VIDEOMOST.COM
video conferencing server

тел.: +7 (499) 995 23 85
info@videomost.com
www.teamspiritim.com
www.videomost.com

TeamSpirit® обеспечивает безопасный обмен и хранение информации

Безопасность — один из основных принципов корпоративного мессенджера TeamSpirit®IM. Для безопасного хранения и обмена данными в TeamSpirit IM предусмотрен набор инструментов для решения следующих задач:

- Защита данных от несанкционированного доступа к ним
- Безопасная работа мессенджера в экстренных ситуациях, таких как: принуждение к запуску приложения, изъятию устройства с запущенным приложением и т.п.
- Защита от кейлоггеров и других средств перехвата данных

TeamSpirit®IM защищает любые данные, которые находятся в мессенджере, включая:

- приватные и групповые чаты
- любые файлы
- аудио и видеовызовы
- задачи
- напоминания
- заметки

Для обеспечения безопасности данных используются различные алгоритмы криптографии:

- Для защиты используются алгоритмы симметричного и асимметричного шифрования
- Для шифрования могут использоваться сертифицированные средства криптографической защиты информации (СКЗИ)
- При использовании СКЗИ методика управления шифрованием и его ключами может варьироваться для соответствия требованиям эксплуатации используемого СКЗИ

Шифрование производится только на устройстве клиента, а ключи дешифровки доступны только пользователю.

На сервер данные поступают в зашифрованном виде и только устройство пользователя может расшифровать их, благодаря этому никто не может перехватить, раскрыть или выкрасть данные пользователя.

Кроме того, TeamSpirit®IM использует дополнительные методы защиты данных, в том числе:

- Редактирование сообщений и удаление истории
- Чёрный список контактов
- Авторизация контактов с целью защиты от спама

Степень защиты данных зависит не только от используемых алгоритмов шифрования, но и того, как создаются, хранятся и передаются секретные ключи шифрования.

Важнейшей функцией TeamSpirit®IM является алгоритм управления ключами шифрования. Система безопасности TeamSpirit®IM выстроена на том, что только пользователь имеет доступ к ключам расшифровки его данных, поэтому посторонние, в том числе разработчик, не имеет доступа к данным пользователя, которые находятся в системе.

Помимо того, что данные в TeamSpirit®IM передаются в защищенных контейнерах, мессенджер также защищает сами каналы передачи данных.

Используются два варианта каналов:

- Соединения клиент-сервер — основное соединение с сервером TeamSpirit®IM, через которое происходит все клиент-серверное взаимодействие
- Прямые P2P-каналы для аудио и видеовызовов