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.

КОМПЛЕКСНАЯ СИСТЕМА ЗАЩИТЫ ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ

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:
_____/ к.т.н., доцент Солодянников А.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 9
9.1 Учебно-методическое и информационное обеспечение дисциплины 9
9.2. Материально-техническое обеспечение учебного процесса **Ошибка! Закладка не определена.**
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 (цели) освоения дисциплины: дать студентам необходимые знания в области создания системы защиты информации на предприятии, умения и навыки комплексного использования методов и средств защиты информации на объектах информатизации, создаваемых и эксплуатируемых в различных сферах народного хозяйства.

Задачи:

- приобретение теоретических знаний в области создания системы защиты информации на предприятии;
- - формирование умения комплексировать современные методы и средства защиты информации;
- - выработка практических навыков контроля эффективности комплексного применения средств защиты информации.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Дисциплина Б1.В «Комплексная система защиты объектов информатизации» относится к вариативной части 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-4 способностью участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты	Первый уровень (пороговый) (ПК-4) –1	Декомпозиция II Знать сущность, задачи, принципы, этапы и методы создания комплексной системы защиты информации объекта информатизации. З1 (II)(ПК-4) Уметь: анализировать и оценивать угрозы информационной безопасности объекта информатизации У1(II) (ПК-4) Владеть: навыками определения и нормативного закрепления состава защищаемой информации В1 (II)(ПК-4)
ПК-5 – способностью принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации	Второй уровень (углубленный) (ПК-5) –2	Знать методологию планировании, развертывании и поддержании комплекса регламентов и процедур, направленных на минимизацию рисков нарушения информационной безопасности З2(ПК-5) Уметь: комплексировать современные методы и средства защиты информации в интересах обеспечения информационной безопасности предприятия У2 (ПК-5)

		Владеть: навыками контроля эффективности комплексного применения средств и мер защиты информации В2(ПК-5)

4. ОБЪЕМ И СТРУКТУРА ДИСЦИПЛИНЫ

Трудоемкость дисциплины составляет 5 зачетных единиц, 180 часов, из которых 36 часов самостоятельной работы обучающегося отводится на подготовку и защиту экзамена.

Форма промежуточной аттестации: экзамен - 7 семестр, курсовая работа – 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*
1.1.Сущность и задачи комплексной защиты информации на предприятии	1			6
1.2. Принципы организации и этапы разработки комплексной системы защиты информации	2			6
1.3. Факторы, влияющие на организацию комплексной системы защиты информации	1			6
1.4. Определение и нормативное закрепление состава защищаемой информации	2	8		6
1.5. Определение объектов защиты	1	8		7
2.1. Определение компонентов комплексной системы защиты информации (6)	2	4		7
2.2. Предпроектное обследование объекта информатизации (на примере ИСПДн) (7)	1	4		7
2.3. Разработка модели комплексной системы защиты информации (8)	2	8		7
2.4. Кадровое обеспечение функционирования комплексной системы защиты информации (9)	1			7
2.5. Материально-техническое и нормативно-методическое обеспечение комплексной системы защиты информации (10)	2			7
2.6. Назначение, структура и содержание управления комплексной системы защиты информации (11)	1			7
2.7. Принципы и методы планирования функционирования комплексной системы защиты информации (12)	2			7
2.8. Сущность и содержание контроля функционирования комплексной системы защиты информации (13)	1			7
2.9. Управление комплексной системой защиты информации в условиях чрезвычайных ситуаций (14)	2	8		7
2.10. Общая характеристика подходов к оценке эффективности комплексной системы защиты информации (15)	1			7
2.11. Состав методов и моделей оценки эффективности комплексной системы защиты информации (16)	2	8		7
Всего по дисциплине:	**24**	**48**		**108**

*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. Принципы, задачи и сущность комплексной системы защиты объектов информатизации

1.1. Сущность и задачи комплексной защиты информации на предприятии

Понятийный аппарат в области обеспечения информационной безопасности на предприятии. Цели, задачи и принципы построения комплексной системы защиты информации. О понятиях безопасности и защищенности. Разумная достаточность и экономическая эффективность. Управление безопасностью предприятия. Международные стандарты. Цели и задачи защиты информации в автоматизированных системах. Современное понимание методологии защиты информации: особенности национального технического регулирования, современная трактовка понятия безопасности информационных технологий, современные требования к средствам обеспечения безопасности.

1.2. Принципы организации и этапы разработки комплексной системы защиты информации

Принципы организации и этапы разработки комплексной системы защиты информации (КСЗИ); факторы, влияющие на организацию КСЗИ. Методологические основы организации комплексной системы защиты информации. Разработка политики безопасности и регламента безопасности предприятия. Основные положения теории сложных систем. Система управления информационной безопасностью предприятия. Принципы построения и взаимодействие с другими подразделениями. Требования, предъявляемые к комплексной системе защиты информации: требования к организационной и технической составляющим комплексной системы защиты информации; требования по безопасности, предъявляемые к изделиям информационной технологии. Этапы разработки комплексной системы защиты информации.

