МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «ЛУГАНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ ВЛАДИМИРА ДАЛЯ»

Краснодонский факультет инженерии и менеджмента (филиал)
Кафедра экономики и управления

УТВЕРЖДАЮ:
Директор
_____ Панайотов К.К.
(подпись)
«14» марта 2025 года

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ
по учебной дисциплине
Кадровая безопасность

(наименование учебной дисциплины, практики)

38.04.02 Менеджмент

(код и наименование направления подготовки (специальности))

«Управление системой экономической безопасности»

(наименование профиля подготовки (специальности, магистерской программы); при отсутствии ставится прочерк)

Разработчик (разработчики):
ст. преп. _____ Лисицына Т.В.
(подпись)

ФОС рассмотрен и одобрен на заседании кафедры экономики и управления от «26» февраля 2025 г., протокол № 7

Заведующий кафедрой
экономики и управления _____ Стрижиченко Н.А.
(подпись)

Краснодон 2025

Комплект оценочных материалов по дисциплине
«Кадровая безопасность»

Задания закрытого типа

Задания закрытого типа на выбор правильного ответа

Выберите один правильный ответ.

1. Укажите основную цель кадровой безопасности на предприятии:
А) Обеспечение соблюдения трудового законодательства.
Б) Предотвращение угроз, связанных с человеческим фактором, для стабильности и развития организации.
В) Контроль за соблюдением сотрудниками правил внутреннего трудового распорядка.
Г) Улучшение условий труда и социальной защиты работников.
Правильный ответ: Б
Компетенции (индикаторы): ПК-3 (ПК-3.2, ПК-3.3)

2. Какие методы наиболее эффективно использовать для проверки благонадежности кандидата перед приемом на работу?
А) Сбор рекомендаций от предыдущих работодателей и проверка предоставленных документов.
Б) Только проверка документов, удостоверяющих личность, и наличие образования.
В) Глубокое изучение социальных сетей кандидата и проверка его личных связей.
Г) Проведение психологического тестирования и проверки на полиграфе (с согласия кандидата), а также сбор информации из открытых источников и от предыдущих работодателей.
Правильный ответ: Г
Компетенции (индикаторы): ПК-3 (ПК-3.2, ПК-3.3)

3. Какие меры необходимо предпринять для защиты конфиденциальной информации?
А) Полностью запретить использование личных устройств на работе.
Б) Внедрить политику информационной безопасности, проводить обучение сотрудников и контролировать ее соблюдение.
В) Ограничить доступ сотрудников к Интернету.
Г) Установить сложные пароли на все компьютеры.
Правильный ответ: Б
Компетенции (индикаторы): ПК-3 (ПК-3.2, ПК-3.3)

4. Какую информацию можно получить в ходе проверки кандидата через социальные сети?

А) Его семейное положение.
Б) Его образование и опыт работы.
В) Его профессиональные навыки.
Г) Общую картину его личности, взглядов и связей.
Правильный ответ: Г
Компетенции (индикаторы): ПК-3 (ПК-3.2, ПК-3.3)

Задания закрытого типа на установление соответствия

Установите правильное соответствие.
Каждому элементу левого столбца соответствует только один элемент правого столбца.

1. Установите соответствия между угрозой кадровой безопасности с соответствующей мерой противодействия.

Угроза кадровой безопасности		Мера противодействия	
1)	Сговор с конкурентами	А)	Усиление контроля за деятельностью подразделений
2)	Саботаж	Б)	Введение режима коммерческой тайны
3)	Разглашение коммерческой тайны	В)	Четкое определение круга обязанностей и зон ответственности

Правильный ответ: 1А, 2В, 3Б
Компетенции (индикаторы): ПК-3 (ПК-3.2, ПК-3.3)

2. Установите соответствия между видом кадровой угрозы и ее примером.

Вид кадровой угрозы		Пример	
1)	Умышленная угроза	А)	Недостаточная квалификация сотрудника, приводящая к ошибкам
2)	Неумышленная угроза	Б)	Разглашение конфиденциальной информации конкурентам
3)	Внешняя угроза	В)	Вербовка сотрудника конкурентами
4)	Внутренняя угроза	Г)	Нарушение сотрудником правил информационной безопасности из-за невнимательности

Правильный ответ: 1Б, 2А, 3В, 4Г
Компетенции (индикаторы): ПК-3 (ПК-3.2, ПК-3.3)

3. Установите соответствия между методом обеспечения кадровой безопасности и его характеристикой.

