

## **СОГЛАСОВАН**

решением Ученого совета  
АНО ВО «МБИ  
имени Анатолия Собчака»  
(протокол от «19» декабря 2024 г. № 6)

## **АКТУАЛИЗИРОВАН**

решением Ученого совета  
АНО ВО «МБИ  
имени Анатолия Собчака»  
(протокол от «25» декабря 2025 г. № 7)

## **УТВЕРЖДЕН**

приказом ректора  
АНО ВО «МБИ  
имени Анатолия Собчака»  
от «27» декабря 2024 г. № 56

## **УТВЕРЖДЕНА**

**актуализированная версия**  
приказом ректора  
АНО ВО «МБИ  
имени Анатолия Собчака»  
от «30» декабря 2025 г. № 59

## **ФОНД ОЦЕНОЧНЫХ СРЕДСТВ**

по дисциплине

### **Управление информационной безопасностью**

направление подготовки

**40.03.01 Юриспруденция**

направленность (профиль)

**Цифровая криминалистика**

уровень образования

**высшее образование - бакалавриат**

форма обучения

**очная**

год набора

**2025**

Санкт-Петербург

2024

## СОДЕРЖАНИЕ

1. ПЕРЕЧЕНЬ КОМПЕТЕНЦИЙ И ЭТАПЫ ИХ ФОРМИРОВАНИЯ В ПРОЦЕССЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ .....	3
2. СТРУКТУРА ФОС ПО ДИСЦИПЛИНЕ .....	3
3. ПОКАЗАТЕЛИ И КРИТЕРИИ ОЦЕНКИ КОМПЕТЕНЦИЙ .....	5
4. ШКАЛА ОЦЕНИВАНИЯ РЕЗУЛЬТАТА.....	6
5. ПЕРЕЧЕНЬ ЗАДАНИЙ ПО ДИСЦИПЛИНЕ .....	6
5.1. ЗАДАНИЯ ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ: .....	6
5.2. КОНТРОЛЬНЫЕ ВОПРОСЫ ДЛЯ ТЕКУЩЕЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ.....	8
5.3. ПРОМЕЖУТОЧНАЯ АТТЕСТАЦИЯ .....	9
6. МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ, ОПРЕДЕЛЯЮЩИЕ ПРОЦЕДУРЫ ОЦЕНИВАНИЯ .....	10
7. ОСОБЕННОСТИ ОСВОЕНИЯ ДИСЦИПЛИНЫ ДЛЯ ИНВАЛИДОВ И ЛИЦ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ.....	11
7.1. ЗАДАНИЯ ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ ДЛЯ ИНВАЛИДОВ И ЛИЦ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ.....	14
7.2. ЗАДАНИЯ ДЛЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ДЛЯ ИНВАЛИДОВ И ЛИЦ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ.....	14

## 1. ПЕРЕЧЕНЬ КОМПЕТЕНЦИЙ И ЭТАПЫ ИХ ФОРМИРОВАНИЯ В ПРОЦЕССЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Фонд оценочных средств предназначен для оценки результатов обучения по учебной дисциплине. Рабочей программой дисциплины (модуля) предусмотрено формирование следующих компетенций:

Код и наименование компетенции выпускника	Код и наименование индикатора достижения компетенций	Планируемые результаты обучения по дисциплине
УК-2 Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений	УК-2.2. Определяет ожидаемые результаты решения поставленных задач	Знать: нормативные акты и стандарты в области управления информационной безопасностью, Уметь: выполнять планирование, идентификацию и анализ рисков, моделировать риски, проводить мониторинг  Владеть: навыком определения ожидаемых результатов решения поставленных задач

Входной уровень знаний, умений, опыта деятельности, требуемых для формирования компетенции

- понимает принципы работы информационных систем и сетей
- обладает знаниями для проведения анализа рисков и оценки
- способен анализировать информационные потоки и выявлять потенциальные угрозы
- обладает навыками построения моделей угроз и нарушителей
- способен проводить анализ и классификацию информационных рисков
- умеет работать с технической и нормативной документацией
- обладает базовыми навыками проведения аудита информационных систем

## 2. СТРУКТУРА ФОС ПО ДИСЦИПЛИНЕ

Оценка проводится методом сопоставления параметров, продемонстрированной обучающимся продукта деятельности с заданными эталонами и стандартами по критериям.

