УДК 004

РАЗРАБОТКА КОРПОРАТИВНОГО МЕССЕНДЖЕРА

Сапун Т.В.
Научный руководитель – Ковалева И.Л., к.т.н., доцент

Мобильные приложения занимают одно из важных мест в жизни почти каждого современного человека. Согласно исследованиям, лидирующими среди приложений являются мессенджеры.

Двумя более популярными ОС считаются iOS и Android. На январь 2022 года доля рынка ОС Android составляет 70%, iOS - 26%, остальные – 4% (рисунок 1).

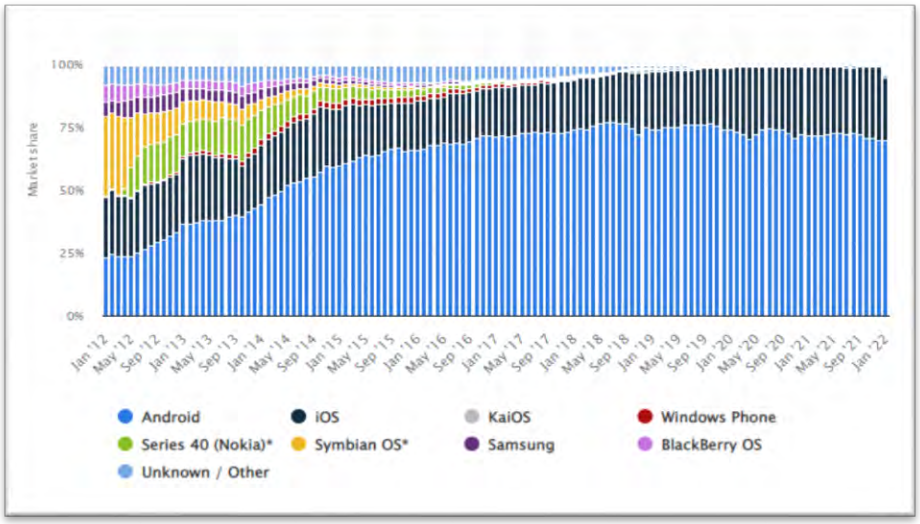

Рис.1. Диаграмма популярности ОС

Основной задачей любого мессенджера является обеспечение безопасности и конфиденциальности. Особенно это актуально для корпоративных мессенджеров. Классические отличия публичных мессенджеров от корпоративных представлены на рисунке 2.

Основные функции	Публичный мессенджер	Корпоративный мессенджер
хранение данных на клиентских серверах	✗	✓
возможность контролировать политику доступа	✗	✓
"администрирование" (подключение/отключение) пользователей	✗	✓

Рис.2. Отличия публичных и корпоративных мессенджеров

Существует множество различных хороших мессенджеров, однако, в некоторых организациях считают целесообразным использовать для коммуникаций мессенджеры собственной разработки. Тем не менее,

функциональность этих мессенджеров, как правило, перекликается с функциональностью популярных открытых мессенджеров. Анализ таких мессенджеров позволил сформировать основной набор функциональностей для разрабатываемого мессенджера (рисунок 3).

