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

ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

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
ОПК-4	Способен участвовать в разработке стандартов, норм и правил, а также технической документации, связанной с профессиональной деятельностью	ОПК-4.1. Знать: основные стандарты оформления технической документации на различных стадиях жизненного цикла информационной системы. ОПК-4.2. Уметь: применять стандарты оформления технической документации на различных стадиях жизненного цикла информационной системы. ОПК-4.3. Владеть: составления технической документации на различных этапах жизненного цикла информационной системы
ОПК-7	Способен участвовать в настройке и наладке программно-аппаратных комплексов	ОПК-7.1. Знать: методы настройки, наладки программно-аппаратных комплексов. ОПК-7.2. Уметь: анализировать техническую документацию, производить настройку, наладку и тестирование программно-аппаратных комплексов. ОПК-7.3. Владеть: навыками проверки работоспособности программно-аппаратных комплексов

1.1 Вопросы к текущему контролю

1 Что такое информационная безопасность?

2 Опишите национальные интересы России в информационной сфере.

3 Какие статьи в Федеральном законе 149-ФЗ касаются способов обмена и распространения информации?

4 Какие положения Федерального закона 149-ФЗ устанавливают обязанности по защите информации?

5 Чем свободно распространяемая информация отличается от общедоступной?

6 Что представляет собой Доктрина информационной безопасности Российской Федерации? Назовите ее основные разделы.

7 Опишите систему государственных органов России, ведущих деятельность в области информационной безопасности.

8 Каким образом следует поддерживать актуальные знания о нормативно-правовом регулировании в сфере информации, информационных технологий и защиты информации?

9 В чем отличие информационной безопасности от безопасности информации?

10 Что такое информационная система и как это понятие связано с информационной безопасностью?
11 Каковы цели защиты информации в информационной системе?
12 Какие вы знаете управляющие документы для составления модели угроз?
13 Какие угрозы разрешается вписывать в модель угроз? Можно ли вписать угрозу, которую сформулировали вы сами?
14 Что такое модель нарушителя? Каким критериям удовлетворяет нарушитель со средним потенциалом?
15 Почему в модели угроз настоятельно не рекомендуется повышать потенциал нарушителя без веских причин?
16 Какие уязвимости обычно включают в модель угроз? Можно ли включать уязвимости, не указанные в стандарте?
17 Что такое частная модель угроз? Почему некоторые угрозы, включенные в рассмотрение ранее, могут быть неактуальными и зачем их оставляют в конечном варианте модели угроз?
18 Почему методика оценки рисков по угрозам и уязвимостям не рекомендуется для больших организаций?
19 Почему суммарные риски при работе по трем базовым угрозам не совпадают с рисками, вычисленными в режиме одной базовой угрозы?
20 Объясните – на чем может быть основан ваш выбор уровня допустимого риска после получения выходных данных работы алгоритма оценки рисков?
21 Какая еще характеристика, кроме эффективности, важна для применения (или неприменения) выбранной контрмеры?
22 Как соотносятся между собой расчетная эффективность комплекса контрмер и бюджет защиты информации в организации?
23 Назовите и охарактеризуйте принципы засекречивания информации.
24 Назовите и охарактеризуйте организационно-правовые формы засекречивания информации.
25 Назовите и охарактеризуйте виды сведений, подлежащих и не подлежащих рассекречиванию.
26 Дайте классификацию защищаемой информации по принадлежности, содержанию и степени секретности.
27 Раскройте понятие государственной тайны.
28 Какие сведения подлежат засекречиванию и какие не могут быть засекречены?
29 Как осуществляется определение грифа секретности сведений, составляющих государственную тайну?
30 Как осуществляется допуск к государственной тайне, какие есть основания для отказа в допуске и для прекращения допуска?
31 Какая предусмотрена ответственность за нарушение законодательства о коммерческой тайне?
32 Охарактеризуйте цели незаконного получения сведений, составляющих коммерческую тайну.
33 Дайте криминологическую характеристику субъектам незаконного собирания сведений, составляющих коммерческую тайну.
34 Назовите способы незаконного получения сведений, составляющих коммерческую тайну.

