МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«САРАТОВСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ Н.Г.ЧЕРНЫШЕВСКОГО»

Кафедра информационных систем и технологий в обучении

МЕТОДИЧЕСКАЯ ПОДДЕРЖКА ПОДГОТОВКИ ОБУЧАЮЩИХСЯ К ОЛИМПИАДЕ ПО КРИПТОГРАФИИ.

АВТОРЕФЕРАТ БАКАЛАВРСКОЙ РАБОТЫ

студента 4 курса 461 группы
направления 44.03.01 Педагогическое образование (профиль Информатика)
факультета компьютерных наук и информационных технологий
Надежкин Евгений Денисович

Научный руководитель:
к.п.н., доцент _____ Н.А. Александрова

подпись, дата

Зав. кафедрой:
к.п.н., доцент _____ Н.А. Александрова

подпись, дата

Саратов 2023

ВВЕДЕНИЕ

Актуальность темы. Проблема защиты информации от прочтения посторонним лицом, волнует человека с далёких времён, именно поэтому люди начали искать способы преобразования информации, которое бы защитило отправленное сообщение от посторонних лиц. Криптография появилась вместе с человеческим языком. Письменность в свою очередь сама по себе была криптографической системой, так как в древние времена её знали и могли применять только определённые люди.

После того, как начала распространяться письменность, криптография стала самостоятельной наукой. О возрасте криптографии мы можем судить исходя из того, что Гай Юлий Цезарь в своей переписке применял шифр, который в последствии получил его имя.

Самое быстрое развитие криптографии произошло во время Первой и второй мировой войны. В наше время появились новые вычислительные мощности, которые способствуют созданию более сложных алгоритмов шифрования.

Методы криптографической защиты информации используются как для защиты информации, которую обрабатывают в ЭВМ или информацию, которая хранится на различных запоминающих устройствах, так и для обеспечения безопасности передачи информации между компонентами системы по сетевым каналам.

Использование криптографических преобразований для защиты информации от несанкционированного доступа имеет долгую историю, и в настоящее время существует огромное количество различных методов шифрования, которые имеют теоретические и практические основы для успешного применения. Большинство из этих методов могут быть успешно использованы для защиты конфиденциальной информации.

Криптография реализуется через применение специализированных алгоритмов, при помощи которых осуществляется шифрование информации. Существует несколько методов кодирования, каждый из которых

применяется в различных ситуациях и обладает своими уникальными свойствами.

Дипломная работа состоит из введения, двух глав, заключения и списка литературы.

В первой главе рассматривается структура и содержание темы «Основы криптографии», проводится анализ УМК на наличие данной темы и тематических учебных пособий, а также проводится анализ школьных олимпиад по информатике, на наличие в них заданий по теме «Криптография».

Во второй главе размещена практическая часть дипломной работы, в которой нами была сформирована система заданий по теме «Основы криптографии», создан тематический квест для детей 8-9 классов, а также создана подборка заданий и повышенного уровня сложности, для подготовки детей к олимпиаде по «Криптографии».

Объект исследования: методика преподавания темы «Криптография» в курсе информатики.

Предмет исследования: изучение разделов криптографии на высоком уровне.

Цель бакалаврской работы – предложить методическую поддержку темы «Криптография» школьного курса информатики.

Поставленная цель определила **следующие задачи**:

1. Проанализировать педагогическую и методическую литературу по теме.
2. Провести анализ УМК на наличие темы «Основы криптографии»
3. Проанализировать школьные олимпиады на наличие темы «Криптография»
4. Подобрать систему заданий по теме «Основы криптографии» для 8-9 классов.

5. Разработать методическую поддержку по криптографии для обучающихся 8-9 классов в формате квеста и системы заданий олимпиадного уровня.

Методологические основы «Методическая поддержка подготовки обучающихся к олимпиаде по криптографии» представлены в работах Абросимов М.Б., Салий В.Н., Жаркова А.В., Коннова А.Д., Лобов А.А., Моденова О.В., Шабаркова А.О., Б.Я. Рябко, А.Н. Фионов., Малюк А.А., Здор С.Е., Баричев С. Г., Босова Л.Л., Босова А.Ю., Семакин И.Г., Угринович Н.Д.

Теоретическая и/или практическая значимость бакалаврской работы.

Работа даёт представление о теме «Криптография», способах шифрования данных, нормативных документах и учебных материалах, а также о видах заданий, используемых в преподавании данной темы в школах. Это позволяет расширить знания о методах и технологиях шифрования.

В работе разработана методическая поддержка подготовки учащихся к олимпиаде по криптографии, что имеет значимость в контексте изучения нового материала, также помогает развить логическое мышление и навыки анализа, что может быть полезно в будущей карьере в области информационной безопасности или компьютерных наук. Кроме того, подготовка к олимпиаде по криптографии может быть интересным и увлекательным опытом для учащихся, который поможет им расширить свой кругозор. В ней представлены системы заданий, которые могут быть использованы преподавателями в школьной программе по информатике.

