



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.В.09 РЕАЛИЗАЦИЯ СПЕЦИФИКАЦИИ КРИПТОГРАФИЧЕСКИХ
СООБЩЕНИЙ»**

Уровень высшего образования: магистратура

Направление подготовки: 10.04.01 Информационная безопасность

Направленность(профиль) подготовки: Защита информации в геоинформационных системах
и системах сбора пространственных данных

Квалификация (степень) выпускника: магистр

Форма обучения: очная

Год набора (приема на обучение): 2024

Срок получения образования: 2 года

Объем:
в зачетных единицах: 4 з.е.
в академических часах: 144 ак.ч.

Москва, 2024

Разработчики:

Преподаватель кафедры Информационно-измерительных систем
Месенгисер Я. Я.

Рабочая программа дисциплины (модуля) составлена в соответствии с требованиями ФГОС ВО по направлению подготовки 10.04.01 Информационная безопасность, утвержденного приказом Минобрнауки от 26.11.2020 № 1455

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 способности решать задачи, связанные с различными форматами криптографических сообщений и правилами построения и конфигурации инфраструктуры открытых ключей в рамках реализации проектных решений уровня предприятия, а также обучение формированию и верификации криптографических сообщений различных форматов, а также создание и конфигурирование инфраструктуры открытых ключей в рамках реализации проектных решений уровня предприятия на базе криптографических библиотек с открытым исходным кодом.

Задачи изучения дисциплины:

- изучить основы принципов формирования и верификации криптографических сообщений различных форматов с использованием криптографических библиотек с открытым исходным кодом;
- изучить основы правил построения и конфигурации Инфраструктуры Открытых Ключей в рамках реализации проектных решений уровня предприятия с использованием криптографических библиотек с открытым исходным кодом.

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

Компетенции, индикаторы и результаты обучения

ПК-3 Способен разрабатывать проектные решения по защите информации автоматизированных систем (в том числе в геоинформационных системах)

ПК-3.1 Классифицирует защищаемую информацию по видам тайны и степеням конфиденциальности

Знать:

ПК-3.1/Зн3 систему нормативных правовых актов, нормативных и методических документов в области информационной безопасности и защиты информации

Уметь:

ПК-3.1/Ум3 обосновывать решения, связанные с реализацией правовых норм по защите информации в пределах должностных обязанностей

Владеть:

ПК-3.1/Нв2 навыками по применению нормативных правовых актов, нормативных и методических документов, регламентирующие деятельность по защите информации

ПК-3.2 Определяет типы субъектов доступа и объектов доступа, являющихся объектами защиты

Знать:

ПК-3.2/Зн4 форматы криптографических сообщений и стандарты их представления

Уметь:

ПК-3.2/Ум2 выполнять проверку цифровых подписей и других криптографических атрибутов сообщений

ПК-3.2/Ум3 анализировать результаты верификации и выявлять случаи нарушения целостности или подлинности сообщения

Владеть:

ПК-3.2/Нв2 навыками работы с криптографическими библиотеками и инструментами верификации

ПК-3.2/Нв3 методиками обеспечения безопасности при обработке и верификации криптографических сообщений

ПК-3.3 Разрабатывает проекты нормативных документов, регламентирующих работу по защите информации

Знать:

ПК-3.3/Зн2 программные, технические и методические средства информационных технологий

Уметь:

ПК-3.3/Ум3 осуществлять разработку и проектирование информационных систем в соответствии с поставленной задачей

Владеть:

ПК-3.3/Нв2 методами анализа и формализации информационных процессов объекта и связей между ними

ПК-3.4 Понимает принципы построения и функционирования современных локальных и глобальных компьютерных сетей и их компонентов (в том числе геоинформационных систем)

Знать:

ПК-3.4/Зн4 особенности архитектуры распределённых информационных систем и роли системного программного обеспечения в них

Уметь:

ПК-3.4/Ум2 выполнять настройку системного программного обеспечения с учетом требований информационной безопасности

Владеть:

ПК-3.4/Нв2 навыками работы с системным программным обеспечением различных платформ в распределённых ИС

3. Место дисциплины в структуре ОП

Дисциплина (модуль) Б1.В.09 «Реализация спецификации криптографических сообщений» относится к формируемой участниками образовательных отношений части образовательной программы и изучается в семестре(ах): 1.