Метод обеспечения кадровой безопасности		Характеристика
1) Проверка кандидатов	А)	Регулярный анализ кадрового состава на предмет лояльности, благонадежности и соответствия требованиям безопасности
2) Контроль доступа к информации	Б)	Комплекс мер, направленных на предотвращение проникновения в компанию лиц, преследующих противоправные цели
3) Мониторинг персонала	В)	Оценка соответствия знаний, навыков и личностных качеств кандидата требованиям должности и безопасности компании
4) Обучение и инструктаж	Г)	Установление правил и ограничений на доступ сотрудников к конфиденциальной информации и ресурсам компании

Правильный ответ: 1В, 2Г, 3А, 4Б
Компетенции (индикаторы): ПК-3 (ПК-3.2, ПК-3.3)

4. Установите соответствия между видом документа с его назначением в системе кадровой безопасности.

Вид документа		Назначение
1) Должностная инструкция	А)	Устанавливает порядок действий сотрудников при возникновении угроз безопасности
2) Политика конфиденциальности	Б)	Определяет требования к знаниям, навыкам и ответственности сотрудника в области безопасности
3) Кодекс корпоративной этики	В)	Закрепляет принципы и нормы поведения сотрудников, направленные на обеспечение безопасности компании
4) Инструкция по безопасности	Г)	Регламентирует правила обработки, хранения и передачи конфиденциальной информации

Правильный ответ: 1Б, 2Г, 3В, 4А
Компетенции (индикаторы): ПК-3 (ПК-3.2, ПК-3.3)

Задания закрытого типа на установление правильной последовательности

Установите правильную последовательность.
Запишите правильную последовательность букв слева направо.

1. Установите последовательность мер по предупреждению и противодействию коррупции:
А) Выявление признаков коррупции.
Б) Проведение служебной проверки.
В) Отстранение сотрудника от занимаемой должности.
Г) Передача материалов в правоохранительные органы.
Д) Принятие мер по предотвращению коррупции в будущем.
Е) Увольнение сотрудника (при подтверждении факта коррупции).
Правильный ответ: А, Б, В, Г, Е, Д
Компетенции (индикаторы): ПК-3 (ПК-3.2, ПК-3.3)

2. Установите последовательность элементов по улучшению кадровой безопасности:
А) Установление цели аудита кадровой безопасности.
Б) Разработка плана аудита кадровой безопасности.
В) Сбор и анализ информации.
Г) Подготовка отчета по результатам аудита.
Д) Разработка рекомендаций по улучшению кадровой безопасности.
Е) Реализация рекомендаций.
Правильный ответ: А, Б, В, Г, Д, Е
Компетенции (индикаторы): ПК-3 (ПК-3.2, ПК-3.3)

3. Перечислите процессы допуска сотрудника к работе с конфиденциальной информацией:
А) Ознакомление с локальными нормативными актами организации.
Б) Обучение правилам работы с конфиденциальной информацией.
В) Инструктаж по информационной безопасности.
Г) Оформление допуска к работе с конфиденциальной информацией.
Д) Получение подписки о неразглашении конфиденциальной информации.
Е) Проверка знаний по информационной безопасности.
Правильный ответ: А, Б, В, Д, Е, Г
Компетенции (индикаторы): ПК-3 (ПК-3.2, ПК-3.3)

4. Перечислите этапы проведение служебного расследования по факту утечки информации:
А) Установление круга лиц, имевших доступ к информации.
Б) Определение размера ущерба, нанесенного компании.
В) Выявление причин утечки информации.
Г) Принятие мер по устранению последствий утечки информации.

Д) Возбуждение уголовного дела (при необходимости).
Правильный ответ: Б, А, Г, В, Д
Компетенции (индикаторы): ПК-3 (ПК-3.2, ПК-3.3)

Задания открытого типа

Задания открытого типа на дополнение

Напишите пропущенное слово (словосочетание).

