

Некоммерческое частное образовательное учреждение высшего образования  
"Невинномысский институт экономики, управления и права"

(НЧОУ ВО "НИЭУП")

УТВЕРЖДАЮ

Проректор по учебной работе



И.П. Мистюкова

27 марта 2024 г.

## Информационная безопасность рабочая программа дисциплины (модуля)

Закреплена за кафедрой	<b>Кафедра экономики и управления</b>	
Учебный план	БВ-24011 38.03.05 -ozfo.plx 38.03.05 Бизнес-информатика, наименование ОПОП (направленность (профиль) программы): Управленческие информационные системы	
Квалификация	<b>бакалавр</b>	
Форма обучения	<b>очно-заочная</b>	
Общая трудоемкость	<b>5 ЗЕТ</b>	
Часов по учебному плану	180	Виды контроля в семестрах:
в том числе:		экзамены 8
аудиторные занятия	36,2	
самостоятельная работа	135	
контактная работа во время промежуточной аттестации (ИКР)		
часов на контроль	8,8	

### Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	8 (4.2)		Итого	
	УП	РП	УП	РП
Неделя	18			
Вид занятий	УП	РП	УП	РП
Лекции	18	18	18	18
Практические	18	18	18	18
Контактная работа при промежуточной аттестации	0,2	0,2	0,2	0,2
В том числе инт.	2	2	2	2
Итого ауд.	36,2	36,2	36,2	36,2
Контактная работа	36,2	36,2	36,2	36,2
Сам. работа	135	135	135	135
Часы на контроль	8,8	8,8	8,8	8,8
Итого	180	180	180	180

Программу составил(и):

д-р техн.наук, доцент, Халкечев К.В.



Рецензент(ы):

Гулин Олег Викторович, генеральный директор ООО ПФ «Вимком-Нев»

Рабочая программа дисциплины

**Информационная безопасность**

разработана в соответствии с ФГОС ВО:

Федеральный государственный образовательный стандарт высшего образования - бакалавриат по направлению подготовки 38.03.05 Бизнес-информатика (приказ Минобрнауки России от 29.07.2020 г. № 838)

составлена на основании учебного плана:

38.03.05 Бизнес-информатика, наименование ОПОП (направленность (профиль) программы): Управленческие информационные системы

утвержденного учёным советом вуза от 27.03.2024 протокол № 8.

Рабочая программа одобрена на заседании кафедры

**Кафедра экономики и управления**

Протокол от 22.03.2024 г. № 8

Зав. кафедрой Мазур Олег Анатольевич



Согласовано с представителями работодателей на заседании МК, протокол № 3 от 25 марта 2024 г.

Председатель МК  И.П. Мистюкова

25 марта 2024 г.

<b>1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)</b>	
1.1	Воспитательная цель - создать условия для воспитания положительного интереса к изучаемой дисциплине "Базы данных".
1.2	Цель формирование у студентов компетенции в соответствии с учебным планом;
1.3	формирование у студентов имитационного мышления, теоретических и практических основ построения экономико-
1.4	-математических моделей и последующего анализа моделируемых экономических систем в целях выработки и принятия обоснованных управленческих решений в области профессиональной деятельности, способных проводить моделирование процессов и си-стем.
1.5	Задачи: ознакомить студентов с сущностью, познавательными возможностями и практическим значением имитационного моделирования как одного из научных методов познания реальности; дать представление о наиболее
1.6	распространённых математических и имитационных ме-годах, используемых в математическом и имитационном моделировании; сформировать устойчивые навыки решения задач математического моделирования и постановки модельного компьютерного эксперимента, проводить моделирование процессов и систем; научить
1.7	интерпретировать результаты имитационного моделирования и применять их для обоснования управленческих решений; сформировать основу для дальнейшего самостоятельного изучения приложений имитационного
1.8	моделирования в процессе профессиональной деятельности зная и понимая основные законы естественнонаучных дисциплин в профессиональной деятельности, применять методы математического анализа и моделирования,
1.9	теоретического и экспериментального исследования.

