

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

fd935d10451b860e912264c037868448452bfdb603f94388008e29877a6bcbf5

**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

**ОРГАНИЗАЦИОННОЕ И ПРАВОВОЕ ОБЕСПЕЧЕНИЕ
ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ**

Направление подготовки

10.03.01 «Информационная безопасность»

Профиль

Безопасность компьютерных систем

Квалификация выпускника: бакалавр

Для всех
форм обучения

Симферополь, 2026 г.

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.

Компетенция УК-1 Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач.		
УК-1.1. Знает	УК-1.2. Умеет	УК-1.3. Владеет
основы системного подхода к осуществлению поиска, критического анализа и синтеза информации для решения поставленных задач.	применять системный подход на основе поиска, критического анализа и синтеза информации для решения задач в профессиональной области.	навыками поиска, синтеза и критического анализа информации в своей профессиональной области; владеет системным подходом для решения поставленных задач.
1.1 № 1-36	1.2. № 1-36	1.3 № 1-35 1.4 № 1-35

1.1 Вопросы к текущему контролю

1. Какие цели преследует правовое обеспечение информационной безопасности?
2. Какие виды нормативных правовых актов регулируют работу с информацией?
3. Чем нормативный правовой акт отличается от локального акта организации?
4. Что понимается под обладателем информации?
5. Как разграничивают общедоступную информацию и информацию ограниченного доступа?
6. Какие обязанности возникают при установлении режима ограниченного доступа?
7. Почему перед применением нормы проверяют ее актуальную редакцию?
8. Как соотносятся закон, подзаконный акт и локальное положение?
9. Какие источники используют для проверки официального текста нормативного акта?
10. Как оформляют правовые основания обработки и передачи информации?
11. Что относится к персональным данным?
12. Какие роли могут участвовать в обработке персональных данных?
13. Для чего определяют цель обработки персональных данных?
14. Как реализуют принцип минимизации обрабатываемых данных?
15. В каких случаях согласие является основанием обработки?
16. Как фиксируют состав и сроки хранения персональных данных?
17. Что учитывают при предоставлении доступа сотруднику к персональным данным?
18. Каким образом организуют исполнение запросов субъектов данных?
19. Что следует сделать при выявлении инцидента с персональными данными?
20. Какие особенности режима коммерческой тайны необходимо учитывать?
21. Что включает политика информационной безопасности?
22. Как распределяют полномочия и ответственность в области защиты информации?
23. Для чего ведут реестр информационных активов?
24. Как определяют владельца информационного актива?
25. Что понимается под принципом минимально необходимых полномочий?

26. Какие этапы включает предоставление доступа?
27. Как пересматривают права доступа при переводе сотрудника?
28. Что включают правила работы с носителями информации?
29. Как организуют обучение и информирование работников?
30. Какие записи подтверждают исполнение организационных мер?
31. Какие вопросы защиты информации отражают в договоре с подрядчиком?
32. Как проверяют допуск внешнего специалиста к информации?
33. Что включают требования к передаче информации третьим лицам?
34. Для чего составляют план внутреннего контроля?
35. Какие признаки позволяют классифицировать событие как инцидент?
36. Какие сведения фиксируют в карточке инцидента?
37. Как разграничивают регистрацию, расследование и устранение причин инцидента?
38. Как организуют сохранение материалов проверки?
39. Каким образом оценивают исполнение корректирующих мер?
40. Зачем проводят периодический пересмотр локальных актов?
41. Какие виды ответственности возможны за нарушение требований в сфере защиты информации?
42. Почему вид ответственности нельзя определять без анализа состава нарушения?
43. Как соотносятся трудовые обязанности и локальные правила работы с информацией?
44. Какие действия нужны перед вводом нового информационного процесса?
45. Как оформить матрицу ролей и доступа для условного подразделения?
46. Что делать при выявлении избыточного права доступа?
47. Как планировать сроки устранения выявленных нарушений?
48. Как проверить исполнимость локальной инструкции?
49. Какие документы нужны для внутренней проверки обработки данных?
50. Как документировать исключения из обычного порядка доступа?
51. Как документируют обучение новых сотрудников правилам защиты информации?
52. Что включают правила использования корпоративной электронной почты?
53. Какие признаки указывают на устаревание локального акта?
54. Как организуют контроль сроков временного доступа?
55. Что нужно проверить перед передачей информации внешнему получателю?
56. Как оформляют исключение из стандартного процесса доступа?
57. Какие обязанности закрепляют за владельцем информационной системы?
58. Как подтверждают удаление доступа после завершения договора?
59. Как отличают факт нарушения от предварительного предположения при проверке?
60. Как оценивают результативность мер после устранения инцидента?

