ПОЛИТИКА КОНФИДЕНЦИАЛЬНОСТИ

Мобильного приложения HighTalk

Дата вступления в силу: 1 ноября 2025 г.
Дата последнего обновления: 31 октября 2025 г.
Версия: 1.0

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1 Информация об операторе данных

Оператор данных (Data Controller):
Oleksandr Mudrytskyi

Статус:
Индивидуальный разработчик (Individual Developer / Sole Proprietor)

Адрес для юридической переписки:
Nawrot 56/38, Łódź, 91-001

Электронная почта:
admin@hightalk.me

Веб-сайт:
https://hightalk.me

Контактное лицо по вопросам конфиденциальности:
admin@hightalk.me

Важное примечание:
HighTalk находится в стадии MVP (Minimum Viable Product) и управляется индивидуальным разработчиком. Юридическое лицо (компания) будет зарегистрировано до выхода полной коммерческой версии приложения. Все обязательства по защите данных выполняются в полном объеме в соответствии с применимым законодательством.

1.2 Область применения политики

Настоящая Политика конфиденциальности применяется к мобильному приложению **HighTalk** (далее — «Приложение», «Сервис») и описывает порядок сбора, обработки, хранения и защиты персональных данных пользователей при использовании Приложения на платформах iOS (App Store) и Android (Google Play).

Приложение представляет собой кроссплатформенную социальную сеть для голосовой и видеосвязи с элементами геймификации, системой виртуальной валюты (HighCoins) и инструментами поддержки личного развития.

1.3 Принятие условий

Используя Приложение, вы подтверждаете, что:

- Ознакомились с настоящей Политикой конфиденциальности и согласны с ее условиями
- Достигли возраста **16 лет** (или возраста цифрового согласия в вашей юрисдикции)
- Понимаете, какие данные собираются и как они используются

Если вы не согласны с какими-либо условиями настоящей Политики, пожалуйста, немедленно прекратите использование Приложения и удалите его со своего устройства.

1.4 Применимое законодательство

Настоящая Политика разработана в соответствии с:

- **GDPR** (General Data Protection Regulation, EU 2016/679) — для пользователей Европейского Экономического Пространства
- **CCPA** (California Consumer Privacy Act) — для пользователей Калифорнии, США
- **UK GDPR** — для пользователей Великобритании
- **Местным законодательством** применимой юрисдикции пользователя

1.5 Роли обработки данных

Контроллер данных (Data Controller):
Индивидуальный разработчик HighTalk, который определяет цели и средства обработки персональных данных.

Процессоры данных (Data Processors):
Сторонние сервисы, обрабатывающие данные по инструкциям контроллера:

Stripe, Inc. — обработка платежей

Firebase Cloud Messaging (Google) — доставка push-уведомлений (Android)

Apple Push Notification Service — доставка push-уведомлений (iOS)

Appwrite — вспомогательная аутентификация и хранилище

Zoho Corporation — отправка транзакционных email

Хостинг-провайдер (DigitalOcean / Google Cloud) — хостинг серверной инфраструктуры

2. ПРИНЦИПЫ ОБРАБОТКИ ДАННЫХ

Мы обрабатываем ваши персональные данные в соответствии со следующими принципами GDPR:

Законность, справедливость и прозрачность: данные собираются только на законных основаниях и с вашего информированного согласия

Целевое ограничение: данные используются только для заявленных целей

Минимизация данных: мы собираем только необходимые данные

Точность: мы поддерживаем актуальность данных и предоставляем инструменты для их обновления

Ограничение хранения: данные хранятся не дольше необходимого

Целостность и конфиденциальность: применяются технические и организационные меры защиты

Подотчетность: мы несем ответственность за соблюдение всех принципов

3. КАТЕГОРИИ СОБИРАЕМЫХ ДАННЫХ

3.1 Идентификационные данные

Что мы собираем:

Имя пользователя (username) — уникальный идентификатор в системе

Адрес электронной почты (email)

Отображаемое имя (display name)

Имя и фамилия (опционально)

Телефон (опционально)

Дата рождения (для проверки возрастных ограничений)

Уникальный идентификатор пользователя (UUID)

Цель сбора:
Регистрация и аутентификация пользователя

Восстановление доступа к аккаунту

Коммуникация с пользователем (уведомления, поддержка)

Соблюдение возрастных ограничений

Правовое основание:

Исполнение договора (Contract — GDPR Art. 6(1)(b))

Законные интересы (Legitimate interests — GDPR Art. 6(1)(f))

Место хранения:

Сервер: PostgreSQL база данных (таблица `Users`)

Клиент (устройство): Expo SecureStore (зашифрованное хранилище iOS Keychain / Android EncryptedSharedPreferences)

Срок хранения:

До момента удаления аккаунта пользователем или по запросу

Передача третьим лицам:

Appwrite (вспомогательная аутентификация) — только userId и username

Zoho SMTP (отправка email) — email адрес для доставки транзакционных писем

3.2 Аутентификационные данные

Что мы собираем:

Пароль (хранится только в виде хэша bcrypt/argon2)

JWT Access Token (срок действия ~15 минут)

JWT Refresh Token (срок действия ~30 дней)

Отозванные токены (Revoked Token JTI)

Коды восстановления пароля (одноразовые, срок действия 1 час)

Цель сбора:

Аутентификация пользователя

Управление сессиями

Восстановление доступа к аккаунту

Предотвращение несанкционированного доступа

Правовое основание:

Исполнение договора (Contract)

Безопасность пользователя (Legitimate interests)

Место хранения:

Сервер: PostgreSQL (таблицы `RefreshTokens`, `RevokedTokens`, `PasswordResetCodes`)

Клиент: Expo SecureStore (только токены, пароль НИКОГДА не хранится на устройстве)

Срок хранения:

Пароль (хэш): до смены пароля или удаления аккаунта

Access Token: 15 минут

Refresh Token: 30 дней или до logout

Revoked tokens: 30 дней после истечения (для предотвращения повторного использования)