35 Как осуществляется закрытие свободного доступа к сведениям, составляющим коммерческую тайну?
36 Как осуществляется выявление, предупреждение и пресечение попыток неправомерного завладения сведениями и документами, составляющими коммерческую тайну?
37 Как осуществляется защита от несанкционированного доступа конфиденциальной информации, обрабатываемой средствами вычислительной техники?
38 Как осуществляется защита конфиденциальной информации от утечки по техническим каналам?
39 Как осуществляется защита информации, составляющей профессиональную тайну?
40 Как осуществляется защита информации, составляющей банковскую тайну?
41 Как осуществляется защита сведений, составляющих личную тайну?
42 Перечислите меры по защите секретных и конфиденциальных сведений: правовые, организационные, инженерно-технические и программно-математические.
43 Дайте общую характеристику средствам защиты информации, перечислите требования к ним и решаемые с их помощью задачи.
44 Какая предусмотрена уголовная ответственность за государственную измену, шпионаж, разглашение государственной тайны и утрату секретных документов, в чем заключается объективная и субъективная сторона этих преступлений?
45 Назовите основные концептуальные положения системы защиты информации.
46 Назовите основные положения концепции информационной безопасности.
47 Дайте характеристику основным видам угроз конфиденциальной информации.
48 Какие действия персонала могу привести к неправомерному овладению защищаемой информацией злоумышленником?

1.2 Темы рефератов:

1. История и современные направления защиты информации.
2. Источники угроз защищаемой информации.
3. Организационно-правовые формы засекречивания информации: перечневая форма и система первоначального засекречивания.
4. Классификация защищаемой информации по принадлежности, содержанию и степени секретности.
5. Правовые основы защиты коммерческой тайны за рубежом и в России.
6. Правовые основы защиты коммерческой тайны за рубежом и в России.
7. Ответственность за нарушение законодательства о коммерческой тайне.
8. Организация защиты от несанкционированного доступа конфиденциальной информации, обрабатываемой средствами вычислительной техники.
9. Организация защиты конфиденциальной информации от утечки по техническим каналам.
10. Защита информации, составляющей профессиональную тайну.
11. Защита информации, составляющей банковскую тайну.
12. Защита сведений, составляющих личную тайну.
13. Защита информации об оперативно-розыскной деятельности.
14. Основные концептуальные положения системы защиты информации.
15. Основные положения концепции информационной безопасности.
16. Угрозы конфиденциальной информации.
17. Действия, приводящие к неправомерному овладению защищаемой информацией.
18. Правовая защита информации.
19. Организационная защита информации.

20. Виды инженерно-технических средств защиты информации и их характеристика.
21. Методы и средства криптографической защиты информации.
22. Современные антивирусные технологии и их роль в обеспечении информационной безопасности.
23. Управление доступом к информационным ресурсам: модели и реализация.
24. Безопасность облачных вычислений и хранения данных.
25. Социальная инженерия: методы, примеры, способы противодействия.
26. Нормативно-правовое регулирование в области защиты персональных данных (ФЗ-152 и зарубежные аналоги).
27. Аудит информационной безопасности: цели, задачи, методы проведения.
28. Защита информации в мобильных устройствах и приложениях.
29. Роль человеческого фактора в обеспечении информационной безопасности.
30. Международные стандарты в области информационной безопасности (ISO/IEC 27001, NIST и др.).

1.3 Тестовые задания

1. Какие статьи в Федеральном законе № 149-ФЗ «Об информации, информационных технологиях и защите информации» посвящены интернету?

а) Статьи 1, 2, 3.
б) Статьи 10, 12, 15.
в) Статьи 15.1, 15.2, 15.3. (*Правильный ответ: в*)
г) Статьи 20, 21, 22.

2. Какие статьи в Федеральном законе № 149-ФЗ описывают виды информации и их особенности?

а) Статьи 1, 2, 3. (*Правильный ответ: а*)
б) Статьи 10, 12, 15.
в) Статьи 15.1, 15.2, 15.3.
г) Статьи 20, 21, 22.