1.2 Темы рефератов:

1. Система правового регулирования информационной безопасности в России.
2. Правовой режим информации ограниченного доступа.
3. Полномочия обладателя информации.
4. Локальные нормативные акты организации по защите информации.
5. Политика информационной безопасности организации.
6. Распределение ролей и ответственности.
7. Инвентаризация информационных активов.
8. Принцип минимально необходимых полномочий.

9. Жизненный цикл учетной записи работника.
10. Организация доступа внешних подрядчиков.
11. Цели и основания обработки персональных данных.
12. Минимизация и сроки хранения персональных данных.
13. Организация приема запросов субъектов персональных данных.
14. Учет операций обработки персональных данных.
15. Порядок реагирования на инциденты с данными.
16. Режим коммерческой тайны в организации.
17. Документирование конфиденциальных обязательств.
18. Контроль обращения с бумажными носителями.
19. Порядок уничтожения носителей информации.
20. Требования к защите информации в договорах.
21. Внутренний контроль информационной безопасности.
22. Аудит выполнения локальных инструкций.
23. Подготовка и обучение работников.
24. Организационные меры удаленной работы.
25. Управление изменениями в информационных процессах.
26. Реестр рисков информационной безопасности.
27. Фиксация и анализ инцидентов.
28. План корректирующих мероприятий.
29. Виды ответственности за нарушения в сфере информации.
30. Актуализация локальных актов при изменении законодательства.

1.3 Тестовые задания

1. Локальный акт организации:

- а) заменяет договоры.
- б) устанавливает внутренний порядок в пределах компетенции организации.
- в) отменяет федеральный закон.
- г) применяется ко всем организациям страны.

Правильный ответ: б.

2. Перед использованием правовой нормы следует:

- а) игнорировать дату вступления в силу.
- б) не уточнять предмет регулирования.
- в) проверить действующую редакцию и область применения.
- г) опираться только на старый конспект.

Правильный ответ: в.

3. Цель обработки персональных данных:

- а) всегда равна сроку трудового договора.
- б) заменяет меры безопасности.
- в) не влияет на сбор данных.
- г) помогает определить необходимый состав данных и операции.

Правильный ответ: г.

4. Принцип минимально необходимых полномочий означает:

- а) предоставление доступа в объеме, необходимом для работы.
- б) доступ ко всем ресурсам каждому сотруднику.
- в) отсутствие пересмотра прав.

г) использование общей учетной записи.

Правильный ответ: а.

5. Владелец информационного актива:

а) не участвует в управлении доступом.

б) отвечает за определение требований к использованию актива в установленном порядке.

в) обязан лично чинить любое оборудование.

г) заменяет всех администраторов.

Правильный ответ: б.

6. Матрица доступа показывает:

а) график отпусков.

б) адреса серверов без ролей.

в) соответствие ролей, ресурсов и разрешенных действий.

г) только стоимость ресурсов.

Правильный ответ: в.

7. При переводе сотрудника нужно:

а) сохранить все прежние права автоматически.

б) передать пароль коллеге.

в) удалить журнал заявок.

г) пересмотреть доступ с учетом новых обязанностей.

Правильный ответ: г.

8. Реестр активов помогает:

а) учитывать ресурсы, владельцев и требования к ним.

б) заменять резервные копии.

в) отменять обучение.

г) исключать договоры.

Правильный ответ: а.

9. Обучение сотрудников требуется для:

а) сокрытия инцидентов.

б) понимания и выполнения установленных правил.

в) замены технической защиты.

г) передачи доступа без проверки.

Правильный ответ: б.

10. Инцидент следует:

а) обсудить только устно.

б) автоматически считать решенным.

в) зарегистрировать и обработать по утвержденному порядку.

г) удалить без записи.

Правильный ответ: в.

11. Срок хранения данных определяют с учетом:

а) предпочтения случайного пользователя.

