

Документ подписан простой электронной подписью

Информация о владельце:

ФИО: Узунов Федор Владимирович

Должность: Ректор

Дата подписания: 30.09.2026 08:54:44

Уникальный программный ключ:

fd935d10451b860e912264c0378b448452bfdb603f94388008e29877a6bcbf5

**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

МЕТОДЫ ОЦЕНКИ БЕЗОПАСНОСТИ КОМПЬЮТЕРНЫХ СИСТЕМ

Направление подготовки

10.03.01 «Информационная безопасность»

Профиль

Безопасность компьютерных систем

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
ОПК-12	Способен проводить подготовку исходных данных для проектирования подсистем, средств обеспечения защиты информации и для технико-экономического обоснования соответствующих проектных решений	ОПК-12.1. Формирует требования и разрабатывает внешние спецификации для разрабатываемого программного обеспечения ОПК-12.2. Разрабатывает основные показатели технико-экономического обоснования соответствующих проектных решений

1.1 Вопросы к текущему контролю

1. Понятие «объект информатизации» (ОИ). Классификация объектов по уровню конфиденциальности обрабатываемой информации в РФ.
2. Жизненный цикл создания комплексной системы защиты информации (КСЗИ): основные этапы от обследования до аттестации.
3. Модель угроз безопасности информации: структура документа, источники угроз, уязвимости и способы реализации.
4. Роль ФСТЭК России в системе защиты информации. Основные нормативные документы (приказы №17, №21, №239) и области их применения.
5. Категорирование объектов критической информационной инфраструктуры (КИИ) согласно Ф3-187: критерии значимости и последствия присвоения категории.
6. Организационно-правовые режимы защиты информации: государственная тайна, коммерческая тайна, персональные данные. Различия в процедурах допуска.
7. Лицензирование деятельности в области защиты информации. В каких случаях организации необходима лицензия ФСБ или ФСТЭК для работы с СЗИ?
8. Аттестация объектов информатизации: цели, порядок проведения испытаний и юридическая сила «Аттестата соответствия».
9. Принципы построения КСЗИ: эшелонированная оборона (*Defense in Depth*), принцип наименьших привилегий, разделение обязанностей.
10. Планирование непрерывности бизнеса (BCP) и восстановления после сбоев (DRP): место информационной безопасности в обеспечении устойчивости предприятия.
11. Технические каналы утечки информации (ТКУИ): классификация и физическая природа возникновения акустических и виброакустических каналов.
12. Побочные электромагнитные излучения и наводки (ПЭМИН): механизмы возникновения информативных сигналов при работе СВТ.

13. Методы оценки защищенности выделенных помещений от утечки речевой информации (инструментальный контроль).
14. Способы предотвращения утечки по каналу ПЭМИН: экранирование, фильтрация цепей питания и заземления.
15. Активные методы защиты речевой информации: генераторы шума (белый шум, речеподобная помеха) и виброизлучатели.
16. Защита телефонных линий связи: методы обнаружения несанкционированных подключений и подавления диктофонов.
17. Специальные проверки (СП) и специальные исследования (СИ) технических средств: задачи процедур и применяемое оборудование.
18. Контроль эффективности принятых мер защиты информации: периодичность проверок и методика инструментального контроля зон доступности.
19. Концепция инженерной защиты периметра объекта: физические барьеры, освещение, технические средства обнаружения вторжения.
20. Системы контроля и управления доступом (СКУД): идентификаторы, считыватели, контроллеры. Интеграция с системами учета рабочего времени.
21. Биометрические системы идентификации: типы сканеров (отпечаток, лицо, радужка), оценка надежности (*FAR*, *FRR*) и защита биометрических шаблонов.
22. Системы охранного телевидения (СОТ): аналоговые и IP-камеры, видеоаналитика, глубина архива и интеграция с СКУД.
23. Обеспечение пожарной безопасности серверных помещений и ЦОД: требования к автоматическим установкам газового пожаротушения.
24. Контроль микроклимата в технологических помещениях: мониторинг температуры, влажности и протечек воды в кроссовых и серверных залах.
25. Защита распределительных пунктов (кроссов) и коммутационных шкафов: пломбирование, датчики вскрытия, ограничение доступа персонала.
26. Противодействие проносу/провозу запрещенных предметов: работа металлодетекторов, интроскопов и систем нелинейной локации.
27. Аппаратный модуль доверенной загрузки (АМДЗ): архитектура («Соболь», «Аккорд»), функции контроля целостности и отличия от парольной защиты BIOS/UEFI.
28. Средства антивирусной защиты централизованного типа: архитектура сервера управления, обновление баз, политики для рабочих станций и почтовых шлюзов.
29. Межсетевое экранирование внутри корпоративной сети (микросегментация): принципы разделения трафика между сегментами бухгалтерии, разработки и гостевым Wi-Fi.
30. Системы обнаружения и предотвращения вторжений (*IDS/IPS*): сигнатурный и аномалийный методы анализа, размещение сенсоров в топологии сети.
31. Управление съемными носителями информации: программные средства блокировки USB-портов и контроля записи на отчуждаемые носители.
32. Резервное копирование как элемент КСЗИ: правило «3-2-1», использование ленточных библиотек (*LTO*) и облачных хранилищ для архивов.
33. Криптографическая защита каналов связи внутри объекта: применение VPN-концентраторов для объединения территориально распределенных сегментов ЛВС.
34. Системы мониторинга событий ИБ (*SIEM*): сбор логов от разрозненных источников (ОС, СУБД, СКУД) и корреляция событий для выявления инцидентов.
35. Особенности защиты платформ виртуализации (VMware vSphere, Hyper-V): изоляция гипервизора, защита консоли управления (*vCenter/vSphere Client*).
36. Безопасность контейнеризации (Docker/Kubernetes): различия в механизмах изоляции по сравнению с полными виртуальными машинами.
37. Защита беспроводных сетей стандарта Wi-Fi: эволюция протоколов шифрования (WEP -> WPA2 -> WPA3), типичные атаки на радиодоступ.

