МИНОБРНАУКИ РОССИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ОБРАЗОВАНИЯ
«УДМУРТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
ФИЛИАЛ ФГБОУ ВО «УДГУ» В Г. ВОТКИНСКЕ
СРЕДНЕЕ ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАНИЕ

«УТВЕРЖДАЮ»
Зам. директора по УМР

В.Н. Бралгина

«23» марта 2023г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

ОП.10 Информационная безопасность

09.02.07 «Информационные системы и программирование»
Квалификация выпускника
Специалист по информационным системам

Утверждена на заседании кафедры «Информационных и инженерных технологий»	Протокол №7 от 14.03.23		Заведующий кафедрой О.В. Мамрыкин
Утверждена на заседании научно-методического совета	Протокол №3 от 21.03.23		Председатель Т.М. Смирнова

Воткинск 2023г.

1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ

ОП.10 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

1.1. Область применения программы

Рабочая программа дисциплины является частью основной образовательной программы в соответствии с ФГОС для специальности: *09.02.07 Информационные системы и программирование* для обучающихся *очной* формы обучения.

Рабочая программа разработана в соответствии с ФГОС среднего общего образования, с учетом примерной программы общеобразовательной учебной дисциплины Физика, рекомендованной ФГАУ «Федеральный институт развития образования» в качестве примерной программы для реализации основной профессиональной образовательной программы СПО на базе основного общего образования с получением среднего общего образования (Протокол № 3 от «21» июля 2015 г.).

1.2. Место учебной дисциплины в структуре программы подготовки специалистов среднего звена:

Учебная дисциплина ОП.10 «Информационная безопасность» относится к циклу общепрофессиональных дисциплин программы подготовки специалистов среднего звена.

1.3. Цель и задачи учебной дисциплины – требования к результатам освоения учебной дисциплины:

В результате освоения учебной дисциплины обучающийся должен уметь:

- выбирать средства обеспечения информационной безопасности информационной системы современного предприятия;
- ограничивать использование ресурсов компьютера на основе раздельного доступа пользователей в операционную систему;
- организовывать защиту информации в локальной сети на уровнях входа в сеть и системы прав доступа;
- организовывать безопасную работу в Интернет и отправку почтовых сообщений в глобальной сети;
- использовать средства защиты данных от разрушающих программных воздействий компьютерных вирусов;
- проводить базовые работы по профилактике нарушений информационной безопасности и построению защищенных информационных систем с использованием стандартных аппаратно-программных решений.

В результате освоения учебной дисциплины обучающийся должен знать:

- вопросы административного и нормативно-правового обеспечения защиты информации;
- основные системы защиты информации в России и в ведущих зарубежных странах;
- основные программно-аппаратные средства и методы защиты информации в компьютерных системах.

1.4. Перечень формируемых компетенций:

В результате освоения учебной дисциплины у обучающегося формируются:

Код	Наименование компетенций
ОК 01.	Выбирать способы решения задач профессиональной деятельности применительно к различным контекстам;
ОК 02.	Использовать современные средства поиска, анализа и интерпретации информации и информационные технологии для выполнения задач профессиональной деятельности;
ОК 04.	Эффективно взаимодействовать и работать в коллективе и команде;
ОК 05.	Осуществлять устную и письменную коммуникацию на государственном языке Российской Федерации с учетом особенностей социального и культурного контекста;
ОК 09.	Пользоваться профессиональной документацией на государственном и иностранном языках.
ПК 2.5	Производить инспектирование компонент программного обеспечения на предмет соответствия стандартам кодирования.
ПК 5.3	Разрабатывать подсистемы безопасности информационной системы в соответствии с техническим заданием.

1.5. Рекомендуемое количество часов на освоение рабочей программы учебной дисциплины (по ФГОС):

Максимальная учебная нагрузка обучающегося 100 часов, в том числе:
- обязательная аудиторная учебная нагрузка 91 час,
- самостоятельная работа обучающегося 9 часов.

2. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

2.1. Объем учебной дисциплины и виды учебной работы

Вид учебной работы	**Объем часов**
Максимальная учебная нагрузка (всего)	100
Обязательная аудиторная учебная нагрузка (всего)	91
в том числе:	
лекции	39
практические занятия	52
контрольные работы	
Самостоятельная работа обучающегося (всего)	9
Итоговая аттестация в форме *Дифференцированного зачета* в 6 семестре	

2.2. Тематический план и содержание дисциплины

Наименование разделов и тем	Содержание учебного материала, практические занятия и лабораторные работы, самостоятельная работа студента		Объем часов	Уровень освоения
1	**2**		**4**	**4**
Введение	**Содержание**		4	
	1.	Введение в проблему информационной безопасности, ее актуальность.		*2*
	2.	Основные объекты информационных систем, подлежащих защите. Цели и задачи обеспечения информационной безопасности для различных объектов (правоохранительные органы, медицинские учреждения, коммерческие организации и др.)		*2*
Раздел 1 Комплексный подход к обеспечению информационной безопасности			**29**	
Тема 1.1 Понятие и составляющие информационной безопасности	**Содержание**		4	
	1.	Основные понятия информационной безопасности.		*1*
	2.	Основные составляющие информационной безопасности: конфиденциальность, целостность, доступность.		*1*
	3.	Комплексный подход к защите информации. Уровни формирования режима информационной безопасности: законодательный, административный, процедурный и программно-технический.		*1*
	4.	Требования к комплексным системам защиты информации.		*1*
	Самостоятельная работа		1	
	1.	Проанализировать профессионально – значимые источники информации с точки зрения основных аспектов: конфиденциальности, целостности и доступности.		
Тема 1.2 Угрозы информационной безопасности в компьютерных системах	**Содержание**		3	
	1.	Компьютерная система как объект защиты информации.		*1*
	2.	Понятие угрозы информационной безопасности в компьютерных системах.		*2*
	3.	Классификация и общий анализ угроз информационной безопасности в компьютерных системах.		*2*
	4.	Случайные угрозы информационной безопасности.		*2*
	5.	Преднамеренные угрозы информационной безопасности		*2*
	Самостоятельная работа		1	

	1.	Для выбранного объекта защиты информации (например, почтовый сервер, одиночно стоящий компьютер в бухгалтерии, телефонная база ограниченного пользования на электронных носителях и др.) провести анализ защищенности объекта по следующим пунктам: вид угроз, характер происхождения угроз, классы каналов несанкционированного получения информации, источники появления угроз, причины нарушения целостности информации, потенциально возможные злоумышленные действия; определить класс защиты информации.		
Тема 1.3 Законодательный уровень информационной безопасности	**Содержание**		4	
	1.	Значимость уровня в комплексном подходе. Меры законодательного уровня.		*2*
	2.	Законодательная и нормативно – правовая база РФ в области информатизации и защиты информации.		*3*
	3.	Ответственность за нарушение законодательства в информационной сфере.		*2*
	4.	Обзор зарубежного законодательства в области информационной безопасности.		*3*
	Практические занятия		8	
	1.	Изучение Доктрины информационной безопасности Российской Федерации.		
	2.	Изучение основных законов в области информационной безопасности.		
	Самостоятельная работа		1	
	1.	Составить перечень основный понятий и определений, используемых в нормативно – правовых документах.		
Тема 1.4 Административный уровень информационной безопасности	**Содержание**		4	
	1.	Основные понятия.		*2*
	2.	Политика безопасности.		*2*
	3.	Программа безопасности.		*2*
	4.	Синхронизация программы безопасности с жизненным циклом систем.		*2*
Тема 1.5 Процедурный уровень информационной безопасности	**Содержание**		2	
	1.	Основные классы мер процедурного уровня.		*2*
	2.	Управление персоналом.		*2*
	3.	Физическая защита.		*2*
	4.	Поддержание работоспособности.		*2*
	5.	Реагирование на нарушения режима безопасности.		*2*
	6.	Планирование восстановительных работ.		*2*
Тема 1.6	**Содержание**		1	

