Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное
учреждение высшего образования
«Комсомольский-на-Амуре государственный университет»

УТВЕРЖДАЮ

Декан факультета____Трещев И.А.___

ФИО декана

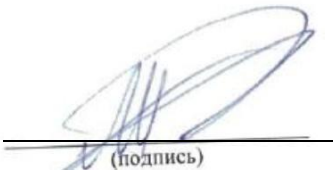
РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
«Защита от хакерских угроз»

Специальность	10.05.03 Информационная безопасность автоматизированных систем
Специализация	Анализ безопасности информационных систем

Обеспечивающее подразделение
Кафедра «Информационная безопасность автоматизированных систем»

Комсомольск-на-Амуре 2025

Разработчик рабочей программы:

Доцент, к.т.н.  Трещев И.А.

(должность, степень, ученое звание) (подпись) (ФИО)

СОГЛАСОВАНО:

Заведующий кафедрой

ИБАС Обласов А.А.

(наименование кафедры) (подпись) (ФИО)

1 Общие положения

Рабочая программа и фонд оценочных средств дисциплины «Защита от хакерских угроз» составлены в соответствии с требованиями федерального государственного образовательного стандарта, утвержденного приказом Минобрнауки Российской Федерации от 26.11.2020 №1457, и основной профессиональной образовательной программы подготовки «Анализ безопасности информационных систем» по специальности «10.05.03 Информационная безопасность автоматизированных систем».

Задачи дисциплины	Изучение основных механизмов защиты информации от потенциальных действий злоумышленников направленных на нарушение конфиденциальности, целостности и доступности информации в автоматизированных системах.
Основные разделы / темы дисциплины	Защита предприятия от хакерских угроз

2 Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с индикаторами достижения компетенций

Процесс изучения дисциплины Защита от хакерских угроз»» направлен на формирование следующих компетенций в соответствии с ФГОС ВО и основной образовательной программой:

Код и наименование компетенции	Индикаторы достижения	Планируемые результаты обучения по дисциплине
Общепрофессиональные		
ОПК-11 Способен разрабатывать компоненты систем защиты информации автоматизированных систем;	ОПК-11.1 Знает программно-аппаратные средства, используемые в качестве компонентов систем защиты информации в программном обеспечении автоматизированных систем; методы проектирования решений по обеспечению безопасности автоматизированных систем ОПК-11.2 Умеет проектировать защищенные распределенные информационные системы и компоненты систем защиты информации автоматизированных систем ОПК-11.3 Владеет навыками разработки компонентов систем защиты информации автоматизированных систем и защищенных распределенные информационные системы	Знает программно-аппаратные средства, используемые в качестве компонентов систем защиты информации в программном обеспечении автоматизированных систем; методы проектирования решений по обеспечению безопасности автоматизированных систем Умеет проектировать защищенные распределенные информационные системы и компоненты систем защиты информации автоматизированных систем Владеет навыками разработки компонентов систем защиты информации автоматизированных систем и защищенных распределенные информационные системы

3 Место дисциплины (модуля) в структуре образовательной программы

Дисциплина входит в состав блока 1 «Дисциплины (модули)» и относится к обязательной части.

Место дисциплины (этап формирования компетенции) отражено в схеме формирования компетенций, представленной в документе *Оценочные материалы*, размещенном на сайте университета *www.knastu.ru / Наш университет / Образование / 10.05.03 Информационная безопасность автоматизированных систем /Оценочные материалы*).

Дисциплина ««Защита от хакерских угроз» частично реализуется в форме практической подготовки. Практическая подготовка организуется путем проведения, лабораторных работ, выполнения курсовых/ работ, иных видов учебной деятельности.

4 Содержание дисциплины (модуля), структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебной работы

4.1 Структура и содержание дисциплины для очной формы обучения

Дисциплина «Защита от хакерских угроз» изучается на 5 курсе, 10 семестре.