38. Интернет вещей (*IoT*) на объекте: специфические угрозы умных устройств (датчики климата, камеры) и методы их безопасной интеграции в сеть.
39. Использование беспилотных летательных аппаратов (БПЛА) для охраны периметра крупных промышленных объектов: преимущества перед стационарными камерами.
40. Организация службы реагирования на компьютерные инциденты (*CSIRT/CERT*) на предприятии: регламенты взаимодействия подразделений при обнаружении атаки.
41. Методология тестирования на проникновение (*Penetration Testing*): планирование работ, правила взаимодействия (*Rules of Engagement*) и отчетность.
42. Аудит физической безопасности методом «Red Teaming»: проведение легализованных попыток проникновения на объект для проверки бдительности охраны.
43. Расследование инцидентов (*Forensics*): порядок изъятия и анализа цифровых доказательств (логи, дампы памяти, видеозаписи).
44. Документационное обеспечение эксплуатации КСЗИ: журналы учета носителей, инструкции администраторов, планы восстановления.

1.2 Темы рефератов:

1. Стандарт ISO/IEC 15408 «Общие критерии» (ОК): история создания, структура документа и основные понятия (профиль защиты, задание по безопасности).
2. Функциональные требования безопасности в ОК: анализ семейств требований FAU (аудит), FRU (использование ресурсов) и FPT (защита функций безопасности).
3. Требования доверия к безопасности (SAR — Security Assurance Requirements): сравнительный анализ уровней оценочного доверия EAL1–EAL7.
4. Процесс сертификации средств защиты информации по профилю защиты: роль регистров сертифицированных продуктов (в РФ и за рубежом).
5. Проектирование задания по безопасности (*Security Target*): методика описания объекта оценки (ОО), его границ и предполагаемой среды эксплуатации.
6. Анализ стойкости криптографических механизмов в рамках ОК: оценка перебора, криптоанализа и соответствие заявленному уровню битовой стойкости.
7. Система сертификации ФСТЭК России: уровни отсутствия недеklarированных возможностей (НДВ) и их сопоставление с уровнями доверия (УД) и EAL.
8. Методология оценки защищенности средств вычислительной техники от НДВ: статический и динамический анализ исходного кода программ.
9. Руководящие документы Гостехкомиссии/ФСТЭК по классам защищенности СВТ: эволюция требований от РД 1992 года до современных методик.
10. Оценка соответствия требованиям приказа ФСТЭК №17 (для ГИС) и №21 (для ИСПДн): выбор мер защиты и способы подтверждения их реализации.
11. Особенности сертификации систем управления базами данных (СУБД): проверка механизмов разграничения доступа и аудита событий на уровне записей.
12. Нормативное регулирование оценки безопасности АСУ ТП критической информационной инфраструктуры (КИИ).
13. Формальные методы доказательства корректности ПО: использование BAN-логики для верификации криптографических протоколов обмена ключами.
14. Модель конечных автоматов для оценки безопасности протокола: выявление состояний гонки (*race conditions*) и логических тупиков (*deadlocks*).
15. Инструменты автоматизированной проверки моделей (*Model Checking*): применение SPIN, NuSMV или Tamarin для поиска уязвимостей в спецификациях.
16. Теоретико-графовые модели компьютерных атак (*Attack Graphs*): построение цепочек эксплуатации уязвимостей и расчет вероятности компрометации системы.
17. Математические модели количественной оценки рисков (*CVSS, FAIR*): методология расчета итогового балла опасности уязвимости.
18. Тестирование на проникновение (*Penetration Testing*): сравнение методологий OSSTMM, OWASP Testing Guide и PTES.

19. Статический анализ защищенности исходного кода (SAST): принципы работы фаззинг-тестирования и инструменты автоматического поиска дефектов (Coverity, SonarQube).
20. Динамический анализ бинарного кода (DAST и IAST): использование эмуляторов (QEMU, Frida) и песочниц для выявления эксплойтов без доступа к исходному коду.
21. Методология Red Teaming: имитация действий реального злоумышленника для оценки эффективности службы мониторинга (Blue Team) и процессов реагирования.
22. Анализ побочных каналов (Side-Channel Analysis): методы измерения времени выполнения (timing attacks) и энергопотребления при оценке аппаратных модулей (HSM, смарт-карты).
23. Bug Bounty программы как непрерывный метод оценки безопасности: экономические стимулы и правовое поле взаимодействия исследователей и компаний.
24. Методы оценки безопасности облачных инфраструктур: анализ матрицы ответственности (Shared Responsibility Model) и фреймворк CIS Benchmarks.
25. Оценка безопасности виртуализации и контейнеризации: изоляция гипервизора, безопасность Docker-демона и оркестратора Kubernetes (Hardening Guidelines).
26. Безопасность мобильных платформ (iOS/Android): модель разрешений приложений, Secure Enclave / TrustZone и методы обхода защитных механизмов ОС.
27. Оценка безопасности интернета вещей (IoT): специфика устройств с ограниченными ресурсами, протоколы связи и угрозы ботнетов (Mirai-подобные атаки).
28. Методы оценки конфигураций операционных систем: сканеры уязвимостей настроек (CIS-CAT) и приведение систем к эталонным образам (Golden Images).
29. Аудит информационной безопасности на соответствие стандарту ISO/IEC 27001: процесс сертификационного аудита, несоответствия и корректирующие действия.
30. Человеческий фактор в оценке безопасности: методы социальной инженерии при проведении тестов на проникновение и способы оценки осведомленности персонала.