<b>2. МЕСТО ДИСЦИПЛИНЫ (МОДУЛЯ) В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ</b>	
Цикл (раздел) ОП:	Б1.В
<b>2.1 Требования к предварительной подготовке обучающегося:</b>	
2.1.1	Моделирование бизнес-процессов
2.1.2	Системы поддержки принятия решений
2.1.3	Производственная практика, Технологическая (проектно-технологическая) практика
2.1.4	Управление закупками и снабжением на предприятии
2.1.5	Учет (финансовый учет, управленческий учет, финансовая отчетность)
2.1.6	Экономика предприятия
2.1.7	Электронный бизнес
2.1.8	Документационное обеспечение профессиональной деятельности
<b>2.2 Дисциплины (модули) и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:</b>	
2.2.1	Системы поддержки принятия решений
2.2.2	Производственная практика, Преддипломная практика
2.2.3	Управление ИТ-сервисами и контентом

<b>3. ФОРМИРУЕМЫЕ КОМПЕТЕНЦИИ И ИНДИКАТОРЫ ИХ ДОСТИЖЕНИЯ</b>
<b>ПК-2:</b> Способен управлять контентом предприятия и Интернет-ресурсов, управлять процессами создания и использования информационных сервисов (контент-сервисов), организовывать взаимодействие с клиентами и партнерами в процессе решения задач управления жизненным циклом ИТ-инфраструктуры предприятия
<b>ПК-2.3:</b> Формирует и согласовывает с заинтересованными лицами цели и требования управления информационной безопасностью ресурсов ИТ
<b>ПК-2.4:</b> Организует взаимодействие с клиентами и партнерами в процессе решения задач управления жизненным циклом ИТ-инфраструктуры предприятия, а также по вопросам управления информационной безопасностью ИТ-инфраструктуры предприятия

<p><b>Знать:</b> основные методики моделирования процессов и систем с помощью информационных технологий; технологии для оформления рабочих результатов и результатов научных исследований в виде статей, презентаций, научно-технических отчетов, протоколов мероприятий</p> <p><b>Уметь:</b> проводить моделирование процессов и систем с помощью с помощью информационных технологий; проводить выбор необходимых исходных данных с целью адаптации (изменению) бизнес-процессов заказчика к возможностям типовой информационной системы и программного обеспечения; распространять информацию о ходе выполнения работ</p> <p><b>Владеть:</b> навыками выбора методик моделирования процессов и систем с помощью с помощью информационных технологий; : информационными технологиями для отражения результатов практической деятельности, в том числе научных исследований</p>
--

#### 4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Код занятия	Наименование разделов и тем /вид занятия/	Семестр / Курс	Часов	Компетенции	Литература и эл. ресурсы	Инте ракт.	Примечание
	<b>Раздел 1.</b>						
1.1	Предпосылки становления предметной области информационной безопасности. /Лек/	8	2	ПК-2.3 ПК-2.4	Л1.1 Л1.2Л2.1 Л2.2 Э1 Э2 Э3		Приложение 1
1.2	Сбор данных об информационной системе с помощью средств администрирования Windows (оснасток MMC) /Пр/	8	2	ПК-2.3 ПК-2.4	Л1.1 Л1.2Л2.1 Л2.2 Э1 Э2 Э3	2	Приложение 2
1.3	Предпосылки становления предметной области информационной безопасности. /Ср/	8	14	ПК-2.3 ПК-2.4	Л1.1 Л1.2Л2.1 Л2.2 Э1 Э2 Э3		Приложение 2
1.4	Концепция информационной безопасности Российской Федерации /Лек/	8	1	ПК-2.3 ПК-2.4	Л1.1 Л1.2Л2.1 Л2.2 Э1 Э2 Э3		Приложение 1
1.5	Сбор данных о топологии сети с помощью средства администрирования сетей 3Com Network Supervisor /Пр/	8	1	ПК-2.3 ПК-2.4	Л1.1 Л1.2Л2.1 Л2.2 Э1 Э2 Э3		Приложение 2
1.6	Концепция информационной безопасности Российской Федерации /Ср/	8	14	ПК-2.3 ПК-2.4	Л1.1 Л1.2Л2.1 Л2.2 Э1 Э2 Э3		Приложение 2
1.7	Правовые аспекты информационной безопасности /Лек/	8	2	ПК-2.3 ПК-2.4	Л1.1 Л1.2Л2.1 Л2.2 Э1 Э2 Э3		Приложение 1
1.8	Выявление уязвимостей с помощью Microsoft Baseline Security Analyzer.Настройка локальной политики паролей /Пр/	8	2	ПК-2.3 ПК-2.4	Л1.1 Л1.2Л2.1 Л2.2 Э1 Э2 Э3		Приложение 2
1.9	Правовые аспекты информационной безопасности /Ср/	8	14	ПК-2.3 ПК-2.4	Л1.1 Л1.2Л2.1 Л2.2 Э1 Э2 Э3		Приложение 2
1.10	Виды защищаемой информации /Лек/	8	1	ПК-2.3 ПК-2.4	Л1.1 Л1.2Л2.1 Л2.2 Э1 Э2 Э3		Приложение 1