Коды восстановления: 1 час или до использования

Шифрование:

Пароли хэшируются с использованием bcrypt/argon2
Токены подписываются HMAC-SHA256

Данные передаются по HTTPS/TLS 1.3

Передача третьим лицам:

Не передаются

3.3 Профильные данные

Что мы собираем:

Биография (bio) — текстовое описание профиля

Местоположение (location) — **текстовое поле** (например, "Москва, Россия"), НЕ GPS-координаты

Языки общения (languages)

URL аватара (avatarUrl) — ссылка на изображение профиля

Веб-сайт (website) — опционально

Настройки приватности (privacySettings JSON)

Настройки уведомлений (notificationSettings JSON)

Статус верификации (isVerified)

Онлайн-статус (isOnline, lastSeen)

Роли пользователя (roles: user/moderator/admin)

Цель сбора:

Отображение профиля пользователя

Персонализация опыта использования

Управление настройками приватности

Поиск пользователей по параметрам

Правовое основание:

Исполнение договора (Contract)

Согласие пользователя (Consent — для опциональных полей)

Место хранения:

Сервер: PostgreSQL (таблица `Users`)

Клиент: Кэш в памяти приложения (не сохраняется постоянно)

Срок хранения:

До момента изменения пользователем или удаления аккаунта

Передача третьим лицам:

Не передаются (публичные данные профиля видны другим пользователям приложения)

Важно:

Геолокация **НЕ собирается**. Поле "location" — это добровольно введенный текст, а не GPS-координаты

Контакты устройства **НЕ собираются**

Биометрические данные **НЕ собираются**

3.4 Финансовые данные и данные о транзакциях

Что мы собираем:

Stripe Customer ID (идентификатор клиента в системе Stripe)

История транзакций (сумма, дата, тип операции, статус)

Баланс виртуальной валюты HighCoins
История покупок предметов в магазине

История покупок/отправки виртуальных подарков

Статус подписки Premium (активна/неактивна, срок действия)

Stripe Subscription ID (для управления подпиской)

VAT Evidence (данные для налогообложения НДС — только для пользователей ЕС)

Что МЫ НЕ собираем и НЕ храним:

❌ Номера банковских карт

❌ CVV/CVC коды

❌ Полные реквизиты платежных инструментов

❌ PIN-коды

Цель сбора:

Обработка платежей за виртуальную валюту и подписку

Учет баланса HighCoins

Предоставление истории транзакций

Выполнение налоговых обязательств (для пользователей ЕС)

Предотвращение мошенничества

Правовое основание:

Исполнение договора (Contract)

Законодательные требования (Legal obligation — для финансовой отчетности)

Место хранения:

Сервер: PostgreSQL (таблицы `PaymentTransactions`, `CoinBalanceLedgers`, `PurchaseHistories`, `Subscriptions`, `VATEvidences`)

Клиент: Кэш баланса (TTL 60 секунд)

Срок хранения:

История транзакций: **7 лет** (в соответствии с налоговым законодательством)

Баланс HighCoins: до момента использования или удаления аккаунта

Статус подписки: до окончания срока действия подписки + 30 дней

Передача третьим лицам:

Stripe, Inc. — полная обработка платежей (Stripe является PCI DSS compliant процессором)

Передаваемые данные: email, сумма платежа, валюта

Платежные данные (карта) вводятся напрямую в защищенную форму Stripe и НЕ проходят через наши серверы

Stripe обрабатывает данные в соответствии с их Политикой конфиденциальности

Безопасность:

Все платежи обрабатываются через PCI DSS Level 1 сертифицированного провайдера (Stripe)

Мы НЕ имеем доступа к полным данным карты (видим только последние 4 цифры и тип карты)

3.5 Коммуникационные данные (User-Generated Content)

Что мы собираем:

Текстовые сообщения в приватных чатах

Текстовые сообщения в групповых чатах

Отправленные и полученные виртуальные подарки

Уведомления (in-app notifications)

Метаданные сообщений: timestamp (время отправки), статус прочтения, ID чата/комнаты

Цель сбора:

Обмен сообщениями между пользователями

Хранение истории чатов

Доставка уведомлений

Модерация контента (при получении жалоб)

Правовое основание:

Исполнение договора (Contract)

Законные интересы (Legitimate interests — для модерации)

Место хранения:

Сервер: PostgreSQL (таблицы `Messages`, `GroupMessages`, `Notifications`)

Клиент: НЕ хранится постоянно (только в памяти активной сессии)

Срок хранения:

Сообщения: до момента удаления пользователем или удаления аккаунта

Уведомления: 90 дней

Шифрование:

Передача: HTTPS/TLS 1.3, WebSocket Secure (WSS)

Хранение: данные хранятся в базе данных (планируется внедрение end-to-end encryption)

Передача третьим лицам:

Не передаются

Модерация:

Сообщения могут быть проверены модераторами только при получении жалобы пользователя

Автоматическая модерация контента в настоящее время НЕ применяется

3.6 Социальные связи и активность

Что мы собираем:

- Список друзей (Friend connections)
- Участие в группах (Group memberships)
- Участие в чат-комнатах (ChatRoom participants)
- Запросы в друзья (Friend requests — отправленные/полученные)
- История звонков (метаданные: участники, время начала/окончания, длительность)
- Разблокированные достижения (achievements)

Цель сбора:

- Управление социальными связями
- Отображение списка друзей и групп
- Аналитика активности для улучшения сервиса
- Геймификация (система достижений)

Правовое основание:

- Исполнение договора (Contract)
- Законные интересы (Legitimate interests)

Место хранения:

- **Сервер:** PostgreSQL (таблицы `Friends`, `GroupMembers`, `ChatRoomParticipants`, `CallAnalytics`, `Achievements`)
- **Клиент:** Кэш (TTL 5-10 минут)

Срок хранения:

- Связи друзей/группы: до момента удаления связи или аккаунта
- Метаданные звонков: **12 месяцев** (для аналитики качества сервиса)
- Достижения: постоянно (до удаления аккаунта)

Важно:

- Звонки **НЕ записываются**
- Аудио/видео потоки передаются напрямую между пользователями (P2P через WebRTC)
- Сервер видит только метаданные (кто с кем связывался и когда)

Передача третьим лицам:

- Не передаются

3.7 Технические данные и данные устройства

Что мы собираем:

Идентификаторы устройства:

- Push Notification Token (FCM для Android, APNS для iOS) — уникальный токен для доставки уведомлений
- Installation ID (Expo) — уникальный идентификатор установки приложения

Что МЫ НЕ собираем:

- ❌ IMEI (International Mobile Equipment Identity)
- ❌ IDFA (Identifier for Advertisers) / GAID (Google Advertising ID)
- ❌ MAC-адрес
- ❌ Серийный номер устройства

Информация об устройстве:

- Тип устройства (Android / iOS)
- Версия операционной системы
- Версия приложения HighTalk
- Модель устройства (для диагностики проблем)

User-Agent (в HTTP-заголовках)

Сетевые данные:

IP-адрес (автоматически при подключении к серверу)

Временная метка активности (последний визит)

Цель сбора:

Доставка push-уведомлений

Обеспечение работы приложения

Диагностика технических проблем

Предотвращение злоупотреблений и мошенничества

Аналитика производительности приложения

Правовое основание:

Исполнение договора (Contract)

Законные интересы (Legitimate interests — безопасность, техподдержка)

Место хранения:

Сервер: PostgreSQL (таблицы `UserActivities`, `InstallationEvents`, `DownloadEvents`), логи Serilog

Клиент: Не хранится

Срок хранения:

Push tokens: до момента удаления приложения или logout

IP-адреса и логи активности: **90 дней**

Логи ошибок: **30 дней**

Передача третьим лицам:

Firebase Cloud Messaging (Google) — push token для Android устройств

Apple Push Notification Service — push token для iOS устройств

3.8 Данные о кастомизации и виртуальных предметах

Что мы собираем:

Инвентарь пользователя (купленные предметы)

Экипированные предметы (аксессуары для маскота HighCat, рамки аватара, баннеры профиля)

Категория предмета: шапка, очки, фон, значок

Редкость предмета: common, rare, epic, legendary

Дата покупки и дата экипировки предмета

Цель сбора:

Персонализация профиля и маскота

Синхронизация инвентаря между устройствами

Отображение купленных предметов

Предотвращение дублирования покупок

Правовое основание:

Исполнение договора (Contract)

Место хранения:

Сервер: PostgreSQL (таблицы `UserInventoryItems`, `UserAccessories`, `UserBackgrounds`, `UserStickers`)

Клиент: Кэш (TTL 5 минут)

Срок хранения:

До момента удаления аккаунта

Передача третьим лицам:

Не передаются

3.9 Медиаконтент

Текущий статус: ПОДГОТОВЛЕНО, НЕ РЕАЛИЗОВАНО

Планируемый сбор (будет реализовано в будущих версиях):

- Фотографии (для аватара профиля, отправки в чатах)
- Аудио (для голосовых звонков через WebRTC)
- Видео (для видеозвонков через WebRTC)

Цель сбора:

- Персонализация профиля (аватар)
- Обмен изображениями в чатах
- Голосовые и видеозвонки

Разрешения приложения:

Android:

- `READ_EXTERNAL_STORAGE` — чтение файлов для выбора аватара/изображений
- `WRITE_EXTERNAL_STORAGE` — сохранение загруженных файлов
- `CAMERA` (планируется) — доступ к камере для видеозвонков
- `RECORD_AUDIO` (планируется) — доступ к микрофону для звонков

iOS:

- `NSPhotoLibraryUsageDescription` — доступ к галерее
- `NSCameraUsageDescription` — доступ к камере (планируется)
- `NSMicrophoneUsageDescription` — доступ к микрофону (планируется)

Важно:

- Звонки **НЕ записываются**
- Медиа передается напрямую между пользователями (P2P)
- Фотографии/видео **НЕ анализируются** и **НЕ используются** для рекламного таргетинга

Передача третьим лицам:

- Не передаются (только P2P между пользователями)

3.10 Данные программ восстановления (Трекер трезвости)

Текущий статус: НЕ РЕАЛИЗОВАНО

Данная функция планируется в будущих версиях приложения. При реализации будет применен следующий подход:

Планируемый сбор:

- Дата начала периода трезвости
- Счетчик дней
- Текстовые заметки/дневниковые записи (опционально)

⚠️ **СПЕЦИАЛЬНАЯ КАТЕГОРИЯ ДАННЫХ (GDPR Art. 9):**
Данные трекера трезвости могут содержать информацию о здоровье и относятся к **специальным категориям персональных данных** согласно GDPR Article 9.

Правовое основание:

- **Явное согласие пользователя (Explicit consent)** — будет запрашиваться отдельным согласием при активации функции

Меры защиты:

- Данные трекера хранятся отдельно от основного профиля пользователя
- Шифрование end-to-end для записей трекера
- Возможность полного удаления данных в любой момент

Данные **НЕ передаются третьим лицам** без явного согласия пользователя

Доступ к данным имеет только пользователь (модераторы/администраторы НЕ имеют доступа)

Срок хранения:

До момента удаления пользователем или удаления аккаунта

4. ЦЕЛИ ОБРАБОТКИ ДАННЫХ

4.1 Предоставление основных функций приложения

Правовое основание: Исполнение договора (Contract — GDPR Art. 6(1)(b))

Регистрация и аутентификация пользователя

Управление профилем пользователя

Обмен сообщениями (текстовые чаты)

Голосовые и видеозвонки

Управление списком друзей и группами

Система виртуальной валюты (HighCoins)

Магазин виртуальных предметов

Персонализация маскота HighCat

4.2 Обработка платежей и финансовые операции

Правовое основание: Исполнение договора (Contract), Законодательные требования (Legal obligation — GDPR Art. 6(1)(c))

Покупка виртуальной валюты (HighCoins)