б) цвета носителя.

в) количества принтеров.

г) цели обработки и применимых обязательных требований.

Правильный ответ: г.

12. Договор с подрядчиком может определять:

а) объем доступа, обязанности по защите и порядок возврата данных.

- б) личные пароли сотрудников.
- в) отмену закона.
- г) доступ без ограничений.

Правильный ответ: а.

13. Внутренний контроль нужен для:

- а) замены всех договоров.
- б) проверки выполнения установленных требований и выявления отклонений.
- в) подмены управления доступом.
- г) исключения учета активов.

Правильный ответ: б.

14. Карточка инцидента содержит:

- а) только дату без описания.
- б) только устную оценку.
- в) время, обстоятельства, последствия и принятые меры.
- г) только номер телефона заявителя.

Правильный ответ: в.

15. Режим коммерческой тайны предполагает:

- а) автоматическую секретность любой информации.
- б) отсутствие учета носителей.
- в) общий доступ без ограничений.
- г) определение защищаемых сведений и введение предусмотренных мер.

Правильный ответ: г.

16. Ограничение доступа к информации вводят:

- а) на соответствующем правовом основании с установленным порядком.
- б) по личному желанию любого работника.
- в) после удаления всех документов.
- г) без указания объекта защиты.

Правильный ответ: а.

17. Правовое основание обработки данных:

- а) не документируют.
- б) устанавливают применительно к конкретной цели и обстоятельствам.
- в) всегда заменяют общим паролем.
- г) определяют только после инцидента.

Правильный ответ: б.

18. Корректирующая мера направлена на:

- а) замену всех сотрудников.
- б) отмену регистрации событий.
- в) устранение причины выявленного несоответствия.
- г) скрытие результатов проверки.

Правильный ответ: в.

19. Передача носителя подрядчику требует:

- а) отсутствия отметок.
- б) передачи через любого посетителя.
- в) общей учетной записи.
- г) установленного порядка учета и подтверждения передачи.

Правильный ответ: г.

20. При изменении законодательства локальные акты:

- а) проверяют на соответствие применимым новым требованиям.
- б) автоматически удаляют.
- в) не пересматривают никогда.
- г) заменяют устным поручением.

Правильный ответ: а.

21. Установите соответствие между понятиями и характеристиками:

Понятие	Характеристика
1. Информационный актив	А. Набор разрешенных действий
2. Владелец актива	Б. Значимый ресурс организации
3. Роль доступа	В. Внутренний порядок операций
4. Локальная инструкция	Г. Лицо, задающее требования к ресурсу

Ответ: 1–Б, 2–Г, 3–А, 4–В.

22. Установите соответствие между понятиями и характеристиками:

Понятие	Характеристика
1. Закон	А. Акт во исполнение закона
2. Подзаконный акт	Б. Внутренний акт организации
3. Договор	В. Акт законодательной власти
4. Локальный акт	Г. Соглашение сторон

Ответ: 1–В, 2–А, 3–Г, 4–Б.

23. Установите соответствие между понятиями и характеристиками:

Понятие	Характеристика
1. Цель обработки	А. Период сохранения сведений
2. Состав данных	Б. Предполагаемый конкретный результат
3. Срок хранения	В. Правовое условие обработки
4. Основание обработки	Г. Перечень обрабатываемых сведений

Ответ: 1–Б, 2–Г, 3–А, 4–В.

24. Установите соответствие между понятиями и характеристиками:

Понятие	Характеристика
1. Заявка на доступ	А. Проверка полномочий
2. Согласование	Б. Прекращение доступа
3. Выдача прав	В. Фиксация потребности
4. Отзыв прав	Г. Техническое предоставление

Ответ: 1–В, 2–А, 3–Г, 4–Б.

25. Установите соответствие между понятиями и характеристиками:

Понятие	Характеристика
1. Владелец процесса	А. Использует разрешенный доступ
2. Администратор	Б. Определяет требования процесса
3. Пользователь	В. Проверяет выполнение правил
4. Контролер	Г. Исполняет настройки

Ответ: 1–Б, 2–Г, 3–А, 4–В.