Общая трудоёмкость дисциплины составляет ___4__з.е., __144__ч., в том числе контактная работа обучающихся с преподавателем __65__ч., промежуточная аттестация в форме экзамена 35ч., самостоятельная работа обучающихся, _44_____ч.

Наименование разделов, тем и содержание материала	Виды учебной работы, включая самостоятельную работу обучающихся и трудоемкость (в часах)					
	Контактная работа преподавателя с обучающимися			ИКР	Пром. аттест.	СРС
	Лекции	Практические занятия	Лабораторные работы			
Защита предприятия от хакерских угроз Сетевые атаки и методы защиты Терминология в сфере атак на сетевую безопасность. Примеры атак сетевого уровня. Примеры атак уровня приложений Примеры атак социальной инженерии. Примеры атак на почтовые сообщения.Примеры специфических атак на мобильные устройства. Примеры атак на облачные сервисы. Примеры атак на беспроводные сети. Методология взлома и фреймворки Цели, результаты и преграды при построении сетевой защиты. Стратегия непрерывной/адаптивной безопасности Стратегия защиты в глубину Управление сетевой безопасностью	32		32			44

Наименование разделов, тем и содержание материала	Виды учебной работы, включая самостоятельную работу обучающихся и трудоемкость (в часах)					
	Контактная работа преподавателя с обучающимися			ИКР	Пром. аттест.	СРС
	Лекции	Практические занятия	Лабораторные работы			
Соответствия требованиям регуляторов. Правовое поле, международные законы и акты. Проектирование и построение политик безопасности Организация обучающего тренинга по основам безопасности. Административные меры обеспечения безопасности. Техническое обеспечение безопасности сети Контроль доступа: терминология, принципы, модели. Контроль доступа в современном мире распределенных вычислений и мобильных устройств. Управление идентификацией и доступом (IAM): идентификация, аутентификация, авторизация и учет. Криптографические инструменты. Криптографические алгоритмы. Сегментирование сетей. Решения по обеспечению безопасности сети. Протоколы безопасного сетевого взаимодействия Обеспечение безопасности периметра сети Межсетевые экраны: преимущества и недостатки. Типы межсетевых экранов и их использование. Топологии сети и размещение межсетевого экрана. Сравнение аппаратного/программного, хостового/сетевого, внутреннего/внешнего межсетевых экранов. Выбор межсетевого экрана в зависимости от трафика. Процесс внедрения и развертывание межсетевых экранов. Рекомендации по внедрению межсетевых экранов Администрирование межсетевого экрана. Системы предупреждения вторжений (IDS): роль, возможно-						

Наименование разделов, тем и содержание материала	Виды учебной работы, включая самостоятельную работу обучающихся и трудоемкость (в часах)					
	Контактная работа преподавателя с обучающимися			ИКР	Пром. аттест.	СРС
	Лекции	Практические занятия	Лабораторные работы			
сти, ограничения и рекомендации по развертыванию. Классификация IDS/IPS. Компоненты IDS. Развертывание локальных и сетевых IDS. Работа с ложноположительными срабатываниями и отсутствием оповещений об атаке. Выбор решений IDS. Возможности обнаружения вторжений сетевых и хостовых IDS Рекомендации по безопасности для коммутаторов и маршрутизаторов. Модель нулевого доверия в программно-определяемом периметре (SDP) Обеспечение безопасности ОС Windows Вопросы безопасности ОС Windows Компоненты безопасности Windows Инструменты управления безопасностью Windows Настройка параметров безопасности Windows Управление аккаунтами и паролями в Windows Управление патчами Windows Управление доступом пользователей Техники «заморозки» Windows Рекомендации мирового сообщества по вопросам безопасности Безопасность сетевых сервисов и протоколов Обеспечение безопасности ОС Linux Вопросы безопасности ОС Linux Установка и управление патчами Linux Техники «заморозки» Linux Управление аккаунтами и паролями в Linux Сетевая безопасность и удаленных доступ в Linux Инструменты управления безопасностью и фреймвороки Linux Обеспечение безопасности мобильных устройств						

