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

Экономический институт
Кафедра экономической кибернетики и прикладной статистики
(наименование кафедры)

УТВЕРЖДАЮ
Директор _____ Тхор Е.С.
(подпись)
«__» _____ 2025 года

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ
по практике

«Производственная (проектно-технологическая) практика»
(наименование учебной дисциплины, практике)
38.04.05 Бизнес-информатика
(код и наименование направления подготовки (специальности))
«Бизнес-аналитика»
(наименование профиля подготовки (специальности, магистерской программы); при отсутствии ставится прочерк)

Разработчик (разработчики):
доцент _____ Воронова А.Г.
(подпись)

ФОС рассмотрен и одобрен на заседании кафедры экономической кибернетики и прикладной статистики от «25» 02 2025 г., протокол № 25

Заведующий кафедрой экономической кибернетики и прикладной статистики
_____ Велигура А.В.
(подпись)

Луганск 2025 г.

Комплект оценочных материалов по практике
«Производственная (проектно-технологическая) практика»

Задания закрытого типа

Задания закрытого типа на выбор правильного ответа

1. *Выберите один правильный ответ.*
   Какой из следующих методов наиболее эффективно помогает повысить производительность и оптимизировать бизнес-процессы в организации?
   А) Использование традиционных методов управления проектами
   Б) Внедрение системы управления качеством (ISO)
   В) Автоматизация процессов с помощью программного обеспечения
   Г) Увеличение численности сотрудников

Правильный ответ: В
Компетенции (индикаторы): УК-1.1; УК-1.2; УК-1.3; УК-2.1; УК-2.2; УК-3.1; УК-3.2; УК-4.1; УК-4.2; УК-5.1; УК-5.2; УК-6.1; УК-6.2; ОПК-1.1; ОПК-1.2; ОПК-1.3; ОПК-2.1; ОПК-2.2; ОПК-2.3; ОПК-3.1; ОПК-3.2; ОПК-3.3; ОПК-5.1; ОПК-5.2; ОПК-5.3; ПК-1.1; ПК-1.2; ПК-1.3; ПК-2.1; ПК-2.2; ПК-2.3; ПК-3.1; ПК-3.2; ПК-3.3

2. *Выберите один правильный ответ.*
   Какой из следующих методов искусственного интеллекта чаще всего используется для анализа больших объемов данных в научных исследованиях?

А) Линейная регрессия
Б) Генетические алгоритмы
В) Машинное обучение
Г) Качественный анализ

Правильный ответ: В
Компетенции (индикаторы): УК-1.1; УК-1.2; УК-1.3; УК-2.1; УК-2.2; УК-3.1; УК-3.2; УК-4.1; УК-4.2; УК-5.1; УК-5.2; УК-6.1; УК-6.2; ОПК-1.1; ОПК-1.2; ОПК-1.3; ОПК-2.1; ОПК-2.2; ОПК-2.3; ОПК-3.1; ОПК-3.2; ОПК-3.3; ОПК-5.1; ОПК-5.2; ОПК-5.3; ПК-1.1; ПК-1.2; ПК-1.3; ПК-2.1; ПК-2.2; ПК-2.3; ПК-3.1; ПК-3.2; ПК-3.3

3. *Выберите все правильные ответы.*

А) Какие из следующих технологий относятся к информационно-коммуникационным технологиям (ИКТ)? Интернет
Б) Операционная система
В) Мобильные приложения
Г) Электронная почта
Д) Блокчейн
Е) Офисное оборудование

Правильный ответ: А,В,Г,Д
Компетенции (индикаторы): УК-1.1; УК-1.2; УК-1.3; УК-2.1; УК-2.2; УК-3.1; УК-3.2; УК-4.1; УК-4.2; УК-5.1; УК-5.2; УК-6.1; УК-6.2; ОПК-1.1; ОПК-1.2; ОПК-1.3; ОПК-2.1; ОПК-2.2; ОПК-2.3; ОПК-3.1; ОПК-3.2; ОПК-3.3; ОПК-5.1; ОПК-5.2; ОПК-5.3; ПК-1.1; ПК-1.2; ПК-1.3; ПК-2.1; ПК-2.2; ПК-2.3; ПК-3.1; ПК-3.2; ПК-3.3

Задания закрытого типа на установление соответствия

1. *Прочитайте текст и установите соответствие между термином и их определением. Соотнесите термины с их определениями в контексте разработки стратегии безопасности. Каждому элементу левого столбца соответствует только один элемент правого столбца.*

	Термин		Определение
1)	Угроза	А)	Возможность возникновения события, которое может нанести ущерб организации или системе
2)	Уязвимость	Б)	Состояние системы или процесса, которое делает его подверженным атакам или инцидентам
3)	Риск	В)	Набор правил и процедур, определяющий, как организация защищает свои активы и информацию
4)	Политика безопасности	Г)	Потенциальное событие, которое может использовать уязвимость для причинения вреда

Правильный ответ: 1 – Г; 2 – Б; 3 – А; 4 – В
Компетенции (индикаторы): УК-1.1; УК-1.2; УК-1.3; УК-2.1; УК-2.2; УК-3.1; УК-3.2; УК-4.1; УК-4.2; УК-5.1; УК-5.2; УК-6.1; УК-6.2; ОПК-1.1; ОПК-1.2; ОПК-1.3; ОПК-2.1; ОПК-2.2; ОПК-2.3; ОПК-3.1; ОПК-3.2; ОПК-3.3; ОПК-5.1; ОПК-5.2; ОПК-5.3; ПК-1.1; ПК-1.2; ПК-1.3; ПК-2.1; ПК-2.2; ПК-2.3; ПК-3.1; ПК-3.2; ПК-3.3

Задания закрытого типа на установление правильной последовательности

1. *Прочитайте текст и установите последовательность. Установите правильную последовательность этапов разработки политики*

безопасности предприятия (от начального). Запишите правильную последовательность букв слева направо.

