



Инструмент для приватного общения в мессенджерах

Автор Работы: Лопатин Андрей

Руководитель: Каравайцев Иван Иванович

Актуальность проблемы

Растущая угроза приватности

В мире стремительного роста цифровой коммуникации, защита личных данных становится критически важной.

Несмотря на заявленное шифрование, многие мессенджеры:

- Хранят метаданные пользователей.
- Предоставляют доступ к данным по запросам регуляторов.
- Используют централизованные серверы, уязвимые к взлому.

Я вижу острую потребность в инструментах, обеспечивающих полный контроль над шифрованием сообщений, независимо от инфраструктуры мессенджера.

Целевая аудитория и решение



Журналисты и
правозащитники

Для безопасного обмена
чувствительной информацией
без риска утечек.



Бизнес-аналитики и
предприниматели

Для защиты коммерческой
тайны и конфиденциальной
корпоративной переписки.



Частные лица

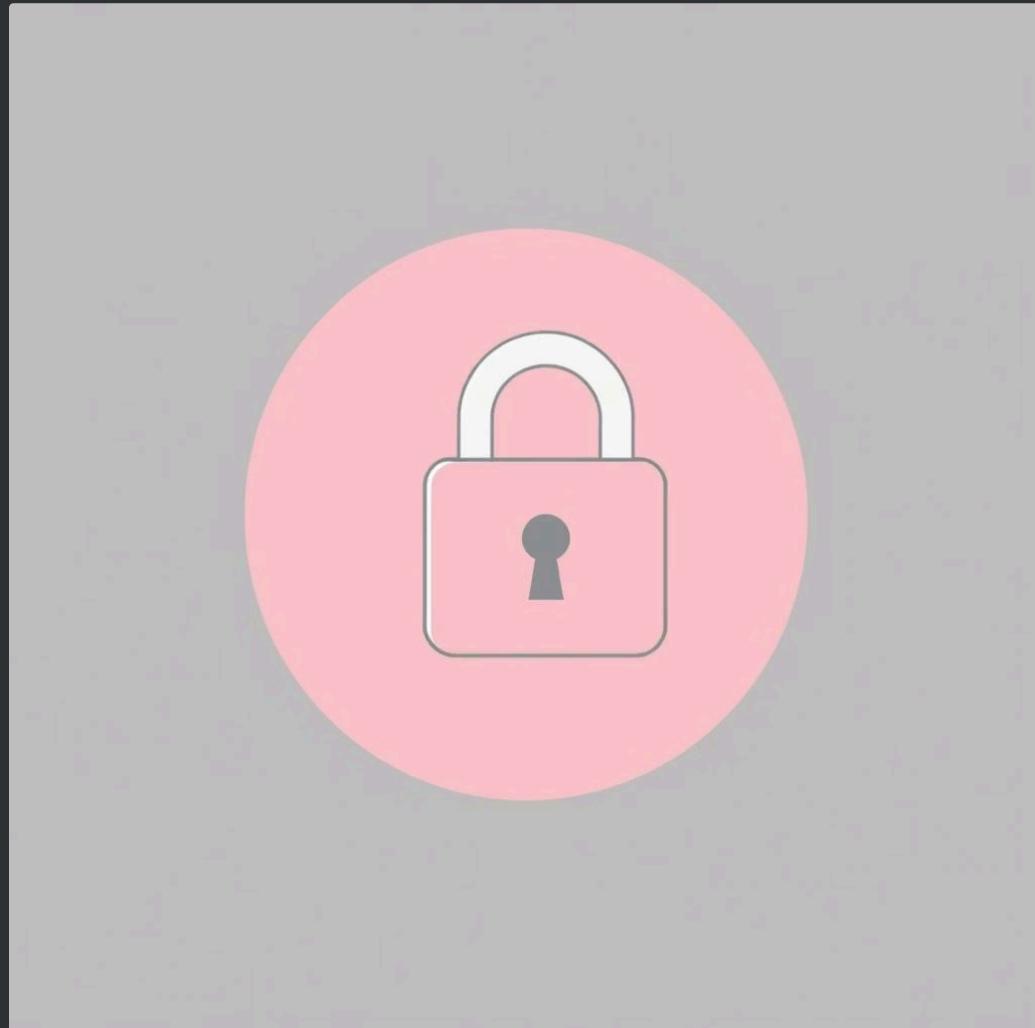
Для всех, кто ценит свою
приватность и хочет защитить
личную переписку.

