ЧАСТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «ВОСТОЧНАЯ ЭКОНОМИКО-ЮРИДИЧЕСКАЯ ГУМАНИТАРНАЯ АКАДЕМИЯ» (Академия ВЭГУ)

ОДОБРЕНА	УТВЕРЖДЕНА
Ученым советом Академии ВЭГУ (протокол от 28 июня 2021 г. , № 4)	приказом ректора Академии ВЭГУ от 31.08. 2021 № 71/а

Рабочая программа дисциплины Информационная безопасность

Кафедра: управления, информатики и общенаучных дисциплин

Основная образовательная программа: 09.03.03 Прикладная информатика, направленности (профиля) «Проектирование и разработка информационных систем» с применением электронного обучения и дистанционных образовательных технологий.

1. Общая характеристика

1.1 Наименование

Данная учебная дисциплина называется «Информационная безопасность», включена в Реестр автономных дидактических компонентов Академии ВЭГУ и реализуется в рамках ООП Академии ВЭГУ: 09.03.03 Прикладная информатика (профиль «Проектирование и разработка информационных систем») по заочной форме обучения, в т.ч. с использованием электронного обучения и дистанционных образовательных технологий.

1.2 Цели реализации

1.2.1 В результате освоения данной дисциплины обучающийся должны овладеть знаниями, умениями и навыками в рамках формирования следующих компетенций:

- способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач (УК-1);
- способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности (ОПК-3);
- способен участвовать в разработке стандартов, норм и правил, а также технической документации, связанной с профессиональной деятельностью (ОПК-4);
- способен принимать участие в организации ИТ-инфраструктуры и управлении информационной безопасностью (ПК-6).

1.2.2 Обучающийся, освоивший данную дисциплину, должен знать:

- принципы сбора, отбора и обобщения информации, методики системного

подхода для решения профессиональных задач;

- принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности;

- основные стандарты оформления технической документации на различных стадиях жизненного цикла информационной системы;

- виды угроз ИС и методы обеспечения информационной безопасности, современные отечественные и международные стандарты в сфере информационных технологий

1.2.3 Обучающийся, освоивший данную дисциплину, должен уметь:

- анализировать и систематизировать разнородные данные, оценивать эффективность процедур анализа проблем и принятия решений в профессиональной деятельности;

- решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности;

- применять стандарты оформления технической документации на различных стадиях жизненного цикла информационной системы;

- выявлять угрозы информационной безопасности, обосновывать организационно-технические мероприятия по защите информации в прикладных ИС

1.2.4 Обучающийся, освоивший данную дисциплину, должен владеть навыками:

- научного поиска и практической работы с информационными источниками; методами принятия решений;

- подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций, и библиографии по научно-исследовательской работе с учетом требований информационной безопасности;

- составления технической документации на различных этапах жизненного цикла информационной системы;

- методикой обеспечения защиты информации в ИС; навыками участия в организации ИТ- инфраструктуры предприятия и управлении информационной безопасностью

1.3 Место в структуре ООП

1.3.1 Данная дисциплина относится к блоку Б1.О.22 обязательных дисциплин обязательной части и изучается по заочной форме с применением ЭО и ДОТ в 5 семестре (на 3 курсе) обучения.

1.3.2 Логически и содержательно-методически данная дисциплина связана с такими автономными дидактическими компонентами данной ООП как: информатика, программирование, вычислительные системы, сети и коммуникации, операционные системы, базы данных, информационные системы и технологии,

информационный менеджмент, методы тестирования программного обеспечения, программирование в 1С, корпоративные информационные системы, автоматизированная система управления предприятия, электронная коммерция, WEB-программирование, интернет-технологии, информационные технологии анализа финансового состояния предприятия, информационные технологии в управлении, разработка интерфейсов информационных систем, все виды практик.

1.3.3 Изучению данной дисциплины должно предшествовать освоение обучающимся программы: информатика, программирование, вычислительные системы, сети и коммуникации, операционные системы, базы данных, информационные системы и технологии.

1.3.4 Освоение данной дисциплины необходимо как предшествующее для прохождения обучения по программам: информационный менеджмент, методы тестирования программного обеспечения, программирование в 1С, корпоративные информационные системы, автоматизированная система управления предприятия, электронная коммерция, WEB-программирование, интернет-технологии, информационные технологии анализа финансового состояния предприятия, информационные технологии в управлении, разработка интерфейсов информационных систем, все виды практик.

1.4 Объем

1.4.1 Общий объем данной дисциплины (трудоемкость учебной нагрузки обучающегося при освоении программы, включающая в себя все виды его учебной деятельности, предусмотренные учебным планом для достижения планируемых результатов обучения) составляет: 4 зачетных единицы или 144 академических часов вне зависимости от формы обучения, применяемых образовательных технологий, реализации по индивидуальному учебному плану, в том числе при ускоренном обучении.

1.4.2 Объемы учебной нагрузки обучающегося при освоении программы дисциплины по видам учебной деятельности составляют:

Виды учебной деятельности	**Объем, в академических часах**
	по заочной форме с применением ЭО и ДОТ
Занятия лекционного типа	**4**
Занятия семинарского типа	**-**
Курсовое проектирование	**-**
Индивидуальная работа с обучающимся	**4**
Самостоятельная работа обучающегося	**120**
Аттестация	**16**
Всего	**144**

2. Структура и содержание

2.1 Содержание разделов и тем

Разделы и Темы	**Содержание (дидактические единицы)**	**Учебные занятия**

№ п/п	Наименование		заочная форма с применением ЭО и ДОТ	
			виды	Объем, академических часов
1	2	3	4	5
1	**Раздел 1. Основные понятия теории информационной безопасности, категории информационной безопасности, угрозы информационной безопасности**		Занятия лекционного типа	2
			Индивидуальная работа с обучающимися	2
			Самостоятельная работа обучающегося	74
1.1	Общая характеристика категорий информационной безопасности	1. Понятие информационной безопасности и защищенной системы. Необходимость защиты информационных систем и телекоммуникаций. Защита информации. Основные принципы обеспечения информационной безопасности в автоматизированных системах. 2. Категории информационной безопасности: конфиденциальность, целостность, аутентичность, аппелируемость. Свойства информационных систем: надежность, контролируемость 3. Понятие угрозы. Виды «нарушителей». Виды возможных нарушений информационной системы. Анализ угроз информационной безопасности. Классификация видов угроз информационной безопасности по различным признакам Угроза нарушения конфиденциальности, угроза нарушения целостности, угроза отказа служб. Примеры реализации угроз информационной безопасности. 4. Формальные модели безопасности их значение для построения защищенных информационных систем. Понятие доступа к данным и монитора безопасности. Функции монитора безопасности. Понятие политики безопасности информационных систем. Разработка и реализация политики безопасности. Управление доступом к данным. Основные типы политики безопасности управления доступом к данным: дискреционная и мандатная политика безопасности. Анализ способов нарушений безопасности. Таксономия нарушений информационной безопасности вычислительной системы и причины, обуславливающие их существование.	Занятия лекционного типа	0,5
			Индивидуальная работа с обучающимися	0,5
		– проработка конспекта лекции; – анализ учебников, учебных пособий, специальной литературы по данной теме (с указанием страниц); – подготовка к практическому занятию; – подготовка к дискуссии по определенной проблеме на базе прочитанной литературы, изучения нормативных актов, практики т.д.; – подготовка списка литературы (библиографии) и	Самостоятельная работа обучающегося	16