А) Мониторинг и пересмотр политики
Б) Оценка рисков
В) Определение целей безопасности
Г) Разработка документации политики
Д) Внедрение и обучение

Правильный ответ: В,Б,Г,Д,А
Компетенции (индикаторы): УК-1.1; УК-1.2; УК-1.3; УК-2.1; УК-2.2; УК-3.1; УК-3.2; УК-4.1; УК-4.2; УК-5.1; УК-5.2; УК-6.1; УК-6.2; ОПК-1.1; ОПК-1.2; ОПК-1.3; ОПК-2.1; ОПК-2.2; ОПК-2.3; ОПК-3.1; ОПК-3.2; ОПК-3.3; ОПК-5.1; ОПК-5.2; ОПК-5.3; ПК-1.1; ПК-1.2; ПК-1.3; ПК-2.1; ПК-2.2; ПК-2.3; ПК-3.1; ПК-3.2; ПК-3.3

Задания открытого типа

Задания открытого типа на дополнение

1. *Напишите пропущенное слово (словосочетание) (с маленькой буквы).* Руководство решило разработать стратегию по укреплению _____(1) безопасности, чтобы минимизировать _____(2) и защитить _____ (3) организации.

Правильный ответ:
1. информационной
2. угрозы/риски
3. данные/информацию/ информационные ресурсы

Компетенции (индикаторы): УК-1.1; УК-1.2; УК-1.3; УК-2.1; УК-2.2; УК-3.1; УК-3.2; УК-4.1; УК-4.2; УК-5.1; УК-5.2; УК-6.1; УК-6.2; ОПК-1.1; ОПК-1.2; ОПК-1.3; ОПК-2.1; ОПК-2.2; ОПК-2.3; ОПК-3.1; ОПК-3.2; ОПК-3.3; ОПК-5.1; ОПК-5.2; ОПК-5.3; ПК-1.1; ПК-1.2; ПК-1.3; ПК-2.1; ПК-2.2; ПК-2.3; ПК-3.1; ПК-3.2; ПК-3.3

Задания открытого типа с развернутым ответом

1. *Прочитайте текст задания. Продумайте логику и полноту ответа. Запишите развернутый и обоснованный ответ.*

   Вы работаете в качестве консультанта для малого предприятия, занимающегося производством и продажей экологически чистых продуктов питания. В последнее время компания сталкивается с проблемами, связанными с эффективностью бизнес-процессов, что приводит к увеличению времени выполнения заказов и снижению уровня удовлетворенности клиентов.

Разработать стратегию оптимизации бизнес-процессов с использованием информационно-коммуникационных технологий (ИКТ) для повышения общей эффективности работы предприятия.

Время решения – 40 мин.

Ожидаемый результат:
Стратегия оптимизации бизнес-процессов
1. Анализ текущих процессов
   - Сбор данных: Провести анализ текущих бизнес-процессов, включая производство, управление запасами, обработку заказов, логистику и взаимодействие с клиентами.
   - Идентификация узких мест: Определить этапы, на которых возникают задержки и проблемы, такие как медленная обработка заказов или недостаток информации о наличии товаров.
2. Внедрение ИКТ
   - Автоматизация управления запасами: Внедрение системы управления запасами (например, ERP-системы), которая позволит отслеживать уровень запасов в реальном времени и автоматически генерировать заказы на поставку при достижении минимального уровня.
   - Система управления заказами: Использование онлайн-платформы для приема и обработки заказов. Это может быть веб-сайт с интеграцией с CRM-системой, что позволит быстро обрабатывать заказы и отслеживать их статус.
   - Логистика и доставка: Внедрение системы управления логистикой, которая будет оптимизировать маршруты доставки и отслеживать статус доставки в реальном времени. Это поможет сократить время доставки и повысить удовлетворенность клиентов.
   - Коммуникация с клиентами: Использование чат-ботов и автоматизированных систем для обработки запросов клиентов и предоставления информации о статусе заказов. Это снизит нагрузку на сотрудников и улучшит клиентский опыт.
3. Обучение сотрудников
   - Тренинги и семинары: Проведение обучающих мероприятий для сотрудников по использованию новых технологий и систем. Это поможет повысить уровень их квалификации и уверенность в работе с новыми инструментами.
4. Мониторинг и анализ
   - Системы аналитики: Внедрение систем аналитики для отслеживания ключевых показателей эффективности (KPI), таких как время выполнения заказов, уровень удовлетворенности клиентов и эффективность логистики. Это позволит оперативно реагировать на проблемы и вносить необходимые коррективы.