1.11	Использование сканеров безопасности для получения информации о сети. /Пр/	8	1	ПК-2.3 ПК-2.4	Л1.1 Л1.2Л2.1 Л2.2 Э1 Э2 Э3		Приложение 2
1.12	Виды защищаемой информации /Ср/	8	14	ПК-2.3 ПК-2.4	Л1.1 Л1.2Л2.1 Л2.2 Э1 Э2 Э3		Приложение 2
1.13	Понятие защищенной информационной системы. /Лек/	8	2	ПК-2.3 ПК-2.4	Л1.1 Л1.2Л2.1 Л2.2 Э1 Э2 Э3		Приложение 1
1.14	Использование Microsoft Security Assessment Tool (MSAT). /Пр/	8	2	ПК-2.3 ПК-2.4	Л1.1 Л1.2Л2.1 Л2.2 Э1 Э2 Э3		Приложение 2
1.15	Понятие защищенной информационной системы. /Ср/	8	14	ПК-2.3 ПК-2.4	Л1.1 Л1.2Л2.1 Л2.2 Э1 Э2 Э3		Приложение 2
1.16	Организационно-распорядительные документы в сфере информационной безопасности /Лек/	8	2	ПК-2.3 ПК-2.4	Л1.1 Л1.2Л2.1 Л2.2 Э1 Э2 Э3		Приложение 1
1.17	Использование цифровых сертификатов /Пр/	8	2	ПК-2.3 ПК-2.4	Л1.1 Л1.2Л2.1 Л2.2 Э1 Э2 Э3		Приложение 2
1.18	Организационно-распорядительные документы в сфере информационной безопасности /Ср/	8	14	ПК-2.3 ПК-2.4	Л1.1 Л1.2Л2.1 Л2.2 Э1 Э2 Э3		Приложение 2
1.19	Управление информационными рисками /Лек/	8	2	ПК-2.3 ПК-2.4	Л1.1 Л1.2Л2.1 Л2.2 Э1 Э2 Э3		Приложение 1
1.20	Создание центра сертификации (удостоверяющего центра) в Windows Server 2008. /Пр/	8	2	ПК-2.3 ПК-2.4	Л1.1 Л1.2Л2.1 Л2.2 Э1 Э2 Э3		Приложение 2
1.21	Управление информационными рисками /Ср/	8	14	ПК-2.3 ПК-2.4	Л1.1 Л1.2Л2.1 Л2.2 Э1 Э2 Э3		Приложение 2
1.22	Стандартизация в сфере информационной безопасности /Лек/	8	2	ПК-2.3 ПК-2.4	Л1.1 Л1.2Л2.1 Л2.2 Э1 Э2 Э3		Приложение 1
1.23	Шифрование данных при хранении - EFS. /Пр/	8	2	ПК-2.3 ПК-2.4	Л1.1 Л1.2Л2.1 Л2.2 Э1 Э2 Э3		Приложение 2
1.24	Стандартизация в сфере информационной безопасности /Ср/	8	13	ПК-2.3 ПК-2.4	Л1.1 Л1.2Л2.1 Л2.2 Э1 Э2 Э3		Приложение 2
1.25	Математические модели систем и процессов защиты информации. /Лек/	8	2	ПК-2.3 ПК-2.4	Л1.1 Л1.2Л2.1 Л2.2 Э1 Э2 Э3		Приложение 1
1.26	Управление разрешениями на файлы и папки /Пр/	8	2	ПК-2.3 ПК-2.4	Л1.1 Л1.2Л2.1 Л2.2 Э1 Э2 Э3		Приложение 2