Таблица – 1.1. Объекты оценивания и наименование оценочных средств

Номер и наименование разделов/тем	Формы текущего контроля успеваемости/ Формы промежуточной аттестации	Объекты оценивания	Вид занятия / Наименование оценочных средств	Форма проведения оценки  Устная/ письменная
Тема 1. Основные понятия информационной безопасности. Угрозы информационной безопасности в информационных системах.	Текущий контроль	Понятие информационной безопасности. Основные определения и критерии классификации угроз. Основные угрозы доступности. Основные угрозы целостности.	СЗ: опрос	устная
Тема 2. Оценочные	Текущий	Международный	СЗ: письменное	письменная

стандарты в информационной безопасности. Стандарты управления информационной безопасностью	контроль	стандарт ISO/IEC 15408. Критерии оценки безопасности информационных систем. Стандарты управления информационной безопасностью BS 7799 и ISO/IEC 17799. Международный стандарт ISO/IEC 27001:2005 "Системы управления информационной безопасности. Требования". Сертификация СУИБ на соответствие ISO 27001.	задание	
Тема 3. Создание СУИБ на предприятии. Методика оценки рисков информационной безопасности компании Digital Security.	Текущий контроль	Этапы создания системы управления ИБ. Содержание этапов разработки и внедрения системы управления ИБ. Внедрение процедур системы управления ИБ.	СЗ: письменное задание	письменная
Тема 4. Современные методы и средства анализа и управление рисками информационных систем компаний.	Текущий контроль	Методика FRAP. Методика OCTAVE. Методика RiskWatch.	ПЗ: практическое задание	письменная
Тема 5. Правовые меры обеспечения информационной безопасности.	Текущий контроль	Законодательно-правовая база обеспечения информационной безопасности на предприятии. Нормативные акты предприятия по информационной безопасности.	СЗ: опрос	устная
Тема 6. Организационные меры обеспечения безопасности компьютерных информационных систем.	Текущий контроль	Особенности организационной защиты компьютерных информационных систем и сетей.	ПЗ: практическое задание	письменная
Тема 7. Программно-технические меры обеспечения информационной безопасности. Идентификация, аутентификация, управление	Текущий контроль	Основные программно-технические меры. Идентификация и аутентификация. Управление доступом.	ПЗ: практическое задание	письменная

доступом				
Тема 8. Протоколирование и аудит, шифрование, контроль целостности	Текущий контроль	Основные задачи протоколирования. Основные методы шифрования. Контроль целостности. Цифровые сертификаты	ПЗ: практическое задание	письменная
Все темы:	Промежуточная аттестация	Обобщенные результаты обучения по овладению теоретическими и знаниями практическими навыками	Тест	письменная

### 3. ПОКАЗАТЕЛИ И КРИТЕРИИ ОЦЕНКИ КОМПЕТЕНЦИЙ

Оценка знаний, умений, владений выражается в пятибалльной системе.

Таблица 3.1 – Текущий контроль

№ п/п	Виды работ	Критерии оценивания			
		Неудовлет- ворительно (2 балла)	Удовлетвори- тельно (3 балла)	Хорошо (4 балла)	Отлично (5 баллов)
1	Работа на лекциях	Отсутствие участия студента в работе на занятии	Единичное высказывание	Высказывание суждений, активное участие в работе на занятии	Высказывание неординарных суждений, активное участие в работе на занятии
2	Работа на семинарских занятиях	Отсутствие участия в обсуждении, решении, неправильное решение	Единичное высказывание, решение с ошибками	Высказывание суждений, активное участие в ходе решения, правильное решение с отдельными замечаниями	Высказывание неординарных суждений, активное участие в ходе решения, правильное решение без ошибок
3	Работа на практических занятиях	Отсутствие участия в обсуждении, решении, неправильное решение	Единичное высказывание, решение с ошибками	Высказывание суждений, активное участие в ходе решения, правильное решение с отдельными замечаниями	Высказывание неординарных суждений, активное участие в ходе решения, правильное решение без ошибок

Критерии оценивания формулируются для каждой компетенции и отражают деятельность обучающегося, поддающуюся измерению.

