



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.07 АУДИТ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»**

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: 3 з.е.
в академических часах: 108 ак.ч.

Москва, 2024

Разработчики:

Преподаватель кафедры Информационно-измерительных систем
Долгова П. В.

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 организацией и проведением аудита информационной безопасности; применением нормативных правовых документов, регламентирующих процесс организации и проведения аудита; разработкой необходимых организационно-распорядительных документов; организацией и управлением деятельности экспертной группы при проведении аудита информационной безопасности.

Задачи изучения дисциплины:

- освоение системного подхода к организации аудита, в том числе умение митигировать риски;
- понимание механизмов работы с основными стандартами в области аудита информационной безопасности;
- понимание основ практического проведения аудита (подход, методы сбора данных, оценка рисков, анализ защищенности);
- формирование умений оценивания информационной безопасности на основе показателей информационной безопасности;
- умение составлять заключения аудиторской проверки в результате аудита информационной безопасности, проведенного в организации.

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

Компетенции, индикаторы и результаты обучения

ОПК-3 Способен разрабатывать проекты организационно-распорядительных документов по обеспечению информационной безопасности

ОПК-3.1 Разрабатывает проекты организационно-распорядительной документации, регламентирующей процесс обеспечения информационной безопасности

Знать:

ОПК-3.1/Зн2 регламенты по аудиту информационной безопасности

Уметь:

ОПК-3.1/Ум2 митигировать риски, выявленные в ходе аудита информационной безопасности

Владеть:

ОПК-3.1/Нв2 навыками и инструментами для проведения аудита информационной безопасности

3. Место дисциплины в структуре ОП

Дисциплина (модуль) Б1.О.07 «Аудит информационной безопасности» относится к обязательной части образовательной программы и изучается в семестре(ах): 2.

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)
2 семестр	108	3	32	32	44	Зачет с оценкой
Всего	108	3	32	32	44	

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 обучения, соответствующие результатам освоения программы
Раздел 1. Аудит	14	4	4	6	ОПК-3.1
Тема 1.1. Аудит	14	4	4	6	
Раздел 2. Аудит информационной безопасности	14	4	4	6	ОПК-3.1
Тема 2.1. Аудит информационной безопасности	8	4	4		
Тема 2.2. Виды аудитов ИБ	6			6	
Раздел 3. Правовые аспекты аудита информационной безопасности	18	6	6	6	ОПК-3.1
Тема 3.1. Правовые аспекты аудита информационной безопасности	18	6	6	6	
Раздел 4. Управление аудитом информационной безопасности	14	4	4	6	ОПК-3.1
Тема 4.1. Управление аудитом информационной безопасности	14	4	4	6	
Раздел 5. Методика проведения аудита информационной безопасности на предприятии	20	6	6	8	ОПК-3.1

Тема 5.1. Методика проведения аудита информационной безопасности на предприятии	20	6	6	8	
Раздел 6. Планирование аудиторской проверки	16	4	4	8	ОПК-3.1
Тема 6.1. Планирование аудиторской проверки	16	4	4	8	
Раздел 7. Анализ и управление рисками ИБ	12	4	4	4	ОПК-3.1
Тема 7.1. Анализ и управление рисками ИБ	12	4	4	4	
Итого	108	32	32	44	

5.2. Содержание разделов, тем дисциплин и формы текущего контроля

Раздел 1. Аудит

Тема 1.1. Аудит

Основные понятия. Виды аудитов и их отличия. Стандарты по аудиту. Обзор стандартов по аудиту информационной безопасности.

Раздел 2. Аудит информационной безопасности

Тема 2.1. Аудит информационной безопасности

Основные этапы аудита ИБ. Виды аудитов: внешний и внутренний, документальный и технический.

Тема 2.2. Виды аудитов ИБ

Обучающийся изучает информацию о различных видах аудита.

Раздел 3. Правовые аспекты аудита информационной безопасности

Тема 3.1. Правовые аспекты аудита информационной безопасности

Документы, которые необходимо изучить до начала аудита. Соглашения, которые необходимо получить до начала аудиторской проверки. Периметр аудита. Программные средства для реализации аудита ИБ.

Раздел 4. Управление аудитом информационной безопасности

Тема 4.1. Управление аудитом информационной безопасности

Как часто и почему необходимо проводить аудит ИБ. Что должно входить в аудиторскую проверку. Кто должен знать об аудиторской проверке.

Раздел 5. Методика проведения аудита информационной безопасности на предприятии

Тема 5.1. Методика проведения аудита информационной безопасности на предприятии

Организация процесса аудита ИБ. В чем отличия в стандартах и процессах аудиторской проверки в зависимости от предприятия. Что нужно обговорить с заказчиком до начала работ. Виды погрешностей в зависимости от выбранной методики аудита. Существенность в аудите.

