контроль над соблюдением условий использования криптосредств. Предотвращение последствий нарушений условий хранения и использования криптосредств.

2.5. Оптимизация системы защиты персональных данных

Использование возможностей средств защиты информации, ОС и прикладного ПО. Дополнительные меры по снижению требований. Сокращение количества точек обработки персональных данных. Оптимизация режима обработки персональных данных. Обезличивание части персональных данных. Сегментирование информационной системы персональных данных. Организация терминального доступа к информационной системе персональных данных. Организация хранения персональных данных на бумажных или иных носителях.

2.6. Организационные и технические меры безопасности при хранение персональных данных на носителях

Присвоение материальному носителю уникального идентификационного номера. Учет количества экземпляров материальных носителей. Идентификации информационной системы персональных данных и оператора персональных данных. Регистрация фактов несанкционированной повторной и дополнительной записи информации. Применение средств электронной цифровой подписи для сохранения целостности и неизменности персональных данных. Процедура уничтожения персональных данных.

2.7. Документальное обеспечение деятельности оператора персональных данных

Состав документов, который необходимо иметь организации, обрабатывающей персональные данные: материалы проектирования СЗИ от НСД к информационной системе персональных данных, эксплуатационные документы, организационно-распорядительные документы.

6. ЗАНЯТИЯ СЕМИНАРСКОГО ТИПА

Таблица 6.1 – Практические занятия/Семинарские занятия/Лабораторные работы

№ темы	Тема занятия	Вид занятия/Оценочное средство
1	*2*	3
2.2	Оценка защищенности информационных систем персональных данных Оценка вероятности реализуемости угроз Оценка реализуемости угроз Оценка опасности угроз персональных данных в информационной системе Правила отнесения угрозы безопасности к актуальной	ЛР/ Решение практических задач
2.4	Установка и ввод в эксплуатацию крипто-средств. Проверка готовности криптосредств к использованию	ЛР/ Решение практических задач/ Тест 2

2.5	Сокращение количества точек обработки персональных данных. Обезличивание части персональных данных. Сегментирование информационной системы персональных данных. Организация терминального доступа к информационной системе персональных данных.	ЛР/ Решение практических задач
2.6	Организация хранения персональных данных на бумажных или иных носителях. Применение средств электронной цифровой подписи для сохранения целостности и неизменности персональных данных. Процедура уничтожения персональных данных и их носителей.	ЛР/ Решение практических 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.

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*
1.1-1.5	Подготовка к выполнению Контрольной точки №1. Подготовка к экзамену
2.1-2.4	Подготовка к выполнению Контрольной точки №2. Подготовка к экзамену
2.5, 2.6	Подготовка к экзамену.

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

8. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

В преподавании дисциплины «Защита информационных систем обработки персональных данных» используются разнообразные образовательные технологии как традиционные, так и с применением активных и интерактивных методов обучения.

К интерактивным методам обучения относится выполнение индивидуальных заданий на ПК в ходе практических занятий и самостоятельной работы по темам 2.2, 2.4-2.6.

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**
Полегенько А.М. Защита информационных систем обработки персональных данных : учебное пособие .— Санкт-Петербург : Изд-во СПбГЭУ, 2018 .— 72 с. — Сведения доступны также по Интернету: opac.unecon.ru .	основная	35	ЭБ OPAC.UNECON.RU
Шаньгин В.Ф. Комплексная защита информации в корпоративных системах : учебное пособие . — Электрон. дан. — М. : ИД «ФОРУМ» : ИНФРА-М, 2020. — 592 с.	основная	–	https://znanium.com/catalog/document?id=358722
Васильева И.Н: Информационные технологии и защита информации: учебное пособие / И.Н. Васильева, Е.В. Стельмашонок .— Санкт-Петербург: СПбГИЭУ, 2011.— 271 с. . – Сведения доступны также по Интернету: opac.unecon.ru.	дополнительная	71	ЭБ OPAC.UNECON.RU
Петренко В.И. Защита персональных данных в информационных системах .— Ставрополь : Северо-Кавказский федеральный университет, 2016 .— 201 .— Режим доступа: book.ru .	дополнительная	–	ЭБС BOOK.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)
4	Falcongaze SecureTower (Лицензионный договор № 12/07/2018-1 от 25.01.2019)
5	MaxPatrol Education (Лицензионный договор № 165-19/Е от 06.12.2019)
6	XSpider Education (Лицензионный договор № 165-19/Е от 06.12.2019)
7	ViPNet (Лицензионный договор № 2-1759797 от 20.03.2020)
8	СЗИ Secret Net Studio (Лицензионный договор № КБ/02117/1/38 от 05.09.2018 г.)

Лабораторные работы по дисциплине проводятся в лаборатории «Инженерно-технической защиты, лаборатория Программно-аппаратной защиты».

Таблица 9.2.2 – Лаборатория «Инженерно-технической защиты, лаборатория Программно-аппаратной защиты»

Вид учебных занятий	**Адрес, № аудитории**	**Лабораторное оборудование**
1	*2*	*3*
Лабораторные работы	191023, г. Санкт-Петербург, ул. Канал	Лаборатория Инженерно-технической защиты, лаборатория Программно-аппаратной защиты.

	Грибоедова, 30/32, литер «А», «Б», «Р», Ауд. 2057	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 TK-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)-ВСЕ – 1 шт. Наборы демонстрационного оборудования и учебно-наглядных пособий: мультимедийные приложения к лекционным курсам и практическим занятиям, интерактивные учебно-наглядные пособия.

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).