Таблица 3.2 – Обобщенные критерии оценивания освоения компетенции

Неудовлетворительно (2 балла)	Удовлетворительно (3 балла)	Хорошо (4 балла)	Отлично (5 баллов)
Компетенция не	Компетенция освоена.	Компетенция освоена.	Компетенция освоена.

освоена. Обучающийся не показывает знания, входящие в состав компетенции, не понимает их необходимость и/или не может их применять	Обучающийся показывает общие знания, входящие в состав компетенции, имеет представление об их применении, умение извлекать и использовать основную (важную) информацию из полученных знаний	Обучающийся показывает полноту знаний, демонстрирует умения и навыки решения типовых задач	Обучающийся показывает глубокие знания, демонстрирует умения и навыки решения сложных задач, умение принимать решения, создавать и применять документы, связанные с профессиональной деятельностью; способен самостоятельно решать проблему/задачу на основе изученных методов, приемов и технологий.
---	---	--	---

#### 4. ШКАЛА ОЦЕНИВАНИЯ РЕЗУЛЬТАТА

Таблица 4.1 – Шкала критериев оценивания компетенций

Оценка	Содержание
Неудовлетворительно (2 балла)	Демонстрирует непонимание проблемы, не восприятие материала. Работа незакончена и/или это плагиат
Удовлетворительно (3 балла)	Демонстрирует частичное понимание проблемы. Большинство требований, предъявляемых, к заданию выполнены. Владение элементами заданного материала. В основном выполненный материал понятен и носит целостный характер
Хорошо (4 балла)	Демонстрирует значительное понимание проблемы обозначенной дисциплиной. Все требования, предъявляемые к заданию выполнены. Содержание выполненных заданий раскрыто и рассмотрено с разных точек зрения
Отлично (5 баллов)	Демонстрирует полное понимание проблемы. Все требования, предъявляемые к заданию выполнены. Продемонстрировано уверенное владение материалом дисциплины. Выполненные задания носят целостный характер, выполнены в полном объеме, структурированы, представлены различные точки зрения, продемонстрирован творческий подход

Шкалы оценивания и процедуры оценивания результатов обучения по дисциплине регламентируются Положением о текущем контроле успеваемости и промежуточной аттестации обучающихся по программам высшего образования.

#### 5. ПЕРЕЧЕНЬ ЗАДАНИЙ ПО ДИСЦИПЛИНЕ 5.1. ЗАДАНИЯ ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ:

Таблица - 5.1 Перечень заданий текущего контроля и их наименование

Наименование оценочных средств	Содержание задания
Опрос	Тема 1: 1. Дайте определение информационной безопасности согласно действующему

