Секция «Цифровая трансформация образования и новые технологии обучения»

Реализация программы по криптоанализу для обучения специалистов по кибербезопасности

Научный руководитель – Корольков Юрий Дмитриевич

Королькова М.Д.[1], *Корольков И.Д.*[2], *Волкорезов С.В.*[3], *Чанков Р.А.*[4]

1 - Иркутский государственный университет, Физический факультет, Иркутск, Россия, *E-mail: masha.korolkova2003@yandex.ru*; 2 - Иркутский государственный университет, Физический факультет, Иркутск, Россия, *E-mail: korolkov.ivan2000@yandex.ru*; 3 - Иркутский государственный университет, Физический факультет, Иркутск, Россия, *E-mail: semavaly@mail.ru*; 4 - Иркутский государственный университет, Физический факультет, Иркутск, Россия, *E-mail: demos99000.rost@gmail.com*

Традиционные методы обучения криптоанализу зачастую опираются на программные инструменты, которые выполняют значительную часть анализа автоматически, предоставляя пользователю готовые результаты. Такой подход, хотя и удобен, существенно ограничивает развитие аналитического мышления и не способствует формированию навыков, необходимых для самостоятельного проведения криптоанализа. Важно не только знакомить обучающихся с существующими алгоритмами, но и давать им возможность самостоятельно исследовать криптографические системы, находить уязвимости и применять различные методы атак.

В данной работе представлена методика и программная разработка, ориентированная на обучение специалистов по кибербезопасности анализу криптостойкости ряда распространенных шифров [1,2]. Основная особенность этой программы заключается в том, что она не предоставляет обучающемуся готовых решений, а лишь предоставляет набор вспомогательных инструментов, которые помогают в процессе исследования зашифрованного текста. В отличие от традиционных обучающих программ, которые фокусируются на автоматическом разборе шифров, этот инструмент требует от пользователя активного участия и применения знаний о криптоанализе.

Такой подход позволяет:

- Повышать уровень практической подготовки специалистов за счет имитации реальных условий взлома шифров.

- Создавать условия для объективной оценки знаний, поскольку программа фиксирует затраченное время и успешность расшифрования.

Для работы с программой на легких уровнях сложности необходимо, чтобы обучающийся имел базовое представление об алгоритмах шифрования и методах их расшифрования без знания ключа.

На начальных этапах обучения работа с программой потребует активного участия преподавателя, который будет направлять обучающегося, помогая ему анализировать зашифрованный текст и определять возможные уязвимости. Первоначально студент может испытывать затруднения при выборе подходящих методов криптоанализа, так как процесс взлома шифров требует не только теоретических знаний, но и навыков практического применения различных аналитических инструментов.

В этот период обучение строится на совместном разборе примеров, пошаговом разъяснении методик и постепенном формировании у обучающегося способности самостоятельно выявлять уязвимости.

По мере накопления практического опыта и освоения базовых техник криптоанализа студент начинает самостоятельно замечать характерные особенности шифротекста, такие как

неравномерность распределения символов, повторяющиеся последовательности или аномалии в структуре текста, которые могут указывать на определенный тип шифрования.

Благодаря модульной структуре программа поддерживает несколько видов шифрования и несколько уровней сложности, что позволяет адаптировать обучение под различные уровни подготовки студентов.

Обучающийся получает доступ к интерфейсу, в котором представлена зашифрованная информация. Его задача — восстановить исходный текст без знания ключа, используя методы криптоанализа.

При выборе метода шифрования в программе выполняются следующие действия:

- агружается фрагмент открытого текста из базы данных;

- применяется выбранный пользователем алгоритм шифрования;

- отображается зашифрованный текст в виде удобного визуального представления, в зависимости от особенностей шифрования.

Далее обучающийся, используя предоставленные инструменты, должен провести анализ криптостойкости шифра и попытаться восстановить исходный текст. В процессе работы доступны функций, адаптированные для криптоанализа конкретного шифра, например:

1. Работа с перестановками – изменение порядка символов в таблице.

2. Генерация гаммы и побитовое сложение – для анализа методов гаммирования.

3. Частотный анализ – подсчет встречаемости символов для выявления закономерностей.

Также есть функционал для отмены действий обучающегося и возврат к предыдущему состоянию – позволяет пошагово корректировать процесс анализа, пользователь может вернуться к тому шагу, на котором была совершена ошибка и продолжить анализ, не теряя прогресса. Это важно также для преподавателя, т.к. используя функцию фиксация времени работы для оценки скорости и эффективности криптоанализа, будет учтено полное время, за которое обучающийся выполнил работу.

Выбор уровня сложности влияет на длину шифротекста и наличие вспомогательных подсказок.

Если обучающийся успешно расшифровал текст, программа фиксирует его время выполнения задания, что позволяет преподавателям оценивать прогресс студентов. В случае неудачи программа предлагает повторить/продолжить попытку, анализируя допущенные ошибки.

Уникальные особенности программы:

1. Комбинация технических инструментов и самостоятельного анализа.

2. Многоуровневая система сложности.

- на базовом уровне обучающийся получает больше подсказок и может использовать упрощенные методы анализа;

- средний уровень предлагает более сложные задания и больший объем шифрованного текста;

- продвинутый уровень требует от обучающегося глубокого понимания принципов криптоанализа, так как подсказки полностью отсутствуют.

3. Оценка эффективности обучающегося.

Программа разработана на языке Python, что обеспечивает удобство ее расширения и интеграции с другими инструментами. В основе работы лежат стандартные библиотеки для обработки текстов и работы с интерфейсом. Основные компоненты:

- модуль работы с текстом и криптографические алгоритмы – обеспечивает загрузку, фильтрацию и шифрование;

- интерфейс пользователя – отображает таблицу с зашифрованным текстом и инструментами для работы;

- модуль анализа – включает частотный анализ, поиск закономерностей и другие криптоаналитические методы;

- система управления сложностью – регулирует количество подсказок и длину текста;

- таймер – фиксирует время выполнения задания.

Разработанная программа представляет собой инструмент для обучения криптоанализу, который сочетает современные технологии с традиционными методами преподавания. Благодаря требованию активного участия обучающегося и наличию вспомогательных инструментов для исследования шифров, программа способствует развитию аналитического мышления и помогает студентам лучше понять принципы криптоанализа. Программа интегрируется в учебный процесс и позволяет применять полученные теоретические знания на практике.

Применение данной программы в образовательном процессе позволит не только повысить уровень подготовки специалистов в области кибербезопасности, но и создать объективную систему оценки их навыков, что особенно важно при подготовке профессионалов, работающих в сфере информационной безопасности.

Источники и литература

1) Глухов М. М., Круглов И. А., Пичкур А. Б. Введение в теоретико-числовые методы криптографии. М.: Лань. 2024. 396 с.

2) Применко Э. А., Борисов А. В. Алгебраические основы криптографии в задачах и упражнениях. Учебное пособие. М.: КУРС. 2023. 104 с.