3. Какой этап решения проблем защиты информации характеризовался тем, что под этой деятельностью подразумевалось предупреждение несанкционированного получения защищаемой информации?

а) Этап, связанный с развитием криптографии.
б) Этап, связанный с внедрением технических средств защиты. (*Правильный ответ: б*)
в) Этап, связанный с формированием комплексного подхода к защите информации.
г) Этап, связанный с законодательным регулированием защиты информации.

4. Какой этап решения проблем защиты информации характеризовался формированием на основе аналитико-синтетической обработки данных всего имеющегося опыта теоретических исследований и практического решения задач защиты научно-методологического базиса защиты информации?

а) Этап, связанный с развитием криптографии.
б) Этап, связанный с внедрением технических средств защиты.
в) Этап, связанный с формированием комплексного подхода к защите информации. (*Правильный ответ: в*)
г) Этап, связанный с законодательным регулированием защиты информации.

5. Какой орган при осуществлении своей деятельности имеет право подготавливать и представлять в установленном порядке Президенту и в Правительство РФ предложения по правовому регулированию вопросов защиты государственной тайны, совершенствованию системы защиты государственной тайны?

а) Межведомственная комиссия по защите государственной тайны. (*Правильный ответ: а*)
б) Министерство обороны РФ.

в) Федеральная служба безопасности России.
г) Служба внешней разведки России.

6. Какие органы государственной системы защиты информации осуществляют подготовку и повышение квалификации специалистов в области обеспечения информационной безопасности, проводят исследования в этой области, разрабатывают учебную и учебно-методическую базу преподавания дисциплин по защите информации?

а) Минцифры России.
б) ФСБ России.
в) ФСТЭК России.
г) Учебно-методические объединения (УМО) и специализированные образовательные организации. (*Правильный ответ: г*)

7. Какой нормативный акт устанавливает порядок обмена между государствами конфиденциальной и массовой информацией?

а) Федеральный закон № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
б) Федеральный закон № 98-ФЗ «О коммерческой тайне».
в) Международные договоры и соглашения между государствами. (*Правильный ответ: в*)
г) Указ Президента РФ «О мерах по обеспечению информационной безопасности Российской Федерации».

8. Какой орган при осуществлении своей деятельности имеет право подготавливать и представлять в установленном порядке Президенту в Правительство РФ предложения по порядку определения размеров ущерба, который может быть нанесен безопасности России вследствие несанкционированного распространения секретных сведений или засекречивания информации, находящейся в собственности предприятий?

а) Министерство обороны РФ.
б) Федеральная служба безопасности России.
в) Межведомственная комиссия по защите государственной тайны. (*Правильный ответ: в*)
г) Служба внешней разведки России.

9. Какой из перечисленных признаков не является обязательным для отнесения информации к категории коммерческой тайны?

а) Информация имеет действительную или потенциальную коммерческую ценности в силу ее неизвестности третьим лицам.
б) К информации нет свободного доступа на законном основании.
в) Обладатель информации принимает меры по охране ее конфиденциальности.
г) Информация обязательно должна быть зафиксирована на материальном носителе. (*Правильный ответ: г*)

10. Какой этап решения проблем защиты информации характеризовался интенсивными поисками, разработкой и реализацией способов и средств защиты информации?

а) Этап, связанный с развитием криптографии.
б) Этап, связанный с внедрением технических средств защиты. (*Правильный ответ: б*)
в) Этап, связанный с формированием комплексного подхода к защите информации.
г) Этап, связанный с законодательным регулированием защиты информации.

11. Какие исходные данные необходимы для работы алгоритма оценки рисков по угрозам и уязвимостям?

а) Перечень информационных активов, подлежащих защите.
б) Список сотрудников, имеющих доступ к конфиденциальной информации.
в) Модель угроз и модель нарушителя информационной безопасности.
г) Бюджет, выделенный на закупку средств защиты информации.

д) Сведения об актуальных угрозах, уязвимостях и мерах защиты.
Ответ: а, в, д.

12. Какие есть методики оценки рисков информационной безопасности?