Оформление подписки Premium

Покупка виртуальных предметов

Отправка виртуальных подарков

Налоговая отчетность (для ЕС — VAT)

Предотвращение мошенничества

4.3 Коммуникация с пользователем

Правовое основание: Исполнение договора (Contract), Законные интересы (Legitimate interests — GDPR Art. 6(1)(f))

Отправка транзакционных email (подтверждение регистрации, восстановление пароля)

Доставка push-уведомлений о новых сообщениях, запросах в друзья, событиях

Техническая поддержка

Уведомления об изменениях в Политике конфиденциальности или Условиях использования

4.4 Обеспечение безопасности и предотвращение злоупотреблений

Правовое основание: Законные интересы (Legitimate interests), Законодательные требования (Legal obligation)

Предотвращение несанкционированного доступа к аккаунтам

Обнаружение и предотвращение мошенничества

Модерация контента (при получении жалоб)

Противодействие спаму и злоупотреблениям

Расследование нарушений Условий использования

Блокировка аккаунтов нарушителей

4.5 Улучшение и развитие сервиса

Правовое основание: Законные интересы (Legitimate interests)

Аналитика использования функций приложения (агрегированная, без персонализации)

Диагностика технических проблем

Тестирование новых функций

Улучшение производительности и стабильности

Анализ качества голосовых/видеозвонков

Важно:

Мы **НЕ используем** сторонние аналитические сервисы (Google Analytics, Mixpanel и т.д.)

Аналитика ведется только на базе собственных агрегированных данных

4.6 Соблюдение законодательных требований

Правовое основание: Законодательные требования (Legal obligation — GDPR Art. 6(1)(c))

Хранение финансовых данных для налоговой отчетности (7 лет)

Предоставление данных по запросам государственных органов (в соответствии с применимым законодательством)

Соблюдение требований GDPR, CCPA и других законов о защите данных

4.7 Реклама (планируется в будущем)

Текущий статус: Рекламные SDK **НЕ установлены**, реклама **НЕ показывается**.

Планируется:
В будущих версиях приложения планируется внедрение неинтрузивной рекламы для пользователей бесплатной версии. При внедрении рекламы:

Пользователи будут проинформированы обновлением данной Политики конфиденциальности

Будет запрошено явное согласие на показ персонализированной рекламы (если применимо)

Будет предоставлена возможность отключить рекламу через подписку Premium

Правовое основание (при внедрении):

Законные интересы (Legitimate interests) — для контекстной рекламы

Согласие (Consent) — для персонализированной рекламы

5. ПЕРЕДАЧА ДАННЫХ ТРЕТЬИМ ЛИЦАМ

Мы минимизируем передачу данных третьим сторонам и передаем их только для выполнения основных функций приложения.

5.1 Процессоры платежей

Stripe, Inc.

Страна: США (с серверами в ЕС для европейских пользователей)

Передаваемые данные: Email, сумма транзакции, валюта, Stripe Customer ID

Цель: Обработка платежей за HighCoins и подписку Premium

Правовое основание: Исполнение договора, PCI DSS compliance

Защита данных: Stripe является PCI DSS Level 1 сертифицированным процессором

Data Processing Agreement (DPA): Stripe предоставляет стандартный DPA

Политика конфиденциальности: https://stripe.com/privacy

Важно: Платежные данные (номер карты, CVV) вводятся напрямую в защищенную форму Stripe и **НЕ проходят** через наши серверы. Мы НЕ имеем доступа к этим данным.

5.2 Провайдеры push-уведомлений

Firebase Cloud Messaging (Google LLC) — для Android

Страна: США (глобальная инфраструктура)

Передаваемые данные: Push token (FCM token), device info

Цель: Доставка push-уведомлений на Android устройства

Правовое основание: Законные интересы
Политика конфиденциальности: https://policies.google.com/privacy

Apple Push Notification Service (Apple Inc.) — для iOS

Страна: США (глобальная инфраструктура)

Передаваемые данные: Push token (APNS token), device info

Цель: Доставка push-уведомлений на iOS устройства

Правовое основание: Законные интересы

Политика конфиденциальности: https://www.apple.com/legal/privacy/

Содержимое уведомлений:

Имена отправителей сообщений

Превью сообщений (первые ~50 символов)

Типы событий (новое сообщение, запрос в друзья и т.д.)

5.3 Провайдеры email

Zoho Corporation Pvt. Ltd.

Страна: Индия (с серверами в ЕС)

Передаваемые данные: Email адрес, имя пользователя (для персонализации писем)

Цель: Отправка транзакционных email (подтверждение регистрации, восстановление пароля, уведомления о платежах)

Правовое основание: Исполнение договора, Законные интересы

Политика конфиденциальности: https://www.zoho.com/privacy.html

5.4 Хостинг-провайдеры инфраструктуры

DigitalOcean LLC / Google Cloud Platform

Страна: США/ЕС (серверы расположены в дата-центрах ЕС)

Передаваемые данные: Полный набор данных, хранимых на сервере (см. раздел 3)

Цель: Хостинг серверной инфраструктуры (база данных, бэкенд API, файловое хранилище)

Правовое основание: Исполнение договора

Защита данных: Провайдеры предоставляют стандартные DPA в соответствии с GDPR

Политика конфиденциальности:

DigitalOcean: https://www.digitalocean.com/legal/privacy-policy

Google Cloud: https://policies.google.com/privacy

5.5 Вспомогательная аутентификация

Appwrite

Страна: ЕС (серверы в Франкфурте, Германия)

Передаваемые данные: User ID, username, email (для синхронизации аутентификации)

Цель: Вспомогательное хранилище пользовательских данных для мобильного SDK

Правовое основание: Исполнение договора

Политика конфиденциальности: https://appwrite.io/privacy

5.6 Данные НЕ передаются следующим сторонам

❌ **Рекламным сетям** — рекламные SDK не установлены
❌ **Аналитическим сервисам** — Google Analytics, Mixpanel, Amplitude и др. не используются
❌ **Социальным сетям** — интеграция с Facebook, Google, Twitter отсутствует
❌ **Data brokers** — мы НЕ продаем данные пользователей
❌ **Маркетинговым платформам** — для таргетированной рекламы