		подборка нормативных источников по определенной тематике, их изучение и т.д.)		
1.2	**Методы защиты средств вычислительной техники**	1. Использование защищенных компьютерных систем. 2.Аппаратные и программные средства для защиты компьютерных систем по категориям информационной безопасности. Средства операционных систем. 3. Аппаратные средства защиты: Средства резервирования данных. Понятие RAID. Проверка целостности. Способы и средства восстановления данных	Занятия лекционного типа	0,5
			Индивидуальная работа с обучающимися	0,5
		– проработка конспекта лекции; – анализ учебников, учебных пособий, специальной литературы по данной теме (с указанием страниц); – подготовка к практическому занятию; – подготовка к дискуссии по определенной проблеме на базе прочитанной литературы, изучения нормативных актов, практики т.д.; – подготовка списка литературы (библиографии) и подборка нормативных источников по определенной тематике, их изучение и т.д.)	Самостоятельная работа обучающегося	16
1.3	**Организационно-правовые методы информационной безопасности**	1. Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы. Назначение и задачи в сфере обеспечения информационной безопасности на уровне государства. Особенности сертификации и стандартизации криптографических услуг. 2. Законодательная база информационной безопасности.	Занятия лекционного типа	0,5
			Индивидуальная работа с обучающимися	0,5
		– проработка конспекта лекции; – анализ учебников, учебных пособий, специальной литературы по данной теме (с указанием страниц); – подготовка к практическому занятию; – подготовка к дискуссии по определенной проблеме на базе прочитанной литературы, изучения нормативных актов, практики т.д.; – подготовка списка литературы (библиографии) и подборка нормативных источников по определенной тематике, их изучение и т.д.)	Самостоятельная работа обучающегося	14
1.4	**Основы криптографии**	1. Методические принципы совершенствования управления предприятием на основе информационных технологий. 2. Разработка информационного обеспечения систем управления предприятий социально-культурной деятельностью. 3. Автоматизированное рабочее место	Занятия лекционного типа	0,25
			Индивидуальная работа с обучающимися	0,25
		– проработка конспекта лекции; – анализ учебников, учебных пособий, специальной литературы по данной теме (с указанием страниц); – подготовка к практическому занятию; – подготовка к дискуссии по определенной проблеме на базе прочитанной литературы, изучения нормативных актов, практики т.д.; – подготовка списка литературы (библиографии) и подборка нормативных источников по определенной тематике, их изучение и т.д.)	Самостоятельная работа обучающегося	14
1.5	**Асимметричное шифрование**	1.Электронно-цифровая подпись. Алгоритмы электронно-цифровой подписи. 2.Способы распространения ключей.	Занятия лекционного типа	0,25
			Индивидуальная работа с обучающимися	0,25
		– проработка конспекта лекции; – анализ учебников, учебных пособий, специальной литературы по данной теме (с указанием страниц); – подготовка к практическому занятию; – подготовка к дискуссии по определенной проблеме на	Самостоятельная работа обучающегося	14

		базе прочитанной литературы, изучения нормативных актов, практики т.д.; – подготовка списка литературы (библиографии) и подборка нормативных источников по определенной тематике, их изучение и т.д.)		
2	**Раздел 2. Технологии построения защищенных систем, информационная безопасность сетей**		Занятия лекционного типа	1
			Индивидуальная работа с обучающимися	1
			Самостоятельная работа обучающегося	26
2.1	**Архитектура защищенных экономических систем**	1. Использование защищенных компьютерных систем. Общие принципы построения защищенных систем. Классы задач защиты информации. 2. Архитектура систем защиты информации. Ядро и ресурсы средств защиты информации. Стратегии защиты информации.	Занятия лекционного типа	0,5
			Индивидуальная работа с обучающимися	0,5
		– проработка конспекта лекции; – анализ учебников, учебных пособий, специальной литературы по данной теме (с указанием страниц); – подготовка к практическому занятию; – подготовка к дискуссии по определенной проблеме на базе прочитанной литературы, изучения нормативных актов, практики т.д.; – подготовка списка литературы (библиографии) и подборка нормативных источников по определенной тематике, их изучение и т.д.)	Самостоятельная работа обучающегося	10
2.2	**Алгоритмы безопасности в компьютерных сетях**	1.Атаки на сервера. Атаки на рабочие станции. Атака типа «отказ в обслуживании». Эксплоиты. 2. Межсетевые экраны (firewall) Снифферы. Протоколирование. Сетевые защищенные протоколы.	Занятия лекционного типа	0,25
			Индивидуальная работа с обучающимися	0,25
		– проработка конспекта лекции; – анализ учебников, учебных пособий, специальной литературы по данной теме (с указанием страниц); – подготовка к практическому занятию; – подготовка к дискуссии по определенной проблеме на базе прочитанной литературы, изучения нормативных актов, практики т.д.; – подготовка списка литературы (библиографии) и подборка нормативных источников по определенной тематике, их изучение и т.д.)	Самостоятельная работа обучающегося	8
2.3	**Арендные отношения в малом и сервисном бизнесе**	1. Анализ рынка информационных технологий в области экономики и управления и их адаптации к изменяющимся условиям бизнеса. 2. Тенденции и перспективы развития информационных технологий. Особенности информатизации российской социально-культурной сферы .	Занятия лекционного типа	0,25
			Индивидуальная работа с обучающимися	0,25
		– проработка конспекта лекции; – анализ учебников, учебных пособий, специальной литературы по данной теме (с указанием страниц); – подготовка к практическому занятию; – подготовка к дискуссии по определенной проблеме на базе прочитанной литературы, изучения нормативных актов, практики т.д.; – подготовка списка литературы (библиографии) и подборка нормативных источников по определенной тематике, их изучение и т.д.)	Самостоятельная работа обучающегося	8
3.	**Раздел 3. Информационная безопасность в системе национальной безопасности России**		Занятия лекционного типа	1
			Индивидуальная	1