а) Качественные (экспертные оценки, матрицы рисков).
б) Количественные (расчет вероятностей ущерба в денежном выражении).
в) Комбинированные (сочетание качественных и количественных подходов).
г) Методика «Дельфи» (многоэтапный анонимный опрос экспертов).
Ответ: а, б, в, г.

13. Какие элементы описания информационной системы являются обязательными?

а) Перечень и состав аппаратных средств (серверы, рабочие станции, сетевое оборудование).
б) Схема информационных потоков и топология сети.
в) Список используемого общесистемного и прикладного программного обеспечения.
г) Предполагаемый срок окупаемости системы.
Ответ: а, б, в.

14. Назовите составляющие автоматизированной системы обработки информации:

а) Эстетическое оформление интерфейса.
б) Программное обеспечение.
в) Техническое обеспечение (аппаратные средства).
г) Организационной обеспечение (регламенты, инструкции, персонал).
д) Информационное обеспечение (данные и базы данных).
Ответ: б, в, г, д.

15. Укажите основные аспекты (свойства) безопасности информации и что они означают:

а) Конфиденциальность.
б) Целостность.
в) Скорость передачи.
г) Доступность.
Ответ: а, б, г.

16. Какие свойства относятся к основным свойствам защищаемой информации?

а) Конфиденциальность.
б) Целостность.
в) Архивирование.
г) Доступность.
Ответ: а, б, в.

17. Какие из перечисленных угроз относятся к угрозам информационной безопасности?

а) Несанкционированный доступ.
б) Вредоносное программное обеспечение.
в) Потеря данных из-за своя оборудования.
г) Использование лицензионного программного обеспечения.
Ответ: а, б, в.

18. Какие средства относятся к техническим средствам защиты информации?

а) Межсетевой экран (Firewall).
б) Антивирусное программное обеспечение.
в) Должностная инструкция сотрудника.
г) Система резервного копирования.
Ответ: а, б, г.

19. Какие способы относятся к методам аутентификации пользователя?

а) Пароль.

б) Архивирование данных.
в) Биометрия.
г) Смарт-карта.
Ответ: а, в, г.

20. Какие методы относятся к криптографическим методам защиты информации?
а) Шифрование.
б) Электронная подпись.
в) Хеширование.
г) Дефрагментация диска.
Ответ: а, б, в.

21. Установить соответствие между термином и определением:

1. Целостность	А) Защита от несанкционированного изменения
2. Доступность	Б) Доступ к информации только уполномоченным лицам
3. Конфиденциальность	В) Возможность получения информации в нужный момент
4. Аутентификация	Г) Проверка подлинности пользователя

22. Установить соответствие между угрозой и примером:

1. Вирус	А) Подбор пароля
2. Фишинг	Б) Вредоносный код в файле
3. DoS-атака	В) Поддельный сайт банка
4. Brute Force	Г) Перегрузка сервера запросами

23. Установить соответствие между средством защиты и функцией:

1. Антивирус	А) Обнаружение вредоносного ПО
2. Межсетевой экран (Firewall)	Б) Фильтрация сетевого трафика
3. VPN	В) Защищенный канал связи
4. IDS	Г) Обнаружение вторжений

24. Установить соответствие между типом аутентификации и примером:

1. По знанию	А) Отпечаток пальца
2. По владению	Б) Пароль
3. Биометрическая	В) Смарт-карта
4. Многофакторная	Г) Пароль и СМС код

25. Установить соответствие между видом шифрования и характеристикой:

1. Симметричное	А) Используются открытый и закрытый

	ключ
2. Асимметричное	Б) Один общий ключ
3. Хеширование	В) Проверка целостности
4. Электронная подпись	Г) Подтверждение авторства

26. Установить соответствие между атакой и уровнем воздействия:

1. Фишинг	А) Веб-приложение
2. Сниффинг	Б) База данных
3. XSS	В) Сетевой трафик
4. SQL-инъекция	Г) Пользователь

27. Установить соответствие между политикой безопасности и содержанием:

1. Парольная политика	А) Правила создания паролей
2. Резервное копирование	Б) Создание копий данных
3. Контроль доступа	В) Разграничение прав
4. Журналирование	Г) Фиксация событий системы

28. Установить соответствие между видом вредоносного ПО и признаком:

1. Троян	А) Самораспространение
2. Червь	Б) Маскировка под полезную программу
3. Шпионское ПО	В) Сбор данных пользователя
4. Ransomware	Г) Шифрование файлов

29. Установить соответствие между методом защиты и назначением:

1. Шифрование	А) Восстановление после себя
2. Аудит	Б) Защита содержания данных
3. Резервное копирование	В) Анализ событий безопасности
4. Обновление ПО	Г) Устранение уязвимостей

30. Установить соответствие между уровнем защиты и примером:

1. Физический	А) Замок серверное
2. Программный	Б) Антивирус
3. Организационный	В) Инструкция ИБ
4. Криптографический	Г) Шифрование AES

1.4 Практические задания

Практическое задание № 1.

Определить полный перечень персональных данных, обрабатываемых в организации. Определить категории обрабатываемых персональных данных. Определить перечень сотрудников, работающих с персональными данными и для каждого установить перечень ПДн. Определить класс информационной системы обработки ПДн. Описать соответствующие меры по защите ПДн.

Практическое задание № 2.

Создать и настроить учетную запись пользователя в семействе ОС Windows и групп пользователей. Настроить локальную политику безопасности для пользователя.

Практическое задание № 3.

Установить антивирусную программу. Настроить основные параметры. Сканировать жесткий диск. Обновить антивирусную программу.

Практическое задание № 4.

Установить файрвол и настроить его параметры. Создать разграничение доступа к сети. Выполнить разрешенные и запрещенные действия в соответствии с настройками. Просканировать сеть.

Практическое задание № 5.

Изучить штатные средства шифрования информации в операционных системах Microsoft Windows.

Практическое задание № 6.

Рассмотреть утилиты и приложения, позволяющие производить аутентификацию в операционной системе при помощи физического объекта — eToken. При этом пароль для входа в операционную систему хранится на физическом объекте, а для доступа к нему используется PIN-код на eToken. Для подключения eToken к компьютеру использовать USB-порт.

Практическое задание № 7.

Оценить риски информационной безопасности на основе программы РискМенеджер. Задайте модель и проведите манипуляции над ней.

Практическое задание № 8.

Выберите информационный процесс, в котором происходит обработка защищаемой информации. Постройте модель «черного ящика» данного процесса в нотации IDEF0. Проведите декомпозицию модели на три-четыре этапа в нотации IDEF0. Скорректируйте модель «черного ящика» после декомпозиции на основе уточненных данных. На основе декомпозиции модели процесса, обрабатывающего защищаемую информацию, выделите перечень защищаемых элементов (все стрелки в декомпозиции) и классифицируйте их на три типа — информационные элементы, исполнители, управление. Приведите по одному примеру угроз конфиденциальности, целостности и доступности для каждого информационного элемента декомпозиции.

Практическое задание № 9.

Изучите нормативно правовые акты, нормативно методические документы по защите информации, в состав которых входят требования и рекомендации по защите информации программными и аппаратными средствами.

Практическое задание № 10.

Выпишите государственные стандарты в области информационной безопасности.

Практическое задание № 11.

Выпишите международные стандарты в области информационной безопасности.

Практическое задание № 12.

Изучите ГОСТ Р ИСО/МЭК 17799-2005 «Информационная технология. Практические правила управления информационной безопасностью». Выпишите

требования и рекомендации по защите информации программными и программно-аппаратными средствами.

Практическое задание № 13.

Изучите технологии учета и хранения информации. Опишите, как происходит сбор и регистрация данных. Назовите основные требования к сбору данных и к хранимым данным. Перечислите основные средства сбора текстовой, графической, звуковой и видеоинформации. Какие еще средства сбора информации вам известны?

Практическое задание № 14.

