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

УТВЕРЖДАЮ
Проректор по учебной и методической работе
_____ / Шубаева В.Г./
«05» 07 20 19 г.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ВНЕШНЕТОРГОВОЙ ДЕЯТЕЛЬНОСТИ

Рабочая программа дисциплины

Специальность	38.05.02 Таможенное дело
Направленность (профиль) программы	Таможенное администрирование
Уровень высшего образования	специалитет
Форма обучения	очная

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

Санкт-Петербург
2019

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 3
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 9
10. ОСОБЕННОСТИ ОСВОЕНИЯ ДИСЦИПЛИНЫ ДЛЯ ИНВАЛИДОВ И ЛИЦ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ 9
11. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕЙ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ 11

1. ЦЕЛЬ И ЗАДАЧИ ДИСЦИПЛИНЫ

Цель (цели) освоения дисциплины: способствовать освоению студентами необходимых знаний, умений и навыков в области информационной безопасности.

Задачи:

определение места и роли информационной безопасности в системе национальной безопасности Российской Федерации;

приобретение теоретических знаний в области основных направлений информационной безопасности;

формирование умения использования современных программных средств защиты информации;

выработка практических навыков работы пользователя для защиты данных в операционной среде;

закрепление теоретических знаний по обработке и защите информации в среде пакетов прикладных программ универсального назначения.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Дисциплина Б1.Б. «Информационная безопасность внешнеторговой деятельности» относится к базовой части Блока 1 и является обязательной для освоения обучающимся вне зависимости от направленности (профиля) программы.

3. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ

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

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

Код и наименование компетенции выпускника	Этапы формирования компетенций	Планируемые результаты обучения/индикаторы достижения компетенций (показатели освоения компетенции)
ОПК-1: способностью решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	Второй уровень (углубленный) (ОПК-1)-2	Декомпозиция I Знать: основополагающие термины, категории, понятия в области информационной безопасности; основы информационной и библиографической культуры с применением информационно – коммуникационных технологий и с учетом требований информационной безопасности З2 (I) (ОПК-1) Уметь: обосновывать выбор наиболее целесообразных информационных технологий с учетом требований информационной безопасности, применяемых в профессиональной деятельности; У2(I) (ОПК-1) Владеть: навыками решения задач с использованием информационно-коммуникационных технологий с учетом требований информационной безопасности. В2(I) (ОПК-1)

4. ОБЪЕМ И СТРУКТУРА ДИСЦИПЛИНЫ

Трудоемкость дисциплины составляет 3 зачетных единиц, 108 часов.

Форма промежуточной аттестации: зачет – 4 семестр.

Распределение фонда времени по темам 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. Составляющие национальных интересов Российской Федерации в информационной сфере. Понятие, сущность и актуальность защиты информации	1			10
Тема 2. Основные определения и задачи информационной безопасности	1	2		4
Тема 3. Риски и угрозы информационной безопасности. Методы обнаружения и блокирования угроз информационной безопасности	0,5			6
Тема 4. Правовое обеспечение информационной безопасности	0,5			6
Тема 5. Классификация методов и средств защиты информации	0,5	2		4
Тема 6. Антивирусная защита	0,5	2		6
Тема 7. Системы идентификации и аутентификации		2		6
Тема 8. Системы разграничения доступа		4		6
Тема 9. Стеганографические методы		4		6
Тема 10. Криптографические методы		4		6
Тема 11. Технология электронной подписи		4		6
Тема 12. Методы защиты в операционных системах		8		6
Всего по дисциплине:	4	32		72

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

5. СОДЕРЖАНИЕ РАЗДЕЛОВ И ТЕМ ДИСЦИПЛИНЫ

Тема 1. Составляющие национальных интересов Российской Федерации в информационной сфере. Понятие, сущность и актуальность защиты информации

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

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

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

Состояние информационной безопасности Российской Федерации и основные задачи по ее обеспечению. Особенности обеспечения информационной безопасности в различных сферах общественной жизни. Основные положения государственной политики

обеспечения информационной безопасности, мероприятия по их реализации. Понятия информационной войны и информационного оружия. Проблема общемирового противодействия угрозам информационной безопасности.

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

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

Тема 2. Основные определения и задачи информационной безопасности

Понятие безопасности автоматизированной информационной системы. Понятие защиты информации. Конфиденциальность, целостность, доступность. Субъекты, заинтересованные в обеспечении информационной безопасности. Уровни обеспечения информационной безопасности. Системы обеспечения информационной безопасности.

Тема 3. Риски и угрозы информационной безопасности. Методы обнаружения и блокирования угроз информационной безопасности

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

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

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

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

Безопасность работы в сети Интернет. Безопасная доставка e-mail сообщений.