1.27	Математические модели систем и процессов защиты информации. /Ср/	8	12	ПК-2.3 ПК-2.4	Л1.1 Л1.2Л2.1 Л2.2 Э1 Э2 Э3		Приложение 2
1.28	Криптографические методы защиты информации /Лек/	8	2	ПК-2.3 ПК-2.4	Л1.1 Л1.2Л2.1 Л2.2 Э1 Э2 Э3		Приложение 1
1.29	Настройка протокола IPSec /Пр/	8	2	ПК-2.3 ПК-2.4	Л1.1 Л1.2Л2.1 Л2.2 Э1 Э2 Э3		Приложение 2
1.30	Криптографические методы защиты информации /Ср/	8	12	ПК-2.3 ПК-2.4	Л1.1 Л1.2Л2.1 Л2.2 Э1 Э2 Э3		Приложение 2
1.31	/КаттЭ/	8	0,2				
1.32	Экзамен /Экзамен/	8	8,8	ПК-2.3 ПК-2.4	Л1.1 Л1.2Л2.1 Л2.2 Э1 Э2 Э3		Приложение 2

## 5. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

### 5.1. Контрольные вопросы и задания

#### Вопросы к зачету

1. Основы защиты информации
2. Основные понятия и определения информационной безопасности.
3. Угрозы информационной безопасности.
4. Защита информации в вычислительных системах.
5. Нормативно-правовые документы, регламентирующие деятельность в области информационной безопасности.
6. Государственная система защиты информации.
7. Защита информационных и сетевых ресурсов в сетях, подключенных к Интернет.
8. Классификация уязвимостей; подходы определения уязвимостей безопасности сетей; сканеры для проверки уязвимостей фирм ISS, CISCO, NMAP и другие; защита се-тей от компьютерных атак.
9. Программно-технические средства защиты информации
10. Типы шифров.
11. Шифры на основе модифицирования подключей.
12. Несимметричные системы шифрования.
13. Двухключевые шифры.
14. Система открытого распределения ключей.
15. Несимметричные системы шифрования.
16. Цифровая электронная подпись.
17. Хэш-функции на основе блочных шифров.
18. Классификация функций защиты по уровням безопасности, поддерживаемых операционной системой (ОС).
19. Ядро безопасности ОС. Аппаратная основа реализации защиты на уровне ОС.
20. Стандарты по оценке уровня безопасности ОС.

#### Вопросы к экзамену

1. Основы защиты информации
2. Основные понятия и определения информационной безопасности.
3. Угрозы информационной безопасности.
4. Защита информации в вычислительных системах.
5. Нормативно-правовые документы, регламентирующие деятельность в области информационной безопасности.
6. Государственная система защиты информации.
7. Защита информационных и сетевых ресурсов в сетях, подключенных к Интернет.
8. Классификация уязвимостей; подходы определения уязвимостей безопасности сетей; сканеры для проверки уязвимостей фирм ISS, CISCO, NMAP и другие; защита се-тей от компьютерных атак.
9. Программно-технические средства защиты информации
10. Типы шифров.
11. Шифры на основе модифицирования подключей.
12. Несимметричные системы шифрования.
13. Двухключевые шифры.
14. Система открытого распределения ключей.
15. Несимметричные системы шифрования.

