



МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное бюджетное образовательное учреждение
высшего образования
МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ГЕОДЕЗИИ И КАРТОГРАФИИ
(МИИГАиК)

Факультет геоинформатики и информационной безопасности
Кафедра информационно-измерительных систем



**ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ**

Сертификат: 5387FD2AF5B17FED816FDE9A1D4973B1
Владелец: Степанченко Алексей Леонидович
Действителен: с 21.07.2025 по 14.10.2026

«УТВЕРЖДАЮ»

Проректор
А. Л. Степанченко
16 февраля 2024 г.

**РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)
«Б1.О.20 МЕТОДЫ И СРЕДСТВА КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ
ИНФОРМАЦИИ»**

Уровень высшего образования: бакалавриат

Направление подготовки: 09.03.02 Информационные системы и технологии

Направленность(профиль) подготовки: Информационные системы и технологии

Квалификация (степень) выпускника: бакалавр

Форма обучения: очная

Год набора (приема на обучение): 2024

Срок получения образования: 4 года

Объем:
в зачетных единицах: 3 з.е.
в академических часах: 108 ак.ч.

Москва, 2024

Разработчики:

Декан факультета кафедры Информационно-измерительных систем, д.т.н. Матерухин А. В.

Старший преподаватель кафедры
Информационно-измерительных систем Бельшева Ю. В.

Преподаватель кафедры Информационно-измерительных систем
Калмыков С. А.

Рабочая программа дисциплины (модуля) составлена в соответствии с требованиями ФГОС ВО по направлению подготовки 09.03.02 Информационные системы и технологии, утвержденного приказом Минобрнауки от 19.09.2017 № 926

Согласование и утверждение

№	Подразделение	Ответственное лицо	ФИО	Виза	Дата, протокол (при наличии)
1	факультет Геоинформатики и информационной безопасности	Председатель ученого совета факультета	Матерухин А. В.	Рассмотрено	14.12.2023, № 7-23

Содержание

1. Цель и задачи освоения дисциплины (модуля)
2. Планируемые результаты обучения по дисциплине (модулю), соотнесенные с планируемыми результатами освоения образовательной программы
3. Место дисциплины в структуре ОП
4. Объем дисциплины и виды учебной работы
5. Содержание дисциплины
 - 5.1. Разделы, темы дисциплины и виды занятий
 - 5.2. Содержание разделов, тем дисциплины и формы текущего контроля
6. Оценочные материалы текущего контроля
7. Оценочные материалы промежуточной аттестации
8. Порядок проведения промежуточной аттестации
9. Материально-техническое и учебно-методическое обеспечение дисциплины
 - 9.1. Перечень основной и дополнительной учебной литературы
 - 9.2. Профессиональные базы данных и ресурсы «Интернет», к которым обеспечивается доступ обучающихся
 - 9.3. Программное обеспечение и информационно-справочные системы, используемые при осуществлении образовательного процесса по дисциплине
 - 9.4. Оборудование и технические средства обучения
10. Методические указания по освоению дисциплины (модуля)

1. Цель и задачи освоения дисциплины (модуля)

Цель освоения дисциплины - формирование у обучающихся профессиональных компетенций в области теоретических основ и практических методов криптографической защиты информации, применения современных криптографических алгоритмов и протоколов для обеспечения конфиденциальности, целостности и аутентичности данных в информационных системах

Задачи изучения дисциплины:

- изучение понятийного аппарата и нормативно-правовых основ криптографической защиты информации, включая базовые принципы обеспечения информационной безопасности в информационных системах;
- освоение теоретических основ криптографии и криптоанализа, современных симметричных и асимметричных алгоритмов шифрования, хэширования, электронной подписи и криптографических протоколов;
- формирование практических навыков применения криптографических средств защиты информации при проектировании, разработке и эксплуатации информационных систем, включая настройку и использование программно-аппаратных средств криптографической защиты.

