АВТОНОМНАЯ НЕКОММЕРЧЕСКАЯ ОРГАНИЗАЦИЯ
«ОБРАЗОВАТЕЛЬНАЯ ОРГАНИЗАЦИЯ ВЫСШЕГО ОБРАЗОВАНИЯ»
«УНИВЕРСИТЕТ ЭКОНОМИКИ И УПРАВЛЕНИЯ»
Факультет экономики, управления и юриспруденции
Кафедра управления и бизнес-информатики

УТВЕРЖДАЮ
Проректор по учебно-
методической работе
_____ / Г.П. Узунова
«02» февраля 2026 г.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ПО ДИСЦИПЛИНЕ

КОМПЬЮТЕРНЫЕ ВИРУСЫ

Направление подготовки
09.03.01 Информатика и вычислительная техника

Профиль: специалист по компьютерным системам

Квалификация выпускника: бакалавр

Для всех
форм обучения

Симферополь, 2026 г.

1. ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ

Средства оценивания в ходе текущего контроля:

– устные опросы в ходе семинарских занятий;
– рефераты;
– тестирование;
– практические задания, выполняемые в ходе семинарского (практического) занятия или рекомендуемые для самостоятельной работы.

Коды компетенции	Результаты освоения ОПОП	Перечень планируемых результатов обучения по дисциплине
ПК-4	Способен разрабатывать, внедрять и адаптировать прикладное программное обеспечение	ПК-4.1. Знать: программные шаблоны; метрики и риски тестирования; базовые понятия качества программного продукта и качества процесса разработки программного обеспечения; основные концепции и атрибуты качества программного обеспечения (надежности, безопасности, удобства использования); функциональные характеристики применения программного обеспечения. ПК-4.2. Уметь: реализовывать программные продукты на языках программирования высокого уровня; описывать архитектуру программного средства включая выделение: функциональных компонентов и модулей, структур данных, внешних и внутренних интерфейсов; применять соответствующие программные или аппаратные архитектурные решения; использовать модели данных; анализировать и оценивать архитектуру на предмет атрибутов качества. ПК-4.3. Владеть: навыками планирования процесса разработки программного продукта; навыками задания функциональных рамок подсистем; навыками определения наиболее значимых критериев качества программного продукта

1.1 Вопросы к текущему контролю

1 Что делает вирус после попадания в систему?
2 Какие типы файлов чаще заражаются вирусами?
3 Может ли вирус существовать без файла-хоста?
4 Что такое резидентный вирус?
5 Что такое нерезидентный вирус?
6 Как вирусы маскируются под легальные программы?
7 Что такое загрузочный сектор?
8 Как вирусы используют автозапуск?
9 Чем опасны макросы в документах?
10 Что такое криптовирус?
11 Какие есть признаки заражения ПК?
12 Как работает самораспространяющийся червь?

13 Что такое эксплойт-кит?
14 Какие функции выполняет троян?
15 Почему антивирус может не обнаружить вирус?
16 Что такое ложное срабатывание антивируса?
17 Как обновление системы снижает риск заражения?
18 Что такое сигнатура вируса?
19 Чем отличается вредоносное ПО от потенциально нежелательного?
20 Какие существуют типы сканирования антивирусом?
21 Что такое карантин в антивирусе?
22 Можно ли восстановить заражённый файл?
23 Какие угрозы создают USB-устройства?
24 Что такое zero-day уязвимость?
25 Как работает фаервол?
26 Чем опасны нелицензионные программы?
27 Как вирусы используют электронную почту?
28 Что такое социальная инженерия?
29 Как определить подозрительное письмо?
30 Что такое DDoS-атака?
31 Как ботнеты используются злоумышленниками?
32 Что такое keylogger?
33 Какие данные могут красть вирусы?
34 Что такое шифрование вредоносных файлов?
35 Как работает антивирус в реальном времени?
36 Что такое песочница?
37 Как вирусы могут скрываться в памяти?
38 Что такое backdoor?
39 Какие методы удаления вирусов существуют?
40 Почему важно обучение пользователей безопасности?

