

АКАДЕМИЯ ТРУДА И
СОЦИАЛЬНЫХ
ОТНОШЕНИЙ; ОУП ВО
"АТИСО"

Подписано цифровой
подписью: АКАДЕМИЯ ТРУДА И
СОЦИАЛЬНЫХ ОТНОШЕНИЙ;
ОУП ВО "АТИСО"
Дата: 2024.01.09 13:57:23 +05'00'

УТВЕРЖДАЮ
Заместитель директора УрСЭИ (филиал)
ОУП ВО "АТИСО" по УВР
 О.В. Зубкова
25.04.2023

ОЦЕНОЧНЫЕ СРЕДСТВА
для проведения текущего контроля и промежуточной аттестации по дисциплине
(модулю)

Информационная безопасность

Направление подготовки
09.03.03 Прикладная информатика
(код и наименование направления подготовки)

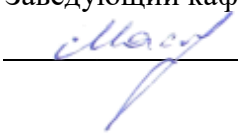
Направленность (профиль)
Корпоративные информационные системы

Квалификация выпускника
Бакалавр

Кафедра: Гуманитарных, естественнонаучных и математических дисциплин

Разработчики программы:
Битехтин Денис Николаевич

Программа обсуждена на заседании кафедры Гуманитарных, естественнонаучных и
математических дисциплин
протокол № 8 от 12.04.2023

Заведующий кафедрой Гуманитарных, естественнонаучных и математических дисциплин
 Маскайкин Е. П.

ОГЛАВЛЕНИЕ

1. ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)	3
1.1 Планируемые результаты обучения по дисциплине	3
1.2 Результаты освоения образовательной программы	3
2. ПОКАЗАТЕЛИ УРОВНЕЙ СФОРМИРОВАННОСТИ КОМПЕТЕНЦИЙ НА ЭТАПАХ ИХ ФОРМИРОВАНИЯ	4
3. ОЦЕНОЧНЫЕ СРЕДСТВА И КРИТЕРИИ СФОРМИРОВАННОСТИ КОМПЕТЕНЦИЙ	6
3.1 Контрольные вопросы для подготовки к экзамену (зачету) при проведении промежуточной аттестации по дисциплине	6
3.2 Курсовая работа/курсовой проект	10
3.3 Типовые контрольные задания или иные материалы при проведении текущего контроля по дисциплине	10

1. ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)

Оценочные средства (ОС) рабочей программы дисциплины Информационная безопасность предназначены для контроля и оценки образовательных достижений обучающихся (в т.ч. по самостоятельной работе обучающихся, далее – СРО), освоивших программу данной дисциплины.

Целью оценочных средств является установление соответствия уровня подготовки обучающихся требованиям ФГОС ВО по направлению подготовки 09.03.03 Прикладная информатика профиль: Корпоративные информационные системы.

1.1 Планируемые результаты обучения по дисциплине

Изучение дисциплины Информационная безопасность направлено на формирование следующих компетенций:

универсальных компетенций и индикаторов их достижения:

Категория (группа) УК	Код и наименование универсальной компетенции
Разработка и реализация проектов	УК-2 Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений.
Гражданская позиция	УК-10 Способен формировать нетерпимое отношение к коррупционному поведению.

общепрофессиональных компетенций и индикаторов их достижения:

Категория (группа) ОПК	Код и наименование универсальной компетенции
Организационно-управленческие	ОПК-3 Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.

1.2. Результаты освоения образовательной программы:

В результате изучения дисциплины студент должен:

Знать:

- 1.законодательство об информационных технологиях (ИТ), структуру информационного законодательства, законодательство об ИТ в системе законодательства России, понятие объектов права ИТ, понятие субъектов права ИТ.
- 2.значение информации в развитии современного информационного общества и возникающие, в связи с этим; опасности и угрозы; стандарты информационной безопасности.

Уметь:

- 1.анализировать правовую ситуацию в информационной сфере, выделяя область информационных технологий.
- 2.уметь разбираться в простейших правовых ситуациях, составлять и анализировать авторские договоры.
- 3.соблюдать основные требования информационной безопасности, в том числе защиты государственной тайны.
- 4.ориентироваться в системе законодательства и нормативных правовых актов, регламентирующих сферу информационной безопасности.
5. использовать правовые нормы в профессиональной и общественной деятельности.