2. Планируемые результаты обучения по дисциплине (модулю), соотнесенные с планируемыми результатами освоения образовательной программы

Компетенции, индикаторы и результаты обучения

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

ОПК-3.1 Готовит обзоры, аннотации, составляет рефераты, научные доклады, публикации и библиографии по научно-исследовательской работе с учетом требований информационной безопасности

Знать:

ОПК-3.1/Зн1 основные сведения об объектах и процессах профессиональной деятельности

Уметь:

ОПК-3.1/Ум1 пользоваться методиками сбора и систематизации информации

Владеть:

ОПК-3.1/Нв1 навыками формальной постановки и решения задачи обеспечения информационной безопасности компьютерных систем

3. Место дисциплины в структуре ОП

Дисциплина (модуль) Б1.О.20 «Методы и средства криптографической защиты информации» относится к обязательной части образовательной программы и изучается в семестре(ах): 5.

В процессе изучения дисциплины студент готовится к решению типов задач профессиональной деятельности, предусмотренных ФГОС ВО и образовательной программой.

4. Объем дисциплины (модуля) и виды учебной работы

Период обучения	Общая трудоемкость (часы)	Общая трудоемкость (ЗЕТ)	Лекционные занятия (часы)	Практические занятия (часы)	Самостоятельная работа (часы)	Промежуточная аттестация (часы)
5 семестр	108	3	34	34	40	Зачет с оценкой
Всего	108	3	34	34	40	

5. Содержание дисциплины (модуля)

5.1. Разделы, темы дисциплины и виды занятий (часы промежуточной аттестации не указываются)

Наименование раздела, темы	Всего	Лекционные занятия	Практические занятия	Самостоятельная работа	Планируемые результаты с обучения, соответствующие результатам освоения программы
Раздел 1. Математические основы криптографии	28	8	9	11	ОПК-3.1
Тема 1.1. Программные реализации шифров	13	4	4	5	
Тема 1.2. Методы получения случайных и псевдослучайных последовательностей	15	4	5	6	
Раздел 2. Симметричные методы	31	9	9	13	ОПК-3.1
Тема 2.1. Криптографическая стойкость шифров	11	3	3	5	
Тема 2.2. Имитостойкость и помехоустойчивость шифров	9	3	3	3	
Тема 2.3. Блочные методы шифрования	11	3	3	5	
Раздел 3. Асимметричные методы	28	9	10	9	ОПК-3.1
Тема 3.1. Асимметричные методы шифрования	14	4	6	4	
Тема 3.2. Битовая стойкость алгоритма RSA	14	5	4	5	
Раздел 4. Методы контроля целостности	21	8	6	7	ОПК-3.1
Тема 4.1. Функции хэширования	10	4	3	3	

Тема 4.2. Электронная цифровая подпись	11	4	3	4	
Итого	108	34	34	40	

5.2. Содержание разделов, тем дисциплин и формы текущего контроля

Раздел 1. Математические основы криптографии

Тема 1.1. Программные реализации шифров

Принципы программной реализации криптографических алгоритмов. Использование библиотек криптографии. Вопросы производительности и безопасности программного кода. Типовые уязвимости при реализации шифров

Текущий контроль

Вид (форма) контроля
Тестирование

Тема 1.2. Методы получения случайных и псевдослучайных последовательностей

Источники энтропии. Генераторы истинно случайных чисел. Псевдослучайные генераторы и их свойства. Критерии оценки качества случайных последовательностей

Текущий контроль

Вид (форма) контроля
Тестирование

Раздел 2. Симметричные методы

Тема 2.1. Криптографическая стойкость шифров

Понятие криптостойкости. Модели атак на шифры. Полный перебор ключей и аналитические методы криптоанализа. Оценка сложности взлома алгоритмов

Текущий контроль

Вид (форма) контроля
Тестирование

Тема 2.2. Имитостойкость и помехоустойчивость шифров

Понятие имитостойкости. Методы защиты от подмены и модификации данных. Контроль целостности сообщений. Основы помехоустойчивого кодирования

Текущий контроль

Вид (форма) контроля
Тестирование

Тема 2.3. Блочные методы шифрования

Принципы построения блочных шифров. Сети Фейстеля и подстановочно-перестановочные сети. Режимы работы блочных шифров. Практическое применение блочного шифрования