			работа с обучающимися	
			Самостоятельная работа обучающегося	20
3.1	**Информационная война, методы и средства ее ведения**	1.Информационная война в современном мире. Признаки информационной войны. Цели, виды, методы ведения информационной войны. Защита от информационной войны. 2.Информационная война в бизнесе, в политике. Информационная война и пропаганда. Последствия информационной войны.	Занятия лекционного типа	0,5
			Индивидуальная работа с обучающимися	0,5
		– проработка конспекта лекции; – анализ учебников, учебных пособий, специальной литературы по данной теме (с указанием страниц); – подготовка к практическому занятию; – подготовка к дискуссии по определенной проблеме на базе прочитанной литературы, изучения нормативных актов, практики т.д.; – подготовка списка литературы (библиографии) и подборка нормативных источников по определенной тематике, их изучение и т.д.)	Самостоятельная работа обучающегося	10
3.2	**Информационная безопасность в системе национальной безопасности России**	1.Понятие национальной безопасности. Интересы и угрозы в области национальной безопасности. 2.Влияние процессов информатизации общества на составляющие национальной безопасности и их содержание. 3. Система обеспечения информационной безопасности. Обеспечение информационной безопасности Российской Федерации.	Занятия лекционного типа	0,5
			Индивидуальная работа с обучающимися	0,5
		– проработка конспекта лекции; – анализ учебников, учебных пособий, специальной литературы по данной теме (с указанием страниц); – подготовка к практическому занятию; – подготовка к дискуссии по определенной проблеме на базе прочитанной литературы, изучения нормативных актов, практики т.д.; – подготовка списка литературы (библиографии) и подборка нормативных источников по определенной тематике, их изучение и т.д.)	Самостоятельная работа обучающегося	10

2.2 Перечень обеспечения СРС

Студенту предлагается выполнить следующие виды самостоятельной работы:

– проработка конспекта лекции;

– анализ учебников, учебных пособий, специальной литературы по данной теме (с указанием страниц);

– подготовка к практическому занятию;

– проведение научных исследований;

– выполнение домашней контрольной работы, письменное или устное решение задач, разбор конкретных ситуаций;

– подготовка к дискуссии по определенной проблеме на базе прочитанной литературы, изучения нормативных актов, практики т.д.;

– подготовка списка литературы (библиографии) и подборка нормативных источников по определенной тематике, их изучение и т.д.).

При выполнении самостоятельной работы, обучающемуся предоставляется следующее учебно-методическое обеспечение:

- информационные ресурсы, перечисленные в разделе 4: Информационные ресурсы данной программы;

- материалы, размещенные в разделах Диск, Задачи, Обсуждение, Сообщения ПГ Информационная безопасность Кампуса ВЭГУ 24;
- электронные курсы, размещенные в вертикальном меню Кампуса ВЭГУ

3. Фонд оценочных средств

3.1 Этапы формирования компетенций

Компетенция		Этапы формирования		
код	**содержание**	**знать**	**уметь**	**владеть**
1	**2**	**3**	**4**	**5**
УК-1	Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач	- принципы сбора, отбора и обобщения информации, методики системного подхода для решения профессиональных задач	- анализировать и систематизировать разнородные данные, оценивать эффективность процедур анализа проблем и принятия решений в профессиональной деятельности	- навыками научного поиска и практической работы с информационными источниками; методами принятия решений
	Типовые контрольные задания - проведите обзор нормативно-правовых документов по защите информации от утечки; - проведите обзор российского законодательства и нормативно-правовых документов по защите информации от несанкционированного воздействия; - проведите обзор российского законодательства и нормативно-правовых документов по защите информации от разглашения - охарактеризуйте внутренних и внешних нарушителей информационной безопасности			
ОПК-3	Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	- принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	- Умеет решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	- навыками подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций, и библиографии по научно-исследовательской работе с учетом требований информационной безопасности
	Типовые контрольные задания - раскройте сущность активного перехвата информации;			

	- раскройте сущность пассивного перехвата информации;			
ОПК-4	-Способен участвовать в разработке стандартов, норм и правил, а также технической документации, связанной с профессиональной деятельностью	-основные стандарты оформления технической документации на различных стадиях жизненного цикла информационной системы	- применять стандарты оформления технической документации на различных стадиях жизненного цикла информационной системы	- навыками составления технической документации на различных этапах жизненного цикла информационной системы.
	Типовые контрольные задания - охарактеризуйте существующие категории информационной безопасности в соответствии со свойствами информации; - рассмотрите аппаратные и программные средствами, обеспечивающие конфиденциальность информации, аутентичность и аппелируемость; - проанализируйте методы защиты информации от несанкционированного воздействия; - опишите процесс настройки firewall для корпоративной сети и проанализируйте его; - сформулируйте основные правила информационной безопасности			
ПК-6	Способен принимать участие в организации ИТ-инфраструктуры и управлении информационной безопасностью.	- виды угроз ИС и методы обеспечения информационной безопасности, современные отечественные и международные стандарты в сфере информационных технологий	- выявлять угрозы информационной безопасности, обосновывать организационно-технические мероприятия по защите информации в прикладных ИС	- методикой обеспечения защиты информации в ИС; навыками участия в организации ИТ-инфраструктуры предприятия и управлении информационной безопасностью
	Типовые контрольные задания - дайте понятие «пользователь (потребитель) информации»; - проанализируйте категории безопасности информационных систем; - рассмотрите возможные варианты расположения субъекта атаки; - проведите анализ различий между понятиями криптоалгоритмов и криптосистем; - проанализируйте методы защиты информации от разглашения; - раскройте сущность метода "взлома" на основе комплексного поиска возможных методов доступа, и предупреждение такого взлома; - раскройте сущность метода "взлома" на основе терминала защищенной информационной системы, и его предупреждение; - раскройте сущность метода "взлома" на основе получение пароля вследствие ошибок администратора и пользователей, и его предупреждение; - раскройте сущность метода "взлома" на основе получение пароля вследствие ошибок реализации, и его предупреждение; - раскройте сущность метода "взлома" на основе применения методов социальной психологии, и его предупреждение			

3.2 Показатели, критерии и шкала оценивания

3.2.1 Для оценивания компетенций обучающегося на этапе их формирования по результатам освоения программы данной дисциплины применяется четырехбалльная шкала оценивания (оценки «зачтено(отлично)», «зачтено(хорошо)», «зачтено(удовлетворительно)» или «не зачтено»).