1. Наиболее важную роль в блоке обеспечения системы управления безопасностью современной организации играет_____.
Правильный ответ: Информационное обеспечение.
Компетенции (индикаторы): ПК-3 (ПК-3.2, ПК-3.3)

2. Наиболее вероятным объектом вербовки со стороны конкурентов в реальном секторе экономики выступают сотрудники _____.
Правильный ответ: Технологического отдела.
Компетенции (индикаторы): ПК-3 (ПК-3.2, ПК-3.3)

3. Конфиденциальную информацию, разглашение которой представляет для организации стратегическую угрозу, наиболее целесообразно хранить _____.
Правильный ответ: на бумажных носителях
Компетенции (индикаторы): ПК-3 (ПК-3.2, ПК-3.3)

4. Основная ответственность за эффективное противодействие угрозе хищений путем фальсификации финансовых документов возлагается на _____.
Правильный ответ: Службу безопасности организации.
Компетенции (индикаторы): ПК-3 (ПК-3.2, ПК-3.3)

Задания открытого типа с кратким свободным ответом

Дайте ответ на вопрос.

1. Как называется политика, устанавливающая правила доступа, использования и распространения конфиденциальной информации в организации?
Правильный ответ: Информационная безопасность / Защита данных.
Компетенции (индикаторы): ПК-3 (ПК-3.2, ПК-3.3)

2. Как называется процесс выявления, оценки и принятия мер по снижению угроз, связанных с деятельностью персонала?
Правильный ответ: Предотвращение / Предупреждение.

Компетенции (индикаторы): ПК-3 (ПК-3.2, ПК-3.3)

3. Какое качество, создающее атмосферу поддержки и уважения, крайне важно для поддержания психологического здоровья персонала и снижения рисков конфликтов?
Правильный ответ: Доверие / Лояльность.
Компетенции (индикаторы): ПК-3 (ПК-3.2, ПК-3.3)

4. Как называется процесс выявления, оценки и принятия мер по снижению вероятности наступления негативных событий, связанных с действиями сотрудников?
Правильный ответ: Управление рисками / Контроль рисков.
Компетенции (индикаторы): ПК-3 (ПК-3.2, ПК-3.3)

Задания открытого типа с развернутым ответом

Дайте развернутый ответ на вопрос

1. Опишите основные угрозы кадровой безопасности, с которыми сталкиваются современные организации.
Время выполнения - 10 мин.
Ожидаемый результат:
Внутренние угрозы. Исходят непосредственно от работников компании или возникают в результате ошибок руководства. К ним относятся, например: кражи, утечки конфиденциальных данных, шантаж увольнением, угрозы, связанные с организацией работы компании, неправильная корпоративная политика (неналаженная коммуникация, несоблюдение трудовой этики, непонятные миссия и цели, отсутствие отлаженных алгоритмов разрешения конфликтов).
Внешние угрозы. Напрямую не зависят от действий сотрудников компании. Сюда входит множество факторов, на которые могут влиять конкуренты, геополитическая, экономическая обстановка.
Критерии оценивания: Наличие в ответе не менее трёх угроз.
Компетенции (индикаторы): ПК-3 (ПК-3.2, ПК-3.3)

2. Какие меры профилактики необходимо предпринять для предотвращения утечки информации?
Время выполнении - 10 мин.
Ожидаемый результат: разработка и внедрение политики в сфере безопасности должна обеспечивать защищённость учётных записей, имеющих доступ к ним.
Минимизация привилегий. Все работники (аккаунты), включая и привилегированных, должны иметь уровень доступа исключительно в соответствии с должностными функциями.
Корпоративный режим контроля паролей. Необходимо внедрить

систематический мониторинг и отключение скомпрометированных или слишком простых паролей.
Систематическое обновление программного обеспечения. Своевременная установка обновлений на компьютере, обновление серверов, проверка и «чистка» ресурсов общего пользования обезопасит закрытую информацию от утечки.
Использование межсетевого экрана. Программное обеспечение инспектирует входящий и исходящий из корпоративной сети трафик в соответствии с правилами и определяет, передать или блокировать сведения в случае нарушения политик безопасности.
Запрет возможности размещения защищаемой информации в облачных сервисах и её передачи через мессенджеры, Google Docs и другие сервисы.
Контроль содержимого файлов, передаваемых посредством электронной почты, с применением систем предотвращения утечки информации (DLP-систем).
Аудит подключаемых к автоматизированным рабочим местам съёмных машинных носителей информации и анализ записываемой на них информации.
Отслеживание геолокации пользователей, осуществляющих удалённое подключение к информационной инфраструктуре.
Мониторинг информационных ресурсов, расположенных в сети «Интернет», на предмет выявления утечек защищаемой информации.
Критерии оценивания: Наличие в ответе не менее трех мер профилактики.
Компетенции (индикаторы): ПК-3 (ПК-3.2, ПК-3.3)