Текущий контроль

Вид (форма) контроля

Тестирование

Раздел 3. Асимметричные методы

Тема 3.1. Асимметричные методы шифрования

Принципы открытого и закрытого ключа. Алгоритмы на основе сложности факторизации и дискретного логарифмирования. Управление ключами. Области применения асимметричной криптографии

Текущий контроль
Вид (форма) контроля
Тестирование

Тема 3.2. Битовая стойкость алгоритма RSA

Математические основы алгоритма RSA. Зависимость стойкости от длины ключа. Анализ атак на RSA. Практические рекомендации по выбору параметров

Текущий контроль
Вид (форма) контроля
Тестирование

Раздел 4. Методы контроля целостности

Тема 4.1. Функции хэширования

Назначение и свойства криптографических хэш-функций. Устойчивость к коллизиям. Применение хэширования для контроля целостности и хранения паролей

Текущий контроль
Вид (форма) контроля
Тестирование

Тема 4.2. Электронная цифровая подпись

Принципы формирования и проверки ЭЦП. Алгоритмы цифровой подписи. Инфраструктура открытых ключей. Правовые и организационные аспекты применения ЭЦП

Текущий контроль
Вид (форма) контроля
Тестирование

6. Порядок проведения промежуточной аттестации

Порядок проведения промежуточной аттестации регламентируется локальными нормативными актами Университета:

- Положением о формах, периодичности, порядке текущего контроля успеваемости и промежуточной аттестации обучающихся по основным образовательным программам высшего образования – программам бакалавриата, программам специалитета, программам магистратуры в федеральном государственном бюджетном образовательном учреждении высшего образования «Московский государственный университет геодезии и картографии», п.6 «Организация и проведение промежуточной аттестации».
- Положением о порядке осуществления образовательного процесса, проведения текущего контроля успеваемости и промежуточной аттестации обучающихся с применением электронного обучения и дистанционных образовательных технологий в федеральном государственном бюджетном образовательном учреждении высшего образования «Московский государственный университет геодезии и картографии», п.8 «Проведение промежуточной аттестации с применением ЭО и ДОТ».

Промежуточная аттестация: Зачет с оценкой, 5 семестр.

Зачет оценивается по пятибалльной шкале:

- зачтено с оценкой «отлично» выставляется, если обучающийся имеет глубокие, исчерпывающие знания в объеме освоенной программы; знание основной (обязательной) литературы; дает правильные и уверенные ответы, свидетельствующие о наличии твердых знаний и навыков в использовании технических средств; полное, четкое, грамотное и логически стройное изложение материала; демонстрирует свободное применение теоретических знаний при анализе практических вопросов;
- зачтено с оценкой «хорошо» выставляется обучающемуся в случае соблюдения тех же требований, но наличии в ответе обучающегося по некоторым перечисленным показателям недостатков принципиального характера, что вызывает замечания или поправки преподавателя;
- зачтено с оценкой «удовлетворительно» выставляется обучающемуся в случае соблюдения тех же требований, но в случае наличия в ответе ошибок, необходимости существенной помощи в виде поправок и наводящих вопросов преподавателя;
- не зачтено («не удовлетворительно») – обучающийся не смог ответить на 2/3 вопросов; не справился с практическим заданием или выполнено менее 50 % практических заданий.

7. Оценочные материалы текущего контроля

Раздел 1. Математические основы криптографии

Контролируемые ИДК: ОПК-3.1

Тема 1.1. Программные реализации шифров

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Что является основной целью программной реализации шифра?

1. Увеличение объёма данных
2. Обеспечение защиты информации при обработке в ИС
3. Сжатие данных
4. Повышение скорости сети

2. Какая проблема часто возникает при некорректной реализации шифра?

1. Увеличение длины ключа
2. Потеря совместимости ОС
3. Появление уязвимостей (side-channel атаки)
4. Снижение разрешения экрана

3. Что рекомендуется использовать при разработке криптографического ПО?