3.2.2 При применении технологий, использующих иные шкалы измерения (тестирование, балльно-рейтинговой, рейтинговой и т.д.), они для окончательного оформления переводятся в четырехбалльную шкалу по следующим параметрам: 90 и более процентов максимально-возможной суммы – «зачтено(отлично)», 70-89% - «зачтено(хорошо)», 50-69% - «зачтено(удовлетворительно)», менее 50 % - «не зачтено».

3.2.3 При формировании оценки обучающегося используются следующие показатели и критерии оценивания результатов освоения программы данной дисциплины и соответствующего этапа формирования компетенций обучающегося:

Оценка	Критерий	Индикатор (показатель)
«зачтено(отлично)»	усвоение программы в полном объеме	задание выполнено без замечаний, полное и логически стройное изложение содержания при ответе или в отчете, тесное увязывание теории вопроса с практикой, отсутствие затруднений с объяснением всех аспектов выполнения задания, хорошее владение умениями и навыками по программе, знание монографической литературы, наличие умений самостоятельно обобщать и излагать материал
«зачтено(хорошо)»	твердое владение материалом в рамках программы	задание выполнено без существенных замечаний, грамотное изложение ответа (отчета), отсутствие существенных неточностей, правильное применение теоретических положений и владение необходимыми навыками при выполнении практических заданий
«зачтено(удовлетворительно)»	владение только основным материалом программы	задание в основном выполнено, допущение неточностей при правильном в основном ответе, нарушение последовательности в его изложении, неусвоение отдельных существенных деталей, наличие затруднений в выполнении практических заданий
«не зачтено»	невладение значительной (и значимой) частью материала программы	задание не выполнено, допуск обучающимся при ответе принципиальных ошибок, большие затруднения при выполнении практических работ, ответ свидетельствует об отсутствии знаний по предмету

3.2.4 Аттестация по данной дисциплине может осуществляться по балльно-рейтинговой системе (далее - БРС), которая представляет собой строго последовательное прохождение обучающимся контрольных (реперных, рубежных) точек (далее – КТ-1, КТ-2 и т.д.) с получением оценки за качество

показанных результатов в виде определенной конечной суммы баллов. При этом используются следующие индикаторы начисления баллов.

3.2.4.1 Общее количество баллов БРС распределяется следующим образом:

- за прохождение предварительного этапа – 20 баллов;
- за прохождение первой контрольной точки – до 20 баллов;
- за прохождение второй контрольной точки – до 20 баллов;
- за прохождение третьей контрольной точки – до 20 баллов.

3.2.4.2 Перевод набранной суммы по итогам всей БРС в четырехбалльную шкалу оценивания осуществляется по следующим параметрам: 72 и более баллов – «зачтено(отлично)», 56-71 баллов - «зачтено(хорошо)», 40-55 баллов - «зачтено(удовлетворительно)», менее 40 баллов - «незачтено».

3.2.4.3 За прохождение предварительного этапа начисляется до 20 баллов пропорционально изученным обучающимся разделам лекционного материала и набранным при тестировании в самом представленном для изучения ресурсе количеству баллов.

3.2.4.4 Начисление баллов по рубежной аттестации по первой контрольной точке осуществляется в зависимости от результативности участия на вебинаре.

3.2.4.4.1 При он-лайн участии на вебинаре баллы начисляются по следующим критериям:

1) 5 баллов, если участие ограничилось только присутствием или одним нерезультативным действием (вопрос или выступление не соответствовали теме);

2) 10 баллов, если были два и более нерезультативных действия;

3) 15 баллов, если среди двух или более произведенных обучающимся действий как минимум одно было результативным (правильное изложение материала, точно заданный вопрос, аргументированная и объективная рецензия);

4) 20 баллов, если все произведенные обучающимся два и более действий были результативными.

3.2.4.4.2 При просмотре вебинара в записи и предоставлении обучающимся письменного отзыва о нем, определяются следующие степени и суммы баллов:

1) 5 баллов, если отзыв написан формально, малосодержательно, но свидетельствует о просмотре всего вебинара;

2) 10 баллов, если в отзыве достаточно аргументировано выделены позитивная (что понравилась, было понятно, интересно) и (или) негативная (что не понравилась, было непонятным, неинтересным) стороны вебинара;

3) 15 баллов, если в отзыве есть обоснованное, логичное сопоставление позитивных и негативных итогов занятия;

4) 20 баллов, если отзыв в дополнение к третьему уровню содержит существенные предложения по улучшению организации вебинара или аргументировано описывает проблему, сформировавшуюся по итогам вебинара.

3.2.4.5 При тестировании по второй контрольной точке, если тестовые задания имеют разные степени сложности, каждые 5% максимально-возможной

суммы правильных ответов приравнивается одному баллу БРС.

При равной сложности всех тестовых заданий каждый правильный ответ приносит 1 балл БРС.

3.2.4.6 Творческая аттестационная работа оценивается по шестибалльной шкале (0 баллов – отсутствует, 1 балл – имеется, но абсолютно не соответствует заданию и (или) дисциплине, 2 балла – в большей части не соответствует заданию (дисциплине), хотя есть определенное приближение к сути задания (дисциплины), 3 балла – суть задания выявлена, но неполно, 4 балла – имеются только отдельные неточности, 5 – нет претензий к исполнению) по следующим направлениям:

- определение и фиксация проблемы;
- формулирование ответа (рабочей гипотезы);
- аргументы и иллюстрации в пользу ответа (рабочей гипотезы);
- использование концептуального и понятийного аппарата дисциплины.

Сумма набранных баллов за все 4 направления является количеством баллов БРС, начисляемых в общий рейтинг за третью контрольную точку.

3.3 Типовые контрольные задания

3.3.1 При подготовке обучающегося к аттестации и при оценивании результатов освоения программы данной дисциплины (для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы) используются типовые контрольные задания по:

- истории развития той отрасли знания, изучению которой посвящена данная дисциплина (модуль); объекту, предмету и методам (инструментам), применяемым в данной дисциплине (модуле); месту, значению данной дисциплины (модуля) в деятельности человека и ее связям с другими дисциплинами (модулями); проблемам и задачам, решаемым в рамках данной дисциплины (модуля) и т.д.;
- существу теорий, концепций, систем описания и объяснения, гипотез, выдвигаемых в рамках данной дисциплины, а также категориям и понятиям (терминам), являющимся существенными для данной дисциплины;
- применению компетенций, сформированных в ходе освоения программы, для решения конкретной задачи, объяснения конкретного факта (явления), разрешения конкретной ситуации и т.д.