Наш инструмент предлагает простое и надёжное решение для локального шифрования, независимого от серверов мессенджеров, сохраняя при этом привычный пользовательский опыт.

Цели и задачи проекта

Цель

Разработать удобный инструмент для сквозного шифрования переписки, интегрированный в браузер и совместимый с популярными мессенджерами



Основные задачи

01

Анализ

.Изучить существующие решения и их ограничения

02

Выбор алгоритмов

Подобрать криптографические алгоритмы,
.соответствующие стандартам

03

Архитектура

Разработать архитектуру приложения

04

Реализация

Внедрить шифрование/десифрование в реальном
.времени

05

Хранение ключей

.Обеспечить безопасное хранение ключей

06

Тестирование

.Проверить устойчивость к типовым угрозам

Алгоритм Работы и Безопасность

Процесс Шифрования

Инициализация

Пользователь устанавливает программу, генерируется ключ шифровки/десифровки.

Шифрование Сообщения

При вводе текста сайт автоматически шифрует его.

Отправка

В поле ввода отображается зашифрованная строка, готовая к отправке.

Десифрование Сообщения

Получение

Пользователь получает сообщение

Десифровка

Полученное сообщение отправляется в программу

Отображение

Текст десифруется и отображается в читаемом виде.

Технологический стек и этапы разработки

Используемые технологии

- **Язык программирования:** python - простой и надёжный язык, на котором можно быстро сделать первую реализацию проекта
- **Сторонняя библиотека:** cryptography - это встроенная библиотека для шифрования
- **Документация:** Markdown - для прозрачности и удобства разработки.



Потенциал применения и распространение

Целевая аудитория

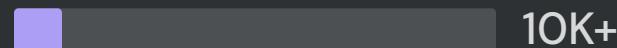


Частные пользователи

Активно ищащие усиленную
защиту личной переписки.

Малые бизнесы

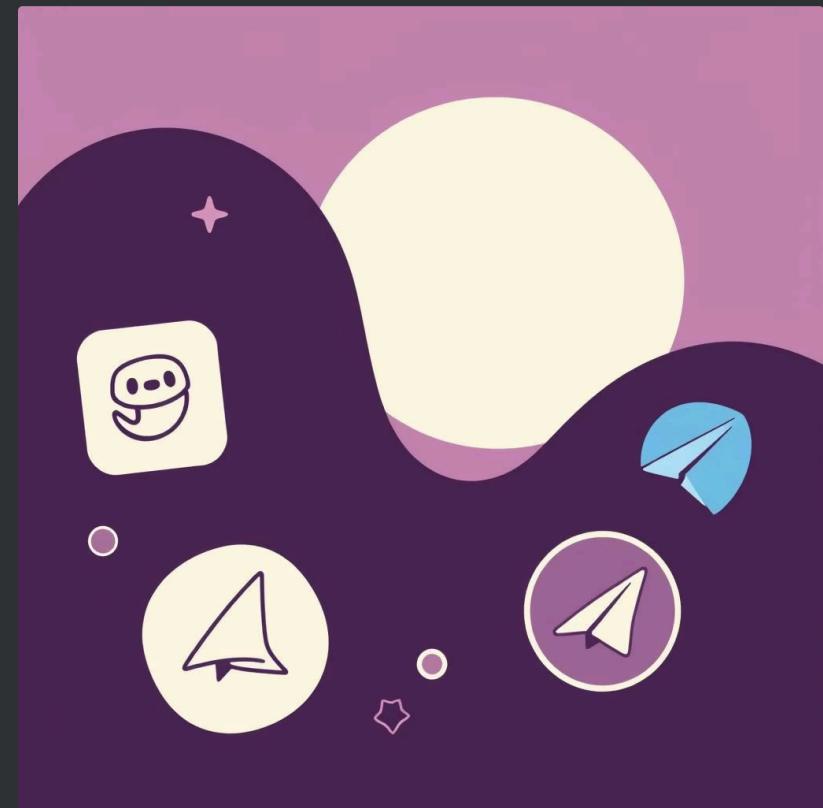
Нуждающиеся в защите
конфиденциальной
корпоративной информации.