Наименование разделов, тем и содержание материала	Виды учебной работы, включая самостоятельную работу обучающихся и трудоемкость (в часах)					
	Контактная работа преподавателя с обучающимися			ИКР	Пром. аттест.	СРС
	Лекции	Практические занятия	Лабораторные работы			
Политики работы с мобильными устройствами в организации Риски и рекомендации по использованию мобильных устройств в организации Управление безопасностью мобильных устройств на корпоративном уровне Рекомендации мирового сообщества и руководства по обеспечению безопасности мобильных устройств Инструменты обеспечения безопасности для Android Инструменты обеспечения безопасности для iOS Обеспечение безопасности устройств IoT IoT устройства: области применения, потребности и приложения Экосистема и модели коммуникаций IoT устройств Вызовы и риски безопасности при использовании IoT устройств Безопасность для IoT устройств Меры по обеспечению безопасности в средах с IoT устройствами Рекомендации мирового сообщества и средства обеспечения безопасности для IoT устройств Стандарты, инициативы и организационные усилия при обеспечении безопасности IoT устройств Управление безопасностью приложений Белые и черные списки для приложений Внедрение песочниц для приложений Управление патчами приложений Фаерволы для веб-приложений Безопасность данных Почему важно обеспечить безопасность данных Внедрение управления доступом к данным Шифрование данных на носителе Шифрование данных при переда-						

Наименование разделов, тем и содержание материала	Виды учебной работы, включая самостоятельную работу обучающихся и трудоемкость (в часах)					
	Контактная работа преподавателя с обучающимися			ИКР	Пром. аттест.	СРС
	Лекции	Практические занятия	Лабораторные работы			
че Концепции маскировки данных Резервное копирование и восстановление Концепции повреждения данных Обеспечение безопасности корпоративных виртуальных сетей Управление безопасностью в среде виртуализации Базовые концепции виртуализации Безопасность виртуальных сетей Безопасность программно-определяемых сетей (SDN) Безопасность виртуализации сетевых функций (NFV) Безопасность виртуальных машин Рекомендации мирового сообщества и руководства по безопасности при использовании контейнеров Рекомендации мирового сообщества и руководства по безопасности при работе с Docker Обеспечение безопасности облачных сетей Основы облачных вычислений Безопасность облаков Выбор решения для обеспечения безопасности перед подключением облачного сервиса Безопасность облаков Amazon Безопасность в облаке Google Рекомендации мирового сообщества и инструменты обеспечения безопасности облака Мониторинг и анализ сетевых журналов Краткий обзор современных технологий беспроводных сетей Угрозы безопасности беспроводных сетей и основные виды атак на них Методы и средства защиты беспроводных сетей Аудит безопасности беспроводных сетей Системы обнаружения и предупреждения вторжений в беспроводные сети (WIDS/WIPS)						

Наименование разделов, тем и содержание материала	Виды учебной работы, включая самостоятельную работу обучающихся и трудоемкость (в часах)					
	Контактная работа преподавателя с обучающимися			ИКР	Пром. аттест.	СРС
	Лекции	Практические занятия	Лабораторные работы			
Настройки безопасности точек доступа и беспроводных маршрутизаторов Реакция на инцидент и расследование инцидента Организация процесса управления инцидентами информационной безопасности Роли и задачи участников процесса обработки инцидента информационной безопасности Что делать и не делать при обнаружении инцидента информационной безопасности Последовательность действий при обработке инцидента информационной безопасности Процесс расследования инцидента информационной безопасности Непрерывность бизнеса и восстановление после сбоя Концепции непрерывности бизнеса и восстановления после сбоя Действия для обеспечения непрерывности бизнеса и восстановления после сбоя План обеспечения непрерывности бизнеса и план восстановления после сбоя Стандарты обеспечения непрерывности бизнеса и восстановления после сбоя Оценка риска и управление рисками Концепции управления рисками Программы управления рисками Фреймворки для управления рисками Программы управления уязвимостями Сканирование и оценка уязвимостей Оценка угроз и анализ поверхности атаки Анализ поверхности атаки Определение и визуализация поверхности атаки Обнаружения индикаторов воздействия (IoE) Прове-						