3.3.2 Данные типовые задания при проведении конкретных аттестационных испытаний переформатируются в вопросы аттестационных билетов или тестовые задания в соответствии с правилами, установленными для Фонда оценочных средств Академии ВЭГУ. По предметам вопросов типовых заданий могут быть сформулированы несколько различающихся по форме и аспекту рассмотрения вопросов аттестационных билетов, тестовых заданий или тем письменных работ. Комплекты вопросов для аттестационных билетов, тестовых заданий и тем в виде соответствующих баз хранятся в Центре аттестации Академии ВЭГУ в режиме конфиденциальности и предъявляются в

виде набора аттестационных билетов, тестов или отдельной темы, формируемых по установленным в Академии ВЭГУ правилам, на каждую конкретную аттестацию.

3.3.3 Типовые контрольные вопросы и задания для подготовки и проведения промежуточной аттестации:

- перечислите категории информационной безопасности в соответствии со свойствами информации;
- сущность категории конфиденциальности информации;
- сущность категории целостности информации;
- сущность категории аутентичности;
- сущность категории аппелируемости;
- сущность категории точности;
- программные средства, обеспечивающие конфиденциальность информации;
- аппаратные и программные средства, обеспечивающие конфиденциальность информации, аутентичность и аппелируемость;
- перечислите категории безопасности информационных систем;
- сущность категории надежности;
- сущность категории точности;
- сущность категории контроля доступа;
- сущность категории контролируемость и чем она отличается от категории контроля доступа;
- сущность категории контроля идентификации;
- чем состоит сущность категории устойчивости к умышленным сбоям;
- перечислите абстрактные модели защиты информации;
- модель Биба (Biba);
- модель Гогена-Мезигера (Goguen-Meseguer);
- модель Сазерлендской (от англ. Sutherland);
- модель защиты Кларка-Вильсона (Clark-Wilson);
- цели использования транзакций;
- раскройте понятие «защищенность третьей стороны»;
- сущность метода "взлома" на основе комплексного поиска возможных методов доступа, его предупреждение;
- сущность метода "взлома" на основе терминала защищенной информационной системы, его предупреждение;
- сущность метода "взлома" на основе получение пароля вследствие ошибок администратора и пользователей, его предупреждение;
- сущность метода "взлома" на основе получение пароля вследствие ошибок реализации, его предупреждение;
- сущность метода "взлома" на основе применения методов социальной психологии, его предупреждение;
- особенности симметричных криптоалгоритмов;
- особенности асимметричных криптоалгоритмов;

- различие между понятиями криптоалгоритмов и криптосистем;
- блочные шифры, их отличие от потоковых шифров;
- понятие «раунд криптоалгоритма»;
- алгоритм RSA, его математический аппарат;
- криптоалгоритм на основе эллиптических кривых, их достоинства и недостатки;
- сущность генерация ключей для криптографии;
- различия между ключем и паролем;
- репозитарии ключей;
- достоинства применения сеансового (сессионного) ключа;
- протоколы обмена ключами в зависимости от стороны, вырабатывающей сеансовый ключ;
- достоинства и недостатки совместной выработки сеансового ключа абонентами;
- достоинства и недостатки выработки сеансового ключа третьей стороной (доверенным центром);
- сущность активного перехвата информации;
- сущность пассивного перехвата информации;
- задачи защиты информации;
- варианты расположения субъекта атаки;
- существование типов информационных процессов;
- сущность подмены доверенного объекта;
- шифрование информации;
- сущность подмены субъекта распределенной вычислительной сети;
- доступ к информации;
- понятие ложный объект распределенной вычислительной сети;
- защита информации от утечки;
- защита информации от несанкционированного воздействия;
- защита информации от разглашения;
- субъекты доступа к информации;
- носители информации;
- шифрование методом подстановки и перестановки;
- понятие собственника информации;
- понятие пользователя (потребителя) информации;
- цели воздействия удаленных атак;
- внутренние нарушители информационной безопасности;
- внешние нарушители информационной безопасности;
- сущность подмены доверенного объекта;
- понятие информационной войны;
- признаки информационной войны;
- цели информационной войны;
- виды информационной войны;
- методы ведения информационной войны;

- информационная война в политике, пропаганда;
- информационная война в бизнесе;
- информационная война в современном мире, ее последствия;
- защита от информационной войны;
- понятие национальной безопасности;
- интересы и угрозы в области национальной безопасности;
- влияние процессов информатизации общества на составляющие национальной безопасности и их содержание;
- система обеспечения информационной безопасности;
- обеспечение информационной безопасности Российской Федерации.

3.3.4 Типовые (примерные) темы для письменных работ.

- Проанализируйте использование криптографически защищенного протокола для защиты приложений корпоративных сетей;
- Перечислите и проанализируйте категории информационной безопасности;
- Расскажите об эффективности использования прокси серверов для защиты виртуальны сетей;
- Опишите процесс настройки firewall для корпоративной сети и проанализируйте его;
- Проанализируйте файловые системы, имеющие криптографическую защиту;
- Перечислите и проанализируйте абстрактные модели защиты информации;
- Проанализируйте эффективность защиты электронных платежных систем;
- Проанализируйте эффективность использования виртуальных сетей для защиты корпоративных сетей;
- Опишите и проанализируйте симметричные криптоалгоритмы;
- Перечислите и проанализируйте ассимметричные криптоалгоритмы;
- Расскажите о Дистрибутивах Linux, сертифицированных для использования в защищенных системах.

3.4 Методические материалы по процедурам оценивания

3.4.1 Методика (в том числе технологические и организационные аспекты), определяющая процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций, установлены положениями об организации образовательной деятельности по программам высшего образования, о текущем контроле успеваемости и промежуточной аттестации, о балльно-рейтинговой системе аттестации, о фонде оценочных средств и изданными в соответствии с ними другими локальными нормативными актами, в т.ч. внутривузовскими стандартами, Академии ВЭГУ.

3.4.2 Обеспечение аттестации в Академии ВЭГУ должно удовлетворять, в первую очередь, требованиям нацеленности на результат обучения, системности, унификации и объективности, что на практике означает следующие:

- применение единых критериев оценивания по всем образовательным программам;

- сопряженность всех видов контрольно-измерительных материалов с конечными компетенциями и друг с другом (высокая степень валидности) и их репрезентативность с содержанием программы;

- выведение итоговых оценок по результатам проверки знаний, умений и навыков по всем дидактическим единицам оцениваемой программы;

- применение единых контрольно-измерительных материалов и процедур аттестации к обучающимся всех форм и технологий обучения;

- привлечение к осуществлению аттестации не задействованных в подпроцессе обучения обучающих, в т.ч. практикующих специалистов необразовательных организаций;

- широкое применение инструментальной среды;

- обязательная экспертиза текстов письменных работ (и других видов оформления результатов проектирования) на авторство (отсутствие заимствований, плагиата, копирования);

- ежегодное обновление тем письменных работ.