1.3 Тестовые задания

1. **Какой международный стандарт является основным для оценки безопасности информационных технологий, известным как «Общие критерии»?** а) ISO/IEC 27001 б) ISO/IEC 15408 в) NIST SP 800-53 г) PCI DSS *Правильный ответ: б*
2. **В терминологии стандарта «Общие критерии» (ОК) объект, который подвергается оценке (программный продукт или система), называется...** а) Профиль защиты (Protection Profile) б) Задание по безопасности (Security Target) в) Объект оценки (Target of Evaluation / TOE) г) Актив (Asset) *Правильный ответ: в*
3. **Какому уровню оценочного доверия EAL («Common Criteria») соответствует методологически протестированный и проверенный проект с применением полуформальных методов?** а) EAL1 (Функциональное тестирование) б) EAL4 (Методическое проектирование, тестирование и проверка) в) EAL7 (Формально верифицированный проект и тестирование) г) EAL2 (Структурное тестирование) *Правильный ответ: в (Примечание: EAL4 — максимальное доверие для коммерческих продуктов без спецтребований; EAL7 — для специализированных/милитари решений).*
4. **Что является основной целью применения метода статического анализа исходного кода (SAST) при оценке безопасности?** а) Поиск уязвимостей в работающем приложении путем отправки вредоносных запросов б) Обнаружение дефектов программирования и небезопасных конструкций в коде без его фактического выполнения в) Проверка физической целостности микросхем процессора г) Измерение производительности сервера под высокой нагрузкой *Правильный ответ: б*
5. **В чем принципиальное отличие динамического анализа (DAST) от статического (SAST)?** а) DAST требует наличия исходного кода приложения на языке C++ б) DAST анализирует приложение во время его работы («черный ящик»), не имея доступа к исходному коду в) DAST работает только с операционными системами Linux г)

DAST предназначен исключительно для поиска грамматических ошибок в документации
Правильный ответ: б

6. Система управления доступом прошла проверку BAN-логикой. Что именно доказывает этот метод оценки? а) Максимальную скорость обработки сетевых пакетов протоколом б) Корректность логики обмена сообщениями и достижение целей аутентификации в криптографическом протоколе в) Отсутствие вирусов в исполняемых файлах системы г) Соответствие цвета корпуса сервера требованиям ГОСТ
Правильный ответ: б

7. Какова основная цель проведения тестирования на проникновение (Penetration Testing) в отличие от обычного сканирования уязвимостей? а) Автоматический сбор списка версий установленного ПО б) Попытка практической эксплуатации найденной уязвимости для подтверждения реальности угрозы и определения вектора атаки в) Установка обновлений безопасности на все рабочие станции г) Подсчет количества компьютеров в локальной сети организации
Правильный ответ: б

8. Оценочный уровень доверия EAL1 отличается от EAL7 прежде всего степенью... а) Стоимости сертификационных испытаний б) Использования формальных математических методов доказательства корректности проекта в) Количества страниц в документации на русском языке г) Поддержки протокола IPv6
Правильный ответ: б

9. При анализе защищенности АСУ ТП критической инфраструктуры какой специфический риск оценивается в первую очередь, помимо конфиденциальности данных? а) Стоимость лицензий на программное обеспечение б) Риск нарушения технологического процесса и физического повреждения оборудования (целостность и доступность) в) Скорость печати документов в бухгалтерии г) Наличие свободного места на жестком диске архивного сервера
Правильный ответ: б

10. Что оценивает метрика «Attack Vector» (AV) в составе CVSS (Common Vulnerability Scoring System)? а) Сложность пароля администратора системы б) Физическое или логическое местоположение злоумышленника относительно уязвимого компонента (локальный доступ или удаленно через сеть) в) Количество сотрудников в отделе информационной безопасности г) Версию операционной системы Windows
Правильный ответ: б

11. Процесс проверки того, что программный модуль выполняет свои функции безопасности именно так, как это описано в спецификации, называется... а) Валидация (Validation) б) Верификация (Verification) в) Виртуализация г) Волатильность
Правильный ответ: б (Подсказка: Verification — "делаем ли мы продукт правильно?" согласно чертежам).