1. Самостоятельно написанные алгоритмы

2. Проверенные криптографические библиотеки
3. Устаревшие версии алгоритмов
4. Только симметричные алгоритмы

Тема 1.2. Методы получения случайных и псевдослучайных последовательностей

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Истинно случайные числа формируются на основе:
 1. Математических формул
 2. Физических процессов
 3. Таблиц логарифмов
 4. Сетевых протоколов
2. Псевдослучайная последовательность отличается тем, что:
 1. Полностью непредсказуема
 2. Генерируется без алгоритма
 3. Формируется детерминированным алгоритмом
 4. Не используется в криптографии
3. Основное требование к криптографическому ГПСЧ:
 1. Высокая скорость печати
 2. Предсказуемость
 3. Криптографическая стойкость
 4. Малый размер файла

Раздел 2. Симметричные методы

Контролируемые ИДК: ОПК-3.1

Тема 2.1. Криптографическая стойкость шифров

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Криптографическая стойкость определяется:
 1. Цветом интерфейса
 2. Сложностью взлома алгоритма
 3. Объёмом памяти
 4. Частотой процессора
2. Атака полного перебора предполагает:
 1. Использование вирусов
 2. Подбор всех возможных ключей
 3. Удаление данных
 4. Изменение протокола
3. Увеличение длины ключа приводит к:
 1. Снижению стойкости
 2. Упрощению криптоанализа
 3. Повышению сложности взлома
 4. Отказу алгоритма

Тема 2.2. Имитостойкость и помехоустойчивость шифров

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Имитостойкость обеспечивает:
 1. Сжатие данных
 2. Защиту от подделки сообщений
 3. Ускорение передачи

4. Кодирование видео

2. Для контроля целостности применяются:

1. Хэш-функции
2. Архиваторы
3. Компиляторы
4. Графические редакторы

3. Помехоустойчивость связана с:

1. Защитой от сетевых атак
2. Исправлением ошибок передачи
3. Удалением ключей
4. Шифрованием паролей

Тема 2.3. Блочные методы шифрования

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Блочный шифр обрабатывает данные:

1. Побайтно
2. Побитно
3. Блоками фиксированной длины
4. Только текстовые файлы

2. Пример структуры блочного шифра:

1. Сеть Фейстеля
2. TCP/IP
3. RAID-массив
4. SQL-запрос

3. Режим CBC используется для:

1. Сжатия
2. Режима работы блочного шифра
3. Генерации ключей
4. Хэширования

Раздел 3. Асимметричные методы

Контролируемые ИДК: ОПК-3.1

Тема 3.1. Асимметричные методы шифрования

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Асимметричная криптография использует:

1. Один секретный ключ
2. Два взаимосвязанных ключа
3. Три ключа
4. Безключевой доступ

2. Открытый ключ предназначен для:

1. Удаления данных
2. Шифрования информации
3. Форматирования диска
4. Архивирования

3. Основой асимметричных алгоритмов является:

1. Простая арифметика
2. Сложные математические задачи
3. Сжатие файлов
4. Табличные данные

Тема 3.2. Битовая стойкость алгоритма RSA

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Стойкость RSA зависит от:

1. Цвета программы
2. Длины модуля (ключа)
3. Типа файла
4. Версии Windows

2. RSA основан на сложности:

1. Сжатия данных
2. Факторизации больших чисел
3. Архивирования
4. Кодирования изображений

3. Увеличение размера ключа RSA:

1. Уменьшает стойкость
2. Упрощает взлом
3. Повышает криптостойкость
4. Делает алгоритм симметричным

Раздел 4. Методы контроля целостности

Контролируемые ИДК: ОПК-3.1

Тема 4.1. Функции хэширования

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Хэш-функция предназначена для:

1. Шифрования с ключом
2. Получения фиксированной длины значения
3. Сжатия видео
4. Удаления вирусов

2. Коллизия — это:

1. Ошибка сети
2. Совпадение хэшей разных сообщений
3. Удаление ключа
4. Взлом пароля

3. Хэш-функции применяются для:

1. Хранения паролей
2. Сжатия файлов
3. Ускорения процессора
4. Форматирования диска

Тема 4.2. Электронная цифровая подпись

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. ЭЦП обеспечивает:

1. Сжатие данных
2. Аутентичность и целостность
3. Ускорение сети
4. Удаление файлов

2. Проверка ЭЦП выполняется с помощью:

1. Закрытого ключа отправителя
2. Открытого ключа отправителя
3. Пароля администратора
4. Хэш-таблицы

3. ЭЦП формируется:

1. Открытым ключом
2. Закрытым ключом владельца
3. Любым пользователем
4. Без ключа

4. Инфраструктура открытых ключей (PKI) предназначена для:

1. Сжатия данных
2. Управления сертификатами и ключами
3. Архивирования
4. Кодирования видео

5. Сертификат открытого ключа подтверждает:

1. Скорость сети
2. Принадлежность ключа владельцу
3. Размер файла
4. Тип шифра

6. Основная цель применения ЭЦП в ИС:

1. Повышение объёма данных
2. Обеспечение юридической значимости электронных документов
3. Удаление информации
4. Сжатие сообщений

8. Оценочные материалы промежуточной аттестации

5 семестр, Зачет с оценкой

Контролируемые ИДК: ОПК-3.1

Вопросы/Задания:

1. Понятие криптографии и её место в системе обеспечения информационной безопасности
2. Основные задачи криптографической защиты информации
3. Классификация криптографических методов защиты информации
4. Понятие ключа и ключевой информации. Управление ключами
5. Модели нарушителя и основные типы криптоаналитических атак
6. Источники истинной случайности и их применение в криптографии
7. Генераторы псевдослучайных последовательностей: принципы построения и требования
8. Криптографические требования к генераторам случайных чисел
9. Методы оценки качества случайных последовательностей

10. Понятие криптографической стойкости и способы её оценки
11. Атака полного перебора и её сложность
12. Влияние длины ключа на безопасность алгоритма
13. Современные методы криптоанализа
14. Принципы построения симметричных алгоритмов шифрования
15. Блочные и потоковые шифры: сравнительная характеристика
16. Структура сети Фейстеля и подстановочно-перестановочной сети
17. Режимы работы блочных шифров (ECB, CBC, CFB, OFB, CTR)
18. Преимущества и недостатки симметричного шифрования
19. Принципы построения асимметричных криптосистем
20. Алгоритм RSA: математические основы и этапы работы
21. Криптографическая стойкость RSA и выбор длины ключа
22. Проблемы распределения ключей и их решения
23. Назначение и основные свойства криптографических хэш-функций
24. Понятие коллизии и устойчивости к коллизиям
25. Применение хэш-функций в информационных
26. Применение хэш-функций для хранения и проверки паролей
27. Принципы формирования и проверки электронной цифровой подписи
28. Инфраструктура открытых ключей (PKI): назначение и основные компоненты
29. Обеспечение юридической значимости электронных документов с использованием ЭЦП
30. Имитостойкость, аутентификация сообщений и комплексное применение криптографических методов в информационных системах

9. Материально-техническое и учебно-методическое обеспечение дисциплины

9.1. Перечень основной и дополнительной учебной литературы

Основная литература

1. Сергиенко Е. Н. Математические методы кодирования и шифрования: учебное пособие: учебное пособие / Е. Н. Сергиенко. - Математические методы кодирования и шифрования - Белгород: Белгородский государственный технологический университет им. В.Г. Шухова, ЭБС АСВ, 2017. - 101 с. - 2227-8397. - Текст: электронный. // IPR SMART: [сайт]. - URL: <https://www.iprbookshop.ru/92262.html> (дата обращения: 16.03.2025). - Режим доступа: по подписке

2. Криптоалгоритм «Люцифер». Основы теории современного шифрования: научное издание: научное издание / К. Д. Ермаков, Ю. В. Кузнецов, А. П. Мартынов, Д. Б. Николаев, М. В. Одинцов. - Криптоалгоритм «Люцифер». Основы теории современного шифрования - Саров: Российский федеральный ядерный центр – ВНИИЭФ, 2022. - 137 с. - 978-5-9515-0504-0. - Текст: электронный. // IPR SMART: [сайт]. - URL: <https://www.iprbookshop.ru/132630.html> (дата обращения: 16.03.2025). - Режим доступа: по подписке

