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

Институт управления и государственной службы
Кафедра производственного менеджмента

УТВЕРЖДАЮ
Директор _____ Р.Г. Харьковский
(подпись)
«12» 02 2025 года

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ
по учебной дисциплине

Обеспечение информационной безопасности
38.05.01 Экономическая безопасность
(код и наименование направления подготовки (специальности))
«Экономика и организация производства на режимных объектах»
(наименование профиля подготовки (специальности, магистерской программы); при отсутствии ставится прочерк)

Разработчик:
Старший преподаватель _____ Омельяненко И.А.
(подпись)

ФОС рассмотрен и одобрен на заседании кафедры производственного менеджмента от «21» 01 2025 г., протокол № 6

Заведующий кафедрой
Производственного менеджмента _____ Родионов А.В.
(подпись)

Луганск 2025 г.

Комплект оценочных материалов по дисциплине
«Обеспечение информационной безопасности»

Задания закрытого типа

Задания закрытого типа на выбор правильного ответа

Выберите один правильный ответ

1. Какой из следующих методов является наиболее распространенным способом аутентификации пользователей?
А) Шифрование данных
Б) Использование паролей
В) Блокировка учетных записей
Г) Файрволы
Правильный ответ: Б
Компетенции (индикаторы): ПК-7 (ПК-7.1, ПК-7.2, ПК-7.3, ПК-7.4, ПК-7.5)

2. Какой тип вредоносного ПО предназначен для шифрования файлов на компьютере и требует выкуп за их восстановление?
А) Троян
Б) Вирус
В) Рансомваре
Г) Червь
Правильный ответ: В
Компетенции (индикаторы): ПК-7 (ПК-7.1, ПК-7.2, ПК-7.3, ПК-7.4, ПК-7.5)

3. Какой из следующих методов защиты информации предполагает использование двух или более факторов аутентификации?
А) Многофакторная аутентификация
Б) Однофакторная аутентификация
В) Аутентификация по IP-адресу
Г) Аутентификация по сертификату
Правильный ответ: А
Компетенции (индикаторы): ПК-7 (ПК-7.1, ПК-7.2, ПК-7.3, ПК-7.4, ПК-7.5)

4. Какой стандарт безопасности информации разработан для защиты персональных данных в США?
A) ISO/IEC 27001
B) GDPR
C) HIPAA
D) PCI DSS
Правильный ответ: В
Компетенции (индикаторы): ПК-7 (ПК-7.1, ПК-7.2, ПК-7.3, ПК-7.4, ПК-7.5)

Задания закрытого типа на установление соответствия

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

1. Установите соответствие между терминами и их определениями.

Термин	Определение
1) Конфиденциальность	А) Процесс обеспечения целостности данных и защиты от их изменения.
2) Целостность	Б) Способ защиты информации от несанкционированного доступа.
3) Доступность	В) Гарантия того, что информация доступна для авторизованных пользователей.
4) Аутентификация	Г) Процесс подтверждения личности пользователя или системы.

Правильный ответ: 1-Б, 2-А, 3-В, 4-Г
Компетенции (индикаторы): ПК-7 (ПК-7.1, ПК-7.2, ПК-7.3, ПК-7.4, ПК-7.5)

2. Установите соответствие между угрозами и мерами защиты.

Угроза	Мера защиты
1) Вирусные атаки	А) Регулярное обновление программного обеспечения и антивирусов.
2) Фишинг	Б) Обучение пользователей распознаванию подозрительных писем.
3) Утечка данных	В) Шифрование данных и контроль доступа к ним.
4) Отказ в обслуживании (DoS)	Г) Установка систем обнаружения и предотвращения атак.

Правильный ответ: 1-А, 2-Б, 3-В, 4-Г
Компетенции (индикаторы): ПК-7 (ПК-7.1, ПК-7.2, ПК-7.3, ПК-7.4, ПК-7.5)

Задания закрытого типа на установление правильной последовательности

Установите правильную последовательность.
Запишите правильную последовательность букв слева направо.

1. Установите правильную последовательность этапов управления инцидентами информационной безопасности:
А) Уведомление о инциденте
Б) Анализ инцидента
В) Реакция на инцидент

Г) Восстановление после инцидента
Д) Закрытие инцидента
Правильный ответ: А, Б, В, Г, Д
Компетенции (индикаторы): ПК-7 (ПК-7.1, ПК-7.2, ПК-7.3, ПК-7.4, ПК-7.5)

2. Установите правильную последовательность этапов оценки рисков в информационной безопасности:
А) Идентификация активов
Б) Оценка угроз
В) Оценка уязвимостей
Г) Оценка рисков
Д) Разработка плана управления рисками
Правильный ответ: А, Б, В, Г, Д
Компетенции (индикаторы): ПК-7 (ПК-7.1, ПК-7.2, ПК-7.3, ПК-7.4, ПК-7.5)