12. Какой российский регулятор устанавливает требования по уровням отсутствия недеklarированных возможностей (НДВ) для средств защиты информации? а) Роскомнадзор б) ФСТЭК России в) Министерство культуры РФ г) Роспотребнадзор
Правильный ответ: б

13. Анализ побочных каналов (Side-Channel Analysis) направлен на оценку безопасности... а) Текстовых конфигурационных файлов б) Аппаратной реализации алгоритмов (по времени выполнения, потреблению энергии или электромагнитному излучению) в) Политик групповой безопасности в Active Directory г) Графического интерфейса пользователя
Правильный ответ: б

14. Что является ключевым отличием Red Teaming от классического Penetration Testing? а) Использование только бесплатных инструментов с открытым исходным кодом б) Оценка готовности всей службы безопасности (людей, процессов и техники) к скрытой и длительной атаке, а не просто поиск технических дыр в) Тестирование проводится только в ночное время г) Обязательное использование радиосвязи между участниками теста
Правильный ответ: б

15. В рамках какого документа разработчик описывает конкретные функции безопасности своего продукта (например, «система осуществляет аудит всех входов

по SSH») для прохождения сертификации? а) Профилю защиты (PP) б) заданию по безопасности (ST) в) Формальной модели политики безопасности г) Руководству администратора *Правильный ответ: б (Примечание: PP — это общие требования заказчика, ST — это то, как конкретный продукт эти требования реализует).*

16. Международный стандарт, определяющий требования к оценке безопасности информационных технологий, известный как «Общие критерии», имеет номер ISO/IEC _____. *(Правильный ответ: 15408)*

17. В рамках методологии CVSS (Common Vulnerability Scoring System) вектор атаки, требующий физического присутствия злоумышленника у устройства, обозначается аббревиатурой ____ (Physical). *(Правильный ответ: P)*

18. Процесс проверки того, что система соответствует заданным требованиям и спецификациям («делаем ли мы систему правильно?»), называется _____. *(Правильный ответ: верификация / verification)*

19. Метод анализа программного обеспечения, при котором изучается исходный или бинарный код без его фактического выполнения на процессоре, называется _____. *(Правильный ответ: статическим / SAST)*

20. Наивысший уровень доверия в «Общих критериях», предполагающий полную формальную верификацию проекта и тестирование, обозначается как EAL _____. *(Правильный ответ: 7)*

21. В российских нормативных документах ФСТЭК отсутствие скрытых функций в программном обеспечении, которые не описаны в документации, называется отсутствием _____ возможностей (НДВ). *(Правильный ответ: недеklarированных)*

22. При тестировании на проникновение этап сбора информации о цели (IP-адреса, домены, версии ПО) называется разведкой или _____. *(Правильный ответ: рекогносцировкой / Reconnaissance)*

23. Модель конечных автоматов и сети Петри используются в методах _____ верификации для доказательства отсутствия логических тупиков в протоколах. *(Правильный ответ: формальной)*

24. Оценка защищенности, при которой специалисты имитируют действия реального государственного хакера для проверки всей службы безопасности (людей и процессов), а не только поиска багов, называется _____ Teaming. *(Правильный ответ: Red)*

25. В стандарте «Общие критерии» документ, описывающий конкретные функции безопасности конкретного продукта (например, конкретной версии СУБД), называется заданием по _____. *(Правильный ответ: безопасности)*

26. Соответствие между методом оценки и его описанием

Метод оценки	Описание
1. Статический анализ (SAST)	А. Попытка практической эксплуатации уязвимости в работающей системе для подтверждения реальности угрозы.
2. Динамический анализ (DAST)	Б. Изучение исходного кода приложения автоматизированными средствами или вручную без запуска программы.
3. Тестирование на проникновение (PenTest)	В. Анализ поведения запущенного приложения путем отправки ему различных входных данных («черный ящик»).
4. Reverse Engineering	Г. Восстановление алгоритмов работы программы путем изучения ее скомпилированного бинарного кода.

Правильные ответы: 1–Б, 2–В, 3–А, 4–Г.

27. Соответствие между уровнем EAL и степенью строгости оценки

Уровень (EAL)	Степень строгости / Характеристика
1. EAL1	А. Полуформальное проектирование и тестирование.
2. EAL4	Б. Функциональное тестирование (самый базовый уровень).
3. EAL5	В. Методическое проектирование, тестирование и проверка (стандарт де-факто для

Уровень (EAL) Степень строгости / Характеристика

коммерческих СЗИ).

4. EAL7 Г. Формально верифицированный проект и тестирование (максимальный уровень).

Правильные ответы: 1–Б, 2–В, 3–А, 4–Г.

28. Соответствие между этапом жизненного цикла разработки и типом анализа безопасности

Этап ЖЦ	Рекомендуемый тип анализа
1. Написание исходного кода	А. Нагрузочное тестирование и аудит конфигурации сервера перед публикацией.
2. Непрерывная интеграция (CI/CD)	Б. Моделирование угроз (<i>Threat Modeling</i>) и статический анализ (SAST).
3. Перед выпуском релиза	В. Автоматизированное сканирование каждого коммита в репозитории.
4. Эксплуатация (промышленная среда)	Г. Регулярный пентест и мониторинг событий ИБ (SIEM).

Правильные ответы: 1–Б, 2–В, 3–А, 4–Г.

29. Соответствие между документом «Общих критериев» и его ролью

Документ	Роль в процессе оценки
1. Protection Profile (PP)	А. Отчет независимого испытательного центра с результатами проверок объекта оценки.
2. Security Target (ST)	Б. Общие требования заказчика к классу продуктов (например, «Требования к межсетевым экранам»).
3. Evaluation Technical Report (ETR)	В. Описание того, как конкретный продукт реализует требования безопасности для получения сертификата.
4. Common Criteria (CC)	Г. Сам фундаментальный стандарт, содержащий каталоги требований и правила оценки.

Правильные ответы: 1–Б, 2–В, 3–А, 4–Г.