Изучить технологический процесс обработки информации. Перечислите и охарактеризуйте технологические процессы процесса обработки информации. В чем заключается различие между централизованным и децентрализованным способами обработки информации? Какие режимы обработки информации вам известны?

Практическое задание № 15.

Изучите технологии передачи и представления информации. Опишите как происходит передача данных.

Практическое задание № 16.

Используя средства Интернета, перечислите устройства защиты технических устройств информатизации от изменения напряжения и тока их электропитания.

Практическое задание № 17.

Создайте учетные записи для двух разных пользователей. Для одного пользователя проверьте действенность флажка — требования смены пароля пользователем, для другого — запрет на использование пароля пользователем.

Практическое задание № 18.

Создайте локальную группу. Поместите в локальную группу созданных вами пользователей и административного пользователя. Проделайте это двумя способами: через окно свойств группы и окно свойств пользователя.

Практическое задание № 19.

Опишите параметры локальной политики безопасности операционной системы Windows.

Практическое задание № 20.

Опишите параметры и значения параметров Политики паролей. Заполните таблицу.

Параметр	Значение
Требовать повторяемости паролей	
Максимальный срок действия пароля	
Минимальный срок действия пароля.	
Минимальная длина пароля.	
Пароль должен отвечать требованиям сложности	
Хранить пароли всех пользователей в домене, используя обратимое шифрование.	

Практическое задание № 21.

Опишите параметры и значения параметров Политики учетной записи. Заполните таблицу.

Параметр	Значение
Пороговое значение блокировки	
Блокировка учетной записи на	
Сброс счетчика блокировки через	

Практическое задание № 21.

Опишите параметры и значения параметров Политики аудита. Заполните таблицу

Параметр	Значение
Аудит событий Входа в систему	
Аудит управления Учетными записями	
Аудит доступа к службе каталогов	
Аудит входа в систему	
Аудит доступа к объектам	
Аудит изменения политики	
Аудит использования привилегий	
Аудит отслеживания процессов	
Аудит системных событий	

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-	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,

Шкала оценивания	Показатели	Критерии
	законодательной базы и терминологии курса	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;
– тестовые задания к зачету.

Коды компетенции	Результаты освоения ОПОП	Перечень планируемых результатов обучения по дисциплине
ОПК-4	Способен участвовать в разработке стандартов, норм и правил, а также технической документации, связанной с профессиональной деятельностью	ОПК-4.1. Знать: основные стандарты оформления технической документации на различных стадиях жизненного цикла информационной системы. ОПК-4.2. Уметь: применять стандарты оформления технической документации на различных стадиях жизненного цикла информационной системы. ОПК-4.3. Владеть: составления технической документации на различных этапах жизненного цикла информационной системы
ОПК-7	Способен участвовать в настройке и наладке программно-аппаратных комплексов	ОПК-7.1. Знать: методы настройки, наладки программно-аппаратных комплексов. ОПК-7.2. Уметь: анализировать техническую документацию, производить настройку, наладку и тестирование программно-аппаратных комплексов. ОПК-7.3. Владеть: навыками проверки работоспособности программно-аппаратных комплексов

3.1. Вопросы к зачету

1. История защиты информации.
2. Современные подходы к определению понятия «информационная безопасность».
3. Сущность и структура понятия «информационная безопасность».
4. Объекты информационной безопасности.
5. Связь информационной безопасности с информатизацией общества.
6. Определение понятия «информационная безопасность».
7. Основные понятия и принципы реализации информационной безопасности.
8. Роль разведки в современном мире.