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)	Практические занятия (часы)	Самостоятельная работа (часы)	Промежуточная аттестация (часы)
1 семестр	144	4	68	76	Зачет с оценкой
Всего	144	4	68	76	

5. Содержание дисциплины (модуля)

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

Наименование раздела, темы	Всего	Практические занятия	Самостоятельная работа	Планируемые результаты с обучением, соотношенные с результатами освоения программы
Раздел 1. Инфраструктура открытых ключей. Компоненты, функции, и архитектуры построения УЦ.	22	8	14	ПК-3.1 ПК-3.2 ПК-3.3 ПК-3.4
Тема 1.1. Инфраструктура открытых ключей.	12	5	7	
Тема 1.2. Понятия удостоверяющего центра.	10	3	7	
Раздел 2. Спецификации PKCS#10, PKCS#12 и X.509	44	24	20	ПК-3.2 ПК-3.3 ПК-3.4
Тема 2.1. Генерация ключевой пары.	7	3	4	
Тема 2.2. Импорт и экспорт ключевой пары.	7	3	4	
Тема 2.3. Создание запроса на сертификат ключа проверки ЭП и получение сертификата ключа проверки ЭП.	7	3	4	
Тема 2.4. Создание самоподписанного сертификата ключа проверки ЭП.	9	5	4	
Тема 2.5. Подпись запроса на сертификат ключа проверки ЭП.	7	5	2	
Тема 2.6. Создание, импорт и экспорт PFX.	7	5	2	
Раздел 3. Спецификации PKCS#7, CMS и CAdES	28	14	14	ПК-3.2 ПК-3.3 ПК-3.4
Тема 3.1. Обзор спецификаций CAdES, PKCS#7 и CMS.	28	14	14	
Раздел 4. Спецификации XMLDSIG и XAdES	26	12	14	ПК-3.2 ПК-3.3 ПК-3.4
Тема 4.1. Обзор спецификаций XMLDSIG и XAdES.	26	12	14	
Раздел 5. Спецификация PAdES	24	10	14	ПК-3.2 ПК-3.3 ПК-3.4
Тема 5.1. Обзор спецификации PAdES.	24	10	14	
Итого	144	68	76	

5.2. Содержание разделов, тем дисциплин и формы текущего контроля

Раздел 1. Инфраструктура открытых ключей. Компоненты, функции, и архитектуры построения УЦ.

Тема 1.1. Инфраструктура открытых ключей.

Инфраструктура открытых ключей. Компоненты и функции.

Текущий контроль
Вид (форма) контроля
Письменный опрос

Тема 1.2. Понятия удостоверяющего центра.

Иерархическая архитектура УЦ, гибридная архитектура УЦ, кросс-сертификационная и мостовая архитектуры УЦ.

Текущий контроль
Вид (форма) контроля
Письменный опрос

Раздел 2. Спецификации PKCS#10, PKCS#12 и X.509

Тема 2.1. Генерация ключевой пары.

Генерация ключевой пары. Практическая реализация компьютерной программы или набора компьютерных программ, реализующих генерацию ключевой пары с использованием криптографических библиотек OpenSSL и BouncyCastle.

Тема 2.2. Импорт и экспорт ключевой пары.

Импорт и экспорт ключевой пары. Практическая реализация компьютерной программы или набора компьютерных программ, реализующих импорт и экспорт ключевой пары с использованием криптографических библиотек OpenSSL и BouncyCastle.

Тема 2.3. Создание запроса на сертификат ключа проверки ЭП и получение сертификата ключа проверки ЭП.

Создание запроса на сертификат ключа проверки ЭП и получение сертификата ключа проверки ЭП. Практическая реализация компьютерной программы или набора компьютерных программ, реализующих создание запроса на сертификат ключа проверки ЭП и получение сертификата ключа проверки ЭП с использованием криптографических библиотек OpenSSL и BouncyCastle.

