

Гудимов Виктор Николаевич, студент 4 курса бакалавриата,
ФГБОУ ВО «Амурский государственный университет»,
г. Благовещенск

Самохвалова Светлана Генадьевна, доцент, канд. техн. наук., доцент,
ФГБОУ ВО «Амурский государственный университет»,
г. Благовещенск

ПРОГРАММНАЯ РЕАЛИЗАЦИЯ КРИПТОГРАФИЧЕСКИХ МЕТОДОВ ЗАЩИТЫ: ПЕРЕСТАНОВКИ И ЗАМЕНЫ

Аннотация: В статье рассматривается процесс разработки и реализации программы криптографических методов защиты, акцент сделан на методы перестановки и замены. Цель реализации данной программы это повышения интереса к криптографии и ее историческим аспектам, а именно визуализация криптографических методов перестановки и замены.

Ключевые слова: криптография, программа, визуализация, методы перестановки, методы замены

Целью разработки программы является привлечение внимания современного поколения к криптографии и её историческим аспектам, а также на создание более доступного и увлекательного образовательного опыта для широкой аудитории. Создаваемый программный модуль обучает пользователей основам криптографии в игровой форме, что делает процесс обучения не только познавательным, но и интересным. Основная задача заключается в том, чтобы пользователи могли наблюдать за процессом шифрования в реальном времени и самостоятельно осваивать простые и известные методы защиты информации, тем самым углубляя свои знания в данной области.

Для реализации проекта были выбраны криптографические методы перестановки и замены, которые известны с древнейших времён и обладают простым алгоритмом шифрования. Перестановка изменяет порядок символов в сообщении, тогда как замена заменяет одни символы на другие, что создаёт разнообразные комбинации и повышает уровень безопасности информации.

В качестве программной реализации был выбран подход, основанный на визуализации криптографических методов. Использование анимации и интерактивных элементов позволяет наглядно продемонстрировать процесс шифрования.

Для создания 3D моделей и анимаций, обеспечивающих наглядную визуализацию, было выбрано приложение Blender. Это простое и удобное средство для моделирования и анимации. Одним из значительных преимуществ Blender является наличие большого количества методических материалов. Модели были созданы в стиле LowPoly, что позволяет избежать излишней детализации и не отвлекать внимание пользователя от сути представляемой информации. Такой подход также снижает нагрузку на систему, обеспечивая плавную работу приложения и комфортное взаимодействие с визуализированным контентом.

В процессе разработки было принято решение создать программу в виде интерактивного приложения. Для реализации этой идеи была выбрана среда разработки Unity, которая предоставляет мощные инструменты для работы с 3D-графикой и создания интерактивных приложений.

Исходя из принципов работы Unity, была разработана структура приложения, где каждый отдельный уровень представлен в виде отдельной сцены. На каждой сцене располагаются модели, созданные в Blender, а также элементы интерфейса. Управление этими моделями и элементами осуществляется через скрипты, написанные на языке C#. Это позволяет реализовать интерактивные элементы, такие как кнопки, переключатели и другие компоненты, которые реагируют на действия пользователя. Переход

между сценами также осуществляется с помощью скриптов. Структура проекта на Unity представлена на рисунке 1.