3. Фороузан Б. А. Криптография и безопасность сетей: учебное пособие: учебное пособие / Б. А. Фороузан; под редакцией А. Н. Берлина. - Криптография и безопасность сетей - Москва: Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2025. - 776 с. - 978-5-4497-0946-2. - Текст: электронный. // IPR SMART: [сайт]. - URL: <https://www.iprbookshop.ru/146352.html> (дата обращения: 16.03.2025). - Режим доступа: по подписке

Дополнительная литература

1. Котов Ю. А. Криптографические методы защиты информации. Шифры: учебное пособие: учебное пособие / Ю. А. Котов. - Криптографические методы защиты информации. Шифры - Новосибирск: Новосибирский государственный технический университет, 2016. - 59 с. - 978-5-7782-2959-4. - Текст: электронный. // IPR SMART: [сайт]. - URL: <https://www.iprbookshop.ru/91377.html> (дата обращения: 16.03.2025). - Режим доступа: по подписке

2. Котов Ю. А. Криптографические методы защиты информации. Стандартные шифры. Шифры с открытым ключом: учебное пособие: учебное пособие / Ю. А. Котов. - Криптографические методы защиты информации. Стандартные шифры. Шифры с открытым ключом - Новосибирск: Новосибирский государственный технический университет, 2017. - 67 с. - 978-5-7782-3411-6. - Текст: электронный. // IPR SMART: [сайт]. - URL: <https://www.iprbookshop.ru/91227.html> (дата обращения: 16.03.2025). - Режим доступа: по подписке

3. Петров А. А. Компьютерная безопасность. Криптографические методы защиты / А. А. Петров. - Компьютерная безопасность. Криптографические методы защиты - Саратов: Профобразование, 2024. - 446 с. - 978-5-4488-0091-7. - Текст: электронный. // IPR SMART: [сайт]. - URL: <https://www.iprbookshop.ru/145915.html> (дата обращения: 16.03.2025). - Режим доступа: по подписке

9.2. Профессиональные базы данных и ресурсы «Интернет», к которым обеспечивается доступ обучающихся

Профессиональные базы данных

Не используются.

Ресурсы «Интернет»

1. <https://znanium.ru/> - Электронно-библиотечная система "Znanium"
2. <https://www.elibrary.ru/> - НЭБ eLIBRARY
3. <http://citforum.ru> - IT-портал CITForum
4. <https://intuit.ru/> - Электронная образовательная среда "ИНТУИТ"

9.3. Программное обеспечение и информационно-справочные системы, используемые при осуществлении образовательного процесса по дисциплине

Перечень программного обеспечения

(обновление производится по мере появления новых версий программы)

Не используется.

Перечень информационно-справочных систем

(обновление выполняется еженедельно)

Не используется.

9.4. Оборудование и технические средства обучения

Учебная аудитория

Маркерная доска - 0 шт.

Моноблок - 64 шт.

Проектор - 4 шт.

Смешанный тип

Автоматизированное рабочее место (АРМ) - 1 шт.

Доска настенная одноэлементная - 2 шт.

Интерактивная панель - 1 шт.

Проектор - 1 шт.

10. Методические указания по освоению дисциплины (модуля)

С целью успешного освоения данного предмета студенту необходимо выполнять домашние работы по указанным преподавателям темам и представленным на занятиях материалам. Для более успешного выполнения работы студенту предлагается использование учебно-методических материалов, соответствующих указанной теме.

Самостоятельная работа студентов описывается и регулируется методическими рекомендациями по дисциплине.

Описание возможностей изучения дисциплины лицами с ОВЗ и инвалидами

При необходимости обучения студентов-инвалидов и лиц с ограниченными возможностями здоровья аудиторные занятия могут быть заменены или дополнены изучением полнотекстовых лекций, презентаций, видео- и аудиоматериалов в электронной информационно-образовательной среде (ЭИОС) университета. Индивидуальные задания подбираются в адаптированных к ограничениям здоровья формах (письменно или устно, в форме презентаций). Выбор методов обучения зависит от их доступности для инвалидов и лиц с ограниченными возможностями здоровья.

Рабочая программа дисциплины для инвалидов и лиц с ограниченными возможностями здоровья разрабатывается индивидуально с учетом особенностей психофизического развития, индивидуальных возможностей и состояния здоровья таких обучающихся.