Пример внедрения системы управления запасами и заказами:

1. Система управления запасами: Внедрение ERP-системы, которая будет отслеживать запасы сырья и готовой продукции. Например, при достижении уровня запасов ниже установленного порога система автоматически генерирует заказ на поставку.
2. Онлайн-платформа для заказов: Создание веб-сайта с функцией онлайн-заказа, где клиенты могут легко выбирать продукты, оформлять заказы и отслеживать их статус. Интеграция с CRM-системой позволит хранить информацию о клиентах и их предпочтениях для будущих маркетинговых кампаний.
3. Оптимизация логистики: Внедрение программного обеспечения для управления логистикой, которое будет анализировать маршруты доставки и предлагать наиболее эффективные варианты. Это может сократить время доставки на 20-30%.
4. Обратная связь от клиентов: Использование автоматизированных опросов для сбора обратной связи от клиентов после получения заказа. Это поможет выявить слабые места в сервисе и внести необходимые улучшения.

Критерии оценивания: наличие в ответе указания основных этапов стратегии оптимизации бизнес-процессов: Сбор данных, Идентификация узких мест, Внедрение ИКТ, Обучение сотрудников, Мониторинг. Наличие в ответе описания хотя бы двух функциональных задач, решаемых внедряемой ИКТ.

Компетенции (индикаторы): УК-1.1; УК-1.2; УК-1.3; УК-2.1; УК-2.2; УК-3.1; УК-3.2; УК-4.1; УК-4.2; УК-5.1; УК-5.2; УК-6.1; УК-6.2; ОПК-1.1; ОПК-1.2; ОПК-1.3; ОПК-2.1; ОПК-2.2; ОПК-2.3; ОПК-3.1; ОПК-3.2; ОПК-3.3; ОПК-5.1; ОПК-5.2; ОПК-5.3; ПК-1.1; ПК-1.2; ПК-1.3; ПК-2.1; ПК-2.2; ПК-2.3; ПК-3.1; ПК-3.2; ПК-3.3

2. *Прочитайте текст задания. Продумайте логику и полноту ответа. Запишите развернутый и обоснованный ответ.*
   Вы работаете в качестве консультанта для малого предприятия, занимающегося разработкой программного обеспечения. В последнее время компания сталкивается с угрозами в области информационной безопасности, включая утечки данных, фишинг и атаки на IT-инфраструктуру. Необходима разработка стратегии по укреплению информационной безопасности.

Время решения – 40 мин.

Ожидаемый результат:
1. Анализ текущего состояния информационной безопасности:
   - Провести аудит существующей системы безопасности, включая анализ политик, процедур и технических средств защиты.

    - Оценить уровень осведомленности сотрудников о вопросах информационной безопасности.
2. Идентификация угроз и уязвимостей:
    - Провести анализ рисков, включая выявление потенциальных угроз (внешние и внутренние) и уязвимостей в системе.
    - Составить список наиболее критичных рисков для бизнеса.
3. Разработка стратегии безопасности:
    - На основе анализа рисков разработать стратегию по улучшению информационной безопасности, включающую технические и организационные меры.
    - Предложить внедрение средств защиты, таких как антивирусные программы, системы обнаружения вторжений (IDS), шифрование данных и многофакторная аутентификация.
4. Обучение и повышение осведомленности сотрудников:
    - Разработать программу обучения для сотрудников по вопросам информационной безопасности, включая распознавание фишинга и безопасное использование корпоративных ресурсов.
    - Оценить эффективность программы через тестирование и опросы.
5. Мониторинг и оценка эффективности:
    - Определить ключевые показатели эффективности (KPI) для оценки уровня информационной безопасности.
    - Разработать план по регулярному мониторингу и обновлению мер безопасности.

Пример реализации стратегии ИБ:

1. Внедрение системы управления информационной безопасностью (ISMS)
    - Исследовать возможности внедрения стандартов ISO/IEC 27001 для создания системы управления информационной безопасностью.
    - Оценить, как это повлияет на защиту данных и доверие клиентов.
2. Защита от фишинга
    - Разработать и внедрить систему защиты от фишинга, включая технологии фильтрации электронной почты и обучение сотрудников.
    - Оценить снижение числа инцидентов, связанных с фишингом, после внедрения мер.
3. Шифрование данных
    - Изучить необходимость шифрования конфиденциальных данных, хранящихся на серверах и в облаке.
    - Оценить влияние шифрования на безопасность и производительность системы.
4. Резервное копирование и восстановление данных

- Разработать стратегию резервного копирования и восстановления данных в случае инцидентов (например, атак программ-вымогателей).
- Оценить риски потери данных и время, необходимое для восстановления.

5. Мониторинг и реагирование на инциденты
   - Создать план реагирования на инциденты, включая определение ролей и обязанностей сотрудников.
   - Оценить, как эффективное реагирование на инциденты может снизить последствия атак.

Критерии оценивания: наличие в ответе указания основных этапов стратегии информационной безопасности: Сбор данных, Идентификация узких мест / Аудит текущей системы, Идентификация угроз и уязвимостей, Разработка стратегии безопасности, Обучение сотрудников, Мониторинг. Наличие в ответе описания хотя бы двух задач, решаемых посредством методов и средств, указанных в стратегии ИБ.

