Практика производственная, педагогическая (1 курс, 2 семестр, КЭО)

Задание 1.5 ИСР

Фатьянов М.А.

1. Общая информация

Название модуля: «Введение в информационную безопасность»

Тип курса: Базовый дистанционный курс

Требования к студенту: Базовые навыки работы с компьютером и интернетом

Платформа: Moodle (SCORM 1.2, HTML5)

2. Цели и результаты обучения

Общие цели:

Познакомить обучающихся с ключевыми понятиями информационной безопасности.

Сформировать представление о наиболее распространённых угрозах и уязвимостях.

Научить применять базовые меры защиты информации.

Результаты обучения (по завершении фрагмента):

Студент сможет определить основные понятия: «угроза», «уязвимость», «контроль доступа».

Студент распознает минимум три типа распространённых атак на информационные системы.

Студент продемонстрирует умение применять простые механизмы защиты (пароли, шифрование, резервное копирование).

3. Структурная схема фрагмента

Раздел	Содержание	Формат	Время	Активности
1. Вводный тест	Короткий диагностический опрос (5 вопросов)	Quiz (Moodle)	5 мин	Самопроверка
2. Лекция: Основные понятия	Текст + инфографика	SCORM-слайд	10 мин	Прогресс-бар
3. Видео-демонстрация угроз	Видео 3–5 мин	Встроенное видео	7 мин	Вопросы по видео

Раздел	Содержание	Формат	Время	Активности
4. Интерактивная схема атак	Drag-and-drop: сопоставить тип атаки и описание	H5P-модуль	10 мин	Drag-and-drop
5. Практическое задание	Настройка пароля и шифрование файла	Интерактивный тренажёр	10 мин	Шаги в симуляторе
6. Итоговый тест	7 вопросов (минимум 70% правильных)	Quiz (Moodle)	3 мин	Самооценка

4. Описание разделов

4.1 Диагностический опрос

Цель: Оценить исходный уровень знаний.

Механика: 5 вопросов типа «одно правильное/несколько правильных ответов».

Техническая реализация: стандартный модуль Quiz Moodle.

4.2 Лекция: Основные понятия

Слайд 1: Определение информационной безопасности.

Слайд 2: Ключевые термины (угроза, уязвимость, риск, контроль доступа).

Слайд 3: Примеры классификации угроз (внешние/внутренние, случайные/намеренные).

Инфографика: Визуальная схема «угроза → уязвимость → инцидент».

Навигация: Кнопки «Вперед», «Назад», прогресс-бар внизу.

4.3 Видео-демонстрация

Содержание: Короткие реальные кейсы фишинга, DDoS и брутфорса.

Вопросы по видео: После каждого кейса всплывает окно с 1 вопросом True/False.

Техническая платформа: встроенное видео HTML5 с триггером H5P Interactive Video.

4.4 Интерактивная схема атак

Содержимое: Список атак (фишинг, SQL-инъекция, XSS, Man-in-the-Middle) и их описания.

Задача: Сопоставить названия атак с их описаниями методом перетаскивания.

Технология: H5P Drag and Drop.

Обратная связь: Правильные пары фиксируются зелёным, неправильные — красным.

4.5 Практическое задание

Сценарий: Студенту предлагается создать надёжный пароль и зашифровать текстовый файл.

Интерфейс: Встроенный эмулятор файловой системы.

Инструкция: Пошаговый гид («Введите пароль», «Выберите алгоритм AES-256», «Нажмите «Зашифровать»»).

Оценка: Автоматическая проверка длины пароля и успешности шифрования.

4.6 Итоговый тест

Формат: 7 вопросов с автоматической проверкой.

Порог прохождения: 5/7.

Отчёт: Генерация сертификата о прохождении модуля.

5. Технические требования

Стандарты: SCORM 1.2, HTML5, WCAG 2.1 AA.

Совместимость: Десктопы (Chrome, Firefox), мобильные браузеры.

Интеграция: Модуль загружается как ZIP-пакет в LMS Moodle.

Адаптивность: Респонсивный дизайн, масштабируемый SVG для инфографики.

6. Дополнительные ресурсы и поддержка

Словарь терминов: PDF со списком ключевых понятий.

Ссылки: Государственные стандарты (ГОСТ, ISO/IEC 27001).

Форум: Тема для обсуждения вопросов и примеров из практики.

Контакты: e-mail педагогической поддержки.

7. Оценка эффективности модуля

Метрики: коэффициент прохождения тестов, время на разделах, активность на форуме.

Сбор обратной связи: встроенный опрос по окончании модуля.