Текущий контроль
Вид (форма) контроля
Письменный опрос

Тема 2.4. Создание самоподписанного сертификата ключа проверки ЭП.

Создание самоподписанного сертификата ключа проверки ЭП. Практическая реализация компьютерной программы или набора компьютерных программ, реализующих создание самоподписанного сертификата с использованием криптографических библиотек OpenSSL и BouncyCastle.

Текущий контроль	
Вид (форма) контроля	
Письменный опрос	

Тема 2.5. Подпись запроса на сертификат ключа проверки ЭП.

Подпись запроса на сертификат ключа проверки ЭП. Практическая реализация компьютерной программы или набора компьютерных программ, реализующих подпись запроса на сертификат с использованием криптографических библиотек OpenSSL и BouncyCastle.

Тема 2.6. Создание, импорт и экспорт PFX.

Создание, импорт и экспорт PFX. Практическая реализация компьютерной программы или набора компьютерных программ, реализующих создание, импорт и экспорт PFX с использованием криптографических библиотек OpenSSL и BouncyCastle.

Раздел 3. Спецификации PKCS#7, CMS и CAdES

Тема 3.1. Обзор спецификаций CAdES, PKCS#7 и CMS.

Обзор спецификаций CAdES, PKCS#7 и CMS. Практическая реализация компьютерной программы или набора компьютерных программ, реализующих создание и проверку криптографических сообщений формата CAdES с использованием криптографических библиотек OpenSSL и BouncyCastle.

Текущий контроль	
Вид (форма) контроля	
Письменный опрос	

Раздел 4. Спецификации XMLDSIG и XAdES

Тема 4.1. Обзор спецификаций XMLDSIG и XAdES.

Обзор спецификаций XMLDSIG и XAdES. Практическая реализация компьютерной программы или набора компьютерных программ, реализующих создание и проверку криптографических сообщений формата XAdES с использованием криптографических библиотек OpenSSL и BouncyCastle

Текущий контроль	
Вид (форма) контроля	
Письменный опрос	

Раздел 5. Спецификация PAdES

Тема 5.1. Обзор спецификации PAdES.

Обзор спецификации PAdES. Практическая реализация компьютерной программы или набора компьютерных программ, реализующих создание и проверку криптографических сообщений формата PAdES с использованием криптографических библиотек OpenSSL и BouncyCastle

Текущий контроль

Вид (форма) контроля

Письменный опрос

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, 1 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. Инфраструктура открытых ключей. Компоненты, функции, и архитектуры построения УЦ.

Контролируемые ИДК: ПК-3.1 ПК-3.2 ПК-3.3 ПК-3.4

Тема 1.1. Инфраструктура открытых ключей.

Форма контроля/оценочное средство: Письменный опрос

Вопросы/Задания:

1. Описание компонентов инфраструктуры открытых ключей
2. Описание назначения и функций инфраструктуры открытых ключей
3. Описание жизненного цикла ключа ЭП

4. Классификация сертификатов ключей проверки ЭП
5. Описание жизненного цикла сертификата ключа проверки ЭП

Тема 1.2. Понятия удостоверяющего центра.

Форма контроля/оценочное средство: Письменный опрос

Вопросы/Задания:

1. Определение и функции удостоверяющего центра
2. Основные виды моделей отношений доверия
3. Описание инфраструктуры единичного УЦ
4. Описание иерархической инфраструктуры подчиненных УЦ
5. Описание гибридной инфраструктуры УЦ
6. Описание кросс-сертификационной инфраструктуры УЦ
7. Описание основных стандартов в области PKI и их назначения
8. Определение и назначение нотации ASN.1

Раздел 2. Спецификации PKCS#10, PKCS#12 и X.509

Контролируемые ИДК: ПК-3.2 ПК-3.3 ПК-3.4

Тема 2.3. Создание запроса на сертификат ключа проверки ЭП и получение сертификата ключа проверки ЭП.