Программно-технический уровень информационной безопасности	1.	Основные понятия и меры уровня.		*2*
	2.	Особенности современных информационных систем.		*2*
	3.	Архитектурная безопасность.		*2*
Раздел 2 Методы и средства обеспечения безопасности информации			**39**	
Тема 2.1 Защита информации от утечки по техническим каналам	**Содержание**		4	
	1.	Основные виды технических каналов утечки информации. Техника промышленного шпионажа.		*2*
	2.	Противодействие наблюдению.		*2*
	3.	Противодействие прослушиванию.		*2*
	4.	Методы и средства защиты от побочных электромагнитных излучений и наводок.		*2*
Тема 2.2 Защита информации от несанкционированного доступа	**Содержание**		6	
	1.	Способы несанкционированного доступа к информации в компьютерных системах.		*2*
	2.	Характеристика средств защиты информации в компьютерных системах от несанкционированного доступа.		*2*
	3.	Идентификация и аутентификация пользователей: основные понятия, парольная аутентификация, виды паролей, биометрическая аутентификация.		*2*
	4.	Управление доступом: основные понятия, мандатного и ролевого управления доступом виды разграничения доступа, особенности дискреционного,		*2*
	5.	Защита программных средств от несанкционированного копирования и исследования.		*2*
	6.	Протоколирование и аудит: основные понятия, активный аудит.		*2*
	7.	Общая характеристика компонентов системы защиты операционной системы Windows XP.		*3*
	8.	Защита информации от несанкционированного доступа в операционных системах семейства Unix.		*2*
	Практические занятия		12	
	1.	Методы аутентификации, использующие пароли.		
	2.	Изучение политики безопасности операционной системы Windows XP.		
	3.	Управление шаблонами безопасности в Windows 2000 (XP).		
	4.	Разграничение полномочий и доступа к объектам операционной системы Unix.		
	5.	Построение системы разграничения доступа в базе данных на основе ролевой модели.		
	Самостоятельная работа		1	

	1.	Рассмотреть неотъемлемые характеристики человека и особенности поведения, используемые при биометрической аутентификации пользователей.		
Тема 2.3 Криптографические методы защиты информации	**Содержание**		4	
	1.	Развитие криптографических систем. Основные понятия криптологии.		*2*
	2.	Классификация криптографических средств.		*2*
	3.	Симметричные криптосистемы: DES и ее модификации, ГОСТ 28147 – 89, принципы их построения.		*2*
	4.	Ассиметричные криптосистемы: однонаправленные функции, RSA, принципы построения.		*2*
	5.	Методы шифрования: замены, перестановки, аналитические, аддитивные, комбинированные.		*2*
	6.	Функция хэширования.		*2*
	7.	Электронная цифровая подпись и ее применение для контроля целостности программ и данных.		*2*
	8.	Компьютерная стеганография и ее применение.		*2*
	Практические занятия		11	
	1.	Использование функций криптографического интерфейса (CryptoAPI) операционной системы Windows для защиты информации.		
	2.	Шифрующая файловая система EFS и управление сертификатами в Windows (2000) XP.		
	Самостоятельная работа		1	
	1.	Рассмотреть особенности и принципы работы стандартных и специализированных программных средств шифрования и компьютерной стеганографии.		
Раздел 3 Компьютерные вирусы и средства антивирусной защиты			**14**	
Тема 3.1 Вирусы как угроза ИБ	**Содержание**		3	
	1.	Общие сведения о компьютерных вирусах.		1
	2.	Классификация компьютерных вирусов.		1
	3.	Жизненный цикл вирусов.		*3*
	4.	Основные каналы распространения вирусов.		*3*
	5.	Вредоносные программы и их классификация.		*3*
	Самостоятельная работа		2	
	1.	Разработать контролирующий, диагностический или демонстрационный материал по теме 3.1 (кроссворд, тест, ребусы, презентация и др.).		
Тема 3.2 Средства	**Содержание**		2	