Владеть (навыки и/или опыт деятельности):

- 1.навыками анализа правовых ситуаций в области информационных технологий.

- 2.навыками составления и анализа авторских договоров и лицензий к программному обеспечению.
- 3.методами обеспечения информационной безопасности.
- 4.навыками поиска необходимых нормативных и законодательных документов.
- 5.навыками работы с нормативными и правовыми документами в профессиональной деятельности.

2. ПОКАЗАТЕЛИ УРОВНЕЙ СФОРМИРОВАННОСТИ КОМПЕТЕНЦИЙ НА ЭТАПАХ ИХ ФОРМИРОВАНИЯ

Результатом освоения дисциплины Информационная безопасность является установление одного из уровней сформированности компетенций: высокий, повышенный, базовый, низкий.

Показатели уровней сформированности компетенций

Уровень	Универсальные компетенции	Общепрофессиональные / профессиональные компетенции
Высокий (количество баллов за освоение компетенции 8-9)	Сформированы четкие системные знания и представления по дисциплине. Ответы на вопросы оценочных средств полные и верные. Даны развернутые ответы на дополнительные вопросы. Обучающимся продемонстрирован высокий уровень освоения компетенции.	Обучающимся усвоена взаимосвязь основных понятий дисциплины, в том числе для решения профессиональных задач. Ответы на вопросы оценочных средств самостоятельны, исчерпывающие, содержание вопроса/задания оценочного средства раскрыто полно, профессионально, грамотно. Даны ответы на дополнительные вопросы. Обучающимся продемонстрирован высокий уровень освоения компетенции.
Повышенный (количество баллов за освоение компетенции 5-7)	Знания и представления по дисциплине сформированы на повышенном уровне. В ответах на вопросы/задания оценочных средств изложено понимание вопроса, дано достаточно подробное описание ответа, приведены и раскрыты в тезисной форме основные понятия. Ответ отражает полное знание материала, а также наличие, с незначительными пробелами, умений и навыков по изучаемой дисциплине. Допустимы единичные негрубые ошибки. Обучающимся продемонстрирован повышенный уровень освоения компетенции.	Сформированы в целом системные знания и представления по дисциплине. Ответы на вопросы оценочных средств полные, грамотные. Пр продемонстрирован повышенный уровень владения практическими умениями и навыками. Допустимы единичные негрубые ошибки по ходу ответа, в применении умений и навыков.

Базовый (количество баллов за освоение компетенции 3-4)	Ответ отражает теоретические знания основного материала дисциплины в объеме, необходимом для дальнейшего освоения ОПОП. Обучающийся допускает неточности в ответе, но обладает необходимыми знаниями для их устранения. Обучающимся продемонстрирован базовый уровень освоения компетенции.	Обучающийся владеет знаниями основного материала на базовом уровне. Ответы на вопросы оценочных средств неполные, допущены существенные ошибки. Продemonстрирован базовый уровень владения практическими умениями и навыками, соответствующий минимально необходимому уровню для решения профессиональных задач.
Низкий (количество баллов за освоение компетенции менее 3)	Демонстрирует полное отсутствие теоретических знаний материала дисциплины, отсутствие практических умений и навыков.	Демонстрирует полное отсутствие теоретических знаний материала дисциплины, отсутствие практических умений и навыков.