5.7 Международная передача данных (трансграничная передача)

Для пользователей из Европейского Экономического Пространства (ЕЭП):

Некоторые из наших сервис-провайдеров находятся в США или других странах за пределами ЕЭП. Для обеспечения адекватного уровня защиты данных при международной передаче мы применяем следующие механизмы:

Стандартные договорные оговорки (Standard Contractual Clauses, SCC) — утвержденные Европейской Комиссией

шаблоны договоров с процессорами данных

Adequacy Decisions — передача данных в страны, признанные ЕС как обеспечивающие адекватный уровень защиты

Data Processing Agreements (DPA) — договоры обработки данных с каждым процессором

Текущее расположение серверов:

Основная база данных (PostgreSQL): ЕС (Франкфурт, Германия или Амстердам, Нидерланды)

Резервные копии: ЕС

Процессоры с серверами в США:

Stripe (использует EU Data Residency для европейских пользователей)

Firebase/Google Cloud (данные могут храниться в ЕС при соответствующей конфигурации)

Apple (APNS — глобальная инфраструктура)

5.8 Передача данных по запросам государственных органов

Мы можем раскрыть ваши персональные данные по запросу государственных органов, правоохранительных органов или судов только в случаях, предусмотренных применимым законодательством:

При наличии судебного решения или официального запроса

Для защиты прав и безопасности пользователей

Для предотвращения преступлений

Для соблюдения законодательных требований

Принципы:

Мы проверяем законность каждого запроса

Передаем только минимально необходимые данные

Уведомляем пользователя о запросе (если это не запрещено законом)

Публикуем отчеты о количестве запросов (планируется)

6. ХРАНЕНИЕ И БЕЗОПАСНОСТЬ ДАННЫХ

6.1 Сроки хранения данных

Мы храним ваши персональные данные только в течение времени, необходимого для достижения целей, для которых они были собраны, или в соответствии с законодательными требованиями.

Категория данных	Срок хранения	Основание
Аккаунт пользователя (профиль)	До момента удаления пользователем	Исполнение договора

Категория данных	Срок хранения	Основание
JWT Access Token	15 минут	Безопасность
JWT Refresh Token	30 дней или до logout	Безопасность
Revoked Tokens	30 дней после истечения	Предотвращение повторного использования
Коды восстановления пароля	1 час или до использования	Безопасность
Сообщения чатов	До удаления пользователем	Функционал приложения
Метаданные звонков	12 месяцев	Аналитика качества сервиса
История транзакций	7 лет	Налоговое законодательство

Баланс HighCoins	До использования или удаления аккаунта	Функционал приложения
Инвентарь (виртуальные предметы)	До удаления аккаунта	Функционал приложения
IP-адреса и логи активности	90 дней	Безопасность, техподдержка
Логи ошибок (Serilog)	30 дней	Диагностика
Push tokens	До удаления приложения или logout	Доставка уведомлений
Уведомления	90 дней	Функционал приложения
Жалобы и репорты модерации	6 месяцев после закрытия	Trust & Safety
Аудит-логи действий администраторов	3 года	Внутренний контроль
Резервные копии базы данных	30 дней	Disaster recovery

После удаления аккаунта:

- Большинство персональных данных удаляется немедленно
- Финансовые данные (история транзакций) анонимизируются и сохраняются в течение 7 лет для выполнения налоговых обязательств
- Данные модерации (жалобы, репорты) могут сохраняться до 6 месяцев для завершения расследований

6.2 Технические меры защиты

Мы применяем современные технические и организационные меры для защиты ваших данных от несанкционированного доступа, изменения, раскрытия или уничтожения:

Шифрование при передаче (Data in Transit):

- **HTTPS/TLS 1.3** для всех API-запросов
- **WebSocket Secure (WSS)** для SignalR real-time коммуникаций
- **SRTP (Secure Real-time Transport Protocol)** для WebRTC медиа-потоков
- Минимальная версия TLS: 1.2

Шифрование при хранении (Data at Rest):

- **Пароли:** хэшируются с использованием bcrypt/argon2 (не обратимое шифрование)
- **JWT токены:** подписываются HMAC-SHA256
- **Локальное хранилище (клиент):**
  - iOS: Keychain (hardware-backed encryption)
  - Android: EncryptedSharedPreferences (Android Keystore System)
- **База данных:** PostgreSQL (планируется внедрение Transparent Data Encryption)

Контроль доступа:

- **Аутентификация:** JWT-токены с коротким сроком действия (15 минут)
- **Авторизация:** Role-based access control (RBAC) — user/moderator/admin
- **Минимальные привилегии:** каждый пользователь и процесс имеет доступ только к необходимым данным
- **Двухфакторная аутентификация (2FA):** планируется внедрение

Защита инфраструктуры:

- **Firewall:** все серверы защищены сетевыми firewall
- **DDoS protection:** защита от атак типа "отказ в обслуживании"

Регулярные обновления: своевременная установка обновлений безопасности

Изолированные среды: разделение production/staging/development окружений

Мониторинг и аудит:

Логирование действий администраторов: все критичные действия записываются в аудит-логи

Мониторинг подозрительной активности: автоматическое обнаружение необычных паттернов доступа

Регулярные проверки безопасности: периодические security audits

Резервное копирование:

Автоматические backup: ежедневные резервные копии базы данных

Географическая избыточность: backup хранятся в отдельном дата-центре

Шифрование backup: все резервные копии зашифрованы

6.3 Организационные меры защиты

Политика конфиденциальности для персонала: все лица, имеющие доступ к данным, обязаны соблюдать конфиденциальность

Ограниченный доступ: персональные данные доступны только уполномоченным лицам

Соглашения о неразглашении (NDA): с подрядчиками и партнерами

План реагирования на инциденты: процедуры на случай утечки данных

Регулярное обучение: обучение персонала вопросам безопасности данных

6.4 Уведомление о нарушениях безопасности данных

В случае нарушения безопасности данных, которое может повлечь риск для ваших прав и свобод, мы:

Уведомим соответствующий надзорный орган в течение **72 часов** с момента обнаружения (требование GDPR)

Уведомим затронутых пользователей **без неоправданной задержки**, если риск является высоким

Предоставим рекомендации по минимизации возможного ущерба

Контакт для сообщений о проблемах безопасности:
security@hightalk.me (планируется создание)

6.5 Хранилище данных на устройстве пользователя

Данные, хранимые локально:

JWT Access Token (зашифрован)

JWT Refresh Token (зашифрован)

Кэш профиля пользователя (зашифрован)
Кэш списка друзей (TTL 5-10 минут)

Кэш баланса HighCoins (TTL 60 секунд)

Данные, НЕ хранимые локально:

❌ Пароли

❌ История сообщений чатов

❌ Платежные данные

❌ Записи звонков

Безопасность локального хранилища:

iOS: данные хранятся в Keychain с атрибутом `kSecAttrAccessibleWhenUnlockedThisDeviceOnly`

Android: данные хранятся в EncryptedSharedPreferences с использованием Android Keystore

Очистка при logout: все локальные данные полностью удаляются при выходе из аккаунта

Защита от извлечения данных:

Root/Jailbreak Detection: планируется внедрение

Certificate Pinning: планируется внедрение

7. ПРАВА ПОЛЬЗОВАТЕЛЕЙ

В соответствии с GDPR, CCPA и другими законами о защите данных, вы имеете следующие права в отношении своих персональных данных:

7.1 Право на доступ (GDPR Art. 15, CCPA)

Вы имеете право получить подтверждение того, обрабатываем ли мы ваши персональные данные, и если да, то получить копию этих данных.

Как реализуется:

- Вы можете просмотреть большинство своих данных в настройках профиля приложения
- Для полного экспорта данных отправьте запрос на admin@hightalk.me с темой "Data Access Request"

Срок ответа: до 30 дней (GDPR)

Формат предоставления:

- Структурированный JSON или CSV файл
- Включает: профиль, историю транзакций, инвентарь, настройки, метаданные активности

7.2 Право на исправление (GDPR Art. 16)

Вы имеете право исправить неточные или неполные персональные данные.

Как реализуется:

- Через раздел "Настройки профиля" в приложении
- Вы можете изменить: отображаемое имя, биографию, email, телефон, местоположение, аватар, настройки приватности

Срок обработки: немедленно (при изменении в приложении)

7.3 Право на удаление ("Право быть забытым") (GDPR Art. 17, CCPA)

Вы имеете право запросить удаление ваших персональных данных.

Как реализуется:

- Через раздел "Настройки → Удалить аккаунт" в приложении (планируется реализация)
- По запросу на admin@hightalk.me с темой "Account Deletion Request"

Что удаляется:

- Профиль пользователя (имя, email, биография и т.д.)
- Сообщения чатов
- Социальные связи (друзья, группы)
- Инвентарь виртуальных предметов
- Push tokens
- Локальные данные на устройстве

Что сохраняется (анонимизировано):

- Финансовые данные (история транзакций) — требование налогового законодательства (7 лет) Данные
- анонимизируются: все идентификаторы пользователя заменяются на "Deleted User [UUID]" Данные
- модерации (жалобы, репорты) — для завершения расследований (до 6 месяцев)

Срок обработки: до 30 дней

Исключения (когда мы не можем удалить данные):

- Выполнение законодательных требований (финансовая отчетность)
- Защита прав других пользователей
- Завершение судебных разбирательств

7.4 Право на ограничение обработки (GDPR Art. 18)

Вы имеете право ограничить обработку ваших данных в определенных случаях (например, при оспаривании точности данных).

Как реализуется:

- По запросу на admin@hightalk.me с темой "Restrict Processing Request"
- Мы временно приостановим обработку ваших данных (кроме хранения) до разрешения вопроса

Срок обработки: до 30 дней

7.5 Право на переносимость данных (Data Portability) (GDPR Art. 20)

Вы имеете право получить свои данные в структурированном, широко используемом, машиночитаемом формате и передать их другому контроллеру.

Как реализуется:

- Отправьте запрос на admin@hightalk.me с темой "Data Portability Request"
- Мы предоставим вам файл JSON или CSV с вашими данными

Включаемые данные:

- Профиль пользователя
- Настройки приватности и уведомлений
- Список друзей (User IDs)
- История транзакций (HighCoins, покупки)
- Инвентарь виртуальных предметов
- Метаданные активности (даты регистрации, последнего входа)

Не включаются:

- Сообщения чатов (технически сложно предоставить в переносимом формате)
- Данные других пользователей

Срок обработки: до 30 дней

7.6 Право на возражение (GDPR Art. 21)

Вы имеете право возразить против обработки ваших данных на основании законных интересов.

Как реализуется:

- Отправьте запрос на admin@hightalk.me с темой "Objection to Processing"
- Мы прекратим обработку, если не сможем продемонстрировать убедительные законные основания

Применимо к:

- Обработке данных для маркетинговых целей (когда будет реализовано)
- Профилированию (когда будет реализовано)
- Аналитике (вы можете запросить исключение из аналитики)

7.7 Право на отзыв согласия (GDPR Art. 7(3))

Если обработка данных основана на вашем согласии, вы имеете право отозвать его в любое время.

Как реализуется:

- Через настройки приложения (для push-уведомлений, настроек приватности)
- Отправьте запрос на admin@hightalk.me

Важно: Отзыв согласия не влияет на законность обработки, которая осуществлялась до отзыва.

7.8 Право подать жалобу в надзорный орган (GDPR Art. 77)

Вы имеете право подать жалобу в надзорный орган по защите данных, если считаете, что обработка ваших данных нарушает GDPR.