Порядок разработки, использования и хранения контрольных измерительных материалов (включая требования к режиму их защиты, порядку и условиям размещения информации, содержащейся в контрольных измерительных материалах, в сети «Интернет») устанавливается в соответствии с федеральными требованиями положением Академии ВЭГУ о фонде оценочных средств.

3.4.3 При организации аттестации обучающихся в Академии ВЭГУ обязательно исполнение следующих положений:

- аттестации подлежат только образовательные программы, назначенные для данного аттестуемого (правилами приема, учебными планами и другими соответствующими документами);

- аттестацию может проводить только тот обучающий (эксперт), который закреплен для данной процедуры по данной группе аттестуемых;

- аттестация проводится только с использованием утвержденных контрольно-измерительных материалов и по утвержденной форме и процедуре;

- аттестация проводится только для тех обучающихся, которые имеют соответствующий допуск;

- результаты аттестации должны быть зафиксированы в утвержденных для этого документах.

4. Информационные ресурсы

4.1 Основная учебная литература

№ п/п	Выходные данные основной учебной литературы	Адрес доступа к полнотекстовому варианту в Электронно-библиотечной системе Академии ВЭГУ
1	Артемов, А. В. Информационная безопасность : курс	http://www.iprbookshop.ru/

	лекций / А. В. Артемов. — Орел : Межрегиональная Академия безопасности и выживания (МАБИВ), 2014. — 256 с.	33430.html
2	Казарин, О. В. Надежность и безопасность программного обеспечения : учебное пособие для вузов / О. В. Казарин, И. Б. Шубинский. — Москва : Издательство Юрайт, 2020. — 342 с.	https://urait.ru/bcode/454453
3	Электронный курс «Информационная безопасность», специально разработанный в Академии ВЭГУ и размещенный в ЭБС.	https://moodle.vegu.ru/course/view.php?id=591

4.2 Дополнительная учебная литература можно статьи

№ п/п	Выходные данные основной учебной литературы	Адрес доступа к полнотекстовому варианту в Электронно-библиотечной системе Академии ВЭГУ
1	Петров, С. В. Информационная безопасность : учебное пособие / С. В. Петров, П. А. Кисляков. — Саратов : Ай Пи Ар Букс, 2015. — 326 с.	http://www.iprbookshop.ru/33857.html
2	Богатырев, В. А. Информационные системы и технологии. Теория надежности : учебное пособие для вузов / В. А. Богатырев. — Москва : Издательство Юрайт, 2020. — 318 с.	https://urait.ru/bcode/451108
3	Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для вузов / О. В. Казарин, А. С. Забабурин. — Москва : Издательство Юрайт, 2020. — 312 с.	https://urait.ru/bcode/452368
4	Щеглов, А. Ю. Защита информации: основы теории : учебник для бакалавриата и магистратуры / А. Ю. Щеглов, К. А. Щеглов. — Москва : Издательство Юрайт, 2020. — 309 с.	https://urait.ru/bcode/449285

4.3 Ресурсы сети «Интернет»

№ п/п	Наименование ресурса	Адрес доступа к полнотекстовому варианту (в ЭБС Академии ВЭГУ или других ресурсах в сети «Интернет»)
Современные профессиональные базы		
1	Отделение нанотехнологий и информационных технологий РАН	http://www.ras.ru/win/db/show_org.asp?P=.oi-336.ln-ru
2	Сайт разработчиков ИС и баз данных	http://www.sql.ru/
3	Сервер информационных технологий	http://citforum.ru/
4	Официальный сайт корпорации IBM	https://www.ibm.com/ru/
5	Официальный сайт корпорации Microsoft	https://www.microsoft.com/ru-ru/
6	Официальный сайт корпорации Oracle	https://www.oracle.com/ru/
Информационные справочные системы		

1	Правовая система КонсультантПлюс	http://www.consultant.ru/
2	Некоммерческие интернет-версии системы КонсультантПлюс	http://www.consultant.ru/online/
3	Информационно-правовой портал Гарант	http://www.garant.ru/
4	Официальный сайт компании 1С	http://v8.1c.ru/edu/
5	Каталог Интернет сайтов	www.list.ru
6	Информационная корпорация Questel-Orbit	www.questel-orbit.com
7	Информационное агентство LEXIS-NEXIS	www.lexis-nexis.com
Иные ресурсы Интернет		
1	Еженедельник PC Week: русская версия международного издания об информационных и коммуникационных технологиях.	https://www.itweek.ru/
2	Портал ERPNEWS - аналитика и новости по системам автоматизации предприятия	http://www.erpnews.ru
3	Сервер программного обеспечения	http://www.freeware.ru/
4	Научный журнал «Вычислительные методы и программирование»	http://num-meth.srcc.msu.ru/
5	Центр инженерных технологий и моделирования	http://exponenta.ru/
6	Современные информационные технологии	https://studopedia.su/7_14531_sovremennie-informatsionnie-tehnologii.html
7	Интернет - журнал о технологиях. digit.ru - информационно-аналитический IT-портал	http://www.big-big.ru/informaczionnyie-texnologii.html
8	Информационно-образовательный сайт	http://self-educ.ru/?page_id=216
9	Электронная библиотека системного администратора	http://it-ebooks.ru/
10	ERP, CRM, MES, EAM, ERP-решения и системы управления предприятием	http://www.belerp.com

4.4 Информационные технологии

4.4.1. АСО Академии ВЭГУ

Образовательный процесс по данной дисциплине в Академии ВЭГУ ведется с широким использованием Автоматизированной системы обучения. В частности, применяются следующие составные части (модули) АСО:

№ п/п	Полное наименование	Область применения в образовательной деятельности
1.	«1С-Битрикс: внутренний портал учебного заведения»	Платформа для интеграции всех сервисов и создания виртуальных рабочих кабинетов участников образовательного процесса. 1. Создание ЭИОС для обучающегося: - редактирование индивидуального учебного плана, обучающегося; - изучение материалов по доступным дисциплина (модулям) (электронный курс, материалы для самоконтроля и прохождение аттестации, расписание трансляций лекций, очных занятий и вебинаров, просмотр видео материалов); - средства электронных коммуникаций (форумы, комментарии,