26. Установите соответствие между понятиями и характеристиками:

Понятие	Характеристика
1. Событие	А. Ситуация, требующая реагирования

2. Инцидент	Б. Устранение причины
3. Расследование	В. Зафиксированный факт
4. Корректирующая мера	Г. Установление обстоятельств

Ответ: 1–В, 2–А, 3–Г, 4–Б.

27. Установите соответствие между понятиями и характеристиками:

Понятие	Характеристика
1. Политика	А. Запись выполнения операций
2. Регламент	Б. Общие принципы защиты
3. Журнал	В. Результаты контроля
4. Акт проверки	Г. Последовательность действий

Ответ: 1–Б, 2–Г, 3–А, 4–В.

28. Установите соответствие между понятиями и характеристиками:

Понятие	Характеристика
1. Предоставление	А. Корректировка объема прав
2. Изменение	Б. Окончательный отзыв
3. Приостановление	В. Начало доступа
4. Прекращение	Г. Временное ограничение

Ответ: 1–В, 2–А, 3–Г, 4–Б.

29. Установите соответствие между понятиями и характеристиками:

Понятие	Характеристика
1. Подрядчик	А. Лицо, к которому относятся данные
2. Работник	Б. Внешний исполнитель
3. Субъект данных	В. Лицо с правом определять доступ
4. Владелец информации	Г. Участник трудового процесса

Ответ: 1–Б, 2–Г, 3–А, 4–В.

30. Установите соответствие между понятиями и характеристиками:

Понятие	Характеристика
1. Инвентаризация	А. Разъяснение правил
2. Обучение	Б. Пересмотр документов
3. Аудит	В. Учет ресурсов
4. Актуализация	Г. Проверка соблюдения

Ответ: 1–В, 2–А, 3–Г, 4–Б.

1.4. Практические задания

Практическое задание № 1.

Нормативная карта

1. Составьте иерархию источников регулирования для условной организации: федеральный закон, подзаконный акт, договор, локальная политика.
2. Выберите два положения локальной инструкции и опишите, как проверить их соответствие действующему регулированию.
3. Составьте карточку применимой нормы с реквизитами, предметом регулирования и датой проверки редакции.

Ожидаемый результат: обоснованный письменный ответ, таблица или схема с указанием исходных данных и выводов.

Практическое задание № 2.

Персональные данные

1. Для приема на работу составьте таблицу «цель — категория данных — операции — срок — ответственный» без избыточных сведений.
2. Предложите маршрут обработки запроса субъекта персональных данных с фиксацией этапов и ответственных.
3. В условном реестре выявлены сведения, не связанные с указанной целью. Предложите документируемые действия по устранению избыточности.

Ожидаемый результат: обоснованный письменный ответ, таблица или схема с указанием исходных данных и выводов.

Практическое задание № 3.

Доступ и роли

1. Для трех ролей — кадровик, системный администратор, руководитель — составьте матрицу доступа к кадровой системе.
2. Опишите порядок изменения полномочий сотрудника при переходе из отдела кадров в отдел закупок.
3. Составьте форму заявки на временный доступ с основанием, сроком и подтверждением закрытия.

Ожидаемый результат: обоснованный письменный ответ, таблица или схема с указанием исходных данных и выводов.

Практическое задание № 4.

Работа с подрядчиком

1. Подрядчику нужен доступ к обезличенной выгрузке для обслуживания системы. Определите необходимые условия договора и порядок предоставления доступа.
2. Составьте чек-лист допуска внешнего специалиста к помещению и информационной системе.
3. Опишите процедуру отзыва доступа и возврата носителей после окончания договора.

Ожидаемый результат: обоснованный письменный ответ, таблица или схема с указанием исходных данных и выводов.

Практическое задание № 5.

Инциденты

1. На общий адрес по ошибке отправлен файл с персональными данными. Составьте карточку инцидента и последовательность внутренних действий.
2. Разграничьте первичное сдерживание, установление обстоятельств, документирование и устранение причин.
3. Предложите три показателя проверки выполнения корректирующих мер.

Ожидаемый результат: обоснованный письменный ответ, таблица или схема с указанием исходных данных и выводов.

Практическое задание № 6.

Внутренний контроль

1. Разработайте план проверки соблюдения порядка выдачи прав доступа и определите проверяемые записи.
2. Выявлено пять учетных записей уволенных сотрудников. Составьте акт несоответствия и план исправления.
3. Опишите, какие документы нужны для проверки выполнения правил обращения с бумажными носителями.