Шкала оценки для проведения промежуточной аттестации по дисциплине

№	Оценка за ответ	Характеристика ответа
1	Зачтено	- Достаточный объем знаний в рамках изучения дисциплины - В ответе используется научная терминология. - Стилистическое и логическое изложение ответа на вопрос правильное - Умеет делать выводы без существенных ошибок - Владеет инструментарием изучаемой дисциплины, умеет его использовать в решении стандартных (типовых) задач. - Ориентируется в основных теориях, концепциях и направлениях по изучаемой дисциплине. - Активен на практических (лабораторных) занятиях, допустимый уровень культуры исполнения заданий. - Количество баллов за освоение компетенций от 3 до 9
2	Не зачтено	- Не достаточно полный объем знаний в рамках изучения дисциплины - В ответе не используется научная терминология. - Изложение ответа на вопрос с существенными стилистическими и логическими ошибками. - Не умеет делать выводы по результатам изучения дисциплины - Слабое владение инструментарием изучаемой дисциплины, не компетентность в решении стандартных (типовых) задач. - Не умеет ориентироваться в основных теориях, концепциях и направлениях по изучаемой дисциплине. - Пассивность на практических (лабораторных) занятиях, низкий уровень культуры исполнения заданий. - Не сформированы компетенции, умения и навыки. Количество баллов за освоение компетенций менее 3. - Отказ от ответа или отсутствие ответа.

Критерии формирования оценок по заданиям закрытого типа (тестам) и заданиям открытого типа, требующих развернутого ответа

Оценка за ответ	Требования к знаниям
Зачтено	50% и более
Не зачтено	менее 50%

3. ОЦЕНОЧНЫЕ СРЕДСТВА И КРИТЕРИИ СФОРМИРОВАННОСТИ КОМПЕТЕНЦИЙ

3.1 Контрольные вопросы для подготовки к зачету, экзамену при проведении промежуточной аттестации по дисциплине

1. Что такое информационная безопасность? Охарактеризуйте методы и основные составляющие информационной безопасности.
2. Перечислите виды защищаемой информации. Классифицируйте и опишите основные угрозы информационной безопасности.
3. Перечислите и опишите модели информационной безопасности.
4. Перечислите основные законы в области защиты информации РФ. Опишите основные положения стратегии национальной безопасности и Доктрины информационной безопасности.
5. Что такое персональные данные? Опишите основные положения Федеральных законов в области персональных данных.
6. Охарактеризуйте биометрические данные как персональные данные. В каких случаях возможно использовать персональные данные без согласия обладателя?
7. Что такое служебная и коммерческая тайна? Охарактеризуйте принципиальные различия. Опишите основные положения Федеральных законов в области служебной и коммерческой тайны.
8. Опишите правовой режим государственной тайны. Какие главные государственные органы РФ в области обеспечения информационной безопасности? Какие государственные органы занимаются сертификацией и лицензированием средств защиты информации?
9. Перечислите и опишите основные международные стандарты в области информационной безопасности? Как связаны международные стандарты и стандарты РФ?
10. Опишите основные положения ГОСТ Р ИСО/МЭК 27002-2012 и ГОСТ Р ИСО/МЭК 27005-2010.
11. Опишите организационные и технические меры по защите персональных данных в системах обработки персональных данных.
12. Перечислите и опишите типы криптографических средств защиты информации в информационных системах обработки персональных данных.
13. Опишите требования к защите информации, не содержащей сведения, составляющие государственную тайну, в государственных информационных системах.
14. Опишите требования к защите объектов критической информационной инфраструктуры.
15. Опишите требование к средствам антивирусной защиты. Классифицируйте средства антивирусной защиты.
16. Опишите требования к межсетевым экранам и средствам доверенной загрузки.
17. Перечислите и опишите основные положения основных руководящих документов Гостехкомиссии.
18. Опишите меры защиты информации в государственных информационных системах.
19. Что такое политика безопасности? Служба безопасности предприятия (структура и функции).
20. Что такое аудит информационной безопасности? Опишите методику проведения аудита информационной безопасности.
21. Опишите методику оценки рисков нарушения информационной безопасности.
24. Что такое инженерная защита объектов? Каким способом описывается инженерная защита? Описать модель.
25. Что такое модель охраны периметра? Описать модель. Какие средства применяются для защиты 1-го, 2-го и 3-го периметров?
26. Какие средства применяются для защиты 2-го периметра?
27. Какие средства применяются для защиты 3-го периметра?
28. Перечислите и опишите технические средства обнаружения несанкционированного доступа к охраняемому объекту.
29. Что такое биометрия. Опишите биометрические характеристики (приведите примеры).
30. Что такое технические каналы утечки информации? Перечислите и опишите основные виды технических каналов утечки информации.
31. Опишите методику спецпроверки, специсследования и спецобследования? В чем состоит принципиальное различие между указанными методиками?
32. Перечислите и опишите методы защиты информации от утечки по зрительному и воздушному каналам.
33. Перечислите методы защиты информации от утечки по электромагнитному и электрическому каналам.
34. Перечислите методы защиты информации от утечки по индукционному каналу и параметрическому каналам.