Надзорные органы ЕС:

- Для пользователей в ЕС: обратитесь в надзорный орган вашей страны

Список органов: https://edpb.europa.eu/about-edpb/board/members_en

Для пользователей США (CCPA):

California Attorney General: https://oag.ca.gov/

7.9 Специальные права для пользователей из Калифорнии (CCPA)

Право на раскрытие информации:

Категории собираемых персональных данных

Категории источников данных

Цели использования данных

Категории третьих сторон, которым передаются данные

Право на удаление:

Запрос на удаление данных (аналогично GDPR Art. 17)

Право на отказ от продажи данных:

Мы **НЕ продаем** ваши персональные данные. Данное право не применимо.

Право на недискриминацию:

Мы не дискриминируем пользователей, которые осуществляют свои права по CCPA

7.10 Как осуществить свои права

Для запросов отправьте email на:
admin@hightalk.me

Тема письма:

Data Access Request (запрос на доступ к данным)

Data Export Request (экспорт данных)

Account Deletion Request (удаление аккаунта)

Restrict Processing Request (ограничение обработки)

Objection to Processing (возражение против обработки)

Обязательно укажите:

Ваш username в приложении

Email, привязанный к аккаунту

Описание запроса

Верификация личности:
Для защиты вашей конфиденциальности мы можем запросить дополнительную информацию для подтверждения вашей личности перед обработкой запроса.

Срок ответа:

GDPR: до 30 дней (может быть продлен до 60 дней в сложных случаях)

CCPA: до 45 дней

Плата:
Осуществление ваших прав **бесплатно**. Мы можем взимать разумную плату только в случае явно необоснованных или чрезмерных запросов.

8. СПЕЦИАЛЬНЫЕ КАТЕГОРИИ ПОЛЬЗОВАТЕЛЕЙ

8.1 Несовершеннолетние пользователи

Возрастные ограничения:
Приложение предназначено для пользователей от **16 лет** и старше.

Сбор данных детей:
Мы **НЕ собираем намеренно** данные детей младше 16 лет (или младше возраста цифрового согласия в вашей юрисдикции).

Если вы родитель или опекун:
Если вы считаете, что ваш ребенок младше 16 лет предоставил нам персональные данные без вашего согласия, немедленно свяжитесь с нами по адресу admin@hightalk.me. Мы удалим такие данные в течение 72 часов.

Проверка возраста:

- При регистрации запрашивается дата рождения
- Аккаунты пользователей младше 16 лет автоматически отклоняются

COPPA (Children's Online Privacy Protection Act):
Для пользователей из США: приложение соответствует требованиям COPPA, не собирая данные детей младше 13 лет.

8.2 Пользователи программ восстановления (Трекер трезвости)

Текущий статус: Функция НЕ реализована (планируется в будущем).

Специальная защита при реализации:

Данные трекера трезвости относятся к **специальным категориям персональных данных (Special Categories of Personal Data)** согласно GDPR Article 9, так как могут содержать информацию о здоровье пользователя.

Правовое основание:

- **Явное согласие (Explicit Consent)** — будет запрашиваться отдельным согласием при активации функции

Меры защиты:

- Данные трекера хранятся отдельно от основного профиля пользователя
- Шифрование end-to-end для записей трекера (планируется)
- Доступ к данным имеет **только пользователь** (модераторы и администраторы НЕ имеют доступа)
- Возможность полного удаления данных в любой момент
- Данные **НЕ передаются третьим лицам** без явного согласия пользователя
- Данные **НЕ используются** для рекламы или аналитики

Анонимность:
Пользователи могут использовать псевдонимы и не раскрывать реальную личность при использовании функций программ восстановления.

Доступ к ресурсам:
Мы предоставляем информацию о профессиональных организациях поддержки (горячие линии, группы поддержки), но НЕ являемся медицинским сервисом.

Disclaimer:
HighTalk **НЕ является медицинским приложением** и не предоставляет медицинские услуги или консультации. Для получения профессиональной медицинской помощи обратитесь к квалифицированному специалисту.

9. COOKIES И АНАЛОГИЧНЫЕ ТЕХНОЛОГИИ

9.1 Использование cookies

Текущий статус:
Мобильное приложение (iOS/Android) **НЕ использует cookies** в традиционном понимании (HTTP cookies), так как это нативное приложение, а не веб-сайт.

Веб-версия (если будет реализована):
При запуске веб-версии приложения (hightalk.me) могут использоваться следующие типы cookies:

- **Strictly Necessary Cookies** (Строго необходимые) — для аутентификации и базовой работы приложения
- **Functional Cookies** (Функциональные) — для запоминания настроек пользователя
- **Analytics Cookies** (Аналитические) — только с согласия пользователя

Будет предоставлен Cookie Consent Banner в соответствии с ePrivacy Directive (EC).

9.2 Локальное хранилище (Local Storage)

Мобильное приложение:
Мы используем локальное хранилище устройства для:

Сохранения JWT токенов (Expo SecureStore)

Кэширования данных профиля (для offline доступа)

Сохранения настроек приложения

Управление:
Все локальные данные удаляются при logout

Пользователь может очистить локальные данные через настройки устройства (Настройки → Приложения → HighTalk → Очистить данные)

9.3 Идентификаторы устройства

Что мы НЕ собираем:

❌ IDFA (Identifier for Advertisers) / GAID (Google Advertising ID)

❌ IMEI

❌ MAC-адрес

Что мы собираем:

✅ Push Notification Token (FCM/APNS) — для доставки уведомлений

✅ Installation ID (Expo) — для идентификации конкретной установки приложения

Цель:
Только для функционала приложения (push-уведомления, синхронизация данных), **НЕ для рекламного трекинга**.

9.4 App Tracking Transparency (iOS 14.5+)

Статус: Приложение **НЕ запрашивает** разрешение на трекинг (ATT prompt).

Причина:
Мы НЕ используем IDFA или другие идентификаторы для трекинга пользователей между приложениями или веб-сайтами третьих сторон.

Декларация в App Store:
"No, we do not collect data for tracking" — приложение НЕ собирает данные для трекинга.

