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

Задание 1.7 ИСР

Фатьянов М.А.

Самоанализ профессиональной деятельности в рамках педагогической практики

Контекст практики

В рамках прохождения педагогической практики мною был проведен урок информатики для учащихся группы 380 по теме «Информационная безопасность». Целью урока было не только ознакомить учащихся с основными понятиями и рисками информационной безопасности, но и развить практические навыки настройки базовых средств защиты на персональном компьютере.

Тема урока: «Информационная безопасность: угрозы, защита и практические настройки»

1. Цели урока

Образовательные:

Ознакомить участников с фундаментальными понятиями информационной безопасности: конфиденциальность, целостность, доступность, социальная инженерия, вредоносное ПО.

Рассмотреть типичные виды угроз (вирусы, трояны, фишинг, брандмауэр).

Научить базовым методам защиты: антивирусное сканирование, настройка брандмауэра, управление паролями, резервное копирование.

Развивающие:

Развивать аналитическое мышление при оценке рисков и выборе инструментов защиты.

Формировать навыки практической работы с операционной системой (Windows) и ее встроенными средствами безопасности.

Развивать умение работать в команде при выполнении лабораторных заданий.

Воспитательные:

Воспитывать ответственность и аккуратность при обращении с конфиденциальными данными.

Формировать осознанное отношение к собственной кибербезопасности и

безопасности учебного процесса.

2. Содержание и структура урока

Урок был построен в формате практико-ориентированного занятия с чередованием теории и лабораторной работы.

Этапы урока:

Организационный момент (5 мин)

Приветствие и проверка готовности оборудования.

Краткое введение в тему и озвучивание целей урока.

Теоретическая часть (15 мин)

Объяснение ключевых понятий: конфиденциальность, целостность, доступность.

Обзор основных угроз: вирусы, трояны, фишинг и методы социальной инженерии.

Демонстрация примеров инцидентов в информационной безопасности.

3. Практическая часть (45 мин)

Лабораторная работа 1: Антивирусное сканирование

Учащиеся работают парами. На тестовых файлах запускают встроенный Защитник Windows.

Анализ отчетов об обнаруженных угрозах.

Лабораторная работа 2: Настройка брандмауэра

Создание правила для блокировки несанкционированного входящего трафика.

Тестирование соединения с внешним сервером и анализ логов.

Лабораторная работа 3: Управление паролями

Обсуждение принципов надежного пароля.

Практика: генерация и сохранение пароля в менеджере (KeePass или аналог).

Лабораторная работа 4: Резервное копирование

Настройка автоматического создания резервной копии документов на внешнем диске.

Проверка восстановления файла из резервной копии.

Рефлексия и закрепление (10 мин)

- Обсуждение выполненных заданий, выявленных трудностей.
- Ответы на вопросы и рекомендации для самостоятельной практики.

Анализ проведенного урока

Сильные стороны:

- Практическая направленность: учащиеся сразу применили знания на практике, что повысило усвоение материала.
- Четкая структура: разбивка на небольшие лабораторные задания позволила контролировать tempo и вовлеченность.
- Межличностное взаимодействие: работа в парах способствовала обмену опытом и решению сложных задач вместе.

Аспекты для улучшения:

- Управление временем: часть учащихся не успели завершить лабораторную работу по брандмауэру. Следует более точно рассчитывать время или сократить число заданий.
- Дифференциация: для слабых студентов предусмотреть инструкционные подсказки или готовые шаблоны, чтобы избежать задержек.
- Обратная связь: добавить короткий тест в конце урока для проверки понимания ключевых понятий.

4. Взаимодействие с учащимися и их вовлеченность

Учащиеся группы 380 активно включились в лабораторные работы. Наибольший интерес вызвало исследование логов брандмауэра и управление паролями. Некоторые затруднения возникли при настройке резервного копирования из-за недостатка практического опыта работы с файловой системой.

5. Выводы и перспективы

Проведенный урок подтвердил важность сочетания теории и практических заданий для эффективного усвоения материала по информационной безопасности. В дальнейшем планируется:

- Обеспечить более гибкое распределение времени между этапами.
- Разработать дополнительные вспомогательные материалы (инструкции, шаблоны).
- Включить элементы самостоятельной оценки (тесты, квизы) для контроля знаний.