16. Цифровая электронная подпись.
17. Хэш-функции на основе блочных шифров.
18. Классификация функций защиты по уровням безопасности, поддерживаемых операционной системой (ОС).
19. Ядро безопасности ОС. Аппаратная основа реализации защиты на уровне ОС.
20. Стандарты по оценке уровня безопасности ОС.
21. Внесение функциональной и информационной избыточности ресурсов на уровне ОС.
22. Способы защиты от несанкционированного использования остаточной информации.
23. Специальные режимы и особенности шифрования данных в режиме реального времени с возможностью мгновенного уничтожения данных.
24. Криптографические методы защиты информации.
25. Типы шифров.
26. Шифры на основе модифицирования подключей.
27. Несимметричные системы шифрования.
28. Двухключевые шифры.
29. Система открытого распределения ключей.
30. Несимметричные системы шифрования.
31. Цифровая электронная подпись.
32. Хэш-функции на основе блочных шифров.
33. Защита информационно-программного обеспечения на уровне операционных систем.
34. Классификация функций защиты по уровням безопасности, поддерживаемых операционной системой (ОС).
35. Ядро безопасности ОС.
36. Аппаратная основа реализации защиты на уровне ОС.
37. Стандарты по оценке уровня безопасности ОС.
38. Внесение функциональной и информационной избыточности ресурсов на уровне ОС.
39. Уничтожение остаточных данных.
40. Способы защиты от несанкционированного использования остаточной информации.
41. Специальные режимы и особенности шифрования данных в режиме реального времени с возможностью мгновенного уничтожения данных.
<b>5.2. Темы письменных работ</b>
не предусмотрено
<b>5.3. Фонд оценочных средств</b>
Оценочные материалы по дисциплине «Информационная безопасность» находятся в приложении 2
<b>5.4. Перечень видов оценочных средств</b>
Перечень видов оценочных средств по дисциплине «Информационная безопасность» находятся в приложении 2

<b>6. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)</b>			
<b>6.1. Рекомендуемая литература</b>			
<b>6.1.1. Основная литература</b>			
	Авторы, составители	Заглавие	Издательство, год
Л1.1	Филиппов, Б. И., Шерстнева, О. Г.	Информационная безопасность. Основы надежности средств связи: учебник	Саратов: Ай Пи Эр Медиа, 2019
Л1.2	Галатенко, В. А.	Основы информационной безопасности: учебное пособие	Москва: Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020
<b>6.1.2. Дополнительная литература</b>			
	Авторы, составители	Заглавие	Издательство, год
Л2.1	Суворова, Г. М.	Информационная безопасность: учебное пособие	Саратов: Вузовское образование, 2019
Л2.2	Шаньгин, В. Ф.	Информационная безопасность и защита информации	Саратов: Профобразование, 2019
<b>6.2. Электронные учебные издания и электронные образовательные ресурсы</b>			
Э1	аналитический ресурс в области ИТ		
Э2	Научная электронная библиотека		
Э3	Информационный портал Betec - «Бизнес-инжиниринговые технологии»		
<b>6.3.1 Лицензионное и свободно распространяемое программное обеспечение, в том числе отечественного производства</b>			
6.3.1.1	Используемое программное обеспечение:		