антивирусной защиты	1.	Методы и средства защиты от компьютерных вирусов.		*1*
	2.	Методы обнаружения и удаления вирусов.		*1*
	3.	Профилактика заражения вирусами компьютерных систем.		*1*
	4.	Программные закладки и методы защиты от них.		*2*
	5.	Антивирусные программные комплексы.		*3*
	Практические занятия			
	1.	Антивирусные программные комплексы.	6	
	2.	Восстановление зараженных файлов. Профилактика проникновения «троянских программ».		
	Самостоятельная работа			
	1.	Построить схему системы антивирусной защиты корпоративной сети (на примере).	1	
Раздел 4 Стандарты защищенности информации в компьютерных системах			**14**	
Тема 4.1 Стандарты и спецификации в области информационной безопасности	**Содержание**			
	1.	Характеристика систем стандартизации в области защиты информации.		*2*
	2.	Оценочные стандарты и технические спецификации: «Оранжевая книга».		*3*
	3.	Информационная безопасность распределенных систем. Рекомендации X.800.	2	*3*
	4.	Стандарт ISO/IEC 15408 «Критерии оценки безопасности информационных технологий».		*3*
	5.	Европейские критерии безопасности информационных технологий.		*3*
	6.	Документы Гостехкомиссии России по защите информации.		*3*
	Практические занятия			
	1.	Для выбранного объекта защиты информации предложить анализ увеличения защищенности по следующим пунктам: определить требования к защите информации, определить факторы, влияющие на требуемый уровень защиты информации, выбрать или разработать способы и средства защиты информации, построить архитектуру систем защиты информации, сформулировать рекомендации по увеличению уровня защищенности.	11	
	Самостоятельная работа			
	1.	Составить перечень понятий и определений, используемых в стандартах и спецификациях.	1	
		Всего:	**100**	

Для характеристики уровня освоения учебного материала используются следующие обозначения:

1 – **ознакомительный** (узнавание ранее изученных объектов, свойств);

2– **репродуктивный** (выполнение деятельности по образцу, инструкции или под руководством)

3 – **продуктивный (**планирование и самостоятельное выполнение деятельности, решение проблемных задач)

3. УСЛОВИЯ РЕАЛИЗАЦИИ УЧЕБНОЙ ДИСЦИПЛИНЫ

3.1. Требования к минимальному материально-техническому обеспечению

Реализация учебной дисциплины требует наличия учебного кабинета программирования и баз данных.
Оборудование: Доска универсальная, 5-ти секционная, Комплект учебной мебели, набор демонстрационного оборудования (проектор, экран), учебно-наглядные пособия (презентации по дисциплине), 16 компьютеров с выходом в сеть Интернет и в ЭИОС вуза
Программное обеспечение: Kaspersky Endpoint Security, Microsoft Office, Microsoft Windows.

3.2. Информационное обеспечение обучения

Перечень рекомендуемых учебных изданий, Интернет-ресурсов, дополнительной литературы

Основные источники:

1. Внуков, А. А. Основы информационной безопасности: защита информации : учебное пособие для среднего профессионального образования / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2021. — 161 с. — (Профессиональное образование). — ISBN 978-5-534-13948-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/475890 (дата обращения: 04.10.2021).
2. Галатенко, В. А. Основы информационной безопасности : учебное пособие / В. А. Галатенко. — 3-е изд. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. — 266 с. — ISBN 978-5-4497-0675-1. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: https://www.iprbookshop.ru/97562.html
3. Суворова, Г. М. Основы информационной безопасности : учебное пособие для СПО / Г. М. Суворова. — Саратов : Профобразование, 2021. — 135 с. — ISBN 978-5-4488-1294-1. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: https://www.iprbookshop.ru/108005.html

Дополнительные источники:

1. Камалова, Г. Г. Информационное право в схемах, определениях и заданиях : учеб. пособие / Г. Г. Камалова, М-во образования и науки РФ, ФГБОУ ВО "Удмуртский государственный университет", Ин-т права, соц. упр. и безопасности, Каф. криминалистики и судеб. экспертиз. - Ижевск : Удмуртский университет, 2017.
2. Мэйволд, Э. Безопасность сетей : учебное пособие для СПО / Э. Мэйволд. — Саратов : Профобразование, 2021. — 571 с. — ISBN 978-