35. Перечислите методы защиты информации от утечки по вибрационному и акустоэлектрическому каналам.
36. Перечислите методы защиты информации от утечки.
37. Перечислите средства и методы защиты информации по оптикоэлектронному каналу и от утечки информации в телефонных линиях.
38. Что такое программно-аппаратные средства защиты информации? Какие механизмы реализуют программно-аппаратные средства защиты информации? Какие компьютерные угрозы безопасности существуют?
39. Что такое сетевая разведка? Какие методы защиты против нее существуют? Что такое инъекция? Какие виды инъекций существуют? Какие методы защиты против них существуют?
40. В чем суть атаки «отказ в обслуживании»? Ее отличия от распределенной кибератаки «отказ в обслуживании»? Какие методы защиты против него существуют?
41. Перечислите и опишите основные виды программных уязвимостей. Какие методы защиты против них существуют?
42. Что такое переполнение буфера? Перечислите и опишите методы защиты.
43. Что такое дефекты форматных строк? Перечислите и опишите методы защиты.
44. Что такое целочисленные переполнения? Перечислите и опишите методы защиты.
45. Что такое «состояние гонки». Перечислите и опишите методы защиты.
46. Что такое атака «Человек по середине»? Что такое IP-спуффинг? Какие методы защиты против указанных атак существуют?
47. В чем суть сетевого протокола ARP (описать в соответствии с эталонной моделью OSI и стеком протоколов TCP/IP)? Что такое ARP-спуффинг? Какие методы защиты против него существуют?
48. В чем суть сетевых протоколов DNS и DHCP (описать в соответствии с эталонной моделью OSI и стеком протоколов TCP/IP)? DNS Cache Poisoning? Какие методы защиты против них существуют?
49. В чем суть сетевых протоколов NAT и PAT (описать в соответствии с эталонной моделью OSI и стеком протоколов TCP/IP)? NetBIOS/NBNS spoofing? Какие методы защиты против них существуют?
50. В чем суть технологии VPN? Можно ли рассматривать использование SSH как реализацию VPN? Может ли шифрование полностью защитить данные, передаваемые через VPN? С чем необходимо комбинировать политику, чтобы обеспечить безопасность VPN?
51. Что такое социальная инженерия? Что такое фрод. Перечислите и опишите методы борьбы с фродом.
52. Что такое фишинг? Какие методы защиты против него существуют? Что такое кардинг? Опишите методы защиты от кардинга.
53. Назначение, цели, описание Honeypot. Как выявлять Honeypot?
54. Что такое и для чего используются средства контекстной фильтрации? Охарактеризуйте DLP-системы и SIEM-системы.
55. Что такое сканеры безопасности? Для чего используется RPC-сканирование? Перечислите и опишите основные методы сканирования.
56. Что такое и для чего используются системы обнаружения вторжений и системы предотвращения вторжений?
57. Что такое вредоносные программы? Классифицируйте компьютерные вирусы. Опишите типовой механизм работы вируса. Что такое эксплоит?
58. Что такое шифр? Какие виды шифров существуют? Опишите принципы построения и принципиальные отличия.
59. Что такое поточный и блочный шифры? Опишите принципы построения и принципиальные отличия.
60. Что такое хеш-функция (описать принцип работы)? Какие виды хеш-функций вы знаете? Что такое Дерево Меркла?
61. Что такое цифровая подпись? Опишите цифровую подпись RSA и Эль-Гамала.

Критерии оценки изложены в шкале оценки для проведения промежуточной аттестации по дисциплине в разделе 2 ФОС.