1.2 Темы рефератов:

1. История развития компьютерных вирусов.
2. Эволюция вредоносного ПО.
3. Современные виды компьютерных вирусов.
4. Полиморфные и метаморфные вирусы.
5. Сетевые черви и их влияние на инфраструктуру.
6. Троянские программы: современные угрозы.
7. Руткиты и методы их обнаружения.
8. Ботнеты и их применение в киберпреступности.
9. Методы социальной инженерии.
10. Фишинг как инструмент кибератак.
11. Антивирусные технологии: история и развитие.
12. Сигнатурные методы защиты.
13. Эвристический анализ вредоносного ПО.
14. Поведенческий анализ в современных антивирусах.
15. Sandbox-технологии в кибербезопасности.
16. Zero-day уязвимости.
17. Эксплойты и эксплуатация уязвимостей.
18. Защита операционных систем от вирусов.
19. Вирусы в мобильных устройствах.
20. Вредоносное ПО в IoT-устройствах.
21. Криптовирусы и программы-вымогатели.
22. DDoS-атаки и роль ботнетов.
23. Информационная безопасность в интернете.

24. Методы обнаружения вредоносного кода.
25. Роль пользователя в информационной безопасности.
26. Антивирусное ПО: сравнительный анализ.
27. Защита корпоративных сетей от вирусов.
28. Резервное копирование как метод защиты информации.
29. Правовые аспекты компьютерных вирусов .
30. Будущее киберугроз и защита от них.

1.3 Тестовые задания

1. Что такое компьютерный вирус?

а) Программа для ускорения работы ПК

б) Программа, способная самовоспроизводиться и внедряться в другие программы (*Правильный ответ: б*)

в) Программа, предназначенная для защиты системы

г) Утилита для очистки диска

2. Какой тип вредоносного ПО распространяется без участия пользователя?

а) Троян

б) Руткит

в) Червь (*Правильный ответ: в*)

г) Макровирус

3. Основная цель троянской программы?

а) Самовоспроизведение

б) Уничтожение всех файлов системы

в) Маскировка под легальное ПО для выполнения скрытых действий (*Правильный ответ: в*)

г) Ускорение работы системы

4. Что такое фишинг?

а) Метод шифрования данных

б) Антивирусная технология

в) Атака через поддельные сайты и письма с целью получения данных (*Правильный ответ: в*)

г) Вид компьютерного вируса

5. Где чаще всего распространяются макровирусы?

а) В исполняемых файлах

б) В документах с макросами (*Правильный ответ: б*)

в) В BIOS

г) В системных драйверах

6. Что делает антивирус в режиме реального времени?

а) Удаляет все файлы системы

б) Проверяет файлы только после перезагрузки

в) Постоянно контролирует активность системы (*Правильный ответ: в*)

г) Отключает интернет

7. Что такое ботнет?

а) Программа для резервного копирования

б) Антивирусная база данных

в) Сеть зараженных компьютеров, управляемых удаленно (*Правильный ответ: в*)

г) Операционная система

8. Какой признак может указывать на заражение ПК?

а) Ускорение работы системы

б) Уменьшение температуры процессора

в) Появление неизвестных процессов и рекламы (*Правильный ответ: б*)

г) Увеличение свободной памяти

9. Что делает IDS (Intrusion Detection System)?

а) Блокирует вирусы на сервере
б) Шифрует сетевой трафик
в) Обнаруживает подозрительную активность (*Правильный ответ: в*)
г) Ускоряет передачу данных

10. Какой порт по умолчанию используется для HTTPS?
а) 21
б) 80
в) 443 (*Правильный ответ: в*)
г) 25

11. Какие свойства относятся к информационной безопасности?
а) Конфиденциальность
б) Масштабируемость
в) Целостность
г) Доступность
Ответ: а, в, г.

12. Какие методы относятся к аутентификации пользователя?
а) Пароль
б) MAC-адрес
в) Биометрия
г) Шифрование трафика
Ответ: а, в.

13. Какие алгоритмы являются асимметричными?
а) AES
б) RSA
в) ECC
г) DES
Ответ: б, в.

14. Какие угрозы относятся к сетевым атакам?
а) DDoS
б) Phishing
в) SQL-инъекция
г) Дефрагментация диска
Ответ: а, б, в

15. Какие протоколы обеспечивают защищённую передачу данных?
а) HTTPS
б) FTP
в) TLS
г) SSH
Ответ: а, в, г.

16. Какие функции выполняет межсетевой экран (firewall)?
а) Фильтрация трафика
б) Шифрование файлов
в) Блокировка портов
г) Мониторинг пакетов
Ответ: а, в, г.