Тема 4. Правовое обеспечение информационной безопасности

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

Тема 5. Классификация методов и средств защиты информации

Обобщенные категории методов защиты информации. Организационные меры защиты информации. Технологические методы и средства защиты информации. Криптографические и правовые методы защиты информации. Особенности защиты на разных уровнях информационной системы. Противодействие инсайдерской деятельности.

Тема 6. Антивирусная защита

Вредоносное программное обеспечение. Классификация вредоносных программ. Понятие компьютерного вируса. Троянские программы. Основные типы компьютерных вирусов. Основные классы вредоносных программ по характеру воздействия на

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

Тема 7. Системы идентификации и аутентификации

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

Тема 8. Системы разграничения доступа

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

Тема 9. Стеганографические методы

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

Тема 10. . Криптографические методы

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

Тема 11. Технология электронной цифровой подписи

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

Тема 12. Методы защиты в операционных системах

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

Защита офисных документов. Технологии защиты баз данных.

6. ЗАНЯТИЯ СЕМИНАРСКОГО ТИПА

Таблица 6.1 – Практические занятия / Семинарские занятия / Лабораторные работы

№ темы	Тема занятия	Вид занятия / Оценочное средство
1	2	3
2	Определение проблем и приоритетов в области информационной безопасности внешнеторговой деятельности.	СЗ: Дискусия
5	Классификация методов и средств защиты информации Защита групповых научных эссе по структурным составляющим обеспечения информационной безопасности	ПЗ: Деловая игра КТ№1 Эссе
6	Классификация вредоносных программ. Понятие компьютерного вируса. Методы и средства антивирусной защиты	ПЗ: Устный фронтальный опрос

7	Системы идентификации и аутентификации: основные определения, типы, область применения, классификация	ПЗ: Решение прикладных задач
8	Дискреционное и мандатное управление доступом Ролевое управление доступом	ПЗ: Решение прикладных задач
9	Сокрытие сообщения методом знаков одинакового начертания Стеганография в ASCII-логотипах.	ПЗ: Решение прикладных задач
10	Изучение шифра «Поворотные решетки Кардано» Анализ шифра табличной перестановки Криптоанализ шифра простой замены Криптоанализ многоалфавитных шифров (шифр Виженера) Изучение шифра RSA	СЗ: Коллоквиум
11	Использование цифровой подписи проектов VBA Изучение электронной цифровой подписи Эль-Гамаля	ПЗ: Устный фронтальный опрос
12	Защита документов MS WORD Защита книг MS EXCEL Защита баз данных MS ACCESS	ПЗ: Решение прикладных задач КТ№ 2 Индивидуальное задание

* 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	Работа в команде над темой. Подготовка к защите дерева понятия «Информационная безопасность внешнеторговой деятельности»
2,3	Творческая работа: подготовка научного эссе.
4	Подготовка научного доклада и презентации.
5	Творческая работа: подготовка научного эссе.
6-12	Изучение материала по теме. Подготовка к ПЗ.

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

8. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

В преподавании дисциплины «Информационная безопасность внешнеторговой деятельности» используются разнообразные образовательные технологии как традиционные, так и с применением активных и интерактивных методов обучения.

Активные и интерактивные методы обучения:

проблемная лекция с элементами дискуссии (тема № 1, 2);

тематическая дискуссия (тема № 1,2, 4);

проблемный семинар (тема № 2, 5-9,12);

деловая (ролевая) игра (тема №5).

Проблемный семинар: предполагает активное вовлечение студентов в процесс обсуждения и решения поставленной проблемы, процесс поиска решения направляется и контролируется преподавателем.

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- 5.

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

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
Баранова Е.К. Информационная безопасность и защита информации : учебное пособие / Баранова Е.К., Бабаш А.В. — 4-е изд., перераб. и доп. — Электрон. дан. — М. : РИОР : ИНФРА-М, 2019. — 322 с.	Основная		ЭБС ZNANIUM
Сухостат В.В. Основы информационной безопасности: учебное пособие / В.В.Сухостат, И.Н.Васильева .— Санкт-Петербург : Изд-во СПбГЭУ, 2019 .— 103 с. — Сведения доступны также по Интернету: opac.unecon.ru .	Основная	35	ЭБ OPAC.UNECON.RU
Нестеров Ф.А. Информационная безопасность : учебник и практикум . — Электрон. дан. — Москва : Издательство Юрайт, 2019. — 321 с.	Основная		ЭБС Юрайт
Васильева И.Н: Информационные технологии и защита информации: учебное пособие / И.Н. Васильева, Е.В. Стельмашонок.— Санкт-Петербург: СПбГИЭУ, 2011.— 271 с. – Сведения доступны также по Интернету: opac.unecon.ru.	Дополнительная	71	ЭБ OPAC.UNECON.RU
Ищейнов В.Я. Информационная безопасность и защита информации: словарь терминов и понятий : словарь . — Электрон. дан. — Москва : Русайнс, 2019. — 226 с.	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, 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).