ПРИЛОЖЕНИЕ ДЛЯ ЗАЩИЩЕННОЙ ПЕРЕДАЧИ SMS-СООБЩЕНИЙ

П.С. Ладыгин, Э.Е. Бауэр
Алтайский государственный университет, г. Барнаул
email: pavel-ladygin@yandex.ru

Аннотация. В работе представлены результаты разработки приложений для шифрования SMS-сообщений на ОС Android. Проведен критический анализ различных программных решений, обоснован выбор оптимального набора технологий для подобных разработок. Рассмотрено содержание предложенного программного решения, призванного повысить защиту пользовательских данных. Описаны существующие аналоги рассматриваемой разработки, а также результаты ее апробации.

Ключевые слова: шифрование, SMS-сообщения, ОС Android, хранилище заметок.

На сегодняшний день проблемы безопасности пользовательских данных вышли на новый уровень. Согласно данным заместителя председателя правительства России Д. Чернышенко, число кибератак в 2022 году выросло на 80% [1]. По итогам первой половины 2022 года Экспертно-аналитическим центром InfoWatch в мире было зарегистрировано почти в два раза больше утечек конфиденциальной информации (на 93,2%), чем за аналогичный период прошлого года. Количество таких утечек в России за первое полугодие 2022 года выросло на 45,9% по сравнению с I полугодием 2021 года [2]. При этом задача разработки отечественных программных решений для защиты данных является одной из наиболее актуальных, поскольку согласно Указу Президента РФ от 1 мая 2022 года [3] установлено, что с 1 января 2025 года организациям запрещается использовать средства защиты информации, странами которых являются иностранные государства.

Одним из вариантов подтверждения входа в личные кабинеты пользователей или подтверждения банковских операций является двухфакторная аутентификация. Она может осуществляться организациями с помощью SMS-сервисов, используемых в том числе для рассылки информации. Однако, по данным сайта «kasperskiy.ru» [4], существуют уязвимости [5], которые позволяют переадресовывать SMS, отправленные на номер абонента, на номер злоумышленника. В связи с этим актуальна задача создания программных средств, обеспечивающих дополнительную безопасность для SMS-сообщений.

Сравнительный анализ функций наиболее популярных приложений для чтения и отправки SMS иллюстрирует таблица 1.

Таблица 1. Функции приложений для работы с SMS.

	Silence	Latebra	Сообщения (Messages)
Шифрование	+	+	-
Хранение пароля	Устройство	Устройство	-
Отправка SMS	+	-	+
Антиспам	+	-	+
Черный список	+	-	+
Отправка электронных писем	-	+	-
Страна производитель	USA	USA	USA

Объединение лучших качеств данных приложений, а именно: шифрование и расшифровка сообщений, отправка сообщений с помощью SMS, добавление дополнительных функций, таких как антиспам и черный список, - обеспечит улучшенную защиту от утечки пользовательских данных.

Для решения данной задачи было разработано приложение, блок-схема которого представлена на рисунке 1. Работа приложения заключается в отправке и приеме SMS, шифровании и расшифровки сообщений (рисунок 2). Приложение разработано в среде Android Studio 4.3.1. В программном обеспечении был использован язык программирования Java. Для шифрования сообщения использован алгоритм двоичного гамма-шифрования с последующим преобразованием результата в строку base64 [6], для безопасной передачи в виде текста. При выборе сообщения в списке отображаются последние 20 принятых сообщений, ограничение сделано в связи с тем, что при большом количестве СМС на телефоне процесс их чтения может занять достаточно длительное время.