	<p>законодательству РФ.</p> <ol style="list-style-type: none"> <li>2. Перечислите и охарактеризуйте основные составляющие информационной безопасности (конфиденциальность, целостность, доступность).</li> <li>3. Дайте определение угрозы информационной безопасности. Приведите классификацию угроз по различным критериям.</li> <li>4. Опишите основные источники угроз информационной безопасности. Как они классифицируются?</li> <li>5. Что такое уязвимость информационной системы? Приведите примеры типичных уязвимостей.</li> <li>6. Как осуществляется оценка рисков информационной безопасности? Опишите основные методы.</li> <li>7. Перечислите основные угрозы доступности информационных систем.</li> <li>8. Что такое DoS-атаки и DDoS-атаки? В чём их принципиальное различие?</li> <li>9. Что понимается под целостностью информации? Приведите примеры нарушений целостности.</li> <li>10. Перечислите основные угрозы целостности информационных систем.</li> </ol> <p>Тема 5:</p> <ol style="list-style-type: none"> <li>1. Перечислите основные федеральные законы Российской Федерации, регулирующие информационную безопасность и защиту информации.</li> <li>2. Опишите роль и значение Федерального закона «О персональных данных» в контексте информационной безопасности предприятий.</li> <li>3. Какие международные стандарты и нормативные документы применяются для обеспечения информационной безопасности? Приведите примеры.</li> <li>4. Что такое политика информационной безопасности предприятия? Какие основные элементы она должна включать?</li> <li>5. Какие документы должны быть включены в пакет нормативных актов по ИБ на предприятии (например, политика ИБ, регламенты, инструкции)?</li> <li>6. Какие меры ответственности предусмотрены в нормативных актах предприятия за нарушение требований информационной безопасности?</li> <li>7. Опишите роль службы информационной безопасности в разработке и внедрении нормативных актов на предприятии.</li> <li>8. Какие методы и средства используются для мониторинга соблюдения нормативных требований по ИБ?</li> </ol>
<p>Письменное задание</p>	<p>Тема 2: Проведите сравнительный анализ стандартов BS 7799 и ISO/IEC 17799. Выделите основные сходства и различия между этими стандартами. Опишите практическое применение каждого стандарта. Опишите процесс сертификации СУИБ на соответствие стандарту ISO 27001. Перечислите основные этапы и требования к документации. Проанализируйте преимущества получения сертификации.</p> <p>Тема 3: Опишите основные этапы создания СУИБ. Для каждого этапа укажите цели и задачи, основные действия и мероприятия, инструменты и методы, используемые на данном этапе.</p>
<p>Практическое задание</p>	<p>Тема 4: Исследовать и подготовить краткие описания методик. Провести первичный анализ рисков по методике FRAP. Выполнить оценку рисков по методике OCTAVE. Подготовить сравнительный отчет, включающий сильные и слабые стороны каждой методики, особенности применения для конкретной компании, результаты оценки рисков по каждой методике, рекомендации по выбору оптимальной методики.</p> <p>Тема 6: Сформулируйте основные положения политики информационной безопасности. Определите ключевые принципы защиты информации. Разработайте план внедрения организационных мер. Разработайте систему оценки эффективности внедренных мер.</p> <p>Тема 7: Проведите анализ требований безопасности организации, выявите ключевые угрозы и риски в процессе идентификации и аутентификации. Разработайте архитектуру системы, включая методы идентификации, способы аутентификации (минимум два метода, включая многофакторную аутентификацию). Определите требования к</p>

	<p>компонентам системы (серверная часть, клиентские приложения, базы данных).</p> <p>Тема 8:  Опишите следующие методы шифрования: Симметричное шифрование (AES, DES), Асимметричное шифрование (RSA, DSA), Хеширование (MD5, SHA-256), Комбинированные методы (гибридные криптосистемы). Определите области применения каждого метода. Проведите тестирование системы на соответствие требованиям безопасности. Оцените производительность системы при различных нагрузках. Проведите анализ уязвимостей и предложите меры по их устранению.</p>
--	---