Ожидаемый результат: обоснованный письменный ответ, таблица или схема с указанием исходных данных и выводов.

Практическое задание № 7.

Итоговый кейс

1. Для небольшой организации определите перечень ключевых локальных документов по информационной безопасности и владельцев процессов.
2. Составьте реестр рисков из пяти записей с вероятностью, последствиями, владельцем и мерой.
3. Подготовьте заключение по условному аудиту с фактами, основаниями, сроками и ответственными за устранение.

Ожидаемый результат: обоснованный письменный ответ, таблица или схема с указанием исходных данных и выводов.

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);	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	4. Правильность ответов на вопросы; 5. Самостоятельность решения (владение дополнительным материалом); 6. Знание нормативно-законодательной базы и терминологии курса	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.

Шкала оценивания	Показатели	Критерии
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 ее актуальность, сделан краткий анализ различных точек зрения на рассматриваемую проблему и логично изложена собственная позиция, сформулированы выводы, тема раскрыта полностью, выдержан объем, 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 недочеты. В частности, имеются неточности в изложении материала; отсутствует логическая последовательность в суждениях; не выдержан объем 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.	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 зачету.

Компетенция УК-1 Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач.		
УК-1.1. Знает	УК-1.2. Умеет	УК-1.3. Владеет
основы системного подхода к осуществлению поиска, критического анализа и синтеза информации для решения поставленных задач.	применять системный подход на основе поиска, критического анализа и синтеза информации для решения задач в профессиональной области.	навыками поиска, синтеза и критического анализа информации в своей профессиональной области; владеет системным подходом для решения поставленных задач.
3.1 № 1-30	3.2. № 1-30.	3.2. № 1-30

3.1. Вопросы на экзамен

1. Какие цели преследует правовое обеспечение информационной безопасности?
2. Какие виды нормативных правовых актов регулируют работу с информацией?
3. Чем нормативный правовой акт отличается от локального акта организации?
4. Что понимается под обладателем информации?
5. Как разграничивают общедоступную информацию и информацию ограниченного доступа?
6. Какие обязанности возникают при установлении режима ограниченного доступа?
7. Почему перед применением нормы проверяют ее актуальную редакцию?
8. Как соотносятся закон, подзаконный акт и локальное положение?
9. Что относится к персональным данным?
10. Какие роли могут участвовать в обработке персональных данных?
11. Для чего определяют цель обработки персональных данных?
12. Как реализуют принцип минимизации обрабатываемых данных?
13. В каких случаях согласие является основанием обработки?
14. Как фиксируют состав и сроки хранения персональных данных?
15. Что учитывают при предоставлении доступа сотруднику к персональным данным?
16. Каким образом организуют исполнение запросов субъектов данных?
17. Что включает политика информационной безопасности?
18. Как распределяют полномочия и ответственность в области защиты информации?
19. Для чего ведут реестр информационных активов?
20. Как определяют владельца информационного актива?
21. Что понимается под принципом минимально необходимых полномочий?
22. Какие этапы включает предоставление доступа?
23. Как пересматривают права доступа при переводе сотрудника?
24. Что включают правила работы с носителями информации?
25. Какие вопросы защиты информации отражают в договоре с подрядчиком?
26. Как проверяют допуск внешнего специалиста к информации?