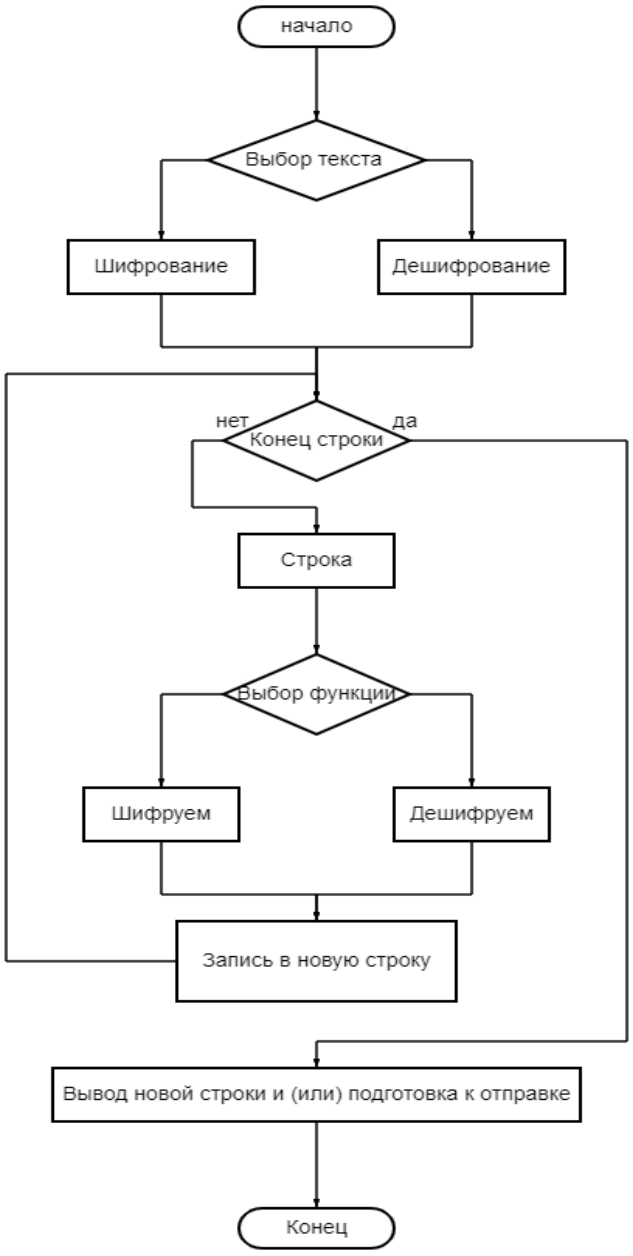

Рисунок 1. Блок-схема приложения.

Рисунок 2. Главный экран отправки и приёма сообщений.

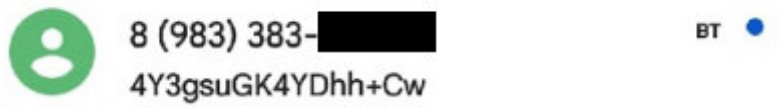

Рисунок 3. полученное SMS сообщение в стандартном приложении.

На рисунке 3 продемонстрировано полученное сообщение в стандартном приложении. Расшифровка принятого SMS сообщения представлена на рисунке 4.

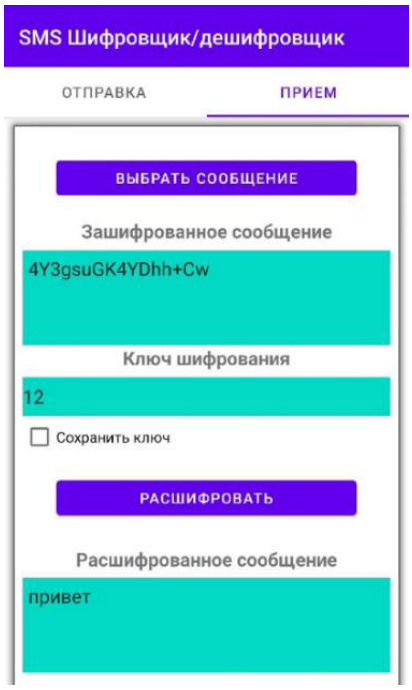

Рисунок 4. Расшифровка SMS сообщения.

Разработанное программное решение в дальнейшем может способствовать адаптации пользовательских данных под отечественные операционные системы и снижению количества угроз в информационных системах, находящихся на территории Российской Федерации.

Библиографический список.

1. Киберучения в национальном масштабе: как работают киберполигоны в России // РБК: [Электронный ресурс] / 2022. Заглавие с экрана. — Режим доступа: https://www.rbc.ru/technology_and_media/01/11/2022/635bfe3f9a794799a7e0b42e (дата обращения: 20.11.2022).
2. Отчёт об исследовании утечек информации ограниченного доступа в I половине 2022 года // Infowatch [Электронный ресурс] / 2022. Заглавие с экрана. — Режим доступа: https://www.infowatch.ru/sites/default/files/analytics/files/otchyot-ob-utechkakh-dannykh-za-1-polugodie-2022-goda_1.pdf (дата обращения 20.11.2022).
3. Указ Президента РФ от 01.05.2022 № 250 № 250 "О дополнительных мерах по обеспечению информационной безопасности Российской Федерации" // Официальный интернет-портал правовой информации. - 01.05.2022. – ст. 6.
4. Kaspersky.ru // Научный блог [Электронный ресурс]: - https://www.kaspersky.ru/blog/ss7-attack-intercepts-sms/17673/ (дата обращения 5.10.2021).
5. siblec.ru: Электронный журнал: сайт URL - /https://siblec.ru/telekommunikatsii/multiservisnye-seti-svyazi/8-sistema-obshchekanalnoj-signalizatsii-7 (дата обращения 10.06.2022).
6. Шнайер Б. Прикладная криптография // ISBN 978-5-9908462-4-1, 2017 – 374с.
7. Factis – Как работает Android. Архитектура приложений [Электронный ресурс]: – Режим доступа: https://bimlibik.github.io/posts/how-does-android-work/ (дата обращения 20.11.2022).

APPLICATION FOR SECURE TRANSMISSION OF SMS MESSAGES

P.S. Ladygin, E.E. Bauer
Altay state university, Barnaul
email: pavel-ladygin@yandex.ru

Annotation. The paper presents the results of the development of applications for encrypting SMS messages on Android OS. A critical analysis of various software solutions is carried out, the choice of the optimal set of technologies for such developments is justified. The content of the proposed software solution designed to improve the protection of user data is considered. The existing analogues of the considered development are described, as well as the results of its testing.

Keywords: encryption, SMS, Android OS.