3. Установите правильную последовательность этапов разработки политики безопасности информации:
Определение целей безопасности
А) Анализ существующих мер безопасности
Б) Разработка документации политики
В) Утверждение политики
Г) Обучение сотрудников
Правильный ответ: А, Б, В, Г, Д
Компетенции (индикаторы): ПК-7 (ПК-7.1, ПК-7.2, ПК-7.3, ПК-7.4, ПК-7.5)

4. Установите правильную последовательность действий при реагировании на угрозу информационной безопасности:
А) Обнаружение угрозы
Б) Оценка угрозы
В) Устранение угрозы
Г) Документирование инцидента
Д) Анализ уроков
Правильный ответ: А, Б, В, Г, Д
Компетенции (индикаторы): ПК-7 (ПК-7.1, ПК-7.2, ПК-7.3, ПК-7.4, ПК-7.5)

Задания открытого типа

Задания открытого типа на дополнение

1. Заполните пропущенное слово (словосочетание):
Информационная безопасность включает в себя защиту _____ данных от несанкционированного доступа.
Правильный ответ: конфиденциальности**.**
Компетенции (индикаторы): ПК-7 (ПК-7.1, ПК-7.2, ПК-7.3, ПК-7.4, ПК-7.5)

2. Заполните пропущенное слово (словосочетание):
Для обеспечения целостности данных используют _____, которые помогают предотвратить их несанкционированное изменение.
Правильный ответ: криптографические методы**.**
Компетенции (индикаторы): ПК-7 (ПК-7.1, ПК-7.2, ПК-7.3, ПК-7.4, ПК-7.5)

3. Заполните пропущенное слово (словосочетание):
Одним из основных принципов обеспечения информационной безопасности является _____ информации для авторизованных пользователей.
Правильный ответ: доступность.
Компетенции (индикаторы): ПК-7 (ПК-7.1, ПК-7.2, ПК-7.3, ПК-7.4, ПК-7.5)

4. Заполните пропущенное слово (словосочетание):
_____ — это событие, которое может угрожать безопасности информационной системы и требует немедленного реагирования.
Правильный ответ: инцидент безопасности**.**
Компетенции (индикаторы): ПК-7 (ПК-7.1, ПК-7.2, ПК-7.3, ПК-7.4, ПК-7.5)

Задания открытого типа с кратким свободным ответом

Дайте ответ на вопрос.

1. В чем состоят основные цели информационной безопасности? Укажите основные аспекты.
Правильный ответ: Основные цели информационной безопасности включают защиту конфиденциальности, целостности и доступности информации. Конфиденциальность обеспечивает защиту данных от несанкционированного доступа, целостность гарантирует, что информация не была изменена или уничтожена без разрешения, а доступность обеспечивает возможность получения информации авторизованными пользователями в любое время.
Компетенции (индикаторы): ПК-7 (ПК-7.1, ПК-7.2, ПК-7.3, ПК-7.4, ПК-7.5)

2. Что такое фишинг и как он угрожает информационной безопасности.
Укажите основные аспекты.
Правильный ответ: Фишинг — это метод мошенничества, при котором злоумышленники пытаются получить конфиденциальную информацию (например, пароли, номера кредитных карт) путем маскировки под доверенные источники в электронных сообщениях или на веб-сайтах. Он угрожает информационной безопасности, так как может привести к утечке личных данных и финансовым потерям.
Компетенции (индикаторы): ПК-7 (ПК-7.1, ПК-7.2, ПК-7.3, ПК-7.4, ПК-7.5)

3. Какие меры можно предпринять для защиты от вирусов и вредоносного ПО? Укажите основные аспекты.

Правильный ответ: Для защиты от вирусов и вредоносного ПО следует использовать антивирусные программы, регулярно обновлять их базы данных, избегать открытия подозрительных вложений и ссылок, а также применять фаерволы и обеспечивать регулярное резервное копирование данных.
Компетенции (индикаторы): ПК-7 (ПК-7.1, ПК-7.2, ПК-7.3, ПК-7.4, ПК-7.5)

4. Что такое шифрование и какую роль оно играет в обеспечении информационной безопасности? Укажите основные аспекты.
Правильный ответ: Шифрование — это процесс преобразования информации в недоступный для чтения формат с использованием алгоритмов и ключей. Оно играет ключевую роль в обеспечении информационной безопасности, так как защищает данные от несанкционированного доступа и обеспечивает их конфиденциальность при передаче или хранении.
Компетенции (индикаторы): ПК-7 (ПК-7.1, ПК-7.2, ПК-7.3, ПК-7.4, ПК-7.5)

Задания открытого типа с развернутым ответом

1. Дайте развернутый ответ на вопрос:
Проведите анализ угроз информационной безопасности для организации, работающей в сфере финансовых услуг. Укажите основные категории угроз и предложите меры по их минимизации?

Время выполнения – 10 мин.