27. Что включают требования к передаче информации третьим лицам?
28. Для чего составляют план внутреннего контроля?
29. Какие признаки позволяют классифицировать событие как инцидент?
30. Какие сведения фиксируют в карточке инцидента?
31. Как разграничивают регистрацию, расследование и устранение причин инцидента?
32. Как организуют сохранение материалов проверки?
33. Какие виды ответственности возможны за нарушение требований в сфере защиты информации?
34. Почему вид ответственности нельзя определять без анализа состава нарушения?
35. Как соотносятся трудовые обязанности и локальные правила работы с информацией?
36. Какие действия нужны перед вводом нового информационного процесса?
37. Как оформить матрицу ролей и доступа для условного подразделения?
38. Что делать при выявлении избыточного права доступа?
39. Как планировать сроки устранения выявленных нарушений?
40. Как проверить исполнимость локальной инструкции?
41. Как документируют обучение новых сотрудников правилам защиты информации?
42. Что включают правила использования корпоративной электронной почты?
43. Какие признаки указывают на устаревание локального акта?
44. Как организуют контроль сроков временного доступа?
45. Что нужно проверить перед передачей информации внешнему получателю?
46. Как оформляют исключение из стандартного процесса доступа?
47. Какие обязанности закрепляют за владельцем информационной системы?
48. Как подтверждают удаление доступа после завершения договора?
49. Какие источники используют для проверки официального текста нормативного акта?
50. Как оформляют правовые основания обработки и передачи информации?
51. Как документируют обучение новых сотрудников правилам защиты информации?
52. Что включают правила использования корпоративной электронной почты?
53. Какие признаки указывают на устаревание локального акта?
54. Как организуют контроль сроков временного доступа?
55. Что нужно проверить перед передачей информации внешнему получателю?
56. Как оформляют исключение из стандартного процесса доступа?
57. Какие обязанности закрепляют за владельцем информационной системы?
58. Как подтверждают удаление доступа после завершения договора?
59. Как отличают факт нарушения от предварительного предположения при проверке?
60. Как оценивают результативность мер после устранения инцидента?

3.2. Задания для зачета:

Задание 1

Составьте карту применимых правовых источников для условного процесса обработки сведений о работниках.

Задание 2

Объясните порядок проверки актуальности правовой нормы и зафиксируйте результаты проверки.

Задание 3

Определите состав локальных актов для организации с 50 работниками и кадровой системой.

Задание 4

Составьте матрицу доступа для трех ролей и двух информационных ресурсов.

Задание 5

Разработайте порядок согласования временного доступа внешнего специалиста.

Задание 6

Составьте план пересмотра прав при увольнении и переводе работника.

Задание 7

Опишите минимальный набор сведений в реестре информационных активов.

Задание 8

Оцените избыточность данных в условной анкете сотрудника и предложите исправление.

Задание 9

Подготовьте схему приема и рассмотрения запроса субъекта персональных данных.

Задание 10

Сформулируйте условия договора с подрядчиком о доступе и защите информации.

Задание 11

Составьте карточку инцидента после ошибочной отправки файла адресату.

Задание 12

Определите этапы внутренней проверки исполнения локальной политики.

Задание 13

Разработайте план устранения трех выявленных нарушений доступа.

Задание 14

Сопоставьте случаи нарушения правил с возможными видами ответственности без квалификации конкретного дела.

Задание 15

Подготовьте порядок ежегодной актуализации локальных актов и обучения работников.

Задание 16

Составьте карту применимых правовых источников для условного процесса обработки сведений о работниках.

Задание 17

Объясните порядок проверки актуальности правовой нормы и зафиксируйте результаты проверки.

Задание 18

Определите состав локальных актов для организации с 50 работниками и кадровой системой.

Задание 19

Составьте матрицу доступа для трех ролей и двух информационных ресурсов.

Задание 20

Разработайте порядок согласования временного доступа внешнего специалиста.

Задание 21

Составьте план пересмотра прав при увольнении и переводе работника.

Задание 22

Опишите минимальный набор сведений в реестре информационных активов.

Задание 23

Оцените избыточность данных в условной анкете сотрудника и предложите исправление.

Задание 24

Подготовьте схему приема и рассмотрения запроса субъекта персональных данных.

Задание 25

Сформулируйте условия договора с подрядчиком о доступе и защите информации.

Задание 26

Составьте карточку инцидента после ошибочной отправки файла адресату.

Задание 27

Определите этапы внутренней проверки исполнения локальной политики.

Задание 28

Разработайте план устранения трех выявленных нарушений доступа.

Задание 29

Сопоставьте случаи нарушения правил с возможными видами ответственности без квалификации конкретного дела.

Задание 30

Подготовьте порядок ежегодной актуализации локальных актов и обучения работников.

4. ОСНОВНЫЕ КРИТЕРИИ ОЦЕНИВАНИЯ ПРИ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

Шкала оценивания уровня сформированности универсальной компетенций (экзамен)

Шкала оценивания	Уровень освоение компетенции	Критерии 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.

Разработчик Фурин А.Д.

Согласовано

Заведующий кафедрой _____ Д.В. Моторина