17. Какие из перечисленного являются криптографическими хэш-функциями?
а) MD5

б) SHA-256
в) RSA
г) SHA-1
Ответ: а, б, г.

18. Какие действия характерны для DDoS-атаки?
а) Перегрузка сервера запросами
б) Удаление файлов с сервера
в) Использование ботнета
Ответ: а, в.
г) Шифрование данных пользователя

19. Какие устройства/системы относятся к защите сети?
а) IDS
б) IPS
в) Firewall
г) Proxy-сервер
Ответ: а, б, в, г.

20. Какие действия относятся к социальной инженерии?
а) Фишинг
б) Подбор паролей
в) Подделка личности
г) Шифрование данных
Ответ: а, б, в.

21. Установить соответствие:

1. Firewall	А) Обнаружение вторжений в сеть
2. IDS	Б) Защищенный туннель поверх интернета
3. VPN	В) Фильтрация сетевого трафика
4. DDos	Г) Массовая перегрузка сервера запросами

22. Установить соответствие:

1. Конфиденциальность	А) Проверка подлинности пользователя
2. Целостность	Б) Защита от несанкционированного доступа
3. Доступность	В) Данные не изменяются без разрешения
4. Аутентификация	Г) Возможность доступа к ресурсам

23. Установить соответствие:

1. RSA	А) Хэш-функция
2. AES	Б) Симметричный алгоритм

3. SHA-256	В) Асимметричный алгоритм
4. ECC	Г) Криптография на эллиптических кривых

24. Установить соответствие:

1. Фишинг	А) Взлом через базу данных
2. Социальная инженерия	Б) Психологическое воздействие на пользователя
3. Brute-force	В) Подбор пароля перебором
4. SQL-инъекция	Г) Поддельные сайты для кражи данных

25. Установить соответствие:

1. HTTPS	А) Протокол передачи файлов
2. SSH	Б) Защищенные веб-протокол
3. FTP	В) Протокол удаленного доступа
4. DNS	Г) Система доменных имен

26. Установить соответствие:

1. Хэш-функция	А) Обратное преобразование зашифрованных данных
2. Шифрование	Б) Преобразование данных в уникальный отпечаток
3. Кодирование	В) Защита информации от чтения без ключа
4. Дешифрование	Г) Представление данных в другом формате

27. Установить соответствие:

1. Proxy-server	А) Маршрутизация сетевых пакетов
2. Firewall	Б) Маскировка IP-адресов
3. NAT	В) Промежуточный сервер
4. Router	Г) Фильтрация трафика

28. Установить соответствие:

1. Malware	А) Саморастространяющийся вирус
2. Trojan	Б) Вредоносное ПО в целом
3. Worm	В) Вирус с маскировкой под полезную

	программу
4. Ransomware	Г) Вирус, шифрующий данные

29. Установить соответствие:

1. SSL/TLS	А) Протокол защищенной передачи
2. IPsec	Б) Защита сетевого уровня
3. VPN	В) Туннелирование трафика
4. HTTPS	Г) Защищенный HTTP

30. Установить соответствие:

1. Логирование	А) Анализ событий безопасности
2. Мониторинг	Б) Запись событий системы
3. Аудит	В) Наблюдение за состоянием сети
4. Система IDS	Г) Обнаружение атак

1.4 Практические задания

Практическое задание № 1.

Признаки заражение компьютера вредоносным ПО.

Задание: определить пять признаков заражения системы по предложенной ситуации.

Практическое задание № 2.

Классификация вредоносных программ.

Задание: Распределите примеры ПО по типам (вирус, червь, троян, вымогатель).

Практическое задание № 3.

Анализ подозрительных процессов ОС.

Задание: Выделить три подозрительных процесса из списка и обосновать выбор.

Практическое задание № 4.

Основные пути заражения ПК.

Задание: перечислить пять способов заражения компьютера и кратко описать каждый.

Практическое задание № 5.

Файловые вирусы.

Задание: опишите принцип заражения файлового вируса.

Практическое задание № 6.

Загрузочные вирусы.

Задание: объясните механизм заражения загрузочного сектора.

Практическое задание № 7.

Троянские программы.

Задание: укажите три функции трояна и приведите пример их действий.

Практическое задание № 8.

Сетевые черви.

Задание: Опишите механизм распространения червя по сети.

Практическое задание № 9.

Макровирусы.

Объясните, как макровирус заражает документы.