## 5.2 КОНТРОЛЬНЫЕ ВОПРОСЫ ДЛЯ ТЕКУЩЕЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ

### Первая контрольная точка по дисциплине - в форме опроса (устная).

1. Из каких элементов состоит трёхуровневая модель оценки защищенности информационной системы?
2. Какими путями осуществляется стандартизация подходов к обеспечению информационной безопасности и какие международные стандарты для этого применяются?
3. Какие уровни реализуются в технологической модели подсистемы информационной безопасности ИС?
4. С какой целью производится шифрование данных и информации и на каком уровне работы с информацией это применяется?
5. Что такое «единое информационное пространство»? Каковы его составляющие?
6. В каком случае возникает несовместимость вычислительных, информационных и телекоммуникационных устройств?
7. Как можно определить понятие «открытая информационная или программная система»?
8. Какими свойствами обладает открытая система?
9. Что такое итология и какие методы лежат в основе итологии?
10. Какие организации образуют структуру международной стандартизации в области информационных технологий?
11. Какие международные организации занимаются вопросами стандартизации в среде Web-сервисов?
12. Что составляет методологическую основу базиса открытых систем?
13. Какие прикладные программы работают в функциональной среде открытых систем?
14. В чём состоит суть эталонной модели взаимосвязи открытых систем (Open Systems Interconnection)?
15. Сколько уровней взаимодействия содержит модель ВОС? Какие это уровни?
16. Каким образом определяют понятие «профиль открытой системы»?
17. Что является базовой основой профиля?
18. С какой целью была разработана таксономия профилей?
19. Что включает в себя международный стандартизированный профиль ISP?
20. Для чего разработан профиль переносимости приложений APP и какое отношение он имеет к профилю GOSIP?
21. Какие четыре основных типа интерфейсов OSE вводит классификация интерфейсов открытых систем?
22. Что является основными целями разработки OSE и OSI профилей?
23. Каким образом и с помощью каких профилей связаны архитектурный и функциональный уровни открытой информационной системы?
24. Что включает в себя процесс проектирования профиля открытой системы?
25. Какие основные функциональные профили выбираются, komponуются и применяются на стадиях реализации жизненного цикла информационной системы?
26. Какие два основных значения имеет термин Internet?
27. Какие информационные услуги реализуют Internet-службы?
28. Что такое пространство Intranet и чем оно отличается от пространства Internet?

29. Перечислите основные архитектуры компьютерных сетей.
30. Приведите классификацию компьютерных сетей по различным классификационным признакам

**Вторая контрольная точка по дисциплине - в форме опроса (устная).**

1. Какие топологии локальных компьютерных сетей существуют? Определите преимущества и недостатки каждой топологии.
2. Назовите основные физические архитектуры локальных компьютерных сетей.
3. Что является содержанием понятия «экономическая безопасность предприятия»?
4. Как можно охарактеризовать понятие «информационная безопасность» и что оно в себя включает (основные составляющие)?
5. О каких основных аспектах следует говорить при построении систем корпоративной информационной безопасности?
6. Для чего необходимо формировать политику информационной безопасности и из каких основных разделов она состоит?
7. Кто разрабатывает политику информационной безопасности предприятия? Какие менеджеры и специалисты входят в рабочую группу?
8. Какие вопросы информационной безопасности являются ключевыми?
9. Из чего складывается инфраструктура информационной безопасности?
10. Какие существуют виды угроз ИБ и каким образом оцениваются соответствующие риски?
11. На какие виды подразделяется защищаемая информация?
12. Что включает в себя модель информационной безопасности?
13. В каких аспектах рассматриваются мероприятия по защите информации?
14. Каким образом оценивается соотношение эффективности и рентабельности систем информационной безопасности?
15. В каком случае информационная система считается защищенной?
16. Каким образом архитектура информационной системы может способствовать общей информационной безопасности и почему?
17. Чем отличается схема симметричной криптосистемы с закрытым ключом от схемы асимметричной криптосистемы с открытым ключом?
18. Что такое VPN и для каких целей используются эти технологии?
19. Какие типы вирусов выделены в настоящее время?
20. Какие существуют общие правила для пользователей для обеспечения антивирусной безопасности?
21. Каким общим требованиям должен удовлетворять качественный антивирусный программный продукт?

### 5.3. ПРОМЕЖУТОЧНАЯ АТТЕСТАЦИЯ

#### Итоговый тест (с ответами) для проверки сформированности компетенций

УК-2 - Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений

**Вопрос № 1. Выберите один правильный ответ.**

Что такое домен безопасности?

а) собрание участников безопасности, имеющих единый центр, использующий единую базу, единую групповую и локальную политики, ограничение времени работы учётной записи и прочие параметры, значительно упрощающие работу системного администратора организации, если в ней эксплуатируется большое число компьютеров

- б) виртуальная частная сеть с единым центром управления
- в) локальная сеть, не имеющая выхода в сети связи общего пользования
- г) сетевая операционная система

Правильный ответ: а

**Вопрос № 2. Выберите один правильный ответ.**

Какое из требований обязательно для операционных систем, сертифицированных по 5 классу РД СВТ?

