# Защищенный корпоративный мессенджер

*Разработали мессенджер, который защищён от компрометирования, перехвата сообщений, подмены устройств и получения доступа к чужим учётным записям.*

## О проекте

Российская компания с офисами в Москве и Лондоне, специализирующаяся на разработке и внедрении blockchain-проектов. Более двух лет сотрудники Polygant создают криптовалюты, токены, смарт-контракты, консультируют клиентов и помогают им реализовывать ICO (первичное размещение криптовалют среди инвесторов).

## Задача

Клиентами заказчика являются крупные компании, для которых корпоративная безопасность и защита конфиденциальных данных имеют приоритетное значение. Использовать для обмена сообщениями и файлами популярные рыночные решения вроде WhatsApp или Telegram можно, но они не являются гарантом того, что данные будут в полной безопасности. Вся информация в этом случае будет храниться на удалённых серверах, откуда может быть извлечена третьими лицами или спецслужбами. Требовалась гарантия того, что мессенджер будет лишён «бэкдоров», не может быть скомпрометирован, а данные невозможно перехватить в процессе передачи.

Было принято решение создать собственное приложение, отвечающее необходимым требованиям безопасности. С этой проблемой заказчик обратился в нашу компанию.

**Индустрия**
Информационные технологии

**Страна**
Россия

**Ключевые моменты**

- использовали нестандартные решения для дополнительной безопасности;
- полностью исключили удалённые серверы из цепочки передачи данных;
- разработали мобильную и десктопную веб-версию мессенджера.

**Команда**
Менеджер проекта — 1
QA инженер — 2
Аналитик — 1
Back-end разработчик — 1
Front-end разработчик — 1
Mobile разработчик — 1

**Продолжительность**
12 месяцев

**Технологии**
Android, JavaScript, React, Node.JS

# Подход

*Работа с клиентом строилась на следующих принципах:*

Быстрый запуск проекта

Прозрачность процессов

Ответ в течение часа

Масштабируемость

Высокий уровень доверия

Необходимо было исключить малейшую возможность перехватить сообщения, скомпрометировать приложение, подменить устройства или получить доступ к чужой учётной записи. Помимо сквозного 256-битного шифрования для обеспечения максимальной защиты переписки пользователей разработчики использовали ряд нестандартных решений:

- Удалённые серверы полностью исключены из цепочки передачи данных;
- Зашифрованная информация хранится только на устройствах пользователей;
- При необходимости сообщения удаляются спустя какое-то время;
- Мессенджер работает только в пределах внутрикорпоративной сети.

Работа над мобильным клиентом для Android и десктопной версией, работающей через веб-интерфейс, велась командой из 7 специалистов на протяжении 12 месяцев.

# Результат

## Обеспечение безопасности

Созданный нами корпоративный мессенджер отвечает всем современным стандартам безопасности. Для получения доступа к учётным записям используется двухфакторная авторизация, привязывающая приложение к номеру мобильного телефона. Исключение из цепочки передачи данных удалённых серверов делает невозможным доступ третьих лиц к корпоративной информации.

## Практическое применение

Сегодня приложение активно используется крупными компаниями со штатом, превышающим 15 000 человек. Оно позволяет осуществлять крупные сделки, совместно работать над важными проектами и при этом не переживать за информационную безопасность.

**contacts@sibedge.com**

**United States**

10362 Leola Ct # 1
Cupertino, CA 95014

**Australia**

1/237 Stirling Hwy,
Claremont, 6010

**Russia**

Tomsk
75 Pushkina Street

Moscow
10 Bolshaja Tulskaja Street