		чат) для общения с участниками процесса обучения (в учебной и предметных группах); - просмотр электронной зачётной книжки; - получение информации о набранных кредитах (оценках); - автоматическое зачисление в предметные и учебные группы; - формирование портфолио обучающегося (данные по IMS ePortfolio Specification (http://www.imsglobal.org/ep/); - биллинговая система (on-line оплата обучения, просмотр истории оплаты). 2. Создание ЭИОС для обучающего: - получение информации по нагрузке; - планирование и проведение вебинаров; - разработка и экспертиза контрольно-измерительных материалов (КИМ); - проверка эссе обучающихся; - средства электронных коммуникаций (форумы, комментарии, чат) для общения с участниками процесса обучения (в учебных и предметных группах); - публикация мультимедийного обучающего контента; - формирование персонального портфолио. 3. Для организаторов образовательного процесса: - система мониторинга (получение информации об активности пользователей; организация опросов пользователей); - участие в группах (учебных, предметных, общих); - поддержка основных элементов коммуникаций (форумы, комментарии); - оценивание и организация объектов социальной сети; - отслеживание рейтингов и достижений; - публичное портфолио пользователя; - работа с заявками (отправка, отслеживание выполнения).
2.	«Компас-В» на платформе «1С: Предприятие 8.2»	Автоматизирует работу: - приёмной комиссии (ведение базы абитуриентов, зачисление на обучение, финансовые и маркетинговые отчёты), - деканата (документооборот приказов по движению обучающихся, репозиторий документов обучающихся, оповещение обучающихся по электронной почте, SMS), - учебно-методического управления (ведение базы преподавателей, формирование и учёт учебной нагрузки).
3.	Программный комплекс «Автоматизированная среда аттестации АСА»	Автоматизирует процедуры: - разработки, экспертизы и публичной экспертизы контрольно-измерительных материалов; - формирования и использования фонда оценочных средств по конкретным программам, дисциплинам (модулям, предметам, видам учебной работы); - проведения обучения с использованием балльно - рейтинговой системы (БРС); - допуска, проведения приема экзаменов, зачетов, письменных аттестационных работ; - видеопротоколирования процесса аттестации; - оформления документации по процессам аттестации

		(аттестационных ведомостей, заявлений на оплату выполненной обучающими работы, отчетов); - контроля успеваемости обучающихся; - мониторинга удовлетворенности обучающимися качеством контрольно-измерительных материалов и процедурами аттестации.
4.	Система программных продуктов LMS Moodle	Используется для: - публикации электронных курсов; - просмотра результата прохождения электронного курса и последующего его учёта в рамках БРС.
5.	Система автоматизации библиотек ИРБИС64	Используется для: организации доступа к электронной библиотеке для: просмотра полнотекстовых вариантов основной и дополнительной литературы; просмотра учебно-методических комплексов дисциплин.
6.	Программный продукт Автоматизированная информационная система библиотеки «Электронная библиотека»	Используется для организации процесса разработки и обновления полнотекстовых электронных версий учебных материалов и рабочих программ дисциплин.
7.	Прикладное программное обеспечение "Мираполис"	On-line сервис интегрированный в АСО, используется для: - организации и проведения вебинаров, интерактивных занятий, on-line консультаций и лекций; - просмотра записей вебинаров.

4.4.2 Специальные информационные технологии

Информационные технологии, используемые при осуществлении образовательного процесса по данной дисциплине, включает следующий перечень программного обеспечения и информационных справочных систем:

Программный продукт	Договор
1) Microsoft Office 2007 2) 7-Zip 16.04 3) Acrobat Reader 4) Антивирус Kaspersky Endpoint Security 10 for Windows 5) Mozilla Firefox 6) Google Chrome 7) VLC 2.2.6 8) Microsoft Windows 7 Professional Academic Open License	1) Лицензия Microsoft Open License №43509314 дата выдачи настоящей Лицензии 19.02.2008 «Microsoft® Office 2007 Russian Academic. Microsoft® Windows® Vista Business Russian Upgrade Academic» 2) лицензия GNU LGPL (Свободное ПО) 3) лицензионное соглашение с компанией Adobe (Свободное ПО) 4) лицензия № 1FB6-170208-101930-190-411 5) лицензия GNU LGPL (Свободное ПО) 6) лицензия LGPL (Свободное ПО) 7) лицензия GNU LGPL (Свободное ПО) 8) лицензия № 62875440

9) Microsoft Windows Server 2008	9) лицензия № 47623222

4.5 Материально-техническая база

4.5.1 В процессе обучения данной дисциплины используется специальный виртуальный учебный кабинет – предметная группа модуля «Кампус ВЭГУ 24» (далее – ПГ).

4.5.2 Информационно-предметная среда ПГ размещается в разделах меню ПГ, а так же в разделах и подразделах меню «Кампус ВЭГУ 24».

Размещение материалов (или обеспечение прямого доступа к информационным ресурсам) в разделах меню «Кампус ВЭГУ 24» осуществляется в централизованном порядке структурными подразделениями Академии ВЭГУ (материалы Электронно-библиотечной системы, локальные нормативные акты Академии ВЭГУ, записи проведенных учебных занятий и т.п.).

В разделах меню ПГ размещение материалов организовывается преподавателем, являющимся владельцем данной ПГ (т.е. закрепленным за реализацией данной дисциплины).

4.5.3 Взаимодействие обучающихся в ПГ осуществляется на принципах тьюторинга и интерактива.

Тьюторинг осуществляется посредством постановки преподавателем задач перед обучающимся, консультирования, проверки и оценивания исполнения задач.

Интерактивный метод обучения обеспечивается организацией преподавателем в ПГ взаимодействия обучающихся друг с другом в сфере освоения программы дисциплины в разных формах и способах, в т.ч.:

- обязательных в рамках этапа (контрольных точек) БРС и факультативных занятий в форме дискуссий, групповой (командной) творческой работы, группового проектирования, кейс-метода, «мозгового штурма» или игры;
- широким использованием ПГ для общего обмена мнениями при постоянном контроле со стороны преподавателя и корректировки оценок и поощрения лучших сообщений;
- вовлечения обучающихся в формирование базы знаний.

4.5.4 Для ведения образовательной деятельности в учебных корпусах Академии ВЭГУ имеются учебные аудитории для проведения занятий лекционного типа, занятий семинарского типа, курсового проектирования (выполнения курсовых работ), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, а также помещения для самостоятельной работы и помещения для хранения и профилактического обслуживания учебного оборудования. Они укомплектованы специализированной мебелью и техническими средствами обучения, служащими для представления учебной информации большой аудитории. Для проведения занятий лекционного типа предлагаются наборы демонстрационного оборудования и учебно-наглядных пособий, обеспечивающие тематические

иллюстрации. Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой с возможностью подключения к сети Интернет и обеспечением доступа в электронно-информационную среду Академии ВЭГУ.

