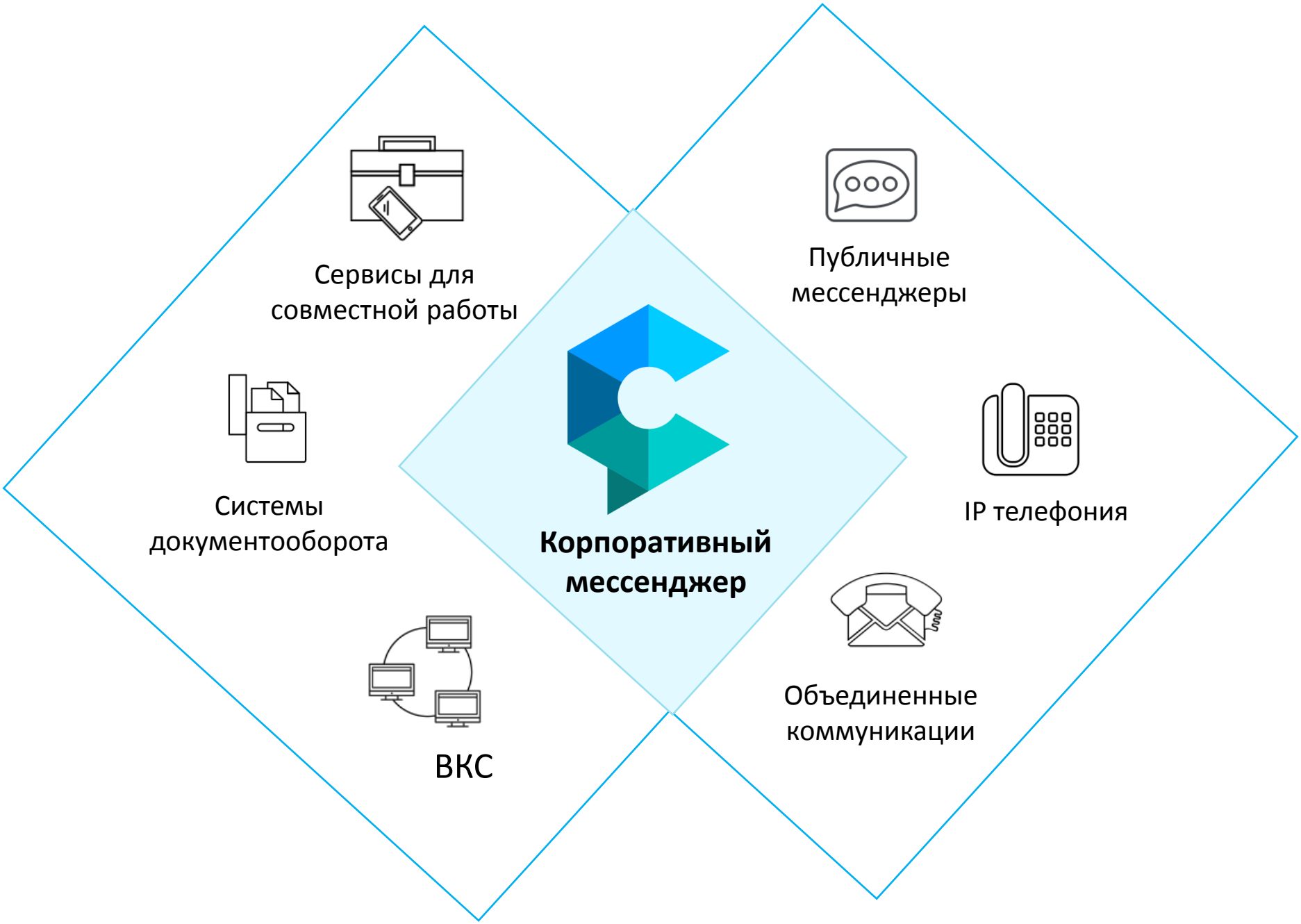
СИБРУС

Технологии безопасности мессенджеров

для облачных сервисов и внутрикорпоративного развертывания

Евгений Сидоров
Директор по технологиям

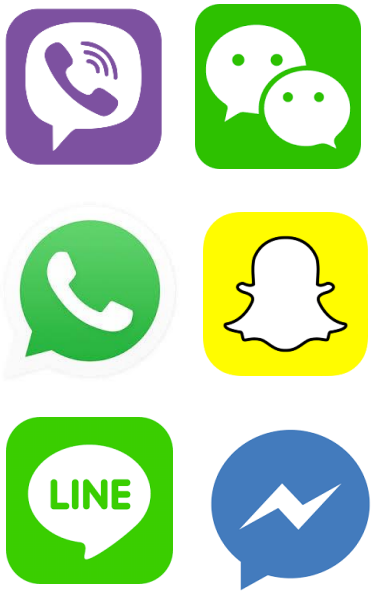

Сервисы для совместной работы
Публичные мессенджеры
Системы документооборота
Корпоративный мессенджер
IP телефония
ВКС
Объединенные коммуникации

Развитие рынка публичных мессенджеров

ICQ, IRC, Skype

1996-2010

Мессенджеры для компьютеров.