Раздел 6. Планирование аудиторской проверки

Тема 6.1. Планирование аудиторской проверки

Что должно и не должно входить в периметр аудиторской проверки. Сроки проведения аудиторской проверки. Процессы, затрагиваемые в ходе аудита. Команда, привлекаемая для достижения целей аудита.

Раздел 7. Анализ и управление рисками ИБ

Тема 7.1. Анализ и управление рисками ИБ

Что такое риск ИБ и как его определить. Как работать с рисками и как их митигировать.

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, 2 семестр.

Зачет оценивается по пятибалльной шкале:

- зачено 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 7. Анализ и управление рисками ИБ

Контролируемые ИДК: ОПК-3.1

Тема 7.1. Анализ и управление рисками ИБ

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Что является основной целью аудита информационной безопасности?
 1. Оценка стоимости информационных активов
 2. Проверка соответствия системы менеджмента информационной безопасности установленным требованиям
 3. Разработка новых политик безопасности
 4. Обучение сотрудников безопасности
2. Какой стандарт является основой для создания системы менеджмента информационной безопасности?
 1. ISO/IEC 27001
 2. ISO/IEC 9001
 3. ISO/IEC 14001
 4. ISO/IEC 27002
3. Что из перечисленного не является объектом аудита информационной безопасности?
 1. Политики и процедуры безопасности
 2. Технические средства защиты
 3. Финансовые отчёты организации
 4. Процессы управления инцидентами
4. Как называется процесс определения и оценки рисков в области информационной безопасности?
 1. Управление инцидентами
 2. Оценка уязвимостей
 3. Оценка рисков
 4. Аудит соответствия
5. Какой документ описывает требования и рекомендации по обеспечению информационной безопасности?
 1. Руководство пользователя
 2. Стандарт ISO/IEC 27002
 3. Отчёт о внутреннем аудите
 4. План реагирования на инциденты
6. Что из перечисленного является примером административного контроля безопасности?
 1. Шифрование данных
 2. Физическая охрана серверов
 3. Политика управления доступом

4. Системы обнаружения вторжений

7. Какой этап аудита включает в себя сбор и анализ информации о текущем состоянии системы безопасности?

1. Планирование аудита
2. Оценка рисков
3. Проведение аудита
4. Подготовка отчёта

8. Что из перечисленного является примером физического контроля безопасности?

1. Фаервол
2. Контроль доступа в серверные помещения
3. Антивирусное ПО
4. Процедуры резервного копирования

9. Какой стандарт описывает требования к системам менеджмента информационной безопасности в контексте защиты персональных данных?

1. ISO/IEC 27001
2. ISO/IEC 27018
3. ISO/IEC 27002
4. ISO/IEC 27005

10. Какой из следующих методов оценки рисков используется в стандарте ISO/IEC 27005?

1. DREAD
2. OCTAVE
3. FAIR
4. Методология на основе сценариев

11. Какой документ содержит результаты аудита и рекомендации по улучшению системы безопасности?

1. План аудита
2. Отчёт по аудиту
3. Политика безопасности
4. Протокол заседания

12. Какой этап аудита включает в себя определение объёма и целей аудита?

1. Планирование аудита
2. Проведение аудита
3. Оценка рисков
4. Подготовка отчёта

13. Что из перечисленного является примером административного контроля безопасности?

1. Шифрование данных
2. Физическая охрана серверов
3. Политика управления доступом
4. Системы обнаружения вторжений

14. Что такое «область аудита»?

1. Географическая зона
2. Список сотрудников
3. Совокупность процессов и ресурсов, попадающих под аудит
4. Сетевой периметр

15. К какому типу аудита относится проверка внешней организацией на соответствие ISO/IEC 27001?

1. Внутренний аудит
2. Вторичный аудит
3. Внешний аудит
4. Комплексный аудит

16. Какой метод анализа риска наиболее детализирует вероятности и ущерб?

1. Качественный
2. Количественный
3. Экспертный
4. Сценарный

17. Какое утверждение верно о концепции "due care" в информационной безопасности?

1. Это сертификационный документ
2. Это защита от вирусов
3. Это принцип разумной ответственности
4. Это часть шифрования

18. Что такое GAP-анализ?

1. Тестирование политик
2. Сравнение текущего состояния с эталонным
3. Взлом системы
4. Модель контроля доступа

19. Какой документ оформляется по итогам аудита?

1. План работ
2. Сертификат соответствия
3. Отчёт по аудиту
4. Бюджет проекта

20. Что НЕ является целью аудита ИБ?

1. Оценка защищённости
2. Повышение осведомлённости
3. Устранение всех уязвимостей
4. Соответствие стандартам

21. Что такое "аудиторское доказательство"?

1. Подпись пользователя
2. Личное мнение специалиста
3. Проверяемый факт, подтверждающий соблюдение требований
4. Секретный документ

22. Что определяет ISO/IEC 27005?