Практическое задание № 10.

Программы вымогатели (Ransomware).

Задание: опишите схему шифрования и требования вымогателя.

Практическое задание № 11.

Антивирусное программное обеспечение.

Задание: перечислите основные функции антивируса.

2. КРИТЕРИИ ОЦЕНИВАНИЯ ПРИ ПРОВЕДЕНИИ ТЕКУЩЕГО КОНТРОЛЯ

Вид контроля	Наименование работы	Наименование оценочных средств	Шкала оценивания
Текущий контроль	- Вопросы для обсуждения на занятиях; - Устные опросы по ранее изученному материалу; - Письменные работы: рефераты, тестовые задания; - Практические задания; - Рефераты и доклады по темам (вопросам), вынесенным на самостоятельную работу.	Оценка выступлений на практическом (семинарском) занятии, проверка заданий и аудиторных работ, устный опрос, оценивание докладов, рефератов	отлично хорошо удовлетворительно неудовлетворительно

Критерии оценивания устных ответов обучающихся

Шкала оценивания	Характеристика оценивания
отлично	оценивается ответ, который показывает прочные знания основных процессов изучаемой предметной области, отличается глубиной и полнотой раскрытия темы; владение терминологическим аппаратом; умение объяснять сущность, явлений, процессов, событий, делать выводы и обобщения, давать аргументированные ответы, приводить примеры; свободное владение монологической речью, логичность и последовательность ответа.
хорошо	оценивается ответ, обнаруживающий прочные знания основных процессов изучаемой предметной области, отличается глубиной и полнотой раскрытия темы; владение терминологическим аппаратом; умение объяснять сущность, явлений, процессов, событий, делать выводы и обобщения, давать аргументированные ответы, приводить примеры; свободное владение монологической речью, логичность и последовательность ответа. Однако допускается одна - две неточности в ответе.
удовлетворительно	оценивается ответ, свидетельствующий в основном о знании процессов изучаемой предметной области, отличающийся недостаточной глубиной и полнотой раскрытия темы; знанием основных вопросов теории; слабо сформированными навыками анализа явлений, процессов, недостаточным умением давать аргументированные ответы и приводить примеры; недостаточно свободным владением монологической речью, логичностью и последовательностью ответа. Допускается несколько ошибок в

	содержании ответа.
неудовлетворительно	оценивается ответ, обнаруживающий незнание процессов изучаемой предметной области, отличающийся неглубоким раскрытием темы; незнанием основных вопросов теории, несформированными навыками анализа явлений, процессов; неумением давать аргументированные ответы, слабым владением монологической речью, отсутствием логичности и последовательности. Допускаются серьезные ошибки в содержании ответа.

Критерии оценивания работы обучающихся на практических и семинарских занятиях

Шкала оценивания	Показатели	Критерии
Отлично	1. Полнота выполнения практического и тестового задания (полнота ответа); 2. Своевременность выполнения задания; 3. Последовательность и рациональность выполнения практического задания (логичность и четкость ответа); 4. Правильность ответов на вопросы; 5. Самостоятельность решения (владение дополнительным материалом); 6. Знание нормативно-законодательной базы и терминологии курса	Задание решено самостоятельно. При этом составлен правильный алгоритм решения задания, в логических рассуждениях, в выборе формул и решении нет ошибок, получен верный ответ, задание решено рациональным способом. Дан правильный и исчерпывающий ответ на поставленные теоретические и тестовые вопросы, в которых обучающийся показал всестороннее системное знание программного материала, усвоение основной и дополнительной литературы, четкое владение понятийным аппаратом.
Хорошо		Задание решено с помощью преподавателя. При этом составлен правильный алгоритм решения задания, в логическом рассуждении и решении нет существенных ошибок; правильно сделан выбор формул для решения; есть объяснение решения, но задание решено нерациональным способом или допущено не более двух несущественных ошибок, получен верный ответ. На поставленные теоретические и тестовые вопросы, при которых обучающийся показал достаточный уровень знаний основного программного материала: освоение информации лекционного курса и учебных пособий, овладение понятийным аппаратом, методикой исследований при попытке анализа различных ситуаций.
Удовлетворительно		Задание решено с подсказками преподавателя. Задание решено в общем виде. Обучающийся показал средний уровень знаний основного программного материала, но не мог убедительно аргументировать свой ответ, ошибся в использовании понятийного аппарата, показал недостаточные знания литературных источников.
Неудовлетворительно		Задание не решено. Обучающийся продемонстрировал значительные пробелы в знаниях основного программного материала, не аргументировал свой ответ, показал неудовлетворительные знания понятийного аппарата и специальной литературы.