30. Соответствие между метрикой CVSS v3.x и её смыслом

Метрика	Смысл показателя
1. Attack Vector (AV)	А. Сложность условий, необходимых для эксплуатации (Low — легко, High — сложно).
2. Attack Complexity (AC)	Б. Требуется ли эксплуатация наличие прав администратора или пользователя (None, Low, High).
3. Privileges Required (PR)	В. Где находится злоумышленник: сеть, соседняя сеть или физический доступ.
4. User Interaction (UI)	Г. Нужно ли участие человека (клик, ввод данных) для успеха атаки.

Правильные ответы: 1–В, 2–А, 3–Б, 4–Г.

1.4 Практические задания

Задание 1. Раскройте структуру стандарта ISO/IEC 15408 «Общие критерии». Опишите назначение следующих компонентов: Профиль защиты (PP), Задание по безопасности (ST) и Объект оценки (TOE).

Задание 2. Сравните уровни оценочного доверия EAL1–EAL7. Почему уровень EAL4 считается «золотым стандартом» для коммерческих продуктов, а EAL7 применяется крайне редко?

Задание 3. Разработайте перечень функциональных требований безопасности (SFR) для системы обнаружения вторжений (IDS). Используйте классы FAU (аудит) и IDS из каталога «Общих критериев».

Задание 4. В чем заключается разница между сертификацией средства защиты информации (СЗИ) в лаборатории и аттестацией объекта информатизации (ОИ) непосредственно на предприятии заказчика?

Задание 5. Опишите процесс сертификации программного продукта в системе ФСТЭК России. Какие российские нормативные документы (уровни НДВ / Уровни Доверия) соответствуют международной методологии ОК?

Задание 6. Что такое «уверенность в корректности» (assurance)? Приведите примеры действий разработчика, повышающих доверие к продукту без изменения его функциональности.

Задание 7. Постройте модель нарушителя для облачного хранилища данных. Определите три типа потенциальных злоумышленников, их ресурсы и вероятные цели.

Задание 8. Используя систему CVSS v3.1, рассчитайте итоговый балл (Base Score) для уязвимости со следующими параметрами:

- Attack Vector (AV): Network (N)
- Attack Complexity (AC): Low (L)
- Privileges Required (PR): None (N)
- User Interaction (UI): None (N)
- Scope (S): Unchanged (U)
- Confidentiality (C): High (H)
- Integrity (I): High (H)
- Availability (A): High (H) (*Правильный ответ: 9.8 — Критическая опасность*).

Задание 9. Сравните качественные и количественные методы оценки рисков. В каких ситуациях предпочтительнее использовать матрицу рисков (например, 5x5), а в каких — математическое ожидание потерь (ALE)?

Задание 10. Примените фреймворк MITRE ATT&CK для моделирования вектора атаки APT-группы на финансовый сектор. Выберите не менее пяти тактик и соответствующих им техник.

Задание 11. Оценка стоимости актива. Рассчитайте ожидаемые годовые потери (ALE), если стоимость сервера составляет 1 000 000 руб., вероятность выхода его из строя за год — 5%, а коэффициент воздействия (EF) при поломке — 40%. (*Формула: $SLE = Asset Value \times EF$; $ARO = частота$; $ALE = SLE \times ARO$*).

Задание 12. Опишите суть BAN-логики. Какую проблему криптографического протокола позволяет выявить анализ с помощью идеализации сообщений и логических выводов субъекта $\$P \equiv Q \mid \sim X\$$?

Задание 13. Построение графа атак (*Attack Graph*). Для сети из трех узлов (Web-сервер -> Брандмауэр -> СУБД) постройте граф возможных путей компрометации, если Web-сервер имеет уязвимость SQLi, а СУБД доступна только через него.

Задание 14. Чем отличается верификация от валидации в контексте проверки безопасности? Приведите пример утверждения для каждого процесса применительно к межсетевому экрану.

Задание 15. Применение метода анализа деревьев отказов (FTA). Постройте дерево для события «Отказ дата-центра», где причиной является либо пожар (событие А), либо одновременный сбой основного и резервного электропитания (события Б и В).

Задание 16. Сравните методологии тестирования на проникновение OSSTMM и PTES. Какой аспект (технический или управленческий) делает акцент каждая из них?

Задание 17. Статический анализ кода (SAST). Найдите уязвимость в следующем фрагменте C++ и предложите способ исправления: `char buffer[10]; strcpy(buffer, user_input_from_network);` (*Ответ: Переполнение буфера, замена на strncpy с проверкой длины*).