1. Методы аутентификации
2. Методики оценки рисков
3. Структуру ИТ-отдела
4. Состав оборудования

23. Какая роль у внутреннего аудита?

1. Проверка только ИТ-отдела
2. Ежегодный внешний контроль
3. Самостоятельная оценка соответствия ИБ-политикам
4. Обновление паролей

24. Что такое "тест на проникновение"?

1. Стресс-тест на сервер
2. Проверка политики безопасности
3. Имитация атаки с целью выявления уязвимостей
4. Обновление антивируса

25. Что такое аттестация ИС?

1. Регистрация ПО
2. Проверка соответствия системы установленным требованиям
3. Установка защиты
4. Отказ от ответственности

26. Какой подход основан на выявлении угроз и уязвимостей?

1. Процессный

- 2. Сетевой
- 3. Риск-ориентированный
- 4. Физический

27. Что такое контроль целостности?

- 1. Резервное копирование
- 2. Мониторинг логов
- 3. Обнаружение изменений в данных
- 4. Установка ПО

28. Что означает принцип "need-to-know"?

- 1. Доступ к информации предоставляется всем
- 2. Доступ основан на ролях
- 3. Доступ только тем, кому это необходимо
- 4. Открытые данные

29. Что такое ISO/IEC 27019?

- 1. Защита информации в энергетике
- 2. Защита медицинских данных
- 3. Защита в правительстве
- 4. Стандарты CRM

30. Чем отличается аудит от мониторинга?

- 1. Аудит — это постоянное наблюдение
- 2. Аудит — это формальная проверка на соответствие
- 3. Мониторинг — это единоразовая проверка
- 4. Аудит не требует доказательств

31. Что включает предварительный этап аудита?

- 1. Взлом систем
- 2. Установка брандмауэров
- 3. Планирование и согласование критериев
- 4. Выдача сертификатов

32. Какая из задач НЕ входит в аудит?

- 1. Анализ журналов
- 2. Разработка стандарта
- 3. Интервью с персоналом
- 4. Проверка уязвимостей

33. Что такое "комплаенс" (compliance)?

- 1. Обнаружение вторжений
- 2. Соответствие требованиям
- 3. Хеш-функция
- 4. Анализ логов

34. Кто обычно проводит внешний аудит?

- 1. Внутренний отдел безопасности
- 2. Независимая третья сторона
- 3. Менеджер проекта
- 4. HR-департамент

35. Какой контроль относится к категории предотвращающих (preventive)?

- 1. IDS
- 2. Видеонаблюдение
- 3. Парольная политика
- 4. Анализ логов

8. Оценочные материалы промежуточной аттестации

1. Дайте определение информационной безопасности согласно стандарту ISO 27001
2. Дайте определение Аудит ИБ в организации согласно п. 2.8.6 ГОСТ 50922-2006 Защита информации. Основные термины и определения
3. Дайте определение «комплексному аудиту» согласно ГОСТ Р ИСО 19011-2021 Оценка соответствия. Руководящие указания по проведению аудита систем менеджмента
4. Дайте определение «программе аудита» согласно ГОСТ Р ИСО 19011-2021 Оценка соответствия. Руководящие указания по проведению аудита систем менеджмента
5. Дайте определение «области аудита» согласно ГОСТ Р ИСО 19011-2021 Оценка соответствия. Руководящие указания по проведению аудита систем менеджмента
6. Что включает в себя область аудита согласно ГОСТ Р ИСО 19011-2021 Оценка соответствия. Руководящие указания по проведению аудита систем менеджмента
7. Дайте определение «аудиторское заключение» согласно СТО БР ИББС-1.1-2007 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Аудит информационной безопасности»
8. Перечислите фазы аудита ИБ
9. Перечислите этапы, которые включает в себя цикл Деминга-Шухарта
10. При аудите финансовой отчетности по стандартам РСБУ и МСФО, какая оценка ИТ контролей проводится?
11. Какие три метода используют аудиторы, проводя проверку мер и средств контроля и управления информационной безопасностью согласно ISO 27008:2011?
12. Укажите последовательность процессов управления программой аудита согласно ГОСТ Р ИСО 19011-2021
13. Основные принципы проведения аудита информационной безопасности организаций БС РФ согласно СТО БР ИББС-1.1-2007
14. Согласно СТО БР ИББС-1.1-2007 Ответственные за управление программой аудита ИБ лица должны?
15. Согласно СТО БР ИББС-1.1-2007 Внедрение программы аудита ИБ должно включать в себя?
16. Каким образом согласно СТО БР ИББС-1.1-2007 должно оформляться аудиторское задание на проведение аудита ИБ?