- а) Должны быть предусмотрены средства управления, ограничивающие распространение прав на доступ
- б) ОС должна содержать механизм, претворяющий в жизнь дискреционные правила разграничения доступа
- в) Контроль доступа должен быть применим к каждому объекту и каждому субъекту (индивиду или группе равноправных индивидов)
- г) В ОС должен быть реализован диспетчер доступа, т.е. средство, осуществляющее перехват всех обращений субъектов к объектам, а также разграничение доступа в соответствии с заданным принципом разграничения доступа

Правильный ответ: г

**Вопрос № 3. Выберите один правильный ответ.**

Что такое РАМ?

- а) набор библиотек подключаемых модулей шифрования
- б) набор открытых библиотек подключаемых модулей аутентификации
- в) набор открытых библиотек подключаемых модулей резервного восстановления
- г) набор открытых библиотек подключаемых модулей доверенной загрузки

Правильный ответ: б

**Вопрос № 4. Выберите один правильный ответ.**

Уязвимость это:

- а) Совокупность действий, направленная на преодоление системы защиты
- б) Злонамеренное внедрение специального ПО
- в) Слабость в средствах защиты, которую можно использовать для нарушения системы или содержащейся в ней информации.
- г) Результат действия вируса

Правильный ответ: в

## **6. МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ, ОПРЕДЕЛЯЮЩИЕ ПРОЦЕДУРЫ ОЦЕНИВАНИЯ**

Комплект оценочных средств хранится на кафедре, подлежит обновлению по мере необходимости. Для промежуточной аттестации в виде экзамена каждое ОС по дисциплине обновляется и утверждается за 14 дней до начала сессионного периода и хранится в недоступном месте от несанкционированного доступа. Ответственность несет кафедра.

Порядок проведения текущего контроля успеваемости и промежуточной аттестации обучающихся по ОПОП регламентируются Положением о текущем контроле успеваемости и промежуточной аттестации обучающихся по программам высшего образования.

Текущий контроль успеваемости является формой контроля качества знаний обучающихся,

осуществляемого в межсессионный период обучения с целью определения качества освоения ОПОП.

Текущий контроль успеваемости осуществляется: на лекциях, практических (семинарских) занятиях, в рамках контроля самостоятельной работы.

Обучающиеся заранее информируются о критериях и процедуре текущего контроля успеваемости преподавателями по соответствующей учебной дисциплине (модуля).

Успеваемость при текущем контроле характеризует объем и качество выполненной обучающимся работы по дисциплине (модулю).

Педагогические виды и формы, используемые в процессе текущего контроля успеваемости обучающихся, определяются методической комиссией кафедры. Выбираемый вид текущего контроля обеспечивает наиболее полный и объективный контроль (измерение и фиксирование) уровня освоения результатов обучения по дисциплине.

Преподаватели предоставляют сведения о текущей успеваемости обучающихся в рамках проведения текущей аттестации в семестре в деканаты/ учебный отдел института в сроки, определенные внутренними распорядительными документами института.

В целях обеспечения текущего контроля успеваемости преподаватель проводит консультации.

Преподаватель, ведущий занятия семинарского типа, проводит аттестацию обучающихся за прошедший период. Аттестация проводится, если проведено не менее 3 практических (семинарских) или лабораторных занятий, в установленные деканатом сроки, не реже 1 раза за учебный семестр. Обучающиеся аттестуются путем выставления в соответствующую групповую ведомость записей по системе: «аттестован» или «не аттестован».

Преподаватель, проставляя итоги текущей аттестации, доводит результаты аттестации до сведения студенческой группы и объясняет причины отрицательной аттестации по запросу обучающегося.

При аттестации обучающихся учитываются следующие факторы:

– результаты работы на занятиях, показанные при этом знания по дисциплине (модулю), усвоение навыков практического применения теоретических знаний, степень активности на практических (семинарских) занятиях;

– результаты и активность участия в семинарах и коллоквиумах;

– результаты выполнения контрольных работ;

– результаты и объем выполненных заданий в рамках самостоятельной работы обучающихся;

– результаты личных бесед со студентами по материалу учебной дисциплины (модуля);

– посещение студентами, семинарских и практических занятий, лабораторных работ;

– своевременная ликвидация задолженностей по пройденному материалу, возникших вследствие пропуска занятий либо неудовлетворительных оценок по результатам работы на занятиях.