- Задание 18.** Динамический анализ (DAST). Опишите алгоритм работы сканера веб-уязвимостей OWASP ZAP при поиске Reflected XSS.
- Задание 19.** Методология Red Teaming. В чем принципиальное отличие целей Red Team (эмуляция врага) от целей классической команды пентестеров (поиск максимального числа дыр)?
- Задание 20.** Bug Bounty. Составьте политику ответственного разглашения (Vulnerability Disclosure Policy) для интернет-сервиса, указав сроки реагирования на отчет исследователя.
- Задание 21.** Анализ побочных каналов (Side-Channel Analysis). Объясните, как атака по времени выполнения (timing attack) может помочь восстановить закрытый ключ RSA при некорректной реализации функции сравнения строк.
- Задание 22.** Особенности оценки безопасности АСУ ТП (КИИ). Почему классический пентест методом активного сканирования портов недопустим на работающем химическом заводе?
- Задание 23.** Оценка безопасности виртуальной инфраструктуры (VMware/Kubernetes). Назовите три основные угрозы уровня гипервизора (Escape attacks) и способы их минимизации.
- Задание 24.** Безопасность встраиваемых систем (Embedded Systems) и IoT. Проведите оценку поверхности атаки для умной IP-камеры (интерфейсы: Ethernet, Wi-Fi, Bluetooth, RTSP).
- Задание 25.** Оценка конфигураций (Hardening). Сравните использование эталонных образов (Golden Images) и инструментов контроля целостности (Tripwire/AIDE) для серверов Linux.
- Задание 26.** Методы оценки безопасности мобильных приложений (iOS/Android). Роль Jailbreak/Root-detection и SSL Pinning в общей оценке защищенности клиента.
- Задание 27.** Аудит на соответствие ISO/IEC 27001. Опишите разницу между «значительным несоответствием» (Major NC) и «малозначительным» (Minor NC) по результатам проверки СУИБ.
- Задание 28.** Человеческий фактор. Разработка сценария теста методами социальной инженерии (вишинг) для оценки бдительности сотрудников бухгалтерии. Какие метрики будут считаться успешными для службы ИБ?
- Задание 29.** Цифровая криминалистика (Forensics) как метод оценки последствий инцидента. Опишите порядок фиксации состояния оперативной памяти (Live Response) перед выключением скомпрометированного сервера.
- Задание 30.** Автоматизация оценки соответствия. Как инструменты комплаенс-сканирования (OpenSCAP, CIS-CAT) помогают поддерживать безопасность сотен рабочих станций в актуальном состоянии согласно политикам CIS Benchmarks?

2. КРИТЕРИИ ОЦЕНИВАНИЯ ПРИ ПРОВЕДЕНИИ ТЕКУЩЕГО КОНТРОЛЯ

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

	(вопросам), вынесенным на самостоятельную работу.	оценивание докладов, рефератов	
--	---	--------------------------------	--

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	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

Шкала оценивания	Показатели	Критерии
	выполнения практического задания (логичность и четкость ответа);	владение понятийным аппаратом.
Хорошо	4. Правильность ответов на вопросы;	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	5. Самостоятельность решения (владение дополнительным материалом);	
Неудовлетворительно	6. Знание нормативно-законодательной базы и терминологии курса	

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;	хорошо

	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.	
	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.	удовлетворительно
	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.	неудовлетворительно

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 экзамена;
- тестовые задания к экзамену.

Коды компетенции	Результаты освоения ОПОП	Перечень планируемых результатов обучения по дисциплине
ОПК-12	Способен проводить подготовку исходных данных для проектирования подсистем, средств обеспечения защиты информации и для технико-экономического обоснования соответствующих проектных решений	ОПК-12.1. Формирует требования и разрабатывает внешние спецификации для разрабатываемого программного обеспечения ОПК-12.2. Разрабатывает основные показатели технико-экономического обоснования соответствующих проектных решений

3.1. Вопросы к экзамену

1. Понятие «оценка безопасности» и «сертификация». Основные цели проведения оценки компьютерных систем.
2. Международный стандарт ISO/IEC 15408 «Общие критерии» (ОК): история создания и область применения.
3. Структура стандарта ОК: понятия Профиля защиты (PP), Задания по безопасности (ST) и Объекта оценки (TOE).
4. Функциональные требования безопасности (SFR) в ОК: классы FPT (защита функций безопасности) и FAU (аудит).
5. Требования доверия к безопасности (SAR) в ОК: уровни оценочного доверия EAL1–EAL7.
6. Сопоставление уровней EAL («Общие критерии») и Уровней Доверия ФСТЭК России.
7. Российская система сертификации средств защиты информации: роль ФСТЭК и ФСБ.
8. Методология оценки отсутствия недекларированных возможностей (НДВ) в РФ: статический и динамический анализ.
9. Приказ ФСТЭК №17 (ГИС) и №21 (ИСПДн): методы проверки реализации мер защиты.
10. Оценка безопасности критической информационной инфраструктуры (КИИ) согласно Ф3-187 и приказу ФСТЭК №239.
11. Стандарт NIST SP 800-53: структура каталога мер контроля и процесс их выбора.
12. Отраслевой стандарт PCI DSS: основные требования и процедура подтверждения соответствия (QSA-аудит).
13. Британский стандарт BS 7799 и его трансформация в международный ISO/IEC 27001.
14. Роль аудита в процессе оценки безопасности. Виды аудита (внутренний, внешний, комплаенс-аудит).
15. Модели количественной оценки рисков: методика OCTAVE и фреймворк FAIR.
16. Система CVSS (Common Vulnerability Scoring System): метрики Base Score, Temporal Score и Environmental Score.
17. Процесс аттестации объектов информатизации: этапы работ и итоговая документация.
18. Лицензирование деятельности в области технической защиты конфиденциальной информации (ТЗКИ).
19. Документация разработчика при оценке безопасности: Руководство администратора, Руководство пользователя, функциональные спецификации.
20. Проблема преемственности стандартов: переход от Гостехкомиссии (РД СВТ) к современным требованиям ФСТЭК.
21. Математические модели управления доступом: модель Харрисона — Руззо — Ульмана (HRU) и доказательство разрешимости задачи безопасности.
22. Использование BAN-логики для верификации криптографических протоколов обмена ключами.
23. Построение графа атак (Attack Graph): алгоритм формирования цепочек эксплуатации уязвимостей.
24. Количественная оценка риска через ожидаемые годовые потери (ALE — Annual Loss Expectancy).
25. Моделирование угроз с использованием методологии STRIDE (Microsoft) и PASTA.
26. Анализ деревьев отказов (FTA) и событий (ETA) как методы оценки надежности и безопасности систем.
27. Формальная верификация программного кода: использование инструментов Model Checking (SPIN, NuSMV).