Критерии оценивания рефератов

Средство контроля	Критерии оценивания	Шкала оценивания
Реферат	Выполнены все требования к написанию и защите реферата: обозначена проблема и обоснована её актуальность, сделан краткий анализ различных точек зрения на рассматриваемую проблему и логично изложена собственная позиция, сформулированы выводы, тема раскрыта полностью, выдержан объём, соблюдены требования к внешнему оформлению, даны правильные ответы на дополнительные вопросы. Реферат раскрывает поднятую проблематику в полном объеме.	отлично
	Основные требования к реферату и его защите выполнены, но при этом допущены недочёты. В частности, имеются неточности в изложении материала; отсутствует логическая последовательность в суждениях; не выдержан объём реферата; имеются упущения в оформлении; на дополнительные вопросы при защите даны неполные ответы. В реферате имеются неточности и предметная область выступления раскрыта не в полной мере.	хорошо
	Имеются существенные отступления от требований к реферированию. В частности: тема освещена лишь частично; допущены фактические ошибки в содержании реферата или при ответе на дополнительные вопросы; во время защиты отсутствует вывод. В реферате не в полной степени раскрыт понятийный аппарат, имеются существенные неточности в процессе формирования выводов.	удовлетвори-тельно
	Тема реферата не раскрыта, обнаруживается существенное непонимание проблемы. Тема реферата не раскрыта или выполнена не по существу ранее поставленного вопроса. Реферат не сдан / доклад не сделан.	неудовлетво-рительно

Критерии оценивания тестов

Средство контроля	Критерии оценивания – процент положительных ответов	Шкала оценивания
Тестирование	90-100	отлично
	70-89	хорошо
	40-69	удовлетворительно
	< 39	неудовлетворительно

3. ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

Средства оценивания в ходе промежуточной аттестации:
– вопросы для зачета с оценкой;
– тестовые задания к зачету с оценкой.

Коды компетенции	Результаты освоения ОПОП	Перечень планируемых результатов обучения по дисциплине
ПК-4	Способен разрабатывать, внедрять и адаптировать прикладное программное обеспечение	ПК-4.1. Знать: программные шаблоны; метрики и риски тестирования; базовые понятия качества программного продукта и качества процесса разработки программного обеспечения; основные концепции и атрибуты качества программного обеспечения (надежности, безопасности, удобства использования); функциональные характеристики применения программного обеспечения. ПК-4.2. Уметь: реализовывать программные продукты на языках программирования высокого уровня; описывать архитектуру программного средства включая выделение: функциональных компонентов и модулей, структур данных, внешних и внутренних интерфейсов; применять соответствующие программные или аппаратные архитектурные решения; использовать модели данных; анализировать и оценивать архитектуру на предмет атрибутов качества. ПК-4.3. Владеть: навыками планирования процесса разработки программного продукта; навыками задания функциональных рамок подсистем; навыками определения наиболее значимых критериев качества программного продукта

3.1. Вопросы к зачету с оценкой

1. Что такое компьютерный вирус и какие его основные признаки?
2. Классификация вредоносных программ.
3. Отличие вируса от червя.
4. Что такое троянская программа?
5. Основные этапы жизненного цикла вируса.
6. Способы заражения файловых систем.
7. Что такое загрузочные вирусы?
8. Полиморфные вирусы: принцип работы.
9. Метаморфные вирусы: особенности.
10. Что такое макровирусы?
11. Вирусы в сетевой среде: особенности распространения.
12. Что такое эксплойт?
13. Руткиты и их назначение.
14. Что такое ботнет?
15. Методы скрытия вредоносного кода.
16. Антивирусные базы данных: принцип работы.
17. Поведенческий анализ в антивирусах.
18. Эвристические методы обнаружения вирусов.
19. Сигнатурный анализ: достоинства и недостатки.
20. Что такое sandbox-анализ?
21. Методы противодействия вирусам на уровне ОС.