5-4488-0990-3. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: https://www.iprbookshop.ru/102183.html
3. Мельников, В.П. Информационная безопасность: учебник для СПО/ В.П. Мельников В.П.; под ред. Куприянова А.И.-Москва: Кнорус, 2018
4. Новожилов, О. П. Информатика в 2 ч. Часть 1 : учебник для среднего профессионального образования / О. П. Новожилов. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2021. — 320 с. — (Профессиональное образование). — ISBN 978-5-534-06372-1. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/474161
5. Прохорова О.В. Информационная безопасность и защита Новожилов, О. П. Информатика в 2 ч. Часть 2 : учебник для среднего профессионального образования / О. П. Новожилов. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2021. — 302 с. — (Профессиональное образование). — ISBN 978-5-534-06374-5. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/474162
6. Костин, В. Н. Методы и средства защиты компьютерной информации: информационная безопасность компьютерных сетей : учебное пособие / В. Н. Костин. — Москва : Издательский Дом МИСиС, 2018. — 31 с. — ISBN 978-5-906953-53-7. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: https://www.iprbookshop.ru/98200.html
7. Фаронов, А. Е. Основы информационной безопасности при работе на компьютере : учебное пособие / А. Е. Фаронов. — 3-е изд. — Москва, Саратов : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. — 154 с. — ISBN 978-5-4497-0338-5. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: https://www.iprbookshop.ru/89453.html
8. Фомин Д.В. Информационная безопасность и защита информации: специализированные аттестованные программные и программно-аппаратные средства [Электронный ресурс] : учебно-методическое пособие / Д.В. Фомин. — Электрон. текстовые данные. — Саратов: Вузовское образование, 2018. — 218 c. — 978-5-4487-0297-6. — Режим доступа: http://www.iprbookshop.ru/77317.html
9. Шаньгин, В. Ф. Информационная безопасность и защита информации / В. Ф. Шаньгин. — 2-е изд. — Саратов : Профобразование, 2019. — 702 с. — ISBN 978-5-4488-0070-2. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: https://www.iprbookshop.ru/87995.html
10. Шаньгин, В.Ф. Комплексная защита информации в корпоративных системах: учеб. пособие/В.Ф. Шаньгин.-Москва: Форум: Инфра-м, 2018

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

Контроль и оценка результатов освоения учебной дисциплины осуществляется преподавателем в процессе проведения практических занятий и лабораторных работ, тестирования, а также выполнения обучающимися индивидуальных заданий, проектов, исследований.

Оценка качества освоения учебной программы включает текущий контроль успеваемости, промежуточную аттестацию по итогам освоения дисциплины.

Текущий контроль проводится в форме устного опроса.

3 Система оценивания комплекта ФОС текущего контроля и промежуточной аттестации

При оценивании практической и самостоятельной работы студента учитывается следующее:

- *качество выполнения практической части работы;*
- *качество оформления контрольной работы;*
- *качество устных ответов на контрольные вопросы при защите работы.*

Каждый вид работы оценивается по пяти бальной шкале.

«5» (отлично) – за глубокое и полное овладение содержанием учебного материала, в котором обучающийся свободно и уверенно ориентируется; за умение практически применять теоретические знания, высказывать и обосновывать свои суждения. Оценка «5» (отлично) предполагает грамотное и логичное изложение ответа.

«4» (хорошо) – если обучающийся полно освоил учебный материал, владеет научно-понятийным аппаратом, ориентируется в изученном материале, осознанно применяет теоретические знания на практике, грамотно излагает ответ, но содержание и форма ответа имеют отдельные неточности.

«3» (удовлетворительно) – если обучающийся обнаруживает знание и понимание основных положений учебного материала, но излагает его неполно, непоследовательно, допускает неточности, в применении теоретических знаний при ответе на практико-ориентированные вопросы; не умеет доказательно обосновать собственные суждения.

«2» (неудовлетворительно) – если обучающийся имеет разрозненные, бессистемные знания, допускает ошибки в

определении базовых понятий, искажает их смысл; не может практически применять теоретические знания.