28. Теория игр в анализе безопасности: взаимодействие защитника и злоумышленника.
29. Методы нечеткой логики (Fuzzy Logic) для оценки уровня защищенности при неполных исходных данных.
30. Семантический анализ конфигурационных файлов политик безопасности.
31. Тестирование на проникновение (Penetration Testing): сравнение методологий OSSTMM, OWASP Testing Guide и PTES.
32. Этапы пентеста: разведка (Reconnaissance), сканирование, эксплуатация, пост-эксплуатация и отчетность.
33. Red Teaming vs Penetration Testing: различия в целях, глубине охвата и имитируемом противнике.
34. Методология Bug Bounty: правовое поле взаимодействия исследователей и компаний, программы вознаграждения.
35. Статический анализ безопасности кода (SAST): принципы работы, ложноположительные срабатывания (False Positives).
36. Динамический анализ безопасности приложений (DAST): тестирование «черного ящика», фаззинг (Fuzzing).
37. Интерактивный анализ (IAST) и анализ состава ПО (SCA — Software Composition Analysis).
38. Инструментальный контроль защищенности от утечки по техническим каналам (ПЭМИН).
39. Аудит конфигураций операционных систем и СУБД на соответствие CIS Benchmarks.
40. Социальная инженерия как метод оценки человеческого фактора: виды атак (фишинг, вишинг, претекстинг) и способы противодействия.
41. Аппаратный модуль доверенной загрузки (АМДЗ): архитектура, функции контроля целостности и отличия от UEFI Secure Boot.
42. Оценка безопасности микропроцессоров: атака Spectre/Meltdown и методы анализа побочных каналов (Side-Channel Attacks).
43. Анализ прошивок (firmware) встраиваемых систем и IoT-устройств.
44. Технология ARM TrustZone: оценка границы раздела между Normal World и Secure World.
45. Безопасность базовой системы ввода-вывода (BIOS/UEFI): защита от буткитов и rootkit-модификаций прошивки.
46. Методика оценки защищенности беспроводных сетей Wi-Fi: атаки WEP, WPA2 KRACK, преимущества WPA3.
47. Оценка безопасности виртуальной инфраструктуры (VMware vSphere, Hyper-V): угрозы типа VM Escape и изоляция гипервизора.
48. Безопасность контейнеризации (Docker/Kubernetes): отличие механизмов изоляции от традиционных ВМ, проверка манифестов YAML.
49. Оценка облачных сред: матрица ответственности (Shared Responsibility Model) и фреймворк Cloud Security Alliance (CCM).
50. Специфика оценки безопасности программно-определяемых сетей (SDN) и NFV (Network Functions Virtualization).
51. Анализ защищенности протокола DNS: атаки отравления кэша (DNS Poisoning) и технология DNSSEC.
52. Оценка безопасности веб-приложений: OWASP Top 10 актуальных лет (SQLi, XSS, Broken Access Control).
53. Проверка корректности настройки TLS/SSL: инструменты SSL Labs, поиск слабых шифров и устаревших версий протокола.
54. Оценка безопасности промышленной сети (АСУ ТП/Purdue Model): риски использования Modbus/TCP и Profinet без шифрования.

55. Микросегментация сети: методы верификации правил межсетевого экранирования внутри дата-центра (Zero Trust).
56. Цифровая криминалистика (Computer Forensics) как метод оценки последствий инцидента: порядок сбора доказательств (Chain of Custody).
57. Blue Teaming: построение центра мониторинга ИБ (SOC) и оценка эффективности SIEM-систем.
58. Purple Teaming: синергия атакующих (Red) и защищающихся (Blue) для улучшения детектирования.
59. Планирование непрерывности бизнеса (BCP) и восстановления после катастроф (DRP) как часть комплексной оценки устойчивости.
60. Управление уязвимостями (Vulnerability Management): жизненный цикл устранения (Remediation Lifecycle) и приоритизация патчей.

3.2. Задания для экзамена:

Задание 1. Раскройте структуру стандарта ISO/IEC 15408 «Общие критерии». Опишите назначение следующих компонентов: Профиль защиты (PP), Задание по безопасности (ST) и Объект оценки (TOE).

Задание 2. Сравните уровни оценочного доверия EAL1–EAL7. Почему уровень EAL4 считается «золотым стандартом» для коммерческих продуктов, а EAL7 применяется крайне редко?

Задание 3. Разработайте перечень функциональных требований безопасности (SFR) для системы обнаружения вторжений (IDS). Используйте классы FAU (аудит) и IDS из каталога «Общих критериев».

Задание 4. В чем заключается разница между сертификацией средства защиты информации (СЗИ) в лаборатории и аттестацией объекта информатизации (ОИ) непосредственно на предприятии заказчика?

Задание 5. Опишите процесс сертификации программного продукта в системе ФСТЭК России. Какие российские нормативные документы (уровни НДВ / Уровни Доверия) соответствуют международной методологии ОК?

Задание 6. Что такое «уверенность в корректности» (assurance)? Приведите примеры действий разработчика, повышающих доверие к продукту без изменения его функциональности.