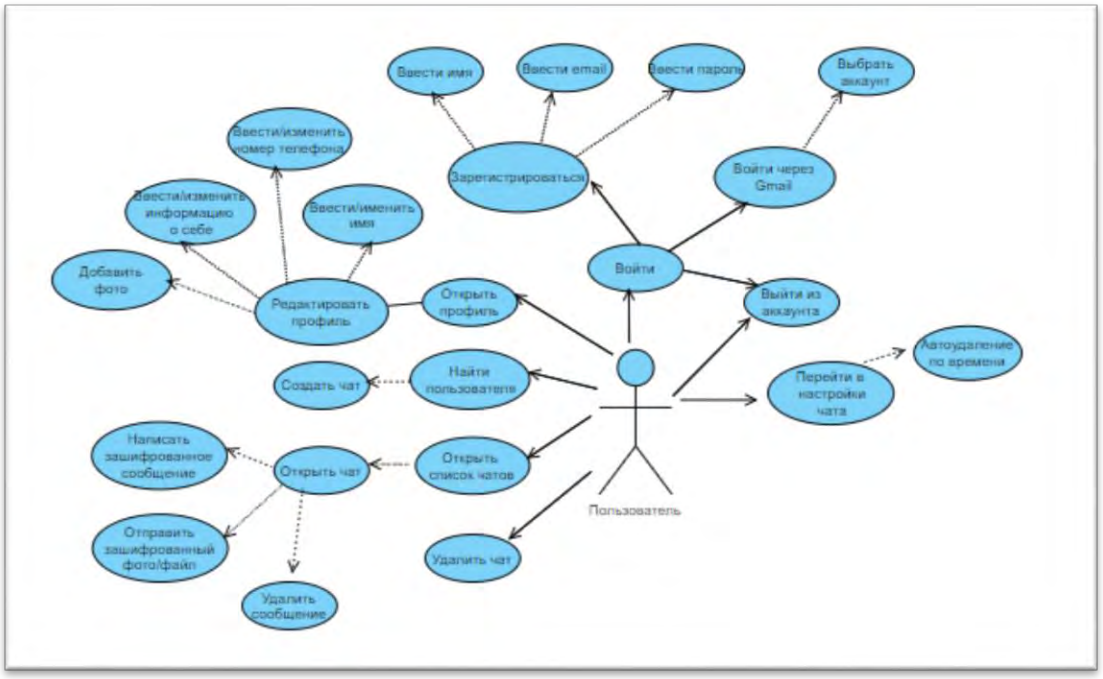

Рис.3.Диаграмма вариантов использования

В разрабатываемой модели описывается одно действующее лицо: пользователь, а также представлены действия, которые он может выполнять.

Одной из важнейших причин, почему многие организации стремятся использовать мессенджер собственной разработки, - это вопрос безопасности. Для ее повышения даже при разработке собственного мессенджера целесообразно применять шифрование.

Существует два метода шифрования: симметричное и асимметричное. При симметричном шифровании используется один и тот же криптографический ключ, который шифрует и дешифрует данные. Применение одного ключа не может обеспечить такую же высокую безопасность данных, как асимметричное шифрование, которое использует несколько ключей: открытый и закрытый. Ассиметричное шифрование отлично подходит для коротких сообщений, которые чаще всего используются в мессенджерах. Поэтому для разработки был выбран метод асимметричного шифрования.

К наиболее распространенным алгоритмам асимметричного шифрования можно отнести алгоритмы RSA (аббревиатура от Rivest, Shamir и Adelman, Diffie-Hellman (DH), DSS (Digital Signature Standard),

схему Эль-Гамаля предствленную и алгоритм EC (Elliptic Curve). Каждый из этих алгоритмов обладает своими преимуществами и недостатками, определяющими область их применения.

Анализ перспективных условий эксплуатации разрабатываемого мессенджера позволил обосновать для его реализации выбор алгоритма асимметричного шифрования RSA (рисунок 4).

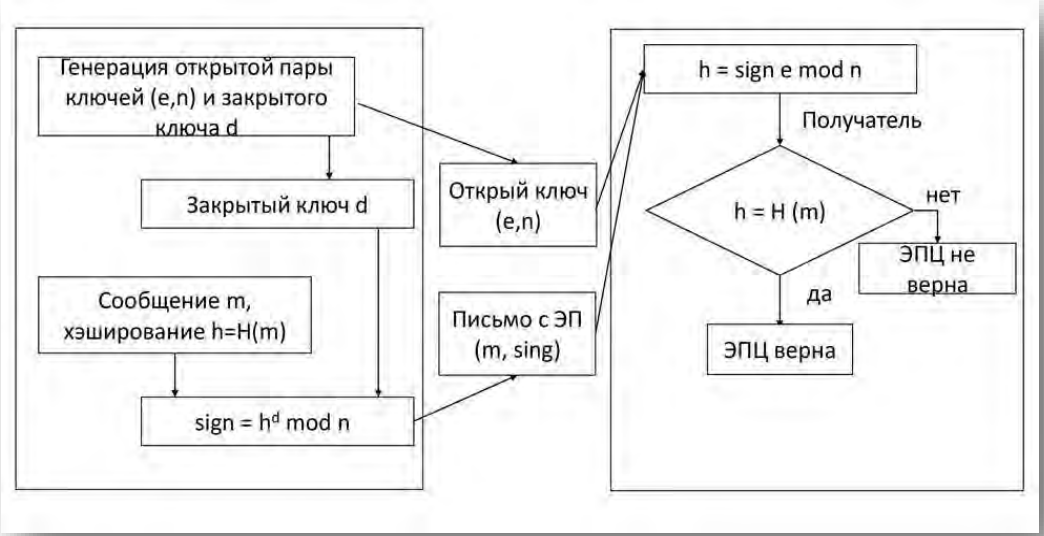

Рис.4. Схема работы алгоритма RSA

RSA применяется как для шифрования данных, так и для создания цифровых подписей. К его преимуществам можно отнести масштабируемость и возможность использования ключей различной длинны шифрования.

Кроме требований по безопасности разрабатываемый мессенджер должен обладать дружественным интерфейсом и хорошей скоростью.

Разработка мессенджера ведется в официальной среде разработки под Android- Android Studio на языке Java/Kotlin с использованием облачной базы данных Firebase.

Литература

1 «Алгоритмы шифрования» [Электронный ресурс] – Режим доступа: https://wiki.merionet.ru/seti/75/algoritmy-shifrovaniya/

«Асимметричное шифрование» [Электронный ресурс] – Режим доступа: https://encyclopedia.kaspersky.ru/glossary/asymmetric-encryption/