10. ИЗМЕНЕНИЯ В ПОЛИТИКЕ КОНФИДЕНЦИАЛЬНОСТИ

10.1 Уведомление об изменениях

Мы можем обновлять настоящую Политику конфиденциальности время от времени для отражения изменений в наших практиках обработки данных или в связи с изменениями законодательства.

Уведомление пользователей:

Существенные изменения: уведомление по email и/или push-уведомление в приложении за 30 дней до вступления в силу

Несущественные изменения: публикация обновленной версии на сайте и в приложении

Дата вступления в силу:
Обновленная Политика вступает в силу с момента публикации (или с указанной даты для существенных изменений).

Продолжение использования:
Продолжая использовать приложение после вступления изменений в силу, вы подтверждаете свое согласие с обновленной Политикой.

История версий:
Предыдущие версии Политики конфиденциальности будут доступны на сайте https://hightalk.me/privacy-history (планируется).

10.2 Что считается существенным изменением

Существенными считаются изменения, которые:

Вводят новые цели обработки данных

Расширяют категории собираемых данных

Изменяют правовое основание обработки
Добавляют новых получателей данных (третьи стороны)

Изменяют сроки хранения данных (в большую сторону)

Влияют на права пользователей

11. КОНТАКТНАЯ ИНФОРМАЦИЯ

11.1 Контакты оператора данных

Общие вопросы:
admin@hightalk.me

Вопросы по конфиденциальности и защите данных:
admin@hightalk.me (пометьте тему: "Privacy Question")

Запросы на осуществление прав пользователя:
admin@hightalk.me (укажите тип запроса в теме письма)

Почтовый адрес:
Nawrot 56/38, Łódź, 91-001

Веб-сайт:
https://hightalk.me

11.2 Официальный представитель в ЕС (GDPR Representative)

Текущий статус: Представитель НЕ назначен (MVP-версия, физическое лицо).

Планируется:
При регистрации юридического лица и активном предоставлении услуг пользователям ЕС будет назначен официальный представитель в ЕС в соответствии с GDPR Article 27.

Информация будет обновлена в данном разделе.

11.3 Надзорные органы

Для пользователей из ЕС:
Вы можете подать жалобу в надзорный орган по защите данных вашей страны. Список надзорных органов: https://edpb.europa.eu/about-edpb/board/members_en

Для пользователей из Калифорнии (США):
California Attorney General
Website: https://oag.ca.gov/
Phone: (916) 210-7580

11.4 Время ответа на запросы

Общие вопросы: 2-5 рабочих дней

Запросы на доступ/экспорт данных: до 30 дней (GDPR)

Запросы на удаление аккаунта: до 30 дней (GDPR)

Срочные вопросы безопасности: немедленно

12. ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ
12.1 Автоматизированное принятие решений и профилирование

Статус: НЕ применяется.

Мы **НЕ используем** автоматизированное принятие решений (включая профилирование) в значении GDPR Article 22, которое может иметь юридические последствия для вас.

Исключение:
Система модерации может использовать автоматические фильтры для обнаружения спама или запрещенного контента, но окончательное решение о блокировке принимается человеком (модератором).

12.2 Добровольность предоставления данных

Обязательные данные:
Для использования основных функций приложения необходимо предоставить:

- Имя пользователя (username)
- Адрес электронной почты (email)
- Пароль
- Дата рождения (для проверки возраста)

Опциональные данные:
Следующие данные предоставляются добровольно и не являются обязательными:

- Полное имя (First Name, Last Name)
- Телефон
- Биография (bio)
- Местоположение (текстовое поле)
- Веб-сайт
- Аватар

Последствия непредоставления данных:
Если вы не предоставите обязательные данные, вы не сможете зарегистрироваться и использовать приложение. Непредоставление опциональных данных не влияет на доступ к основным функциям.

12.3 Ссылки на сторонние сервисы

Приложение может содержать ссылки на сторонние веб-сайты или сервисы (например, политики конфиденциальности Stripe, Firebase).

Важно:
Мы **НЕ несем ответственности** за практики конфиденциальности сторонних сервисов. Мы рекомендуем ознакомиться с их политиками конфиденциальности перед использованием.

12.4 Data Protection Impact Assessment (DPIA)

В соответствии с GDPR Article 35, мы провели оценку влияния на защиту данных (DPIA) для высокорисковых операций обработки, включая:

- Обработку финансовых данных
- Хранение сообщений чатов
- Планируемую обработку данных трекера трезвости (Special Category Data)

Результаты DPIA доступны по запросу надзорных органов.

12.5 Применимое право и юрисдикция

Применимое право:
Настоящая Политика конфиденциальности регулируется законодательством Республики Польши с учетом обязательных требований:

- GDPR (для пользователей из ЕС)
- CCPA (для пользователей из Калифорнии)
- Местного законодательства пользователя

Разрешение споров:
Споры, связанные с обработкой персональных данных, разрешаются в соответствии с применимым законодательством. Пользователи из ЕС имеют право обратиться в суд своей страны проживания.

13. ПРИНЯТИЕ УСЛОВИЙ

Используя приложение HighTalk, вы подтверждаете, что:

✅ Ознакомились с настоящей Политикой конфиденциальности
✅ Понимаете, какие данные собираются и как они используются
✅ Достигли возраста 16 лет (или возраста цифрового согласия в вашей юрисдикции)

✅ Согласны с условиями обработки ваших персональных данных

Если вы не согласны с какими-либо условиями, пожалуйста, не используйте приложение.

14. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

14.1 Язык документа

Настоящая Политика конфиденциальности составлена на русском языке. В случае перевода на другие языки, при возникновении противоречий приоритет имеет русскоязычная версия.

14.2 Делимость положений

Если какое-либо положение настоящей Политики будет признано недействительным или не подлежащим исполнению, остальные положения остаются в силе.

14.3 Благодарность

Спасибо за доверие и использование HighTalk. Мы ценим вашу конфиденциальность и прилагаем все усилия для защиты ваших данных.

Документ составлен: 31 октября 2025 г.
Дата вступления в силу: 1 ноября 2025 г.
Версия: 1.0