3. Какие меры необходимо предпринять для обеспечения кадровой безопасности на этапе приема на работу?
Время выполнения - 15 мин.
Ожидаемый результат: Обеспечение кадровой безопасности на этапе приема на работу является критически важным шагом для минимизации рисков, связанных с персоналом. Этот процесс включает в себя комплекс мер, направленных на оценку благонадежности и соответствия кандидата требованиям должности. Вот основные этапы и меры:
Предварительная проверка:
анализ резюме и сопроводительного письма; оценка соответствия квалификации, опыта работы и информации, указанной кандидатом, требованиям вакансии. Обращение внимания на пробелы в стаже, частую смену мест работы.
Сбор рекомендаций:
связь с предыдущими работодателями для получения объективной информации о кандидате (дисциплина, надежность, отношение к работе, причины увольнения). Важно: получить согласие кандидата на предоставление рекомендаций.
Проверка открытых источников:

анализ информации о кандидате в интернете (социальные сети, поисковые системы) для выявления нежелательных фактов: публикации компрометирующего характера, участие в сомнительных сообществах, признаки асоциального поведения.
Углубленная проверка:
собеседование: структурированное собеседование, включая вопросы о мотивации, целях, профессиональных и личных качествах. Использование поведенческих вопросов для оценки реакции кандидата в различных ситуациях;
проверка документов: анализ оригиналов документов, удостоверяющих личность, образование, трудовой стаж;
медицинское освидетельствование: если этого требует специфика работы (например, работа с секретными сведениями, управление транспортом, работа на вредном производстве).
Проверка на судимость: если это требуется в соответствии с законодательством (например, для работы с детьми).
Критерии оценивания: Наличие в ответе не менее пяти мер.
Компетенции (индикаторы): ПК-3 (ПК-3.2, ПК-3.3)

4. Какие меры необходимо соблюдать при разработке политики и процедур кадровой безопасности?
Время выполнения - 15 мин.
Ожидаемый результат: При разработке политики и процедур кадровой безопасности необходимо соблюдать следующие меры: определение общих принципов и целей кадровой безопасности, а также распределение ответственности между различными подразделениями и сотрудниками.
Разработка должностных инструкций: четкое определение обязанностей и ответственности каждого сотрудника, включая требования к соблюдению режима конфиденциальности, правил информационной безопасности и других аспектов кадровой безопасности.
Разработка процедур отбора и проверки персонала: определение методов проверки кандидатов при приеме на работу (например, сбор рекомендаций, проверка документов, психологическое тестирование, проверка на полиграфе) и порядка их проведения.
Разработка процедур управления рисками: определение мер по предотвращению, выявлению и реагированию на риски, связанные с персоналом (например, мониторинг действий сотрудников, контроль доступа к информации, проведение служебных расследований).
Разработка плана реагирования на инциденты: определение действий, которые необходимо предпринять в случае выявления нарушений кадровой безопасности (например, утечка информации, хищения, саботаж), а также распределение ответственности за их выполнение.
Критерии оценивания: Ответ должен охватывать широкий спектр мер. Должны быть упомянуты меры, касающиеся разных этапов работы с персоналом.
Компетенции (индикаторы): ПК-3 (ПК-3.2, ПК-3.3)

Экспертное заключение

Представленный фонд оценочных средств (далее – ФОС) по дисциплине «Кадровая безопасность» соответствует требованиям ФГОС ВО.

Предлагаемые формы и средства текущего и промежуточного контроля адекватны целям и задачам реализации основной профессиональной образовательной программы по направлению подготовки 38.04.02 Менеджмент.

Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины представлены в полном объеме.

Виды оценочных средств, включенные в представленный фонд, отвечают основным принципам формирования ФОС.

Разработанный и представленный для экспертизы фонд оценочных средств рекомендуется к использованию в процессе подготовки обучающихся по указанному направлению 38.04.02 Менеджмент.

Председатель учебно-методической
комиссии Краснодонского факультета
инженерии и менеджмента (филиала) _____ Родионова О.Ю.

Лист изменений и дополнений

№ п/п	Виды дополнений и изменений	Дата и номер протокола заседания кафедры (кафедр), на котором были рассмотрены и одобрены изменения и дополнения	Подпись (с расшифровкой) заведующего кафедрой (заведующих кафедрами)