6.3.1.2	Подписка Azure Dev Tools for Teaching Подписка на программное обеспечение «Azure Dev Tools for Teaching», OrderNumber: ICM-182009, идентификатор подписки: 7562a8d2-e5ab-4243-bfb1-ea70a9eca784, Customer №: 1831121443;
6.3.1.3	Microsoft Office 2016 Лицензия: V0878238 OfficeProPlusEdu ALNG LicSAPk OLV E 1Y Acdmc Ent;
6.3.1.4	Линко 6.5 (сетевая версия) Договор от 16.08.2012 № 4608;
6.3.1.5	Stadia 8.0 Лицензионное соглашение от 20.08.2012;
6.3.1.6	EclipseIDEforJavaEEDevelopers Eclipse Public License - v 1.0;
6.3.1.7	NetBeans (свободно распространяемое программное обеспечение);
6.3.1.8	AndroidStudio (свободно распространяемое программное обеспечение);
6.3.1.9	IntelliJIDEA Соглашение о подписке на toolbox для студентов и преподавателей
6.3.1.10	Версия 4.0, от 1 сентября 2021 г.;
<b>6.3.2 Перечень профессиональных баз данных и информационных справочных систем</b>	
6.3.2.1	<a href="http://www.idc.com">http://www.idc.com</a> / IDC - аналитический ресурс в области ИТ
6.3.2.2	<a href="http://bpms.ru">http://bpms.ru</a> / BPMS.ru - Аналитический ресурс в области ИТ и BPM
6.3.2.3	<a href="http://www.finexpert.ru">http://www.finexpert.ru</a> / - Портал FineXpert.ru
6.3.2.4	<a href="http://www.betec.ru">http://www.betec.ru</a> / - Информационный портал Betec - «Бизнес-инжиниринговые технологии»
6.3.2.5	<a href="http://www.elibrary.ru/">http://www.elibrary.ru/</a> - Научная электронная библиотека
6.3.2.6	Справочно-правовая система «КонсультантПлюс-СК»;
6.3.2.7	Справочно-правовая система «Гарант»

### 7. МТО (оборудование и технические средства обучения)

7.1	учебная аудитория № 302 «Аудитория для проведения занятий лекционного типа, для занятий семинарского типа, для групповых и индивидуальных консультаций, для текущего контроля и промежуточной аттестации» Стол преподавателя, стул преподавателя, доска ученическая, комплект специализированной учебной мебели (ученические столы и стулья), полка навесная для учебно-наглядных пособий и рекомендаций, информационные стенды, портреты выдающихся ученых, телевизионная система, ноутбук с доступом к информационно-коммуникационной сети Интернет и электронной информационно-образовательной среде организации
7.2	учебная аудитория № 310 «Аудитория для проведения занятий лекционного типа, для занятий семинарского типа, для групповых и индивидуальных консультаций, для текущего контроля и промежуточной аттестации»
7.3	Стол преподавателя, стул преподавателя, доска ученическая, комплект специализированной учебной мебели (ученические столы и стулья), интерактивная доска, комплект технических средств обучения (проектор, ноутбук с доступом к информационно-коммуникационной сети Интернет и электронной информационно-образовательной среде организации, колонки для воспроизведения звука), стеллаж офисный для учебно-методических материалов, научной и монографической литературы, информационный стенд
7.4	учебная аудитория № 502 «Лаборатория системного программирования. Полигон учебных баз практик. Аудитория для проведения занятий лекционного типа, для занятий семинарского типа, для групповых и индивидуальных консультаций, для текущего контроля и промежуточной аттестации и итоговой аттестации, для самостоятельной работы, для курсового проектирования (выполнения курсовых работ)»
7.5	Стол преподавателя, стул преподавателя, доска ученическая, комплект специализированной учебной мебели (ученические столы и стулья, компьютерные ученические столы, кресла), колонки для воспроизведения звука (1 шт.), наушники (4 шт.), системный блок ИТТ Ryzen 5 1600/A320/16Gb/120Gb SSD/1Tb HDD/GT 1030 2Gb/mATX 450W (11 шт.), монитор 23.8 AOC 24B2XDM Black (11 шт.), сервер ASUS B560 / Core i7 x8 11700 4.9ГГц/ 250Гб SSD / 2000Гб HDD / 2*16Гб ОЗУ / БП 600W. Монитор Viewsonic 23.6" VA2406-H-2 VA SuperClear, клавиатура (12 шт.), компьютерная мышь (12 шт.). Сетевой маршрутизатор, информационный стенд, сейф. Проектор. Экран. Обеспечен доступ к сети Интернет и в электронную информационную образовательную среду организации.
7.6	специальное помещение № 801 «Помещение для хранения и профилактического обслуживания учебного оборудования»
7.7	Набор инструментов для профилактического обслуживания учебного оборудования, комплектующие для компьютерной и офисной техники

### 8. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

Методические материалы по дисциплине «Информационная безопасность» находится в приложении 3.

