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

Задание 1.6 ИСР

Фатьянов М.А.

Выполнил: студент группы «380» Фатьянов Максим Александрович Дата проведения занятия: 10 мая 2025 г. Предмет: Вычислительная техника Место проведения: Колледж «Звёздный» Преподаватель: Фатьянов М. А. Тема занятия: Основы информационной безопасности

1. Структура и последовательность проведения занятия Занятие было организовано поэтапно и включало следующие компоненты:

Актуализация знаний: краткий обзор понятий вычислительной техники и обоснование необходимости защиты информации.

Изложение нового материала: определение ключевых принципов информационной безопасности (конфиденциальность, целостность, доступность), классификация угроз (вредоносное ПО, фишинговые атаки, подбор паролей).

Иллюстрация теории на примерах: анализ реальных инцидентов информационной безопасности и методов их предотвращения.

Практическая работа: оценка надёжности паролей, выявление признаков фишинговых сообщений, выполнение задания по шифрованию методом Цезаря.

Подведение итогов: резюме основных выводов, ответы на вопросы студентов и постановка домашнего задания.

2. Деятельность преподавателя Преподаватель продемонстрировал высокий уровень профессиональной компетентности и систематичности изложения материала. Теоретические положения были подкреплены визуальными и программными демонстрациями с использованием проекторной системы и специализированного программного обеспечения для анализа уязвимостей. В ходе практического блока преподаватель осуществлял дифференцированный подход, предоставляя индивидуальную поддержку и осуществляя оперативный контроль за ходом выполнения заданий.

3. Деятельность студентов Студенты проявили активную познавательную мотивацию на этапах обсуждения теоретических аспектов и анализа кейсов. При выполнении практических заданий большинство участников адекватно оценивали криптостойкость паролей и распознавали фишинговые сообщения. В отдельных случаях возникали затруднения при ручном шифровании, которые были преодолены посредством методического сопровождения преподавателя. Уровень вовлечённости оставался высоким на всех этапах занятия.

4. Методы и средства обучения Использовались компьютерный класс и мультимедийный проектор для демонстрации теоретического материала и примеров киберинцидентов. Применялись онлайн-инструменты для проверки слабых мест в паролях и анализа фишинговых шаблонов. В учебном процессе были задействованы интерактивные презентации и раздаточные материалы с алгоритмами и определениями основных понятий.

5. Организация учебного пространства и психологический климат Аудитория была спланирована таким образом, что преподаватель мог осуществлять визуальный контроль за действиями каждого студента. Создана комфортная и доброжелательная атмосфера, способствующая активному включению в образовательную деятельность; ошибки рассматривались в конструктивном ключе, без излишнего давления.

6. Достижение учебных целей Поставленные цели занятия — ознакомление с фундаментальными принципами информационной безопасности и приобретение практических навыков в области создания надёжных паролей, распознавания фишинговых угроз и применения алгоритмических методов шифрования — были в полном объёме реализованы.

Общая оценка Занятие проведено на высоком методическом уровне: достигнут баланс между теоретическим изложением и практической отработкой навыков, что обеспечило эффективное усвоение материала.

Рекомендации

Организовать фронтальный разбор типичных ошибок при ручном шифровании для закрепления алгоритмических приёмов.

Использовать виртуальные стенды и специализированные лаборатории информационной безопасности для более углублённых практических занятий.

Внедрить онлайн-платформу с автоматизированной проверкой заданий по криптографии для обеспечения мгновенной обратной связи.