Структура и объём работы. Бакалаврская работа состоит из введения, двух разделов, заключения, списка использованных источников и одного приложения. Общий объем работы – 56 страниц, из них 53 страницы – основное содержание, включая 16 рисунков и одну таблицу, цифровой носитель в качестве приложения, список использованных источников информации – 20 наименований.

КРАТКОЕ СОДЕРЖАНИЕ РАБОТЫ

Первая глава «Структура и содержание темы «Основы криптографии в курсе информатики»»

Посвящена знакомству с методами шифрования информации, анализу школьных УМК, учебных пособий, а также школьных олимпиад, на наличие темы «Криптография».

В первом параграфе данной работы рассматриваются методы основные теоретические разделы курса. В данном разделе мы знакомимся с основными понятиями криптографии, рассматриваем основные криптографические системы, которые используются в наши дни, к каждой криптографической системе написано определение и теоретический материал, необходимый, чтобы понять, принцип их работы и для каких целей используется каждая система.

Дальше мы рассматриваем УМК базового курса на наличие темы «Криптография» в школьной программе, для рассматриваемых учебников мы проводим анализ на наличие темы, далее изучаем теоретический материал учебника, а так же практические задания, в конце анализа каждого учебника мы выделяем плюсы и минусы, а также делаем вывод на основе полученных данных, после анализа учебников базового курса мы сделали вывод о том, что тема «Криптография» не раскрывается в достаточном объёме в курсе информатики, затрагивается лишь тема «Кодирование информации», которая является лишь составной частью темы «Криптография» .

В следующем параграфе мы анализируем учебные пособия по теме «Основы криптографии в школьном курсе информатики». Проводим анализ теоретического материала данных учебных пособий, разбираем практические задания, выделяем плюсы и минусы каждого пособия, на основе полученных данных, мы смогли сделать вывод о том, что все они направлены на изучение данной темы студентами вузов, задания в них не рассчитаны на изучение в школьном курсе информатики, так как рассматриваются с точки зрения математики с использованием сложных формул и подсчётов. Поэтому нами

было принято решение о создании системы заданий, для школьников, которая бы способствовала вовлеченности и заинтересованности учащихся в изучении темы «Криптография».

Последний параграф первой части направлен на рассмотрение олимпиад по информатике, которые способствуют практическому применению знания темы «Криптография». Проанализировав данные олимпиады, мы сделали вывод, что наиболее подходящей нам по теме является “олимпиада школьников и студентов по криптографии”, в ней тема криптографии раскрывается лучше всего, поэтому нами было принято решение создать материал, который поможет в подготовке к данной олимпиаде.

В первой главе мы познакомились с темой «Криптография». рассмотрели структуру и содержание темы «Основы криптографии», провели анализ УМК и тематических учебных пособий на наличие данной темы, а также провели анализ школьных олимпиад по информатике, на наличие в них заданий по теме «Криптография».

Второй раздел «Подборка заданий по теме «Криптография»» посвящен разработке авторских заданий, которые помогут подготовить детей к решению олимпиадных задач.

В первом параграфе мы создали авторскую систему заданий, для введения детей 8-9 классов в тему «Основы криптографии». После каждого задания была добавлена информация, о новом для детей способе шифрования информации. Данная система состоит из десяти заданий, она создана с целью вовлечь детей в изучение новой для них темы, благодаря тому что преподносимая детям информация даётся не целиком, а частями, после выполнения определённых заданий.

В следующем разделе мы разработали авторский квест. Данный квест был создан нами с целью вовлечения детей в решение заданий для закрепления темы «Криптография», благодаря тому что преподносимые

детям задания даются в игровой форме, с иллюстрациями, а также интересным сюжетом, о космическом исследователе.

Далее мы разобрали задания XXI олимпиады школьников и студентов по криптографии, для детей 8-9 классов. После каждого задания было добавлено решение с объяснением. Данный раздел создан с целью ознакомления детей с заданиями и способами их решения.

В последнем разделе мы разработали два собственных варианта с задания на основе задач, предложенных для решения в XXI олимпиаде школьников и студентов по криптографии, для детей 8-9 классов. Первый вариант был аналогичен заданиям из олимпиады и необходим для закрепления детьми пройденного в предыдущем параграфе материала. Следующий вариант состоит из заданий повышенной сложности, в котором для каждого задания необходимо применить несколько способов шифрования информации, данный вариант не только поможет детям закрепить пройденный материал, но и поспособствует лучшему ориентированию в теме, при решении олимпиадных заданий по теме «Криптография».

ЗАКЛЮЧЕНИЕ

Данная работа была проведена с целью изучить теоретические основы криптографии и предложить систему заданий для обучения по данной теме.

Знания учащегося формируются через теоретическую и практическую подготовку.

Проанализировав педагогическую и методическую литературу, мы выявили определённые проблемы и условия формирования вовлечённости и заинтересованности детей во время обучения, мы можем сделать вывод о том, что знания умения и навыки учащегося будут формироваться, если будут соблюдаться предложенные нами условия.