Наименование разделов, тем и содержание материала	Виды учебной работы, включая самостоятельную работу обучающихся и трудоемкость (в часах)					
	Контактная работа преподавателя с обучающимися			ИКР	Пром. аттест.	СРС
	Лекции	Практические занятия	Лабораторные работы			
дение симуляции атаки Уменьшение поверхности атаки Анализ поверхности атаки для облаков и IoT Противодействие угрозам с помощью разведки кибер-угроз (Threat Intelligence) Роль разведки кибер-угроз в организации защиты сети Различные типы разведки кибер-угроз Индикаторы разведки кибер-угроз: IoC и AoC Уровни разведки кибер-угроз Использование разведки кибер-угроз для организации проактивной защиты						
Экзамен	-	-	-	1	35	-
ИТОГО по дисциплине	**32** в том числе в форме практической подготовки: 8	-:	**32** в том числе в форме практической подготовки: 8	1	35	44

* реализуется в форме практической подготовки

5 Оценочные средства для проведения текущего контроля и промежуточной аттестации обучающихся по дисциплине (модулю)

Фонды оценочных средств для проведения текущего контроля успеваемости и промежуточной аттестации обсуждаются и утверждаются на заседании кафедры. Полный комплект контрольных заданий или иных материалов, необходимых для оценивания результатов обучения по дисциплине (модулю) хранится на кафедре-разработчике в бумажном или электронном виде, также фонды оценочных средств доступны студентам в личном кабинете – раздел учебно-методическое обеспечение.

6 Учебно-методическое и информационное обеспечение дисциплины (модуля)

6.1 Основная и дополнительная литература

Перечень рекомендуемой основной и дополнительной литературы представлен на сайте университета *www.knastu.ru / Наш университет / Образование / 10.05.03 Информационная безопасность автоматизированных систем / Рабочий учебный план / Реестр литературы*.

6.2 Современные профессиональные базы данных и информационные справочные системы, используемые при осуществлении образовательного процесса по дисциплине

Каждому обучающемуся обеспечен доступ (удаленный доступ), в том числе в случае применения электронного обучения, дистанционных образовательных технологий, к современным профессиональным базам данных и информационным справочным системам, с которыми у университета заключен договор.

Перечень рекомендуемых профессиональных баз данных и информационных справочных систем представлен на сайте университета *www.knastu.ru / Наш университет / Образование / 10.05.03 Информационная безопасность автоматизированных систем / Рабочий учебный план / Реестр ЭБС.*

Актуальная информация по заключенным на текущий учебный год договорам приведена на странице Научно-технической библиотеки (НТБ) на сайте университета

https://knastu.ru/page/3244

6.3 Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины (модуля)

На странице НТБ можно воспользоваться интернет-ресурсами открытого доступа по укрупненной группе направлений и специальностей (УГНС) 10.00.00 Информационная безопасность:

https://knastu.ru/page/539

Название сайта	Электронный адрес
Сайты электронных фондов нормативно-технической документации по строительству	
База данных нормативных документов для строительства бесплатная).	http://www.norm-load.ru
Бесплатная информационно-справочная система онлайн доступа к полному собранию технических нормативно правовых актов РФ.	http://gostrf.com
Техноэксперт. Электронный фонд правовой и нормативно-технической документации.	http://docs.cntd.ru

С целью повышения качества ведения образовательной деятельности в университете создана электронная информационно-образовательная среда. Она подразумевает организацию взаимодействия между обучающимися и преподавателями через систему личных кабинетов студентов, расположенных на официальном сайте университета в информационно-телекоммуникационной сети «Интернет» по адресу https://student.knastu.ru. Созданная информационно-образовательная среда позволяет осуществлять взаимодействие между участниками образовательного процесса посредством организации дистанционного консультирования по вопросам выполнения практических заданий. Материалы данного курса (5 семестр) выложены на портал ДО КнАГУ и организация взаимодействия в рамках данной дисциплины проводится с привлечением дистанционных технологий.