Компетенции (индикаторы): УК-1.1; УК-1.2; УК-1.3; УК-2.1; УК-2.2; УК-3.1; УК-3.2; УК-4.1; УК-4.2; УК-5.1; УК-5.2; УК-6.1; УК-6.2; ОПК-1.1; ОПК-1.2; ОПК-1.3; ОПК-2.1; ОПК-2.2; ОПК-2.3; ОПК-3.1; ОПК-3.2; ОПК-3.3; ОПК-5.1; ОПК-5.2; ОПК-5.3; ПК-1.1; ПК-1.2; ПК-1.3; ПК-2.1; ПК-2.2; ПК-2.3; ПК-3.1; ПК-3.2; ПК-3.3

3. *Прочитайте текст задания. Продумайте логику и полноту ответа. Запишите развернутый и обоснованный ответ.*
   Малое предприятие "СофтТек", занимающееся разработкой программного обеспечения, столкнулось с несколькими инцидентами, связанными с утечкой данных и фишингом. Руководство решило разработать стратегию по укреплению информационной безопасности.

Время решения – 40 мин.

Ожидаемый результат:
Шаг 1: Анализ текущего состояния информационной безопасности
Аудит существующих систем:

- Проведен аудит инфраструктуры: выявлены устаревшие антивирусные программы и отсутствие систем мониторинга.
- Опрос сотрудников показал, что 60% не знают, что такое фишинг и как его распознавать.

Вывод: Необходима модернизация систем безопасности и обучение сотрудников.
Шаг 2: Идентификация угроз и уязвимостей
Анализ рисков:

- Выявлены следующие угрозы:
    - Утечка конфиденциальных данных (например, клиентских баз).
    - Атаки через фишинг и социальную инженерию.
    - Уязвимости в программном обеспечении.

Критичные риски:

- Высокий риск утечки данных из-за недостаточной защиты.
- Увеличение числа фишинговых атак.

Шаг 3: Разработка стратегии безопасности

Технические меры:

1. Внедрение антивирусного ПО и IDS:
    - Установить современные антивирусные решения и системы обнаружения вторжений.
2. Шифрование данных:
    - Все конфиденциальные данные должны быть зашифрованы как на серверах, так и при передаче.
3. Многофакторная аутентификация (MFA):
    - Внедрить MFA для доступа к критически важным системам.

Организационные меры:

1. Политика безопасности:
    - Разработать и утвердить политику информационной безопасности, включая правила работы с данными.
2. Регулярные аудиты:
    - Установить график регулярных аудитов безопасности.

Шаг 4: Обучение и повышение осведомленности сотрудников

Программа обучения:

- Провести тренинги по вопросам безопасности, включая:
    - Распознавание фишинга.
    - Правила безопасного использования паролей.
    - Основы защиты данных.

Оценка эффективности:

- Провести тестирование сотрудников после обучения для оценки уровня усвоения материала.

Шаг 5: Мониторинг и оценка эффективности

Ключевые показатели эффективности (KPI):

- Снижение числа инцидентов безопасности на 50% в течение года.
- Увеличение уровня осведомленности сотрудников о фишинге до 90% после тренингов.

План мониторинга:

- Установить регулярный мониторинг безопасности с отчетами раз в квартал.
- Проводить повторные аудиты каждые 6 месяцев.

Разработанная стратегия включает в себя как технические, так и организационные меры, направленные на повышение уровня информационной безопасности в компании "СофтТек". Внедрение предложенных решений позволит снизить риски утечек данных и повысить

осведомленность сотрудников, что в свою очередь укрепит общую защиту предприятия.

Критерии оценивания: наличие в ответе указания основных этапов стратегии информационной безопасности: Сбор данных, Идентификация узких мест / Аудит текущей системы, Идентификация угроз и уязвимостей, Разработка стратегии безопасности, Обучение сотрудников, Мониторинг. Наличие в ответе описания хотя бы двух задач, решаемых посредством методов и средств, указанных в стратегии ИБ.

Компетенции (индикаторы): УК-1.1; УК-1.2; УК-1.3; УК-2.1; УК-2.2; УК-3.1; УК-3.2; УК-4.1; УК-4.2; УК-5.1; УК-5.2; УК-6.1; УК-6.2; ОПК-1.1; ОПК-1.2; ОПК-1.3; ОПК-2.1; ОПК-2.2; ОПК-2.3; ОПК-3.1; ОПК-3.2; ОПК-3.3; ОПК-5.1; ОПК-5.2; ОПК-5.3; ПК-1.1; ПК-1.2; ПК-1.3; ПК-2.1; ПК-2.2; ПК-2.3; ПК-3.1; ПК-3.2; ПК-3.3

4. *Прочитайте текст задания. Продумайте логику и полноту ответа. Запишите развернутый и обоснованный ответ.*

   Компания "TechSolutions" — небольшой стартап, занимающийся разработкой программного обеспечения для управления проектами. В команде 15 человек, и вся работа ведется удаленно. У компании есть веб-приложение, которое используется клиентами для управления проектами и задачами. Необходима разработка стратегии по укреплению информационной безопасности.

Время решения – 40 мин.