Таким образом, если в процессе обучения осуществляется формирование наглядных заданий, происходит вовлечение учеников в процесс изучения новой темы, благодаря этому дети будут обладать высоким уровнем готовности к усвоению новых знаний.

В качестве одного из условий формирования заинтересованности и вовлечённости может выступать разработанная нами и апробированная на практике система заданий, для детей 8-9 классов, она способствует лучшему усвоению изучаемого материала, благодаря визуальному сопровождению и теоретическому подкреплению каждого задания.

Если предложенные нами условия создания заданий соблюдаются - то учащиеся будут обладать высоким уровнем готовности к изучению новых тем.

Продолжением нашей выпускной квалификационной работы является включение педагогических условий по формированию знаний, умений и навыков, в процессе олимпиадной подготовки. Были проанализированы олимпиады, связанные с темой «Криптография», выделены плюсы и минусы каждой олимпиады. На основе заданий олимпиады школьников и студентов по криптографии был выполнен разбор с объяснением каждого задания, а также нами был создан тренировочный вариант, который способствует закреплению пройденного материала.

В практической части дипломной работы мы предлагаем систему авторских задач, которые постепенно усложняются, такие задания помогут лучше разобраться со способами шифрования информации, а также в будущем помогут лучше ориентироваться в изученном материале темы «Критография». Нами был разработан квест по теме «Криптография» для детей 8-9 класса, задания квеста представлены в игровой форме, каждое задание сопровождается авторским сюжетом, который будет интересен детям, тем самым способствуя заинтересованности и вовлечённости учащихся в решении заданий. Выполнен полный разбор с объяснением принципа решения заданий XXI олимпиады школьников и студентов по криптографии, для детей 8-9 классов, создан тренировочный вариант с заданиями аналогичными олимпиадным, для закрепления полученных знаний, а так же был разработан авторский вариант, с более сложными заданиями, которые объединяют в себе несколько методов шифрования информации, такой вариант будет способствовать лучшему понимаю темы «Криптография», а так же поможет детям быстрее находить шифры, необходимые для решения олимпиадных заданий.

Отдельные части бакалаврской работы были представлены на конференции:

VII Всероссийская научно-практическая конференция «Образование. Технологии. Качество» «ОТК-Саратов-2023»: Надежкин Е.Д. «Особенности изучения темы "криптография" в школе», 6 с. // Дискуссионная площадка «Цифровая кафедра СГУ: ИТразработки для педагогического образования». Вед. Литвинова О.А., Гаврилова Е.А., ауд. 215 – Саратов: Саратовский университет (ОТК-Саратов-2023), 24 – 25 марта 2023 г., Саратов. – 21с.

Основные источники информации:

1) Методы защиты информации: практикум по выполнению лабораторных работ для студентов специальности 1-40 04 01 "Информатика и технологии программирования" дневной формы

обучения / сост. Д. В. Прокопенко. - Гомель: ГГТУ им. П. О. Сухого, 2020. - 77 с.

2) Теория и практика обучения школьников и студентов СПО основам защиты информации / Е.И. Деза, Л.В. Котова, Е. С. Лебедева — Наука и школа. 2020.
3) Информационная безопасность (обязанности) / Зарипова Г.К., Рамазонов Ж.Ж. — Научные исследования. 2019.
4) Здор С.Е. Кодированная информация. От первых природных кодов до искусственного интеллекта / С.Е. Здор. — Изд. Стереотип: 2021. - 166 с.
5) Информатика: учебник для 7 класса / Л.Л. Босова, А.Ю. Босова. – М.: БИНОМ. Лаборатория знаний, 2022. – 240 с.
6) Информатика: учебник для 5 класса / Л.Л. Босова, А.Ю. Босова. – 4-е изд. - М.: БИНОМ. Лаборатория знаний, 2021. – 184 с.
7) Информатика: учебник для 8 класса / И.Г. Семакин, Л.А. Заглова, С.В. Русаков, Л.В. Шестакова. – 4-е изд. – М.: БИНОМ. Лаборатория знаний, 2022. – 176с.
8) Информатика: учебник для 8 класса / Н.Д. Угринович. – 4-е изд. – М.: БИНОМ. Лаборатория знаний, 2020. – 160 с.
9) Информатика: учебник для 9 класса / Н.Д. Угринович. – 4-е изд. – М.: БИНОМ. Лаборатория знаний, 2019. – 152 с.
10) Абросимов М.Б., Салий В.Н., Жаркова А.В., Коннова А.Д., Лобов А.А., Моденова О.В., Шабаркова А.О. Саратовская олимпиада по криптографии 2020-2021 учебного года. / Информационные технологии в образовании: сборник / редакционная коллегия: С. Г. Григорьев [и др.]. – Саратов: Саратовский университет, 2021. – Вып. 4: материалы XIII Всероссийской научно-практической конференции «Информационные технологии в образовании» (ИТО-Саратов-2021), 5-6 ноября 2021 г., г.Саратов. – 284 с.