7 Организационно-педагогические условия

Организация образовательного процесса регламентируется учебным планом и расписанием учебных занятий. Язык обучения (преподавания) - русский. Для всех видов аудиторных занятий академический час устанавливается продолжительностью 45 минут.

При формировании своей индивидуальной образовательной траектории обучающийся имеет право на перезачет соответствующих дисциплин и профессиональных модулей, освоенных в процессе предшествующего обучения, который освобождает обучающегося от необходимости их повторного освоения.

7.1 Образовательные технологии

Учебный процесс при преподавании курса основывается на использовании традиционных, инновационных и информационных образовательных технологий. Традиционные образовательные технологии представлены лекциями и семинарскими (практическими) занятиями. Инновационные образовательные технологии используются в виде широкого применения активных и интерактивных форм проведения занятий. Информационные образовательные технологии реализуются путем активизации самостоятельной работы студентов в информационной образовательной среде.

7.2 Занятия лекционного типа

Лекционный курс предполагает систематизированное изложение основных вопросов учебного плана.

На первой лекции лектор обязан предупредить студентов, применительно к какому базовому учебнику (учебникам, учебным пособиям) будет прочитан курс.

Лекционный курс должен давать наибольший объем информации и обеспечивать более глубокое понимание учебных вопросов при значительно меньшей затрате времени, чем это требуется большинству студентов на самостоятельное изучение материала.

7.3 Занятия семинарского типа

Семинарские занятия представляют собой детализацию лекционного теоретического материала, проводятся в целях закрепления курса и охватывают все основные разделы.

Основной формой проведения семинаров является обсуждение наиболее проблемных и сложных вопросов по отдельным темам, а также разбор примеров и ситуаций в аудиторных условиях. В обязанности преподавателя входят: оказание методической помощи и консультирование студентов по соответствующим темам курса.

Активность на семинарских занятиях оценивается по следующим критериям:

· ответы на вопросы, предлагаемые преподавателем;

· участие в дискуссиях;

· выполнение проектных и иных заданий;

· ассистирование преподавателю в проведении занятий.

Ответ должен быть аргументированным, развернутым, не односложным, содержать ссылки на источники.

Доклады и оппонирование докладов проверяют степень владения теоретическим материалом, а также корректность и строгость рассуждений.

Оценивание заданий, выполненных на семинарском занятии, входит в накопленную оценку.

7.4 Самостоятельная работа обучающихся по дисциплине (модулю)

Самостоятельная работа студентов – это процесс активного, целенаправленного приобретения студентом новых знаний, умений без непосредственного участия препода-

вателя, характеризующийся предметной направленностью, эффективным контролем и оценкой результатов деятельности обучающегося.

Цели самостоятельной работы:

· систематизация и закрепление полученных теоретических знаний и практических умений студентов;

· углубление и расширение теоретических знаний;

· формирование умений использовать нормативную и справочную документацию, специальную литературу;

· развитие познавательных способностей, активности студентов, ответственности и организованности;

· формирование самостоятельности мышления, творческой инициативы, способностей к саморазвитию, самосовершенствованию и самореализации;

· развитие исследовательских умений и академических навыков.

Самостоятельная работа может осуществляться индивидуально или группами студентов в зависимости от цели, объема, уровня сложности, конкретной тематики.

Технология организации самостоятельной работы студентов включает использование информационных и материально-технических ресурсов университета.

Контроль результатов внеаудиторной самостоятельной работы студентов может проходить в письменной, устной или смешанной форме.

Студенты должны подходить к самостоятельной работе как к наиважнейшему средству закрепления и развития теоретических знаний, выработке единства взглядов на отдельные вопросы курса, приобретения определенных навыков и использования профессиональной литературы.

7.5 Методические рекомендации для обучающихся по освоению дисциплины

При изучении дисциплины обучающимся целесообразно выполнять следующие рекомендации:

1. Изучение учебной дисциплины должно вестись систематически.