Ожидаемый результат:
Стратегия по укреплению информационной безопасности
1. Оценка текущего состояния безопасности
   - Провести полный аудит существующих мер безопасности, включая анализ уязвимостей веб-приложения и инфраструктуры.
   - Использовать сторонние инструменты для тестирования на проникновение (pen testing) и сканирования уязвимостей.
2. Политика управления доступом
   - Внедрить многофакторную аутентификацию (MFA) для всех сотрудников, особенно для доступа к критически важным системам.
   - Установить четкие роли и права доступа, чтобы ограничить доступ к данным и функциям в зависимости от необходимости.
3. Обучение сотрудников
   - Организовать регулярные тренинги по кибербезопасности для сотрудников, охватывающие темы, такие как фишинг, безопасное использование паролей и управление конфиденциальной информацией.

- Внедрить программу повышения осведомленности о киберугрозах, включая периодические тесты и симуляции атак.

4. Шифрование данных
   - Использовать шифрование для защиты данных как в состоянии покоя, так и при передаче (например, HTTPS для веб-приложения и шифрование баз данных).
   - Настроить регулярное резервное копирование зашифрованных данных для защиты от потери данных.
5. Мониторинг и реагирование на инциденты
   - Внедрить систему мониторинга безопасности (SIEM) для отслеживания подозрительной активности и быстрого реагирования на инциденты.
   - Разработать план реагирования на инциденты, который включает процедуры уведомления, расследования и восстановления после атак.
6. Управление обновлениями и патчами
   - Установить регулярный график обновления программного обеспечения и патчей для всех систем, чтобы минимизировать риски от известных уязвимостей.
   - Автоматизировать процесс обновлений, где это возможно, чтобы гарантировать, что все системы всегда находятся в актуальном состоянии.
7. Безопасная работа с удаленными сотрудниками
   - Внедрить виртуальные частные сети (VPN) для безопасного доступа сотрудников к корпоративным ресурсам.
   - Настроить политику использования личных устройств (BYOD), чтобы минимизировать риски, связанные с использованием незащищенных устройств.

Пример реализации

1. Аудит безопасности: Провести аудит с использованием сторонних экспертов, чтобы выявить уязвимости.
2. Внедрение MFA: Настроить многофакторную аутентификацию для всех сотрудников в течение следующего месяца.
3. Тренинги: Организовать первый тренинг по кибербезопасности через две недели после внедрения MFA.
4. Шифрование: Настроить шифрование данных в базе данных и внедрить HTTPS на веб-приложении в течение трех месяцев.
5. Мониторинг: Установить систему мониторинга безопасности в течение следующего квартала и разработать план реагирования на инциденты.

Эта стратегия поможет "TechSolutions" создать надежную основу для защиты своих данных и систем, а также повысить осведомленность сотрудников о киберугрозах.

Критерии оценивания: наличие в ответе указания основных этапов стратегии информационной безопасности: Сбор данных, Идентификация узких мест / Аудит текущей системы, Идентификация угроз и уязвимостей, Разработка стратегии безопасности, Обучение сотрудников, Мониторинг. Наличие в

ответе описания хотя бы двух задач, решаемых посредством методов и средств, указанных в стратегии ИБ.

Компетенции (индикаторы): УК-1.1; УК-1.2; УК-1.3; УК-2.1; УК-2.2; УК-3.1; УК-3.2; УК-4.1; УК-4.2; УК-5.1; УК-5.2; УК-6.1; УК-6.2; ОПК-1.1; ОПК-1.2; ОПК-1.3; ОПК-2.1; ОПК-2.2; ОПК-2.3; ОПК-3.1; ОПК-3.2; ОПК-3.3; ОПК-5.1; ОПК-5.2; ОПК-5.3; ПК-1.1; ПК-1.2; ПК-1.3; ПК-2.1; ПК-2.2; ПК-2.3; ПК-3.1; ПК-3.2; ПК-3.3

5. *Прочитайте текст задания. Продумайте логику и полноту ответа. Запишите развернутый и обоснованный ответ.*

   Компания "EcoShop" — интернет-магазин, специализирующийся на продаже экологически чистых товаров. В компании работают 20 сотрудников, и она обрабатывает большое количество личных данных клиентов. Необходима разработка стратегии по укреплению информационной безопасности.

Время решения – 40 мин.

Ожидаемый результат:
Стратегия по укреплению информационной безопасности для "EcoShop"
1. Оценка текущего состояния безопасности
   - Провести аудит информационной безопасности, включая анализ рисков и уязвимостей, связанных с обработкой личных данных клиентов.
   - Определить критически важные данные и системы, которые требуют особого внимания.
2. Политика управления доступом
   - Внедрить принцип минимального доступа, чтобы сотрудники имели доступ только к тем данным и системам, которые необходимы для выполнения их работы.
   - Настроить многофакторную аутентификацию (MFA) для всех учетных записей, особенно для доступа к системам, содержащим личные данные клиентов.
3. Шифрование данных
   - Использовать шифрование для защиты личных данных клиентов как в состоянии покоя (например, в базе данных), так и при передаче (например, с использованием HTTPS).
   - Обеспечить шифрование резервных копий данных для защиты от потери информации.
4. Обучение сотрудников
   - Организовать регулярные тренинги по кибербезопасности для всех сотрудников, включая темы, такие как фишинг, безопасное использование паролей и управление конфиденциальной информацией.

- Внедрить систему обратной связи, чтобы сотрудники могли сообщать о подозрительной активности или инцидентах.