– результаты прохождения контрольных точек по дисциплине.

**Промежуточная аттестация** обучающихся института является формой контроля результатов обучения по дисциплине с целью комплексного определения соответствия уровня и качества знаний, умений и навыков обучающихся требованиям, установленным образовательной программой.

Формирование оценки текущего контроля успеваемости и промежуточной аттестации по итогам освоения дисциплины осуществляется с использованием пятибалльной системы оценки знаний обучающихся.

## **7. ОСОБЕННОСТИ ОСВОЕНИЯ ДИСЦИПЛИНЫ ДЛЯ ИНВАЛИДОВ И ЛИЦ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ**

Адаптированные оценочные материалы содержатся в адаптированной ОПОП. Обучение обучающихся с ограниченными возможностями здоровья при необходимости осуществляется на основе адаптированной рабочей программы с использованием специальных методов

обучения и дидактических материалов, составленных с учетом особенностей психофизического развития, индивидуальных возможностей и состояния здоровья таких обучающихся (обучающегося).

Самостоятельная работа обучающихся с ограниченными возможностями здоровья и инвалидов позволяет своевременно выявить затруднения и отставание и внести коррективы в учебную деятельность. Конкретные формы и виды самостоятельной работы обучающихся лиц с ограниченными возможностями здоровья и инвалидов устанавливаются преподавателем. Выбор форм и видов самостоятельной работы, обучающихся с ограниченными возможностями здоровья и инвалидов осуществляется с учетом их способностей, особенностей восприятия и готовности к освоению учебного материала. Формы самостоятельной работы устанавливаются с учетом индивидуальных психофизических особенностей (устно, письменно на бумаге или на компьютере, в форме тестирования, электронных тренажеров и т.п.).

Основные формы представления оценочных средств – в печатной форме или в форме электронного документа. Для обучающихся с нарушениями зрения предусматривается возможность проведения текущего и промежуточного контроля в устной форме. Для обучающихся с нарушениями слуха предусматривается возможность проведения текущего и промежуточного контроля в письменной форме.

Таблица 7.1. – Категории обучающихся с ОВЗ, способы восприятия ими информации и методы их обучения.

Категории обучающихся по нозологиям		Методы обучения
с нарушениям и зрения	Слепые. Способ восприятия информации: осязательно-слуховой	Аудиально-кинестетические, предусматривающ ие поступление учебной информации посредством слуха и осязания. Могут использоваться при условии, что визуальная информация будет адаптирована для лиц с нарушениями зрения:
	Слабовидящие. Способ восприятия информации: зрительно-осязательно-слуховой	визуально-кинестетические, предполагающие передачу и восприятие учебной информации при помощи зрения и осязания; аудио-визуальные, основанные на представлении учебной информации, при которых задействовано зрительное и слуховое восприятие; аудио-визуально-кинестетические, базирующиеся на представлении информации, которая поступает по зрительному, слуховому и осязательному каналам восприятие.
С нарушениям и слуха	Глухие. Способ восприятия информации: зрительно-осязательный	визуально-кинестетические, предполагающие передачу и восприятие учебной информации при помощи зрения и осязания. Могут использоваться при условии, что аудиальная информация будет адаптирована для лиц с нарушениями слуха:

	Слабослышащие Способ восприятия информации: Зрительно- осязательно- слуховой	аудио-визуальные, основанные на представлении учебной информации, при которых задействовано зрительное и слуховое восприятие; аудиально-кинестетические, предусматривающ ие поступление учебной информации посредством слуха и осязания; аудио-визуально-кинестетические, базирующиеся на представлении информации, которая поступает по зрительному, слуховому и осязательному каналам восприятия.
С нарушениям и опорно- двигательно го аппарата	Способ восприятия информации: зрительно- осязательно- слуховой	<ul style="list-style-type: none"> <li>– визуально-кинестетические;</li> <li>– аудио-визуальные;</li> <li>– аудиально-кинестетические;</li> <li>– аудио-визуально-кинестетические.</li> </ul>

Таблица 7.2. – Способы адаптации образовательных ресурсов.