Форма билета для проведения промежуточной аттестации по дисциплине

Уральский социально-экономический институт (филиал)
Образовательного учреждения профсоюзов высшего образования
"Академия труда и социальных отношений"

Социально-экономический факультет
Прикладная информатика
профиль Корпоративные информационные системы
Для всех форм обучения
Дисциплина Информационная безопасность

Билет № 1

Вопрос 1. Электронная подпись. Алгоритм создания и удостоверения сертификатом (3 этапа).
Вопрос 2. Понятие угрозы. Виды противников или нарушителей. Виды нарушений информационной системы.
Аутентификация и идентификация.

Утверждено на заседании кафедры, протокол от _____ № _____

Зав. кафедрой _____

Критерии оценки изложены в шкале оценки для проведения промежуточной аттестации по дисциплине (раздел 2 ФОС).

3.2 Курсовая работа / курсовой проект

Курсовая работа (курсовой проект) по учебному плану не предусмотрена.

3.3 Типовые контрольные задания или иные материалы при проведении текущего контроля по дисциплине

Проверка сформированности компетенций

Пояснение:

Вид задания "Открытое" предполагает развернутый ответ студента.

Вид задания "Закрытое" (тест) предполагает выбор правильного варианта ответа из предложенных.

Компетенция	УК-2 Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений.
Вид задания	Закрытое
Подвид задания	Выбор одного правильного ответа
Вопрос	К правовым методам, обеспечивающим информационную безопасность, относятся: 1. Разработка аппаратных средств обеспечения правовых данных 2. Разработка и установка во всех компьютерных правовых сетях журналов учета действий 3. Разработка и конкретизация правовых нормативных актов обеспечения безопасности
Ключ	3

Компетенция	УК-10 Способен формировать нетерпимое отношение к коррупционному поведению.
Вид задания	Закрытое
Подвид задания	Выбор нескольких правильных ответов

Вопрос	Выберите правильные ответы. Виды информационной безопасности включают: а) персональная б) серверная в) корпоративная г) государственная
Ключ	Правильные ответы: а, в, г

Компетенция	УК-2 Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений.
Вид задания	Закрытое
Подвид задания	Задание на сопоставление
Вопрос	Установите соответствие между следующими понятиями и их характеристиками: 1. Компьютерные сети: 2. Базы данных 3. Информационные системы а) Таблицы и структуры данных. SQL (Structured Query Language). Индексы и оптимизация запросов. б) Протоколы передачи данных. Маршрутизаторы и коммутаторы. IP-адреса в) CRM (Customer Relationship Management). ERP (Enterprise Resource Planning). BI (Business Intelligence)
Ключ	Правильное сопоставление: 1 - б, 2 - а, 3 - в

Компетенция	УК-10 Способен формировать нетерпимое отношение к коррупционному поведению.
Вид задания	Открытое
Подвид задания	Задание с развернутым ответом
Вопрос	Поясните, что такое ЭЦП.
Ключ	ЭЦП (электронная цифровая подпись) - это метод аутентификации и обеспечения целостности данных в электронном документе или сообщении. Она служит аналогом обычной подписи, используемой в бумажных документах, и позволяет подлинно определить автора документа и убедиться в его неизменности после создания. ЭЦП создается на основе криптографических алгоритмов.

Компетенция	ОПК-3 Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.
Вид задания	Открытое
Подвид задания	Задание на дополнение
Вопрос	Дополните определени. _____ - это комплекс руководств и требований обеспечения необходимого уровня безопасности.
Ключ	Политика безопасности в системе (сети)

Компетенция	ОПК-3 Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.
Вид задания	Открытое
Подвид задания	Задание с развернутым ответом

Вопрос	Поясните, какие типы угроз информационной безопасности существуют.
Ключ	Существуют различные типы угроз информационной безопасности, такие как вирусы, черви, троянские программы, фишинг, сетевые атаки, социальная инженерия и многие другие.