Whatsapp, Viber, Snapchat, WeChat

2009-2012

Бум мобильных мессенджеров как замена смс сообщениям.

Telegram, Signal, Wickr, Threema

2012-2017

Стремительный рост популярности защищенных мессенджеров.

При этом массовые мессенджеры уделяют все больше внимания безопасности и повсеместно внедряют end-to-end шифрование.

Тренды в корпоративных коммуникациях

Microsoft exchange, Google apps

Связь через корпоративную почту.

Slack, HipChat, Symphony

С 2014 года бизнес активно переводит общение в различные корпоративные мессенджеры и сервисы управления проектами.

Защищенная корпоративная связь

Явных лидеров в нише нет и рынок только начинает разрабатывать здесь продукты.

Владельцы компаний уделяют все больше внимания защите данных.

Что такое «безопасный мессенджер» с точки зрения большинства?

- Безопасная авторизация
- Шифрование сетевого трафика
- Автоматическое удаление сообщений
- Безсерверная p2p связь

Какие требования предъявляют клиенты?

- Криптографическая защита данных, которые уходят с клиентского устройства в сеть.
- Клиент-серверная архитектура с обеспечением отказоустойчивости.
- Защищенное долговременное и отказоустойчивое хранение данных.
- Настраиваемый и централизованный контроль параметров безопасности и сервера, и клиентов.
- Интеграция с существующей ИТ инфраструктурой.

Какие потребности встречаются у клиентов?

- Единое защищенное рабочее пространство, доступное с различных устройств.
- Защищенная работа как на серверах внутри организации, так и в облаках и сторонних ЦОДах.
- Работа в замкнутом сетевом периметре, изолированном от экосистемы производителей мобильных платформ.
- Наличие защиты от экстренных и нештатных ситуаций.
- Избирательный контроль за действиями и данными пользователей со стороны службы безопасности.

Криптографическая защита данных

- **Защита всего сетевого трафика** с клиентского устройства от перехвата:
  - защита сетевых каналов «клиент-сервер» (например, TLS или, VPN);
  - защита голосового и видео трафика (например, шифрование UDP-пакетов медийного трафика илиVPN).
- **Защита абонентских данных** от несанкционированного доступа на сервере с использованием абонентского шифрования (например, контейнеры CMS, PGP или сеансовое потоковое шифрование).
- **Защита данных на клиентском устройстве.**

Принципы построения криптографической подсистемы

1. Шифрование всех типов данных, которыми обмениваются пользователи.
2. Данные пользователя доступны с разных устройств с возможностью синхронизации.
3. Возможность доступа к данным пользователей со стороны службы безопасности организации.

Востребованы дополнительные механизмы защиты

- Контроль подключений пользователя
- Защита от «забывчивости»
- Защита от кейлоггеров
- Контроль отправленных сообщений
- Скрытие IP адреса
- Скрытые контакты
- Механизм подменных секретов

Централизованное управление и контроль

Задачи техперсонала и системных администраторов	Задачи служб безопасности и руководителей
▪ Развертывание системы и настройка, ▪ Мониторинг функционирования системы, ▪ Обеспечение отказоустойчивости, ▪ Масштабирование под требуемые нагрузки.	▪ Управление пользователями, ▪ Управление параметрами безопасности устройств, ▪ Аудит активности пользователей, ▪ Аудит данных и расследование инцидентов.

Архитектурные особенности и среда функционирования

1. Зависимость от стека технологий.
2. Зависимость от каналов дистрибуции.
3. Зависимость от экосистемы мобильных платформ.

Зависимость от стека технологий

Общепринятый подход	Рекомендованный подход
Состав ПО: База данных - Сторонний сервер Приложений - Набор прикладных скриптов серверного ПО. **Основан на web-технологиях:** • на сервере node.js или ruby on rails; • на клиенте node.js + chromium/electron или браузер.	**Состав ПО**: Монолитное серверное ПО, которое выполняется в среде окружения ОС без посредника в виде виртуальных машин. **Основан на технологиях:** • C++/C/Objective-C; • SDK, который является основным для мобильной платформы.

Каналы дистрибуции

Производители ряда платформ усложняют, ограничивают и даже запрещают свободное распространение ПО .

Примеры:

- На Windows могут быть сложности установки ПО, которое не подписано сертификатом производителя, аккредитованного в корневых центрах сертификации США.
- Для iOS распространение приложений очень строго регламентировано и в сильной степени контролируется Apple.

Экосистема производителей мобильных платформ

Мобильная платформа может ограничивать доступ к ключевым функциям без доступа устройства к облачной экосистеме производителя платформы.

Примеры:

- Для полноценной работы мессенджера на iOS необходимо использовать облачные сервисы Apple, как систему нотификаций APNS.
- В изолированном сетевом периметре затруднительно пользоваться мессенджером без доступа устройств Apple и сервера мессенджера к серверам Apple.

СИБРУС

Контакты

Евгений Сидоров

Директор по технологиям

+7 (495) 150 55 95

sea@cybrus.ru

www.cybrus.ru