Журналисты

Для защиты источников и
обеспечения безопасности
коммуникаций.

Каналы распространения



- **Открытые источники:** github, различные социальные сети

Заключение: новизна и Перспективы

Мой проект предлагает уникальное и своевременное решение для проблемы конфиденциальности переписки, сочетая новизну, значимость и применимость.



Новизна

Интеграция сквозного шифрования в любой веб-мессенджер без изменения его архитектуры.



Значимость

Существенное повышение уровня информационной безопасности для широкой аудитории.



Применимость

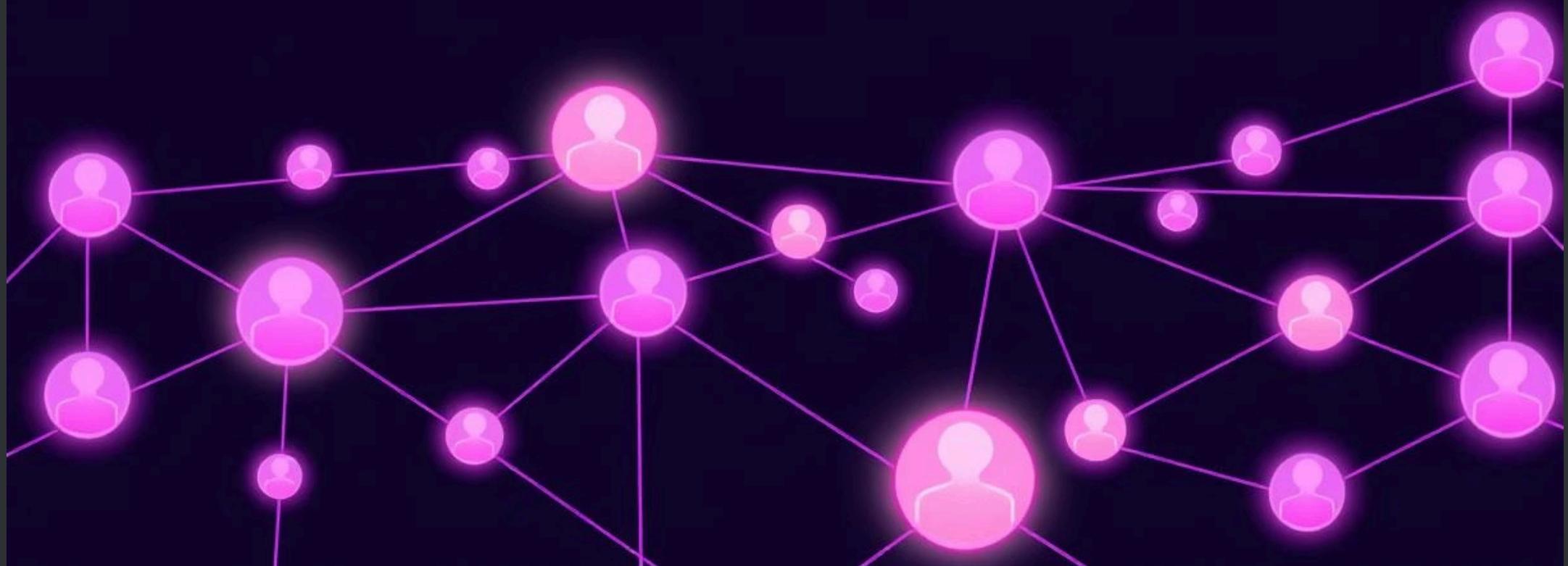
Готовый к использованию продукт с низким порогом входа для пользователей.

Карта развития

- Переписывание проекта на js и создания расширения для браузера
- Интеграция с популярными мессенджерами
- Улучшение приватности и способа шифрования

Спасибо за внимание!

Audidience Engagement



Буду рад ответить на ваши вопросы и предоставить дополнительную информацию по проекту.

Telegram канал: [@bacat86](https://t.me/bacat86)

GitHub проекта: [BaCat86/privacy-everywhere](https://github.com/BaCat86/privacy-everywhere)