5. Мониторинг и реагирование на инциденты
   - Установить систему мониторинга безопасности, чтобы отслеживать аномальную активность и потенциальные угрозы.
   - Разработать и протестировать план реагирования на инциденты, который включает в себя действия в случае утечки данных или кибератаки.
6. Регулярное обновление программного обеспечения
   - Установить график регулярного обновления всех программных продуктов, используемых в компании, для устранения известных уязвимостей.
   - Автоматизировать процесс обновления, где это возможно, чтобы минимизировать риски от устаревшего ПО.
7. Защита данных клиентов
   - Внедрить политику конфиденциальности, которая четко объясняет, как обрабатываются и защищаются личные данные клиентов.
   - Обеспечить возможность клиентам управлять своими данными, включая их удаление по запросу.

Пример реализации

1. Аудит безопасности: Провести аудит в течение первого месяца, чтобы определить уязвимости.
2. Внедрение MFA: Настроить многофакторную аутентификацию для всех сотрудников в течение следующих двух месяцев.
3. Тренинги: Организовать первый тренинг по кибербезопасности через месяц после внедрения MFA.
4. Шифрование: Настроить шифрование данных клиентов и внедрить HTTPS на сайте в течение трех месяцев.
5. Мониторинг: Установить систему мониторинга безопасности в течение следующего квартала и провести тестирование плана реагирования на инциденты.

Эта стратегия поможет "EcoShop" защитить личные данные клиентов и создать безопасную среду для работы с экологически чистыми товарами.

Критерии оценивания: наличие в ответе указания основных этапов стратегии информационной безопасности: Сбор данных, Идентификация узких мест / Аудит текущей системы, Идентификация угроз и уязвимостей, Разработка стратегии безопасности, Обучение сотрудников, Мониторинг. Наличие в ответе описания хотя бы двух задач, решаемых посредством методов и средств, указанных в стратегии ИБ.

Компетенции (индикаторы): УК-1.1; УК-1.2; УК-1.3; УК-2.1; УК-2.2; УК-3.1; УК-3.2; УК-4.1; УК-4.2; УК-5.1; УК-5.2; УК-6.1; УК-6.2; ОПК-1.1; ОПК-1.2; ОПК-1.3; ОПК-2.1; ОПК-2.2; ОПК-2.3; ОПК-3.1; ОПК-3.2; ОПК-3.3; ОПК-

5.1; ОПК-5.2; ОПК-5.3; ПК-1.1; ПК-1.2; ПК-1.3; ПК-2.1; ПК-2.2; ПК-2.3; ПК-3.1; ПК-3.2; ПК-3.3

6. *Прочитайте текст задания. Продумайте логику и полноту ответа. Запишите развернутый и обоснованный ответ.*

   Компания "HealthTech" — стартап в области медицинских технологий, разрабатывающий приложения для мониторинга здоровья. В компании есть 10 сотрудников, и она обрабатывает чувствительные медицинские данные. Необходима разработка стратегии по укреплению информационной безопасности.

Время решения – 40 мин.

Ожидаемый результат:
Стратегия по укреплению информационной безопасности для "HealthTech"
1. Оценка рисков и уязвимостей
   - Провести комплексный аудит текущей системы безопасности, чтобы выявить уязвимости и оценить риски, связанные с обработкой медицинских данных.
   - Определить критически важные данные и системы, которые требуют особого внимания.
2. Политика доступа и аутентификации
   - Внедрить строгую политику управления доступом, чтобы сотрудники имели доступ только к тем данным, которые необходимы для выполнения их работы.
   - Настроить многофакторную аутентификацию (MFA) для всех учетных записей, особенно для доступа к системам, содержащим медицинские данные.
3. Шифрование данных
   - Использовать шифрование для защиты медицинских данных как в состоянии покоя (например, в базе данных), так и при передаче (например, с использованием HTTPS).
   - Обеспечить шифрование резервных копий данных для защиты от потери информации.
4. Обучение сотрудников
   - Провести регулярные тренинги по кибербезопасности для всех сотрудников, включая темы, такие как фишинг, безопасное использование паролей и управление конфиденциальной информацией.
   - Внедрить систему обратной связи, чтобы сотрудники могли сообщать о подозрительной активности или инцидентах.
5. Мониторинг и реагирование на инциденты
   - Установить систему мониторинга для отслеживания аномальной активности и потенциальных угроз.

- Разработать и протестировать план реагирования на инциденты, который включает действия в случае утечки данных или кибератаки.

6. Соответствие законодательству
   - Ознакомиться с требованиями законодательства в области защиты данных, такими как Федеральный закон № 152-ФЗ "О персональных данных", Федеральный закон № 149-ФЗ "Об информации, информационных технологиях и о защите информации", Приказы и рекомендации Роскомнадзора и обеспечить их соблюдение.
   - Разработать и внедрить политику конфиденциальности, которая четко объясняет, как обрабатываются и защищаются медицинские данные.
7. Регулярное обновление программного обеспечения
   - Установить график регулярного обновления всех программных продуктов, используемых в компании, для устранения известных уязвимостей.
   - Автоматизировать процесс обновления, где это возможно, чтобы минимизировать риски от устаревшего ПО.