22. Основные каналы распространения вредоносного ПО.
23. Социальная инженерия как способ заражения.
24. Фишинг и его роль в распространении вирусов.
25. Методы защиты файловых систем.
26. Резервное копирование как метод защиты.
27. Обновления ПО и их роль в безопасности.
28. Что такое уязвимость системы?
29. Антивирусное программное обеспечение: классификация.
30. Принципы комплексной защиты информации.

3.2. Задания для зачета:

Задание 1

Перечислить 5 признаков заражения ПК вирусом.

Задание 2

Указать 3 возможных источника заражения системы.

Задание 3

Определить тип угрозы по ситуации: «самопроизвольно открываются окна рекламы».

Задание 4

Назвать 3 признака подозрительного процесса в ОС.

Задание 5

Указать 4 типа файлов, наиболее часто используемых для заражения.

Задание 6

Перечислить 5 функций антивирусного ПО.

Задание 7

Указать разницу между сигнатурным и эвристическим анализом.

Задание 8

Назвать 3 причины, почему антивирус может не обнаружить вирус.

Задание 9

Описать назначение режима «карантин».

Задание 10

Перечислить 4 правила обновления антивируса.

Задание 11

Критерии, по которым можно дать определение компьютерного вируса.

Задание 12

Отличить вирус от червя.

Задание 13

Указать 3 особенности троянских программ.

Задание 14

писать принцип работы ransomware (вымогателя).

Задание 15

Назвать 3 способа скрытия вирусов в системе.

Задание 16

Перечислить 4 способа распространения вирусов по сети.

Задание 17

Описать принцип работы фишинга.

Задание 18

Указать 3 признака фишингового письма.

Задание 19

Назвать 3 признака DDoS-атаки.

Задание 20

Указать, что такое ботнет.

Задание 21

Написать алгоритм действий при подозрении на вирус.

Задание 22
Перечислить 5 правил безопасной работы в интернете.
Задание 23
Указать 3 меры защиты USB-носителей.
Задание 24
Назвать 4 способа предотвращения заражения ПК.
Задание 25
Описать роль резервного копирования.
Задание 26
ПК стал сильно тормозить после установки программы — указать возможную причину.
Задание 27
Антивирус отключился сам — назвать 3 возможные причины.
Задание 28
Пользователь перешёл по ссылке из письма и ввёл пароль — что это за атака?
Задание 29
В сети резко вырос трафик — возможная угроза?
Задание 30
Составить 5 мер защиты для учебного компьютерного класса.

4. ОСНОВНЫЕ КРИТЕРИИ ОЦЕНИВАНИЯ ПРИ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

Шкала оценивания уровня сформированности универсальной компетенций (зачет с оценкой)

Формируемые уровни освоения компетенций	Критерии оценивания	Шкала оценивания
Высокий уровень	Изложено правильное понимание вопроса, четко и самостоятельно дан исчерпывающий ответ, содержание раскрыто полно, профессионально, грамотно. Обучающимся усвоена взаимосвязь основных понятий дисциплины в их значении для приобретаемой профессии. Отражает успешное и систематическое применение навыков и умений по данной дисциплине в соответствии с ФГОС.	отлично
Базовый уровень	Изложено правильное понимание вопроса, дано достаточно подробное описание предмета ответа, приведены и раскрыты в тезисной форме основные понятия, относящиеся к предмету ответа. Ответ отражает полное знание учебно-программного материала, систематический характер знаний по дисциплине, а также наличие базового уровня овладения практическими умениями и навыками по данной дисциплине в соответствии с ФГОС	хорошо
Пороговый уровень	Ответ отражает теоретические знание	удовлетвори

	основного учебно-программного материала в объеме, необходимом для дальнейшей учебы и предстоящей работы по профессии. Данная оценка может быть выставлена обучающемуся, допустившему неточности в ответе, но обладающими необходимыми знаниями для их устранения под руководством преподавателя, отмечен начальный уровень овладения практическими умениями и навыками по данной дисциплине в соответствии с ФГОС	тельно
Неудовлетворительный уровень	При ответе обучающегося обнаружено отсутствие знаний, умений и навыков и/или фрагментарные знания основного учебно-программного материала.	неудовлетворительно

Текущий контроль и промежуточная аттестация осуществляются в соответствии с «Положением о текущей и промежуточной аттестации обучающихся в Автономной некоммерческой организации «Образовательная организация высшего образования» «Университет экономики и управления».

Вид промежуточной аттестации – зачет с оценкой.

Форма проведения промежуточной аттестации – письменный зачет.