УДК 004.056

РАЗРАБОТКА ЗАЩИЩЕННОГО МЕССЕНДЖЕРА ДЛЯ МЕДИЦИНСКОЙ ОРГАНИЗАЦИИ НА ОСНОВЕ СЕРТИФИЦИРОВАННЫХ АЛГОРИТМОВ ПЕРЕДАЧИ ДАННЫХ

Комышан В.В. (Университет ИТМО), **Ливада Е.А.** (Университет ИТМО), **Хахилев Н.И.** (Университет ИТМО)

Научный руководитель – доцент, кандидат технических наук, Коржук В.М. (Университет ИТМО)

Введение. Большое количество медицинского персонала по всему миру пользуется личными устройствами для обмена информацией, связанной с пациентами, специализированные защищенные мессенджеры [1]. Информация, передаваемая через личные средства и незащищенные приложения уязвима к атакам, и должна быть защищена. За рубежом создано большое количество специальных мессенджеров для медицинских организаций, разработанных с применением современных криптоалгоритмов, обеспечивающих необходимый уровень защиты для конфиденциальных данных. В России медицинские работники используют неспециализированные общедоступные мессенджеры [2], такие как Viber, Telegram и WhatsApp, так как готовых аналогов зарубежным решениям не существует.

Основная часть. Представленный проект направлен на решение проблемы отсутствия квалифицированной системы сообщений, соответствующей действующему законодательству Российской Федерации. С помощью российский криптоалгоритмов [3-5], алгоритма End-To-End Encryption протокола MTProto 2.0 и применения микросервисной архитектуры, будет создано новое решение, содержащее следующие модули:

1) Модуль сообщений, позволяющий управлять сообщениями;
2) Модуль шифрования, отвечающий за криптографическую защиту данных;
3) Протокол обмена сообщениями, позволяющий установить защищенный канал связи между двумя респондентами;
4) Модуль, использующий технологию Web-Socket для общения в режиме реального времени.

Предлагаемое решение использует технологию сквозного шифрования, основанную на создании сессионного ключа между сторонами на базе алгоритмов «ВКО» и хэщ-функции «Стрибог» [6] и последующего шифрования сообщений алгоритмом «Кузнечик» [5]. Сервер будет использоваться для установления соединения между сторонами, а также для хранения сообщений в зашифрованном виде. Клиентская сторона будет инициировать создание канала для общения, а также хранить ключи для дешифровки сообщений.

Также будут реализованы специальные методы интеграции мессенджера, разработанные и подобранные с учетом технических и социальных особенностей приложения, а также из соображений безопасности, а именно:

1) Метод хранения информации будет реализован на стороне сервера, на стороне клиента будет функция кэширования информацией, с возможностью установки времени хранения кэширования, а также ручной очисткой памяти устройства.
2) Метод авторизации разработан специально для данного мессенджера, он заключается в следующем: пациенту необходимо получить приглашение по SMS от врача или администратора мед организации, затем пациенту следует ввести необходимую информацию, после чего она отправляется на проверку, после которой пациент получает доступ к функционалу приложения.

Выводы. Проведен анализ существующих решений в сфере безопасного общения в медицине. Разработан прототип приложения для безопасного общения в медицинской организации.

Список использованных источников:

1. Kuhlmann S, Ahlers-Schmidt C R, Steinberger E. Pediatric hospitalists and text messaging // Telemed J E Health. – 2014. – 20(07). – С. 647–652.
2. Врачи и Мессенджеры // Общество с ограниченной ответственностью «Медицинские Информационные Решения» [Электронный доступ]. Режим доступа: https://medsolutions.ru/#/researches/vrachi-i-messendzhery (дата обращения 31.01.2023)
3. ГОСТ 34.10-2018. КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ. Процессы формирования и проверка электронной цифровой подписи (2018) // Информационная технология.
4. ГОСТ 34.11-2018. КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ. Функция хэширования (2018) // Информационная технология.
5. ГОСТ 34.12-2018. КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ. Блочные шифры (2018) // Информационная технология.
6. S. Smyshlyaev, Ed., E. Alekseev, I. Oshkin, V. Popov, S. Leontiev. Guidelines on the Cryptographic Algorithms to Accompany the Usage of Standarts GOST R 34.10-2012 and GOST R 34.11-2012 // Request for Comments. – 2016. – № 7836 – С. 8–10.

Комышан В.В. (автор)	Подпись
Ливада Е.А. (автор)	Подпись
Хахилев Н.И. (соавтор)	Подпись
Коржук В.М. (научный руководитель)	Подпись