Пример реализации

1. Аудит безопасности: Провести аудит в течение первого месяца для выявления уязвимостей.
2. Внедрение MFA: Настроить многофакторную аутентификацию для всех сотрудников в течение следующих двух месяцев.
3. Тренинги: Организовать первый тренинг по кибербезопасности через месяц после внедрения MFA.
4. Шифрование: Настроить шифрование медицинских данных и внедрить HTTPS на сайте в течение трех месяцев.
5. Мониторинг: Установить систему мониторинга безопасности в течение следующего квартала и протестировать план реагирования на инциденты.

Эта стратегия поможет "HealthTech" защитить чувствительные медицинские данные пользователей и создать безопасную среду для разработки и использования медицинских приложений.

Критерии оценивания: наличие в ответе указания основных этапов стратегии информационной безопасности: Сбор данных, Идентификация узких мест / Аудит текущей системы, Идентификация угроз и уязвимостей, Разработка стратегии безопасности, Обучение сотрудников, Мониторинг. Наличие в ответе описания хотя бы двух задач, решаемых посредством методов и средств, указанных в стратегии ИБ.

Компетенции (индикаторы): УК-1.1; УК-1.2; УК-1.3; УК-2.1; УК-2.2; УК-3.1; УК-3.2; УК-4.1; УК-4.2; УК-5.1; УК-5.2; УК-6.1; УК-6.2; ОПК-1.1; ОПК-1.2; ОПК-1.3; ОПК-2.1; ОПК-2.2; ОПК-2.3; ОПК-3.1; ОПК-3.2; ОПК-3.3; ОПК-5.1; ОПК-5.2; ОПК-5.3; ПК-1.1; ПК-1.2; ПК-1.3; ПК-2.1; ПК-2.2; ПК-2.3; ПК-3.1; ПК-3.2; ПК-3.3

7. *Прочитайте текст задания. Продумайте логику и полноту ответа. Запишите развернутый и обоснованный ответ.*

   Компания "FinTech Innovations" — небольшая финансовая компания, предоставляющая онлайн-услуги по управлению личными финансами. В компании работает 25 сотрудников, и она обрабатывает финансовую информацию клиентов. Необходима разработка стратегии по укреплению информационной безопасности.

Время решения – 40 мин.

Ожидаемый результат:
Стратегия по укреплению информационной безопасности для "FinTech Innovations"

1. Оценка рисков
   - Провести аудит текущих систем безопасности и оценить риски, связанные с обработкой финансовой информации.
   - Выявить уязвимости в инфраструктуре и определить критически важные данные, требующие защиты.
2. Политика управления доступом
   - Внедрить строгую политику управления доступом, чтобы только авторизованные сотрудники имели доступ к финансовым данным клиентов.
   - Использовать многофакторную аутентификацию (MFA) для всех учетных записей, особенно для доступа к системам, содержащим чувствительную информацию.
3. Шифрование данных
   - Применять шифрование для защиты финансовых данных как в состоянии покоя (например, в базе данных), так и при передаче (например, с использованием протокола HTTPS).
   - Обеспечить шифрование резервных копий данных.
4. Обучение сотрудников
   - Регулярно проводить тренинги по кибербезопасности для всех сотрудников, включая вопросы о фишинге, безопасном использовании паролей и управлении конфиденциальной информацией.
   - Внедрить систему обратной связи, чтобы сотрудники могли сообщать о подозрительной активности.
5. Мониторинг и реагирование на инциденты
   - Установить систему мониторинга для отслеживания аномальной активности и потенциальных угроз.
   - Разработать и протестировать план реагирования на инциденты, который включает действия в случае утечки данных или кибератаки.
6. Соответствие законодательству

- Ознакомиться с требованиями законодательства в области защиты данных, такими как закон о персональных данных и другие нормативные акты, и обеспечить их соблюдение.
- Разработать политику конфиденциальности, которая четко объясняет, как обрабатываются и защищаются финансовые данные клиентов.

7. Регулярное обновление программного обеспечения
   - Установить график регулярного обновления всех программных продуктов, используемых в компании, для устранения известных уязвимостей.
   - Автоматизировать процесс обновления, где это возможно.

Пример реализации

1. Аудит безопасности: Провести аудит в течение первого месяца для выявления уязвимостей и оценки рисков.
2. Внедрение MFA: Настроить многофакторную аутентификацию для всех сотрудников в течение следующих двух месяцев.
3. Тренинги: Организовать первый тренинг по кибербезопасности через месяц после внедрения MFA.
4. Шифрование: Настроить шифрование финансовых данных и внедрить HTTPS на сайте в течение трех месяцев.
5. Мониторинг: Установить систему мониторинга безопасности в течение следующего квартала и протестировать план реагирования на инциденты.

Эта стратегия поможет "FinTech Innovations" защитить финансовую информацию клиентов, создать безопасную среду для предоставления услуг и минимизировать риски, связанные с киберугрозами. Подход к безопасности должен быть комплексным и включать как технические, так и организационные меры.

Критерии оценивания: наличие в ответе указания основных этапов стратегии информационной безопасности: Сбор данных, Идентификация узких мест / Аудит текущей системы, Идентификация угроз и уязвимостей, Разработка стратегии безопасности, Обучение сотрудников, Мониторинг. Наличие в ответе описания хотя бы двух задач, решаемых посредством методов и средств, указанных в стратегии ИБ.