1.3. Факторы, влияющие на организацию комплексной системы защиты информации

Влияние формы собственности на особенности защиты информации ограниченного доступа. Влияние организационно-правовой формы предприятия на особенности защиты информации ограниченного доступа. Характер основной деятельности предприятия. Состав, объекты и степень конфиденциальности защищаемой информации. Структура и территориальное расположение предприятия. Режим функционирования предприятия. Конструктивные особенности предприятия. Количественные и качественные показатели ресурсообеспечения. Степень автоматизации основных процедур обработки защищаемой информации.

1.4. Определение и нормативное закрепление состава защищаемой информации

Классификация информации по видам тайны и степеням конфиденциальности. Нормативно-правовые аспекты определения состава защищаемой информации. Определение состава защищаемой информации, отнесенной к коммерческой тайне предприятия. Методика определения состава защищаемой информации. Порядок внедрения Перечня сведений, составляющих коммерческую тайну, внесение в него изменений и дополнений.

1.5. Определение объектов защиты

Значение носителей защищаемой информации как объектов защиты. Методика выявления состава носителей защищаемой информации. Особенности взаимоотношений с контрагентами как объект защиты информации ограниченного доступа. Факторы, определяющие необходимость защиты периметра и здания предприятия. Особенности помещений как объектов защиты для работы по защите информации. Транспортные средства и особенности транспортировки. Состав средств обеспечения, подлежащих защите.

Раздел 2. Компоненты комплексной системы защиты объектов информатизации

2.1. Определение компонентов комплексной системы защиты информации

Особенности системы защиты информации (СЗИ) от несанкционированного доступа (НСД). Методика синтеза СЗИ: общее описание архитектуры АС, системы защиты информации и политики безопасности; формализация описания архитектуры исследуемой автоматизируемой системы (АС); формулирование требований к системе защиты информации; выбор механизмов и средств защиты информации; определение важности параметров средств защиты информации; оптимальное построение системы защиты для АС. Выбор структуры СЗИ АС. Проектирование системы защиты информации для существующей АС.

2.2. Предпроектное обследование объекта информатизации (на примере ИСПДн)

Содержание концепции построения комплексной системы защиты информации. Объекты защиты. Цели и задачи обеспечения безопасности информации. Основные угрозы безопасности информации АС организации. Анализ и оценка угроз безопасности информации: выявление и оценка источников, способов и результатов дестабилизирующего воздействия на информацию. Определение потенциальных каналов и методов несанкционированного доступа к информации. Определение возможностей несанкционированного доступа к защищаемой информации. Основные положения технической политики в области обеспечения безопасности информации АС организации. Основные принципы построения комплексной системы защиты информации. Меры, методы и средства обеспечения требуемого уровня защищенности информационных ресурсов. Первоочередные мероприятия по обеспечению безопасности информации АС организации.

2.3. Разработка модели комплексной системы защиты информации

Общая характеристика задач моделирования комплексной системы защиты информации. Формальные модели безопасности и их анализ: классификация формальных моделей безопасности; модели обеспечения конфиденциальности; модели обеспечения целостности; субъектно-ориентированная модель. Прикладные модели защиты информации в АС. Формальное построение модели защиты: описание объекта защиты; декомпозиция АС на субъекты и объекты; модель безопасности: неформальное описание; декомпозиция системы защиты информации; противостояние угрозам; реализация системы защиты информации субъекта АС субъектно-объектной модели. Формализация модели безопасности: процедура создания пары субъект–объект, наделение их атрибутами безопасности; осуществление доступа субъекта к объекту; взаимодействие с внешними сетями; удаление субъекта–объекта.

2.4. Кадровое обеспечение функционирования комплексной системы защиты информации

Специфика персонала предприятия как объекта защиты. Распределение функций по защите информации: функции руководства предприятия; функции службы защиты информации; функции специальных комиссий; обязанности пользователей защищаемой информации. Обеспечение взаимодействия между субъектами, защищающими и использующими информацию ограниченного доступа. Подбор и обучение персонала.

2.5. Материально-техническое и нормативно-методическое обеспечение комплексной системы защиты информации

Состав и значение материально-технического обеспечения функционирования комплексной системы защиты информации. Перечень вопросов защиты информации (ЗИ), требующих документационного закрепления.

2.6. Назначение, структура и содержание управления комплексной системы защиты информации

Понятие, сущность и цели управления комплексной системой защиты информации. Принципы управления комплексной системы защиты информации. Структура процессов управления. Основные процессы, функции и задачи управления комплексной системой защиты информации. Основные стили управления. Структура и содержание общей технологии управления комплексной системой защиты информации.