Форма контроля/оценочное средство: Письменный опрос

Вопросы/Задания:

1. Описание стандарта сертификатов формата X.509
2. Описание стандартов семейства PKCS и их назначение
3. Описание нормативных правовых актов, регулирующих функционирование инфраструктуры открытых ключей в РФ
4. Описание нормативных правовых актов, регулирующих применение ЭП в РФ
5. Определение термина ЭП, виды электронной подписи
6. Назначение и функции ЭП

Тема 2.4. Создание самоподписанного сертификата ключа проверки ЭП.

Форма контроля/оценочное средство: Письменный опрос

Вопросы/Задания:

1. Описание требований, предъявляемых к неквалифицированной ЭП
2. Описание требований, предъявляемых к квалифицированной ЭП
3. Описание требований, предъявляемых к средствам ЭП для создания квалифицированной ЭП
4. Описание требований, предъявляемых к квалифицированному сертификату ЭП

Раздел 3. Спецификации PKCS#7, CMS и CAdES

Контролируемые ИДК: ПК-3.2 ПК-3.3 ПК-3.4

Тема 3.1. Обзор спецификаций CAdES, PKCS#7 и CMS.

Форма контроля/оценочное средство: Письменный опрос

Вопросы/Задания:

1. Описание формата ЭП PKCS#7
2. Описание формата ЭП CMS

Раздел 4. Спецификации XMLDSIG и XAdES

Контролируемые ИДК: ПК-3.2 ПК-3.3 ПК-3.4

Тема 4.1. Обзор спецификаций XMLDSIG и XAdES.

Форма контроля/оценочное средство: Письменный опрос

Вопросы/Задания:

1. Описание формата ЭП XMLDSig

Раздел 5. Спецификация PAdES

Контролируемые ИДК: ПК-3.2 ПК-3.3 ПК-3.4

Тема 5.1. Обзор спецификации PAdES.

Форма контроля/оценочное средство: Письменный опрос

Вопросы/Задания:

1. Описание формата ЭП CAdES / XAdES / PAdES - BES
2. Описание формата ЭП CAdES / XAdES / PAdES – T
3. Описание формата ЭП CAdES / XAdES / PAdES – C
4. Описание формата ЭП CAdES / XAdES / PAdES – X Type 1 / 2
5. Описание формата ЭП CAdES / XAdES / PAdES – X Long Type 1 / 2
6. Описание формата ЭП CAdES / XAdES / PAdES – A

8. Оценочные материалы промежуточной аттестации

1 семестр, Зачет с оценкой

Контролируемые ИДК: ПК-3.1 ПК-3.2 ПК-3.3 ПК-3.4

Вопросы/Задания:

1. Вывести координаты открытого ключа для заданного файла
2. Сформировать запрос на выпуск сертификата ключа проверки ЭП формата PKCS#10
3. Проверить математическую корректность ЭП для заданного запроса на выпуск сертификата ключа проверки ЭП формата PKCS#10
4. Добавить критический атрибут 1.2.643.1.1.1.1.1 в запрос на выпуск сертификата ключа проверки ЭП формата PKCS#10
5. Получить открытый ключ из запроса на выпуск сертификата ключа проверки ЭП формата PKCS#10
6. Получить информацию о субъекте, сформировавшем запрос на выпуск сертификата ключа проверки ЭП формата PKCS#10
7. Вывести список критических и некритических атрибутов в запросе на выпуск сертификата ключа проверки ЭП формата PKCS#10
8. Вывести параметры открытого ключа в запросе на выпуск сертификата ключа проверки ЭП формата PKCS#10
9. Сформировать самоподписанный сертификат ключа проверки ЭП формата X.509