Ожидаемый результат:
Анализ угроз информационной безопасности в финансовой организации включает в себя идентификацию, оценку и управление потенциальными рисками, которые могут повлиять на конфиденциальность, целостность и доступность информации. Основные категории угроз можно разбить на следующие группы:
Внутренние угрозы:
Неумышленные действия сотрудников: Ошибки при работе с данными, неправильная настройка систем.
Злонамеренные действия: Угон учетных записей, кража данных.
Меры по минимизации:
Регулярное обучение сотрудников по вопросам информационной безопасности.
Внедрение системы контроля доступа и мониторинга действий пользователей.
Использование многофакторной аутентификации.
Внешние угрозы:
Кибератаки: Фишинг, DDoS-атаки, вирусы и трояны.
Социальная инженерия: Манипуляции с целью получения конфиденциальной информации.
Меры по минимизации:

Установка и регулярное обновление антивирусного ПО и систем защиты от вторжений.
Проведение тестов на проникновение для выявления уязвимостей.
Разработка и реализация политики безопасности.
Физические угрозы:
Кража оборудования: Утеря или кража ноутбуков, серверов.
Природные катастрофы: Пожары, наводнения.
Меры по минимизации:
Использование замков и систем видеонаблюдения для защиты помещений.
Регулярное резервное копирование данных и их хранение в удаленных местах.
Технологические угрозы:
Уязвимости программного обеспечения: Использование устаревших версий ПО.
Ошибки в конфигурации систем: Неправильные настройки серверов и сетевых устройств.
Меры по минимизации:
Проведение регулярных аудитов безопасности и обновление программного обеспечения.
Внедрение практики DevSecOps для обеспечения безопасности на всех этапах разработки.
Критерии оценивания: частичное содержательное соответствие приведенному выше пояснению.
Компетенции (индикаторы): ПК-7 (ПК-7.1, ПК-7.2, ПК-7.3, ПК-7.4, ПК-7.5)

2. Дайте развернутый ответ на вопрос:
Опишите основные элементы политики информационной безопасности для организации, работающей с персональными данными. Какова роль данной политики в обеспечении безопасности.

Время выполнения – 10 мин.

Ожидаемый результат:
Политика информационной безопасности (ПИБ) — это документ, который определяет подходы и принципы, регулирующие защиту информации в организации. Основные элементы ПИБ включают:
Цели и задачи политики:
Определение целей безопасности информации, таких как защита конфиденциальности, целостности и доступности данных.
Установление задач по минимизации рисков и соблюдению законодательства.
Область применения:
Определение, какие данные и системы подлежат защите, включая персональные данные клиентов и сотрудников.
Указание на сотрудников, системы и процессы, к которым применяется политика.
Управление доступом:

Описание правил доступа к информации и системам, включая уровни доступа и авторизацию пользователей.
Внедрение многофакторной аутентификации и регулярного пересмотра прав доступа.
Обработка и хранение данных:
Установление правил обработки, хранения и передачи персональных данных.
Определение требований к шифрованию и анонимизации данных.
Обучение и осведомленность:
Регулярное обучение сотрудников по вопросам информационной безопасности и осведомленности о рисках.
Проведение семинаров и тренингов для повышения уровня знаний о безопасности.
Мониторинг и аудит:
Установление процессов для мониторинга соблюдения политики и проведения регулярных аудитов.
Описание методов выявления и реагирования на инциденты безопасности.
Ответственность и дисциплинарные меры:
Определение ответственности сотрудников за соблюдение политики.
Указание возможных дисциплинарных мер за нарушение правил безопасности.
Роль политики информационной безопасности: Политика информационной безопасности играет ключевую роль в обеспечении безопасности данных и систем.
Она: Устанавливает четкие ожидания и стандарты для сотрудников.
Обеспечивает соответствие законодательству и требованиям регуляторов.
Снижает риски утечек и инцидентов безопасности.
Создает основу для реагирования на инциденты и восстановления после атак.
Таким образом, наличие четкой и хорошо разработанной политики информационной безопасности является критически важным для защиты персональных данных и обеспечения доверия со стороны клиентов и партнеров.
Критерии оценивания: частичное содержательное соответствие приведенному выше пояснению.
Компетенции (индикаторы): ПК-7 (ПК-7.1, ПК-7.2, ПК-7.3, ПК-7.4, ПК-7.5)

Экспертное заключение

Представленный фонд оценочных средств (далее – ФОС) по дисциплине «Обеспечение информационной безопасности» соответствует требованиям ФГОС ВО.

Предлагаемые формы и средства текущего и промежуточного контроля адекватны целям и задачам реализации основной профессиональной образовательной программы по направлению подготовки 38.05.01 Экономическая безопасность.

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 38.05.01 Экономическая безопасность.

Председатель учебно-методической комиссии
института управления и государственной службы _____ Студеникина В.П.

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)