Компетенция	ОПК-3 Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.
Вид задания	Открытое
Подвид задания	Задание на дополнение
Вопрос	Дополните определение. _____ - это процесс проверки подлинности пользователя или устройства.
Ключ	Аутентификация

Компетенция	ОПК-3 Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.
Вид задания	Открытое
Подвид задания	Задание на дополнение
Вопрос	Дополните определение. _____ - это процесс предоставления прав доступа пользователю после успешной аутентификации.
Ключ	Авторизация

Компетенция	ОПК-3 Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.
Вид задания	Открытое
Подвид задания	Задание с развернутым ответом
Вопрос	Поясните, что такое шифрование информации.
Ключ	Шифрование - это процесс преобразования информации в нечитаемый вид для защиты от несанкционированного доступа.

Компетенция	ОПК-3 Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.
Вид задания	Открытое
Подвид задания	Задание с развернутым ответом
Вопрос	Поясните, какие методы защиты от вредоносных программ существуют.
Ключ	Существуют различные методы защиты от вредоносных программ, такие как использование антивирусного программного обеспечения, фильтрация трафика, регулярные обновления программного обеспечения и многие другие.

Компетенция	ОПК-3 Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.
Вид задания	Открытое
Подвид задания	Задание с развернутым ответом
Вопрос	Поясните, что такое бэкап.

Ключ	Бэкап - это процесс создания резервной копии данных для защиты от потери информации.
------	--

Компетенция	ОПК-3 Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.
Вид задания	Открытое
Подвид задания	Задание с развернутым ответом
Вопрос	Поясните, что такое фаервол.
Ключ	Фаервол - это программное или аппаратное устройство, которое контролирует доступ к сети и защищает компьютерную систему от несанкционированного доступа.

Компетенция	ОПК-3 Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.
Вид задания	Закрытое
Подвид задания	Задание на выбор последовательности
Вопрос	Упорядочите следующие этапы в процессе обеспечения информационной безопасности: 1. Идентификация и анализ уязвимостей системы. 2. Разработка и внедрение политики безопасности. 3. Резервное копирование и защита данных. 4. Мониторинг и обнаружение инцидентов безопасности.
Ключ	Правильная последовательность: 2-1-3-4

Компетенция	ОПК-3 Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.
Вид задания	Открытое
Подвид задания	Задание с развернутым ответом
Вопрос	Что следует сделать, если вы получили спам по e-mail с приложенным файлом.
Ключ	Необходимо удалить письмо с приложением, не раскрывая (не читая) его.

Компетенция	ОПК-3 Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.
Вид задания	Закрытое
Подвид задания	Выбор одного правильного ответа
Вопрос	Утечкой информации в системе называется ситуация, характеризующаяся: 1. Потерей данных в системе 2. Изменением формы информации 3. Изменением содержания информации
Ключ	1

Компетенция	ОПК-3 Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.
-------------	--

Вид задания	Открытое
Подвид задания	Задание на дополнение
Вопрос	Дополните предложение. _____ являются наиболее рискованным для компании компонентом, с точки зрения вероятного мошенничества и нарушения безопасности.
Ключ	Сотрудники предприятия.

Компетенция	ОПК-3 Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.
Вид задания	Закрытое
Подвид задания	Выбор одного правильного ответа
Вопрос	К правовым методам, обеспечивающим информационную безопасность, относятся: 1. Разработка аппаратных средств обеспечения правовых данных 2. Разработка и установка во всех компьютерных правовых сетях журналов учета действий 3. Разработка и конкретизация правовых нормативных актов обеспечения безопасности
Ключ	3

Компетенция	ОПК-3 Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.
Вид задания	Закрытое
Подвид задания	Выбор одного правильного ответа
Вопрос	Виды информационной безопасности: 1. Персональная, корпоративная, государственная 2. Клиентская, серверная, сетевая 3. Локальная, глобальная, смешанная
Ключ	1

Компетенция	ОПК-3 Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.
Вид задания	Закрытое
Подвид задания	Выбор одного правильного ответа
Вопрос	Цели информационной безопасности – своевременное обнаружение, предупреждение: 1. несанкционированного доступа, воздействия в сети 2. инсайдерства в организации 3. чрезвычайных ситуаций
Ключ	1

Компетенция	ОПК-3 Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.
Вид задания	Закрытое
Подвид задания	Выбор одного правильного ответа