Задание 7. Постройте модель нарушителя для облачного хранилища данных. Определите три типа потенциальных злоумышленников, их ресурсы и вероятные цели.

Задание 8. Используя систему CVSS v3.1, рассчитайте итоговый балл (Base Score) для уязвимости со следующими параметрами:

- Attack Vector (AV): Network (N)
- Attack Complexity (AC): Low (L)
- Privileges Required (PR): None (N)
- User Interaction (UI): None (N)
- Scope (S): Unchanged (U)
- Confidentiality (C): High (H)
- Integrity (I): High (H)
- Availability (A): High (H) (*Правильный ответ: 9.8 — Критическая опасность*).

Задание 9. Сравните качественные и количественные методы оценки рисков. В каких ситуациях предпочтительнее использовать матрицу рисков (например, 5x5), а в каких — математическое ожидание потерь (ALE)?

Задание 10. Примените фреймворк MITRE ATT&CK для моделирования вектора атаки APT-группы на финансовый сектор. Выберите не менее пяти тактик и соответствующих им техник.

Задание 11. Оценка стоимости актива. Рассчитайте ожидаемые годовые потери (ALE), если стоимость сервера составляет 1 000 000 руб., вероятность выхода его из строя за год

— 5%, а коэффициент воздействия (EF) при поломке — 40%. (Формула: $SLE = Asset Value \times EF$; $ARO = частота$; $ALE = SLE \times ARO$).

Задание 12. Опишите суть BAN-логики. Какую проблему криптографического протокола позволяет выявить анализ с помощью идеализации сообщений и логических выводов субъекта $\$P \equiv Q \mid \sim X\$$?

Задание 13. Построение графа атак (*Attack Graph*). Для сети из трех узлов (Web-сервер -> Брандмауэр -> СУБД) постройте граф возможных путей компрометации, если Web-сервер имеет уязвимость SQLi, а СУБД доступна только через него.

Задание 14. Чем отличается верификация от валидации в контексте проверки безопасности? Приведите пример утверждения для каждого процесса применительно к межсетевому экрану.

Задание 15. Применение метода анализа деревьев отказов (*FTA*). Постройте дерево для события «Отказ дата-центра», где причиной является либо пожар (событие А), либо одновременный сбой основного и резервного электропитания (события Б и В).

Задание 16. Сравните методологии тестирования на проникновение OSSTMM и PTES. Какой аспект (технический или управленческий) делает акцент каждая из них?

Задание 17. Статический анализ кода (*SAST*). Найдите уязвимость в следующем фрагменте C++ и предложите способ исправления: `char buffer[10]; strcpy(buffer, user_input_from_network);` (Ответ: *Переполнение буфера, замена на strncpy с проверкой длины*).

Задание 18. Динамический анализ (*DAST*). Опишите алгоритм работы сканера веб-уязвимостей OWASP ZAP при поиске Reflected XSS.

Задание 19. Методология Red Teaming. В чем принципиальное отличие целей Red Team (эмуляция врага) от целей классической команды пентестеров (поиск максимального числа дыр)?

Задание 20. Bug Bounty. Составьте политику ответственного разглашения (*Vulnerability Disclosure Policy*) для интернет-сервиса, указав сроки реагирования на отчет исследователя.

Задание 21. Анализ побочных каналов (*Side-Channel Analysis*). Объясните, как атака по времени выполнения (*timing attack*) может помочь восстановить закрытый ключ RSA при некорректной реализации функции сравнения строк.

Задание 22. Особенности оценки безопасности АСУ ТП (КИИ). Почему классический пентест методом активного сканирования портов недопустим на работающем химическом заводе?

Задание 23. Оценка безопасности виртуальной инфраструктуры (VMware/Kubernetes). Назовите три основные угрозы уровня гипервизора (Escape attacks) и способы их минимизации.

Задание 24. Безопасность встраиваемых систем (*Embedded Systems*) и IoT. Проведите оценку поверхности атаки для умной IP-камеры (интерфейсы: Ethernet, Wi-Fi, Bluetooth, RTSP).

Задание 25. Оценка конфигураций (*Hardening*). Сравните использование эталонных образов (*Golden Images*) и инструментов контроля целостности (Tripwire/AIDE) для серверов Linux.

Задание 26. Методы оценки безопасности мобильных приложений (iOS/Android). Роль Jailbreak/Root-detection и SSL Pinning в общей оценке защищенности клиента.

Задание 27. Аудит на соответствие ISO/IEC 27001. Опишите разницу между «значительным несоответствием» (Major NC) и «малозначительным» (Minor NC) по результатам проверки СУИБ.

Задание 28. Человеческий фактор. Разработка сценария теста методами социальной инженерии (вишинг) для оценки бдительности сотрудников бухгалтерии. Какие метрики будут считаться успешными для службы ИБ?

Задание 29. Цифровая криминалистика (*Forensics*) как метод оценки последствий инцидента. Опишите порядок фиксации состояния оперативной памяти (Live Response) перед выключением скомпрометированного сервера.

Задание 30. Автоматизация оценки соответствия. Как инструменты комплаенс-сканирования (OpenSCAP, CIS-CAT) помогают поддерживать безопасность сотен рабочих станций в актуальном состоянии согласно политикам CIS Benchmarks?

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 знания 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	удовлетворительно

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 – экзамен.

Форма проведения промежуточной аттестации – письменный экзамен.