2.7. Принципы и методы планирования функционирования комплексной системы защиты информации

Понятие и задачи планирования функционирования комплексной системы защиты информации. Способы и стадии планирования. Факторы, влияющие на выбор способов планирования. Основы подготовки и принятия решений при планировании. Методы сбора, обработки и изучения информации, необходимой для планирования. Организация выполнения планов.

2.8. Сущность и содержание контроля функционирования комплексной системы защиты информации

Виды контроля функционирования комплексной системы защиты информации. Цель проведения контрольных мероприятий в комплексной системе защиты информации. Анализ и использование результатов проведения контрольных мероприятий.

2.9. Управление комплексной системой защиты информации в условиях чрезвычайных ситуаций

Понятие и основные виды чрезвычайных ситуаций (ЧС). Технология принятия решений в условиях ЧС. Факторы, влияющие на принятие решений в условиях ЧС. Подготовка мероприятий на случай возникновения ЧС.

2.10. Общая характеристика подходов к оценке эффективности комплексной системы защиты информации

Вероятностный подход. Оценочный подход. Требования РД СВТ и РД АС. Задание требований безопасности информации и оценка соответствия им согласно ГОСТ 15408–2002. Экспериментальный подход.

2.11. Состав методов и моделей оценки эффективности комплексной системы защиты информации

Показатель уровня защищенности, основанный на экспертных оценках. Методы проведения экспертного опроса. Экономический подход к оценке эффективности комплексной системы защиты информации.

6. ЗАНЯТИЯ СЕМИНАРСКОГО ТИПА

Таблица 6.1 – Практические занятия/Семинарские занятия/Лабораторные работы

№ темы	Тема занятия	Вид занятия/Оценочное средство
1	2	3
1.4	Определение и нормативное закрепление состава защищаемой информации	ПЗ/Решение практических задач
1.5	Определение объектов защиты	ПЗ/Решение практических задач
2.1	Определение компонентов комплексной системы защиты информации	ПЗ/Решение практических задач
2.2	Определение порядка предпроектного обследования объекта информатизации	ПЗ/Решение практических задач
2.3	Разработка модели комплексной системы защиты информации	ПЗ/Решение практических задач
2.9	Управление комплексной системой защиты информации в условиях чрезвычайных ситуаций	ПЗ/Решение практических задач

2.11	Методы и модели оценки эффективности комплексной системы защиты информации	ПЗ/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.

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 экзамену.
2.1	Подготовка к экзамену. Подготовка к курсовой работе.
2.2	Подготовка к выполнению и защите индивидуального задания 1. Подготовка к экзамену.
2.3	Подготовка к выполнению и защите индивидуального задания 2. Подготовка к экзамену.
2.4	Подготовка к экзамену.
2.5	Подготовка к экзамену.
2.6	Подготовка к экзамену.
2.7	Подготовка к экзамену.
2.8	Подготовка к экзамену.
2.9	Подготовка к экзамену.
2.10	Подготовка к экзамену.
2.11	Подготовка к экзамену

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

8. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

В преподавании дисциплины «*Комплексная система защиты объектов информатизации*» используются разнообразные образовательные технологии как традиционные, так и с применением активных и интерактивных методов обучения.

Активные и интерактивные методы обучения:

К интерактивным методам обучения относится выполнение индивидуальных заданий на ПК в ходе практических занятий и самостоятельной работы по темам 1.4, 1.5, 2.1, 2.2, 2.3, 2.9, 2.11.

Выполнение индивидуальных заданий на ПК предполагает выполнение индивидуальных заданий по изучению профессиональной литературы и предметно-ориентированных сайтов.

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. 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
Шаньгин В.Ф. Комплексная защита информации в корпоративных системах : учебное пособие . —	Основная	–	https://znanium.com/catalog/d

Электрон. дан. — М. : ИД «ФОРУМ» : ИНФРА-М, 2020. — 592 с.			ocument?id=358722
Солодянников А.В. Информационно-аналитическая деятельность по обеспечению комплексной безопасности : учебное пособие — Санкт-Петербург : Изд-во СПбГЭУ, 2018 .— 94 с. – Сведения доступны также по Интернету: opac.unecon.ru .	Дополнительная	35	ЭБ OPAC.UNECON.RU
Комплексная система защиты объектов информатизации : методические рекомендации по выполнению курсовой работы : направление подготовки 10.03.01 Информационная безопасность : направленность Безопасность компьютерных систем (в экономике и управлении) / Минобрнауки России, Санкт-Петербургский государственный экономический университет, Кафедра вычислительных систем и программирования ; [сост. А.В. Солодянников]Санкт-Петербург : [б. и.], 2020 1 файл (284 КБ)	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, курсового проектирования (выполнения курсовой работы), 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)

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).