Вопрос	Основные объекты информационной безопасности: 1. Компьютерные сети, базы данных 2. Информационные системы, психологическое состояние пользователей 3. Бизнес-ориентированные, коммерческие системы
Ключ	1

Компетенция	ОПК-3 Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.
Вид задания	Закрытое
Подвид задания	Выбор одного правильного ответа
Вопрос	Основными рисками информационной безопасности являются: 1. Искажение, уменьшение объема, перекодировка информации 2. Техническое вмешательство, выведение из строя оборудования сети 3. Потеря, искажение, утечка информации
Ключ	3

Компетенция	ОПК-3 Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.
Вид задания	Открытое
Подвид задания	Задание с развернутым ответом
Вопрос	Когда получен спам по e-mail с приложенным файлом, следует..
Ключ	Удалить письмо с приложением, не раскрывая (не читая) его.

Компетенция	ОПК-3 Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.
Вид задания	Закрытое
Подвид задания	Выбор одного правильного ответа
Вопрос	Наиболее распространены угрозы информационной безопасности сети: 1. Распределенный доступ клиент, отказ оборудования 2. Моральный износ сети, инсайдерство 3. Сбой (отказ) оборудования, нелегальное копирование данных
Ключ	3

Компетенция	ОПК-3 Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.
Вид задания	Закрытое
Подвид задания	Выбор одного правильного ответа
Вопрос	Утечкой информации в системе называется ситуация, характеризующаяся: 1. Потерей данных в системе 2. Изменением формы информации 3. Изменением содержания информации
Ключ	1

Компетенция	ОПК-3 Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.
-------------	--

Вид задания	Открытое
Подвид задания	Задание на дополнение
Вопрос	Информация, которую следует защищать (по нормативам, правилам сети, системы) называется...
Ключ	Защищаемой.

Компетенция	ОПК-3 Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.
Вид задания	Закрытое
Подвид задания	Выбор одного правильного ответа
Вопрос	Разновидностями угроз безопасности (сети, системы) являются все перечисленные в списке: 1. Программные, технические, организационные, технологические 2. Серверные, клиентские, спутниковые, наземные 3. Личные, корпоративные, социальные, национальные
Ключ	1

Компетенция	ОПК-3 Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.
Вид задания	Открытое
Подвид задания	Задание с развернутым ответом
Вопрос	Окончательно, ответственность за защищенность данных в компьютерной сети несет?
Ключ	Владелец компьютерной сети.

Компетенция	ОПК-3 Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.
Вид задания	Открытое
Подвид задания	Задание с развернутым ответом
Вопрос	Политика безопасности в системе (сети) – это комплекс...
Ключ	Комплекс руководств и требований обеспечения необходимого уровня безопасности.

Компетенция	ОПК-3 Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.
Вид задания	Открытое
Подвид задания	Задание с развернутым ответом
Вопрос	Какая категория является наиболее рискованной для компании с точки зрения вероятного мошенничества и нарушения безопасности?
Ключ	Сотрудники предприятия.

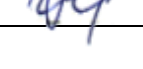
Компетенция	ОПК-3 Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.
Вид задания	Открытое
Подвид задания	Задание с развернутым ответом

Вопрос	Когда целесообразно не предпринимать никаких действий в отношении выявленных рисков?
Ключ	Когда стоимость контрмер превышает ценность актива и потенциальные потери.

Критерии формирования оценок по заданиям закрытого типа (тестам) и заданиям открытого типа, требующих развернутого ответа

Оценка за ответ	Требования к знаниям
Зачтено	50% и более
Не зачтено	менее 50%

ЛИСТ СОГЛАСОВАНИЯ

№	Подразделение	ФИО	Подпись	Дата
1	Кафедра экономики	О.В. Зубкова		25.04.2023
2	Кафедра МиУП	Е.В. Маскайкина		25.04.2023
3	Кафедра ГЕМД	Е.П. Маскайкин		25.04.2023
4	Учеб. метод. отдел	М.О. Дерябичева		25.04.2023
5	Библиотека	Г.В. Шпакова		25.04.2023