2. После изучения какого-либо раздела по учебнику или конспектным материалам рекомендуется по памяти воспроизвести основные термины, определения, понятия раздела.

3. Особое внимание следует уделить выполнению отчетов по практическим занятиям и индивидуальным комплексным заданиям на самостоятельную работу.

4. Вся тематика вопросов, изучаемых самостоятельно, задается на лекциях преподавателем. Им же даются источники (в первую очередь вновь изданные в периодической научной литературе) для более детального понимания вопросов, озвученных на лекции.

При самостоятельной проработке курса обучающиеся должны:

· просматривать основные определения и факты;

· повторить законспектированный на лекционном занятии материал и дополнить его с учетом рекомендованной по данной теме литературы;

· изучить рекомендованную литературу, составлять тезисы, аннотации и конспекты наиболее важных моментов;

· самостоятельно выполнять задания, аналогичные предлагаемым на занятиях;

· использовать для самопроверки материалы фонда оценочных средств.

8 Материально-техническое обеспечение, необходимое для осуществления образовательного процесса по дисциплине (модулю)

8.1 Лицензионное и свободно распространяемое программное обеспечение, используемое при осуществлении образовательного процесса по дисциплине

Университет обеспечен необходимым комплектом лицензионного и свободно распространяемого программного обеспечения, в том числе отечественного производства. Состав программного обеспечения, необходимого для освоения дисциплины, приведен на сайте университета *www.knastu.ru / Наш университет / Образование / 10.05.03 Информационная безопасность автоматизированных систем / Рабочий учебный план / Реестр ПО.*

Актуальные на текущий учебный год реквизиты / условия использования программного обеспечения приведены на странице ИТ-управления на сайте университета:

https://knastu.ru/page/1928

8.2 Учебно-лабораторное оборудование

Аудитория	Наименование аудитории (лаборатории)	Используемое оборудование
202/5	Лаборатория программно-аппаратных средств защиты информации	СЗИ НСД Secret Net, СЗИ НСД Dallas Lock, СЗИ НСД Страж NT, СЗИ НСД Щит РЖД, СЗИ НСД Аура ,СЗИ НСД Криптон ,СЗИ НСД Аккорд, ФИКС, Ревизор 1,2 как для операционных систем семейства Windows так и для Linux, Ревизор Сети 2.0, Анализатор сетевого траффика Астра,Агент инвентаризации сети,Сканер сетевой безопасности XSpider, Терьер, Secret Net Touch Memory Card, Криптон АМДЗ, Аккорд АМДЗ, КриптоПРО АРМ, ,CryptoPro CSP 3.6, VipNet firewall, Etoken PKI Client, Etoken, Ноутбук с Windows 7+проектор. 16 ПЭВМ на базе процессоров не ниже Intel Pentium IV
319/3	Лаборатория защищенных автоматизированных систем	Dallas Lock 8.0-C номер лицензии 47488-9375-279, Secret Net Studio автономные и сетевые варианты номер лицензии 13A6E7. 8 ПЭВМ, СУБД. Анализатор спектра электро-магнитного поля R&S FSC3, измерительная антенна П6-50, селективный микровольтметр SMV 8.5, SMV 11, генератор тестового акустического сигнала АС-1, система защиты от утечки по виброакустическому каналу Камертон, измеритель шума и вибрации ОКТАВА 110А в комплекте с предусилителем, микрофоном, акселерометром.
201/5	Лаборатория технических средств и методов защиты информации	специализированное оборудование по защите информации от утечки по акустическому каналу и каналу побочных электромагнитных излучений и наводок: Соната АВ с оконечными устройствами (виброизлучатели, акустические излучатели), генератор шума электромагнитного поля ВетоМ, генератор ЛГШ 503, ге-