17. Согласно СТО БР ИББС-1.1-2007 руководство проверяемой организации несет ответственность за:

18. Какие работы должны включать в себя в рамках проведения аудита ИБ на месте согласно СТО БР ИББС-1.1-2007?

19. Как называется пункт АЗ в приложении А в ISO 27008:2011?

20. Каким требованиям должна соответствовать организация, осуществляющая внешний аудит?

21. Какие компетенции аудитора СУИБ указываются в ISO/IEC 27007?

22. Опишите цели и задачи стандарта СТО БР ИББС в рамках обеспечения информационной безопасности организаций финансового сектора

23. Какие уровни соответствия требованиям СТО БР ИББС предусмотрены для организаций и как определяется необходимый уровень?

24. Назовите ключевые элементы (компоненты) системы управления информационной безопасностью (СУИБ2., согласно требованиям СТО БР ИББС

25. Какие требования предъявляются СТО БР ИББС к проведению оценки соответствия (аудит1. информационной безопасности?

26. Какие особенности организации управления инцидентами информационной безопасности предусмотрены стандартом СТО БР ИББС?

27. Какие методы оценки рисков предлагает использовать ISO/IEC 27005 и чем они отличаются?

28. Какова основная цель стандарта ISO/IEC 27007 и какие аспекты аудита он охватывает?

29. Какие особенности аудита по ISO/IEC 27007 отличают его от общих рекомендаций ISO 19011?

30. Что такое ITGC и какую роль эти контроли играют в аудите информационных систем?

31. Приведите примеры трёх основных категорий ITGC и кратко опишите каждую

32. Какие риски могут возникнуть при отсутствии надлежащих ITGC в организации?

9. Материально-техническое и учебно-методическое обеспечение дисциплины

9.1. Перечень основной и дополнительной учебной литературы

Основная литература

1. Гулак М. Л. Аудит информационной безопасности. Прикладная статистика: учебное пособие: учебное пособие / М. Л. Гулак, М. Ю. Рытов, О. М. Голембиовская. - Аудит информационной безопасности. Прикладная статистика - Москва: Ай Пи Ар Медиа, 2020. - 121 с. - 978-5-4497-0713-0. - Текст: электронный. // IPR SMART: [сайт]. - URL: <https://www.iprbookshop.ru/97630.html> (дата обращения: 16.03.2025). - Режим доступа: по подписке

2. Макаренко С. И. Аудит безопасности критической инфраструктуры специальными информационными воздействиями: монография: монография / С. И. Макаренко. - Аудит безопасности критической инфраструктуры специальными информационными воздействиями - Санкт-Петербург: Научные технологии, 2018. - 123 с. - 978-5-6041427-8-3. - Текст: электронный. // IPR SMART: [сайт]. - URL: <https://www.iprbookshop.ru/130084.html> (дата обращения: 16.03.2025). - Режим доступа: по подписке

Дополнительная литература

1. Подольский В. И. Компьютерные информационные системы в аудите: учебное пособие для студентов вузов, обучающихся по специальности «бухгалтерский учет, анализ, аудит»: учебное пособие для студентов вузов, обучающихся по специальности «бухгалтерский учет, анализ, аудит» / В. И. Подольский, Н. С. Щербакова, В. Л. Комиссаров; под редакцией В. И. Подольского. - Компьютерные информационные системы в аудите - Москва: ЮНИТИ-ДАНА, 2023. - 160 с. - 5-238-01141-5. - Текст: электронный. // IPR SMART: [сайт]. - URL: <https://www.iprbookshop.ru/142668.html> (дата обращения: 16.03.2025). - Режим доступа: по подписке

2. Осташенко Е. Г. Организация внутреннего аудита: учебное пособие: учебное пособие / Е. Г. Осташенко. - Организация внутреннего аудита - Омск: Издательство Омского государственного университета, 2022. - 94 с. - 978-5-7779-2586-2. - Текст: электронный. // IPR SMART: [сайт]. - URL: <https://www.iprbookshop.ru/128909.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

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

Ресурсы «Интернет»

1. <https://www.iprbookshop.ru/> - IPR BOOKS
2. <https://rusneb.ru/> - Национальная электронная библиотека (НЭБ)
3. <https://www.elibrary.ru/> - НЭБ eLIBRARY
4. <https://znanium.ru/> - Электронно-библиотечная система "Znanium"
5. <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

LED-экран - 1 шт.

Автоматизированное рабочее место (АРМ) - 7 шт.

Доска настенная одноэлементная - 1 шт.

Проектор - 1 шт.

Смешанный тип

Автоматизированное рабочее место (АРМ) - 1 шт.

Доска настенная одноэлементная - 2 шт.

Интерактивная панель - 1 шт.

Проектор - 1 шт.

Лекционная аудитория

LED-экран - 1 шт.

Автоматизированное рабочее место (АРМ) - 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;
- 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.