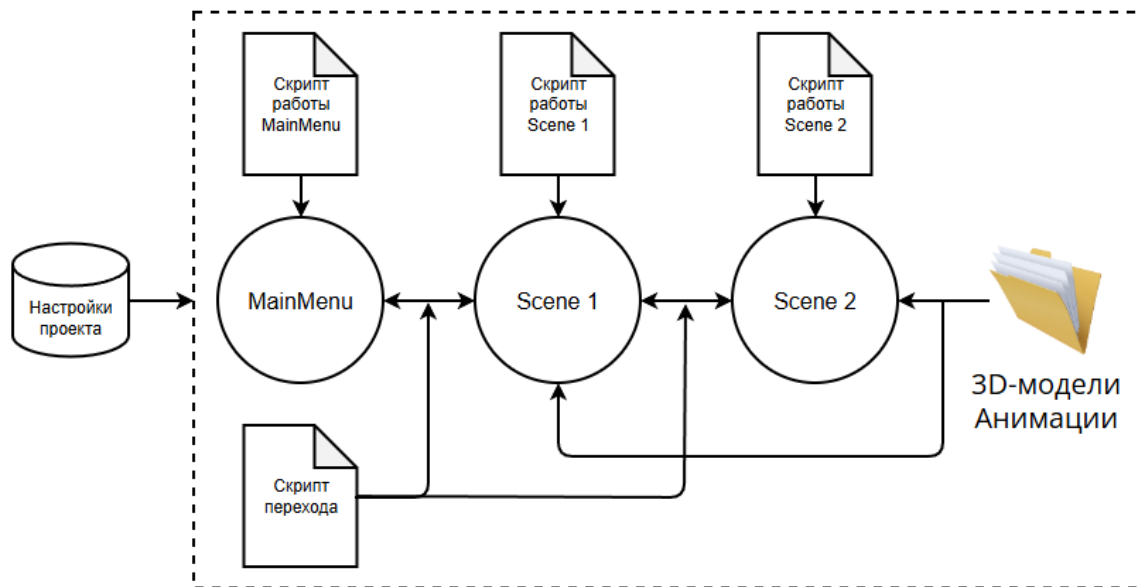


Рисунок 1 – Структура проекта на Unity

В результате проведенной разработки был создан программный модуль, представляющий собой интерактивную лекцию, в которой сочетаются теоретический и практический материал, дополненный иллюстрациями и визуализацией методов криптографии, рисунок 2.



Рисунок 2 – Теоретический материал

Структура программы организована таким образом, что практические элементы следуют после теоретического материала. Практические задания охватывают как аспекты шифрования, так и дешифрования. Эти упражнения позволяют пользователям самостоятельно экспериментировать с входными данными, тем самым лучше закрепляя изучаемый материал. Демонстрация практического задания представлена на рисунке 3.

Задание на шифрование

Пауза

☒ Перестановка по ключу

☐ Двойная перестановка

Ширина : 7

Высота : 5

Слово ключ : Пеликан

Выписывать сообщение по :

По горизонтали (слева направо)

Н	А	П	А	Д	А	Й
Т	Е	_	З	А	В	Т
Р	А	_	Н	А	_	Р
А	С	С	В	Е	Т	Е
_	С	_	Ю	Г	А	*

Сгенерировать

Зашифровать

Обратно

Назад

Далее

0

Рисунок 3 – Пример практического задания

Данный программный модуль подойдёт для проведения интерактивных занятий и также отлично подойдёт для самостоятельного изучения. Программная визуализация будет распространяться на бесплатной основе, поскольку она создана для обучения. Это обеспечит доступность для широкой аудитории пользователей. В рамках данного проекта планируется создание специализированного веб-сайта, на котором будет представлено краткое описание программы. На этом сайте будет размещена ссылка для скачивания архива с программой. Дополнительно рассматривается возможность размещения программы на игровой интернет-платформе Яндекс.Игры. Это решение позволит пользователям запускать программу с минимальными требованиями к аппаратному обеспечению, так как для её работы потребуется лишь стабильное интернет-соединение.

Список литературы:

1. Бонд, Д.Г. Unity и C#. Геймдев от идеи до реализации. 2-е изд./ Д.Г. Бонд –Питер, 2023. –928. –ISBN 978-5-4461-0715-5.
2. Гудимов В.Н., Самохвалова С.Г. Программная визуализация криптографических методов защиты [Электронный ресурс] / Хроники Объединенного фонда электронных ресурсов «Наука и образование». –2025. – №03(190). –URL: <https://ofernio.ru/portal/newspaper/ofernio/2025/3.pdf> (дата обращения 17.04.2025)
3. Гудимов В.Н., Самохвалова С.Г. Проектирование программной визуализации криптографических методов защиты [Электронный ресурс] / Вестник АмГУ. –2024. –№107. –URL: https://vestnik.amursu.ru/wpcontent/uploads/2024/12/n107_139-146.pdf (дата обращения 17.04.2025)
4. Гудимов В.Н., Самохвалова С.Г. Разработка программы для знакомства с криптографией [Электронный ресурс] / Перспективы развития науки и образования. –2025. –URL: http://science-peace.ru/files/PRNO_2025.pdf (дата обращения 17.04.2025)
5. Саллинс, С. Low Poly 3D Modeling in Blender / С. Саллинс–Packt Publishing, 2024. –318. –ISBN 978-1-8032-4123-4
6. Фомичёв, В. Криптография – наука о тайнописи / В. Фомичёв. –ЛитРес, 2021. –168. –ISBN 978-5-0430-6670-1