#### СПЕЦИАЛЬНЫЕ УСЛОВИЯ ИНВАЛИДАМ И ЛИЦАМ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ

Специальные условия обучения и направления работы с инвалидами и лицами с ограниченными возможностями здоровья (далее - обучающиеся с ограниченными возможностями здоровья) определены на основании:

- Федерального закона от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации»;



- Федерального закона от 24.11.1995 № 181-ФЗ «О социальной защите инвалидов в Российской Федерации»;  
- приказа Министерства науки и высшего образования России от 06.04.2021 № 245 «Об утверждении Порядка организации и осуществления образовательной деятельности по образовательным программам высшего образования – программам бакалавриата, программам специалитета, программам магистратуры»;  
- методических рекомендаций по организации образовательного процесса для обучения инвалидов и лиц с ограниченными возможностями здоровья в образовательных организациях высшего образования, в том числе оснащённости образовательного процесса, утвержденных Минобрнауки России 08.04.2014 № АК-44/05вн).

Под специальными условиями для получения образования обучающихся с ограниченными возможностями здоровья понимаются условия обучения, воспитания и развития таких студентов, включающие в себя использование при необходимости адаптированных образовательных программ и методов обучения и воспитания, специальных учебников, учебных пособий и дидактических материалов, специальных технических средств обучения коллективного и индивидуального пользования, предоставление услуг ассистента (помощника), оказывающего необходимую помощь, проведение групповых и индивидуальных коррекционных занятий, обеспечение доступа в здания вуза и другие условия, без которых невозможно или затруднено освоение образовательных программ обучающихся с ограниченными возможностями здоровья.

Обучение в рамках учебной дисциплины обучающихся с ограниченными возможностями здоровья осуществляется институтом с учетом особенностей психофизического развития, индивидуальных возможностей и состояния здоровья таких обучающихся.

Обучение по учебной дисциплине обучающихся с ограниченными возможностями здоровья может быть организовано как совместно с другими обучающимися, так и в отдельных группах.

В целях доступности обучения по дисциплине обеспечивается:

1) для лиц с ограниченными возможностями здоровья по зрению:

- наличие альтернативной версии официального сайта института в сети «Интернет» для слабовидящих;
- весь необходимый для изучения материал, согласно учебному плану (в том числе, для обучающихся по индивидуальным учебным планам) предоставляется в электронном виде на диске.
- индивидуальное равномерное освещение не менее 300 люкс;
- присутствие ассистента, оказывающего обучающемуся необходимую помощь;
- обеспечение возможности выпуска альтернативных форматов печатных материалов (крупный шрифт или аудиофайлы);
- обеспечение доступа обучающегося, являющегося слепым и использующего собаку-проводника, к зданию института.

2) для лиц с ограниченными возможностями здоровья по слуху:

- наличие микрофонов и звукоусиливающей аппаратуры коллективного пользования (аудиоколонки);

3) для лиц с ограниченными возможностями здоровья, имеющих нарушения опорно-двигательного аппарата, материально-технические условия должны обеспечивать возможность беспрепятственного доступа обучающихся в учебные помещения, столовые, туалетные и другие помещения организации, а также пребывания в указанных помещениях (наличие пандусов, поручней, расширенных дверных проемов и других приспособлений).

Перед началом обучения могут проводиться консультативные занятия, позволяющие студентам с ограниченными возможностями адаптироваться к учебному процессу.

В процессе ведения учебной дисциплины профессорско-преподавательскому составу рекомендуется использование социально-активных и рефлексивных методов обучения, технологий социокультурной реабилитации с целью оказания помощи обучающимся с ограниченными возможностями здоровья в установлении полноценных межличностных отношений с другими обучающимися, создании комфортного психологического климата в учебной группе.

Особенности проведения текущей и промежуточной аттестации по дисциплине для обучающихся с ограниченными возможностями здоровья устанавливаются с учетом индивидуальных психофизических особенностей (устно, письменно на бумаге, письменно на компьютере, в форме тестирования и другое). При необходимости предоставляется дополнительное время для подготовки ответа на экзамене и зачете.