Условные обозначения:

«+» — образовательный ресурс, не требующий адаптации;

«АФ» — адаптированный формат к особенностям приема-передачи информации обучающихся инвалидов и лиц с ОВЗ формат образовательного ресурса, в том числе с использованием специальных технических средств;

«АЭ» — альтернативный эквивалент используемого ресурса

Категории обучающихся по нозологиям		Образовательные ресурсы				
		Электронные				Печатные
		мультимедиа	графические	аудио	текстовые, электронные аналоги печатных изданий	
С нарушениями зрения	Слепые	АФ	АЭ (например, создание материальной модели графического объекта (3Dмодели))	+	АЭ (например, аудио описание)	АЭ (например, печатный материал, выполненный рельефно-точечным шрифтом Л.Брайля)
	Слабовидящие	АФ	АФ	+	АФ	АФ
С нарушениями слуха	Глухие	АФ	+	АЭ (например, текстовое описание, гиперссылки)	+	+
	Слабослышащие	АФ	+	АФ	+	+

С нарушениями опорно-двигательного аппарата	+	+	+	+	+
---	---	---	---	---	---

Таблица 7.3. - Формы контроля и оценки результатов обучения инвалидов и лиц с ОВЗ

<b>Категории обучающихся по нозологиям</b>	<b>Форма контроля и оценки результатов обучения</b>
С нарушениями зрения	– устная проверка: дискуссии, тренинги, круглые столы, собеседования, устные коллоквиумы и др.; – с использованием компьютера и специального ПО: работа с электронными образовательными ресурсами, тестирование, рефераты, курсовые проекты, дистанционные формы, если позволяет острота зрения - графические работы и др.
С нарушениями слуха	– письменная проверка: контрольные, графические работы, тестирование, домашние задания, эссе, письменные коллоквиумы, отчеты и др.; – с использованием компьютера и специального ПО: работа с электронными образовательными ресурсами, тестирование, рефераты, курсовые проекты, графические работы, дистанционные формы и др.
С нарушениями опорно-двигательного аппарата	– письменная проверка, с использованием специальных технических средств (альтернативных средства ввода, управления компьютером и др.): контрольные, графические работы, тестирование, домашние задания, эссе, письменные коллоквиумы, отчеты и др.; – устная проверка, с использованием специальных технических средств (средств коммуникаций): дискуссии, тренинги, круглые столы, собеседования, устные коллоквиумы и др.; – с использованием компьютера и специального ПО (альтернативных средств ввода и управления компьютером и др.): работа с электронными образовательными ресурсами, тестирование, рефераты, курсовые проекты, графические работы, дистанционные формы - предпочтительнее обучающимся, ограниченным в передвижении и др.

### **7.1. ЗАДАНИЯ ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ ДЛЯ ИНВАЛИДОВ И ЛИЦ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ**

Текущий контроль и промежуточная аттестация обучающихся инвалидов и лиц с ОВЗ осуществляется с использованием оценочных средств, адаптированных к ограничениям их здоровья и восприятия информации, в том числе с использованием специальных технических средств.

Текущий контроль успеваемости для обучающихся инвалидов и лиц с ОВЗ направлен на своевременное выявление затруднений и отставания в обучении и внесения коррективов в учебную деятельность. Возможно осуществление входного контроля для определения его способностей, особенностей восприятия и готовности к освоению учебного материала.

### **7.2. ЗАДАНИЯ ДЛЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ДЛЯ ИНВАЛИДОВ И ЛИЦ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ**

Форма промежуточной аттестации устанавливается с учетом индивидуальных психофизических особенностей (устно, письменно на бумаге, письменно на компьютере, в форме тестирования и т.п.). При необходимости обучающимся предоставляется дополнительное время для подготовки ответа.

Промежуточная аттестация, при необходимости, может проводиться в несколько этапов. Для этого рекомендуется использовать рубежный контроль, который является контрольной точкой по завершению изучения раздела или темы дисциплины, междисциплинарного курса, практик и ее разделов с целью оценивания уровня освоения программного материала. Формы и срок проведения рубежного контроля определяются