		нератор Соната РС-1 Технические средства контроля эффективности защиты информации от утечки по указанным каналам: Комплект измерительных антенн Альбатрос 3, селективный микровольтмерт SMV 8,5, селективный микровольтметр SMV 11, комплекс Спрут-мини-А в комплекте с программным обеспечением, Unipan 233, ПЭВМ семества Secret, Поисковый прибор ST033P Пиранья в комплекте с програмнным обеспечением. иное дополнительное оборудование: нелинейный локатор NR-m, генератор сигналов АКИП 3410, комплект измерительных антенн Альбатрос, пробник напряжения СРФ-1, антенны DP-1 и DP-3, генераторы сигналов серии Г3 и Г4. Комплект тестовых программ Зебра для Windows, для МСВС лицензия номер 592

8.3 Технические и электронные средства обучения

Лекционные занятия.

Аудитории для лекционных занятий укомплектованы мебелью и техническими средствами обучения, служащими для представления учебной информации большой аудитории (наборы демонстрационного оборудования (проектор, экран, компьютер/ноутбук), учебно-наглядные пособия, тематические иллюстрации).

Лабораторные занятия *(при наличии).*

Для лабораторных занятий используется аудитория, оснащенная оборудованием, указанным в табл. п. 8.2.

Самостоятельная работа.

Помещения для самостоятельной работы оснащены компьютерной техникой с возможностью подключения к сети «Интернет» и доступом к электронной информационно-образовательной среде КнАГУ:

- зал электронной информации НТБ КнАГУ;
- компьютерные классы факультета.

9 Иные сведения

Методические рекомендации по обучению лиц с ограниченными возможностями здоровья и инвалидов

Освоение дисциплины обучающимися с ограниченными возможностями здоровья может быть организовано как совместно с другими обучающимися, так и в отдельных группах. Предполагаются специальные условия для получения образования обучающимися с ограниченными возможностями здоровья.

Профессорско-педагогический состав знакомится с психолого-физиологическими особенностями обучающихся инвалидов и лиц с ограниченными возможностями здоровья, индивидуальными программами реабилитации инвалидов (при наличии). При необходимости осуществляется дополнительная поддержка преподавания тьюторами, психологами, социальными работниками, прошедшими подготовку ассистентами.

В соответствии с методическими рекомендациями Минобрнауки РФ (утв. 8 апреля 2014 г. N АК-44/05вн) в курсе предполагается использовать социально-активные и рефлексивные методы обучения, технологии социокультурной реабилитации с целью оказания помощи в установлении полноценных межличностных отношений с другими студентами, создании комфортного психологического климата в студенческой группе. Подбор и разработка учебных материалов производятся с учетом предоставления материала в различных формах: аудиальной, визуальной, с использованием специальных технических средств и информационных систем.

Освоение дисциплины лицами с ОВЗ осуществляется с использованием средств обучения общего и специального назначения (персонального и коллективного использования). Материально-техническое обеспечение предусматривает приспособление аудиторий к нуждам лиц с ОВЗ.

Форма проведения аттестации для студентов-инвалидов устанавливается с учетом индивидуальных психофизических особенностей. Для студентов с ОВЗ предусматривается доступная форма предоставления заданий оценочных средств, а именно:

· в печатной или электронной форме (для лиц с нарушениями опорно-двигательного аппарата);

· в печатной форме или электронной форме с увеличенным шрифтом и контрастностью (для лиц с нарушениями слуха, речи, зрения);

· методом чтения ассистентом задания вслух (для лиц с нарушениями зрения).

Студентам с инвалидностью увеличивается время на подготовку ответов на контрольные вопросы. Для таких студентов предусматривается доступная форма предоставления ответов на задания, а именно:

· письменно на бумаге или набором ответов на компьютере (для лиц с нарушениями слуха, речи);

· выбором ответа из возможных вариантов с использованием услуг ассистента (для лиц с нарушениями опорно-двигательного аппарата);

· устно (для лиц с нарушениями зрения, опорно-двигательного аппарата).

При необходимости для обучающихся с инвалидностью процедура оценивания результатов обучения может проводиться в несколько этапов.