10. Указать срок окончания действия сертификата ключа проверки ЭП формата X.509 спустя 28 лет после его формирования
11. Получить открытый ключ из сертификата ключа проверки ЭП формата X.509
12. Получить информацию о владельце из сертификата ключа проверки ЭП формата X.509
13. Получить информацию об издателе из сертификата ключа проверки ЭП формата X.509
14. Проверить математическую корректность ЭП для заданного сертификата ключа проверки ЭП формата X.509
15. Вывести список критических и некритических атрибутов для заданного сертификата ключа проверки ЭП формата X.509
16. Сформировать PFX
17. Импортировать PFX
18. Определить, является ли ЭП отсоединенной или присоединенной
19. Вывести подписанные данные для заданной присоединенной ЭП
20. Вывести список сертификатов, хранящихся в заданной ЭП
21. Вывести список подписанных атрибутов для заданной ЭП
22. Вывести хэш-код, вычисленный для подписанных данных, который хранится в заданной ЭП
23. Определить количество подписантов для заданной ЭП
24. Проверить математическую корректность заданной ЭП
25. Определить, хранится ли метка локального времени в заданной ЭП
26. Определить, является ли подпись формата *AdES-BES
27. Определить, является ли подпись формата *AdES-T
28. Определить, является ли подпись формата *AdES-C
29. Определить, является ли подпись формата *AdES-X Type 1/2
30. Определить, является ли подпись формата *AdES-X Long Type 1/2
31. Определить, является ли подпись формата *AdES-A

9. Материально-техническое и учебно-методическое обеспечение дисциплины

9.1. Перечень основной и дополнительной учебной литературы

Основная литература

1. 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
2. Фомин Д. В. Защита информации: специализированные аттестованные программные и программно-аппаратные средства: практикум: практикум / Д. В. Фомин. - Защита информации: специализированные аттестованные программные и программно-аппаратные средства - Саратов: Вузовское образование, 2021. - 218 с. - 978-5-4487-0795-7. - Текст: электронный. // IPR SMART: [сайт]. - URL: <https://www.iprbookshop.ru/110329.html> (дата обращения: 16.03.2025). - Режим доступа: по подписке

Дополнительная литература

1. Жиль Земор Курс криптографии / Земор Жиль; перевод В. В. Шуликовская. - Курс криптографии - Москва, Ижевск: Регулярная и хаотическая динамика, Институт компьютерных исследований, 2019. - 256 с. - 978-5-4344-0770-0. - Текст: электронный. // IPR SMART: [сайт]. - URL: <https://www.iprbookshop.ru/91941.html> (дата обращения: 16.03.2025). - Режим доступа: по подписке
2. Лапони́на О. Р. Основы сетевой безопасности: криптографические алгоритмы и протоколы взаимодействия: учебное пособие: учебное пособие / О. Р. Лапони́на; под редакцией В. А. Сухомлина. - Основы сетевой безопасности: криптографические алгоритмы и протоколы взаимодействия - Москва: Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2024. - 605 с. - 978-5-4497-3470-9. - Текст: электронный. // IPR SMART: [сайт]. - URL: <https://www.iprbookshop.ru/142292.html> (дата обращения: 16.03.2025). - Режим доступа: по подписке
3. Введение в криптографию. / Под общ. ред. В.В. Яценко.. - 3-е изд., доп. - Издательство МЦНМО: "ЧеРо", 2000. - 288 - 5-900916-65-0. - Текст: непосредственный.
4. Баричев С.Г. Основы современной криптографии : Учебный курс / С.Г. Баричев, В.В. Гончаров, Р.Е. Серов. - 2-е изд., испр. и доп. - Издательство Горячая линия - Телеком, 2002. - 175 - 5-93517-075-2. - Текст: непосредственный.

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

Профессиональные базы данных

1. <https://student2.consultant.ru/cgi/online.cgi> - Правовой Сервер КонсультантПлюс

Ресурсы «Интернет»

1. <https://znanium.ru/> - Электронно-библиотечная система "Znanium"
2. <https://www.elibrary.ru/> - НЭБ eLIBRARY
3. <https://e.lanbook.com/> - Электронная библиотечная система "Лань"
4. <https://rusneb.ru/> - Национальная электронная библиотека (НЭБ)

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.

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;
- Методическими рекомендациями по организации самостоятельной работы студентов МИИГАиК;

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.