Компетенции (индикаторы): УК-1.1; УК-1.2; УК-1.3; УК-2.1; УК-2.2; УК-3.1; УК-3.2; УК-4.1; УК-4.2; УК-5.1; УК-5.2; УК-6.1; УК-6.2; ОПК-1.1; ОПК-1.2; ОПК-1.3; ОПК-2.1; ОПК-2.2; ОПК-2.3; ОПК-3.1; ОПК-3.2; ОПК-3.3; ОПК-5.1; ОПК-5.2; ОПК-5.3; ПК-1.1; ПК-1.2; ПК-1.3; ПК-2.1; ПК-2.2; ПК-2.3; ПК-3.1; ПК-3.2; ПК-3.3

8. *Прочитайте текст задания. Продумайте логику и полноту ответа. Запишите развернутый и обоснованный ответ.*

   Компания "Creative Agency" — небольшое рекламное агентство, состоящее из 12 сотрудников. В компании активно используется электронная почта и облачные сервисы для обмена информацией. Необходима разработка стратегии по укреплению информационной безопасности.

Время решения – 40 мин.

Ожидаемый результат:
Стратегия по укреплению информационной безопасности для "Creative Agency"

1. Оценка текущего состояния безопасности
   - Провести оценку текущих систем безопасности, включая анализ использования электронной почты и облачных сервисов.
   - Выявить уязвимости и определить критические данные, требующие защиты.
2. Политика управления доступом
   - Внедрить политику управления доступом, чтобы определить, кто может получать доступ к каким данным и сервисам.
   - Использовать многофакторную аутентификацию (MFA) для всех учетных записей, особенно для доступа к облачным сервисам.
3. Обучение сотрудников
   - Провести регулярные тренинги по кибербезопасности, включая темы фишинга, безопасного использования электронной почты и защиты конфиденциальной информации.
   - Создать внутренние руководства и ресурсы по безопасному использованию технологий.
4. Безопасность электронной почты
   - Настроить фильтры спама и антивирусные решения для защиты от фишинговых атак и вредоносных вложений.
   - Внедрить шифрование электронной почты для отправки конфиденциальной информации.
5. Использование облачных сервисов
   - Выбрать надежных провайдеров облачных услуг с высокими стандартами безопасности и конфиденциальности.
   - Настроить шифрование данных в облаке и обеспечить резервное копирование информации.
6. Мониторинг и реагирование на инциденты
   - Установить систему мониторинга для отслеживания аномальной активности в сетях и сервисах.
   - Разработать план реагирования на инциденты, который включает действия в случае утечки данных или кибератаки.
7. Регулярные обновления и патчи

- Установить график регулярного обновления программного обеспечения и операционных систем для устранения известных уязвимостей.
- Автоматизировать процесс обновления, где это возможно.

8. Создание резервных копий
   - Настроить регулярное резервное копирование всех важных данных в облаке и на локальных носителях.
   - Проверять целостность резервных копий и возможность их восстановления.

Пример реализации

1. Аудит безопасности: Провести аудит в течение первого месяца для выявления уязвимостей.
2. Внедрение MFA: Настроить многофакторную аутентификацию для всех сотрудников в течение следующих двух месяцев.
3. Тренинги: Организовать первый тренинг по кибербезопасности через месяц после внедрения MFA.
4. Фильтры электронной почты: Настроить фильтры спама и антивирусные решения в течение трех месяцев.
5. Резервное копирование: Настроить регулярное резервное копирование данных в течение следующего квартала.

Эта стратегия поможет "Creative Agency" защитить данные клиентов и сотрудников, создать безопасную рабочую среду и минимизировать риски, связанные с киберугрозами. Подход к безопасности должен быть комплексным и включать как технические, так и организационные меры.

Критерии оценивания: наличие в ответе указания основных этапов стратегии информационной безопасности: Сбор данных, Идентификация узких мест / Аудит текущей системы, Идентификация угроз и уязвимостей, Разработка стратегии безопасности, Обучение сотрудников, Мониторинг. Наличие в ответе описания хотя бы двух задач, решаемых посредством методов и средств, указанных в стратегии ИБ.

Компетенции (индикаторы): УК-1.1; УК-1.2; УК-1.3; УК-2.1; УК-2.2; УК-3.1; УК-3.2; УК-4.1; УК-4.2; УК-5.1; УК-5.2; УК-6.1; УК-6.2; ОПК-1.1; ОПК-1.2; ОПК-1.3; ОПК-2.1; ОПК-2.2; ОПК-2.3; ОПК-3.1; ОПК-3.2; ОПК-3.3; ОПК-5.1; ОПК-5.2; ОПК-5.3; ПК-1.1; ПК-1.2; ПК-1.3; ПК-2.1; ПК-2.2; ПК-2.3; ПК-3.1; ПК-3.2; ПК-3.3

Экспертное заключение

Представленный фонд оценочных средств (далее – ФОС) по дисциплине «Производственная (проектно-технологическая) практика» соответствует требованиям ФГОС ВО.

Предлагаемые формы и средства текущего и промежуточного контроля адекватны целям и задачам реализации основной профессиональной образовательной программы по направлению подготовки 38.04.05 Бизнес-информатика.

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.

Председатель учебно-методической
комиссии экономического института Шаповалова Е.Н.

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)