Тест оценивается по пяти бальной шкале следующим образом: за правильный ответ студент получает 1 балл. За неверный ответ или его отсутствие ответа баллы не начисляются.

Оценка «5» соответствует 86% – 100% правильных ответов.

Оценка «4» соответствует 73% – 85% правильных ответов.

Оценка «3» соответствует 53% – 72% правильных ответов.

Оценка «2» соответствует 0% – 52% правильных ответов.

Критерии оценивания устного ответа:

– оценка «отлично» ставится в случае, если студент демонстрирует прекрасное знание материала, умение оперировать основными понятиями, определениями и может уверенно, последовательно, грамотно и логически стройно, исчерпывающе изложить в своем ответе материал, касающийся затронутой темы, не затрудняясь с ответом при видоизменении задания, умеет самостоятельно обобщать материал;

– оценка «хорошо» ставится за хорошее знание студентом материала по теме, умение ясно и чѐтко осветить рассматриваемый материал, однако его ответ содержит некоторые незначительные неточности, студент во время изложения материала не вполне уверенно рассказывает о некоторых деталях вопроса, и поэтому его ответ остается недостаточно четким и исчерпывающим;

– оценка «удовлетворительно» выставляется в случае, если студент в целом знает рассматриваемую тему, в основном верно отвечает на поставленные вопросы, однако его ответ содержит существенные ошибки, неточности, а сам студент демонстрирует заметные пробелы в знаниях по курсу;

– оценка «неудовлетворительно» выставляется в случае, если студент не в состоянии более или менее чѐтко и внятно изложить материал, его ответ

содержит настолько грубые ошибки, существенные неточности, что тема рассматриваемого вопроса остается на деле нераскрытой; кроме того, студент демонстрирует очень существенные пробелы в знании или полное незнание рассматриваемой темы и совершенное неумение пользоваться еѐ методами.

Критерии оценивания (конспект урока, контрольная, практическая)

1. Оценка «**отлично»** выставляется при условии, что студент полностью выполнил задание и проявил отличные знания учебного материала. При этом работа оформлена в соответствии с требованиям, к ней можно предъявить минимум замечаний.
2. **«Хорошо»** ставится тогда, когда студент выполнил все задания, показал хорошие знания по пройденному материалу, но есть недочеты в оформлении работы и общие небольшие замечания, не влияющие на ее качество.
3. Оценку «**удовлетворительно»** студент получает за полностью выполненное задание при наличии в ней существенных неточностей и недочетов, не умении студента верно применить полученные знания, в оформлении работы есть нарушения, не аргументированные ответы, неактуальные или ненадежные источники информации.

4. **«Неудовлетворительно»** студент получает в том случае, когда он не полностью выполнил задание проявил недостаточный уровень знаний, не смог объяснить полученные результаты. Такая работа не отвечает требованиям, содержит противоречивые сведения.

5. ОСОБЕННОСТИ ОРГАНИЗАЦИИ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ ДЛЯ ИНВАЛИДОВ И ЛИЦ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ

Реализация дисциплины для лиц с ограниченными возможностями здоровья осуществляется с учетом особенностей психофизического развития, индивидуальных возможностей и состояния здоровья таких обучающихся.

Для маломобильных групп населения имеется необходимое материально-техническое обеспечение (пандусы, оборудованные санитарные комнаты, кнопки вызова персонала, оборудованные аудитории для лекционных и практических занятий)

Для адаптации программы освоения дисциплины используются следующие методы:

- Для лиц с нарушениями слуха используются методы визуализации информации (презентации, использование компьютера для передачи текстовой информации и др.)
- Для лиц с нарушениями зрения используются такие методы, как увеличение текста и картинки (в программах Windows), программы-синтезаторы речи, в том числе в ЭБС.

Форма проведения текущей и промежуточной аттестации для инвалидов и лиц с ограниченными возможностями здоровья устанавливается с учетом индивидуальных психофизических особенностей (устно, письменно на бумаге, письменно на компьютере, в форме тестирования и т.п.), при необходимости выделяется дополнительное время на подготовку.