9. Национальные интересы в информационной сфере и их содержание.
10. Социальные интересы личности в информационной сфере.
11. Интересы общества в информационной сфере.
12. Интересы государства в информационной сфере.
13. Интересы сохранения национальной идентичности в информационной сфере.
14. Безопасность национальных интересов в информационной сфере. Соотношение национальных интересов и национальной безопасности. Существующие подходы к содержательной части понятия «защита информации».
15. Понятие уязвимости информации.
16. Виды уязвимости информации.
17. Формы и причины проявления уязвимости информации.
18. Несовершенство или нарушения организации работы с информацией как причина ее утечки.
19. Несовершенство системы защиты информации или нарушения в обеспечении информационной безопасности, как причины утечки информации.
20. Негативные социальные и психологические явления, происходящие в организации или ее структурном подразделении, как причина утечки информации.
21. Высокая ценность информации как причина ее утечки.
22. Уязвимость и информационный риск.
23. Понятие, причины и условия утечки защищаемой информации.
24. Формы и причины проявления уязвимости информации.
25. Классификация угроз информационной безопасности.
26. Основные методы и средства защиты информации.
27. Нормативно-правовое регулирование в области информационной безопасности.
28. Современные тенденции и вызовы в обеспечении информационной безопасности.
29. Роль человеческого фактора в обеспечении и нарушении информационной безопасности.
30. Особенности обеспечения информационной безопасности в условиях цифровой трансформации общества

3.2. Задания для зачета:

Задание 1

Определите основные угрозы информационной безопасности для автоматизированной системы.

Задание 2

Классифицировать возможные каналы утечки информации в организации.

Задание 3

Провести анализ рисков для заданного информационного ресурса.

Задание 4

Разработать перечень мер защиты персональных данных.

Задание 5

Настроить политику сложности паролей для пользователей системы.

Задание 6

Составить модель нарушителя для заданной информационной системы.

Задание 7

Выявить уязвимости в предложенной схеме сетевого взаимодействия.

Задание 8

Выполнить разграничение прав доступа пользователей по ролям.

Задание 9

Разработать политику резервного копирования данных.

Задание 10
Выполнить настройку базовых параметров межсетевого экрана.
Задание 11
Определите способы защиты от вредоносного программного обеспечения.
Задание 12
Проведите анализ инцидента несанкционированного доступа.
Задание 13
Разработайте меры защиты от фишинговых атак.
Задание 14
Выполните настройку двухфакторной аутентификации.
Задание 15
Определите способы защиты информации при передаче по сети.
Задание 16
Выполните шифрование данных с использованием симметричного алгоритма.
Задание 17
Примените электронную подпись для проверки подлинности документа.
Задание 18
Провести проверку целостности файла с использованием хеш-функции.
Задание 19
Настройте параметры антивирусной защиты рабочей станции.
Задание 20
Разработайте план реагирования на инциденты информационной безопасности.
Задание 21
Выполните анализ журналов событий безопасности.
Задание 22
Определите меры защиты веб-приложения от типовых атак.
Задание 23
Проведите аудит безопасности пользовательских учетных записей.
Задание 24
Разработайте правила безопасной работы пользователей в сети Интернет..
Задание 25
Выполните настройку защищенного удаленного соединения.
Задание 26
Определите меры защиты информации в беспроводной сети.
Задание 27
Проведите анализ угроз социальной инженерии.
Задание 28
Разработайте организационные меры защиты информации в учебной организации.
Задание 29
Выполните оценку соответствия системы базовым требованиям информационной безопасности.
Задание 30
Подготовьте рекомендации по повышению уровня защищенности информационной системы.

4. ОСНОВНЫЕ КРИТЕРИИ ОЦЕНИВАНИЯ ПРИ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

Шкала оценивания уровня сформированности универсальной компетенций (зачет)

Шкала	Уровень освоение компетенции	Критерии оценивания

оценивания		
Зачет	Базовый уровень освоения компетенции	Дан правильный и исчерпывающий ответ на вопрос. Обучающийся демонстрирует знание теоретического материала, изложено правильное понимание вопроса, дано достаточно подробное описание предмета ответа, приведены и раскрыты в тезисной форме основные понятия, относящиеся к предмету ответа. Имеется базовый уровень овладения практическими умениями и навыками по данной дисциплине в соответствии с ФГОС .
Незачет	Неудовлетворительный уровень	Отсутствует ответ или в ответе есть грубые ошибки, свидетельствующие о отсутствии знаний соответствующего программного материала; отсутствие умений и навыков по данной дисциплине в соответствии с ФГОС и/или фрагментарные знания основного учебно-программного материала.

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.

Форма проведения промежуточной аттестации – письменный зачет.