Полный перечень материально-технического обеспечения по дисциплине указан в Справке о материально-техническом обеспечении основной профессиональной образовательной программы высшего образования.

5. Методические указания обучающемуся

Общая трудоемкость дисциплины составляет 4 зачетные единицы, 144 часа.

В рамках дисциплины предполагается изучение следующих разделов:

- Основные понятия теории информационной безопасности, категории информационной безопасности, угрозы информационной безопасности
- Технологии построения защищенных систем, информационная безопасность сетей

Ключевыми понятиями раздела 1. «Основные понятия теории информационной безопасности, категории информационной безопасности, угрозы информационной безопасности» являются: понятие информационной безопасности и защищенной системы; категории информационной безопасности; понятие угрозы; формальные модели безопасности их значение для построения защищенных информационных систем; понятие политики безопасности информационных систем; аппаратные и программные средства для защиты компьютерных систем по категориям информационной безопасности; особенности сертификации и стандартизации криптографических услуг; методы криптографии; электронно-цифровая подпись

Изучая раздел 1, студент познакомится с: понятием информационной безопасности и защищенной системы; категориями информационной безопасности; понятием угрозы; формальными моделями безопасности их значением для построения защищенных информационных систем; понятием политики безопасности информационных систем; с аппаратными и программными средствами для защиты компьютерных систем по категориям информационной безопасности; особенностями сертификации и стандартизации криптографических услуг; методами криптографии; алгоритмами электронно-цифровой подписи.

Ключевыми понятиями раздела 2. «Технологии построения защищенных систем, информационная безопасность сетей» являются: общие принципы построения защищенных систем; классы задач защиты информации; архитектура систем защиты информации; атаки на сервера; атаки на рабочие станции.

Изучая раздел 2, студент познакомится с: общими принципами построения

защищенных систем; классами задач защиты информации; архитектурой систем защиты информации; видами атак на сервера и на рабочие станции.

По каждому разделу предусмотрено выполнение студентами различных видов самостоятельной работы:

- самостоятельная работа во время основных аудиторных занятий (лекций, семинаров, лабораторных работ);
- самостоятельная работа под контролем преподавателя в форме плановых консультаций и творческих контактов;
- внеаудиторная самостоятельная работа при выполнении студентом домашних заданий учебного и творческого характера.

По итогам освоения дисциплины предусмотрена рубежная и промежуточная, аттестация. Рубежная аттестация предусмотрена в форме БРС, промежуточная аттестация предусмотрена в форме зачета (тестирование).

Для подготовки к аттестации рекомендуется:

- изучить лекционный и практический материал;
- изучить материалы, представленные по данной дисциплине в библиотеке Академии ВЭГУ или воспользоваться электронной библиотекой;
- использовать самообучающие программы;
- контролировать уровень своих знаний тестами-тренингами.

6. Особенности освоения дисциплины (модуля) для инвалидов и лиц с ограниченными возможностями здоровья.

6.1 Выбор методов обучения лиц с ограниченными возможностями здоровья и инвалидов определяются исходя из их доступности для данной категории обучающихся, определяется содержанием обучения, исходным уровнем имеющихся знаний, уровнем профессиональной подготовки педагогов, особенностями восприятия информации обучающимися. В образовательном процессе предполагается использование социально-активных и рефлексивных методов обучения, технологий социальной реабилитации с целью оказания помощи в установлении полноценных межличностных отношений с другими студентами, создании комфортного психологического климата.

6.2 В целях освоения учебной программы дисциплины инвалидами и лицами с ограниченными возможностями здоровья кафедра обеспечивает:

1) 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);

2) для инвалидов и лиц с ограниченными возможностями здоровья по слуху: – надлежащими звуковыми средствами воспроизведения информации;

3) 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, а также пребывание в указанных помещениях.

6.3 Образование обучающихся с ограниченными возможностями здоровья может быть организовано как совместно с другими обучающимися, так и в отдельных группах или в отдельных организациях.

6.4 Учебно-методические материалы для самостоятельной работы обучающихся из числа инвалидов и лиц с ограниченными возможностями здоровья предоставляются в формах, адаптированных к ограничениям их здоровья и восприятия информации:

Категории обучающихся	Формы предоставления
С нарушением слуха	в печатной форме; в форме электронного документа
С нарушением зрения	в печатной форме увеличенным шрифтом; в форме электронного документа; в форме аудиофайла;
С нарушением опорно-двигательного аппарата	в печатной форме; в форме электронного документа; в форме аудиофайла;

Данный перечень может быть конкретизирован в зависимости от контингента обучающихся.

6.5 Процедура промежуточной аттестации для обучающихся с ограниченными возможностями здоровья и инвалидов устанавливается с учетом индивидуальных психофизических особенностей. При необходимости предусматривается увеличение времени на подготовку к промежуточной аттестации, а также предоставляется дополнительное время для подготовки ответа в ходе контроля текущей успеваемости и промежуточной аттестации.

При проведении процедуры оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья по дисциплине (модулю) обеспечивается выполнение следующих дополнительных требований в зависимости от индивидуальных особенностей обучающихся:

1. инструкция по порядку проведения процедуры оценивания предоставляется в доступной форме (устно, в письменной форме, устно с использованием услуг сурдопереводчика);

2. доступная форма предоставления заданий оценочных средств (в печатной форме, в печатной форме увеличенным шрифтом, в форме электронного документа, задания зачитываются ассистентом, задания предоставляются с использованием сурдоперевода);

3. доступная форма предоставления ответов на задания (письменно на бумаге, набор ответов на компьютере, с использованием услуг ассистента, устно).

При необходимости для обучающихся с ограниченными возможностями здоровья и инвалидов процедура оценивания результатов обучения по дисциплине (модулю) может проводиться в несколько этапов. Проведение процедуры оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья допускается с использованием дистанционных образовательных технологий.

6.6 Для освоения дисциплины инвалидами и лицами с ограниченными возможностями здоровья предоставляются основная и дополнительная учебная литература в виде электронного документа в фонде библиотеки и / или в электронно-библиотечных системах, а также предоставляются бесплатно специальные учебники и учебные пособия, иная учебная литература и специальные технические средства обучения коллективного и индивидуального пользования, а также услуги сурдопереводчиков и тифлосурдопереводчиков.

Проректор по учебно-научной
и воспитательной работе А.О. Целищев