



Система для безпечного спілкування та передачі особливої інформації, створена для військових, поліцейських і спеціалізованих підрозділів



Усі системи зв'язку, які ви не контролюєте — **контролюють вас!**

В подальшому треба називати цю групу – відкритий зв'язок.

Популярні месенджери створені для збору інформації про володаря та продажу цієї інформації заінтересованим особам та компаніям. Вони збирають і продають дані користувачів. Це їх офіційна бізнес модель. Через відкриті канали ворог отримує геолокацію, повідомлення, документи.

Проблема та наслідки використання відкритого зв'язку

Сучасні військові та силові структури стикаються з критичною проблемою – відсутністю безпечних систем зв'язку, які б гарантували повну конфіденційність і контроль над переданою інформацією – фото, новітні розробки, плани, відео випробувань та інше – все це ворог може отримувати віддалено чи за допомогою соціальної інженерії.

Використання масових месенджерів створює високі ризики перехоплення, збору метаданих, зламу або втручання сторонніх суб'єктів

У бойових умовах це призводить до втрат життя, витоку розвідданих і зриву масштабних операцій.

Проблема та наслідки використання відкритого зв'язку

Супротивник перехоплює дані, координати та всі перемовини — і готує відповіді саме тоді, коли війська довіряють маркетинговій інформації про “безпечність”.



Бізнес, партії, армія — вразливі через закладені модулі контролю в додатках та сервери, де ця інформація обробляється.

Через месенджери, які маскуються під “безпечні”, зовнішні сили впливають на політичні рішення та вибори в цілих країнах.

Рішення та Українська відповідь

WeWe3 Military — це ізольована криптосистема, побудована на ядрі WeWe3 Core, призначена для бойових підрозділів, силових структур і спеціальних операцій. Архітектура створена таким чином, що жоден зовнішній суб'єкт, жоден адміністратор і навіть власник серверної інфраструктури фізично не здатні отримати доступ до змісту повідомлень чи службових даних користувачів.

Проста в розгортанні та підтримці система усуває зовнішні канали передачі, використовує власну серверну інфраструктуру та протоколи з рівнем шифрування, еквівалентним або вищим за стандарти НАТО, але це частина успіху.

Додаткові рішення — антиінсайдер, антипредатель, антифішинг та багато інших — створені для того, щоб забезпечити не лише знищення даних у разі компрометації, але й усвідомлення рівня захищеності всіма, хто користується системою.

Основні переваги WeWe3 Military для армії

Персональні сервери до тактичного рівня; просте розгортання та обслуговування. Втрата сервера або його компрометація не призводить до перехоплення чи втрати інформації.

Завдання технічного персоналу — забезпечити працездатність сервера; доступ до змісту повідомлень технічно неможливий.

Повна довіра для всіх учасників системи.

Дані зберігаються виключно на пристрої користувача.

Реалізовані сценарії командного, ручного та автоматичного гарантованого знищення інформації — як на всіх пристроях одночасно, так і на вибраних окремих пристроях.

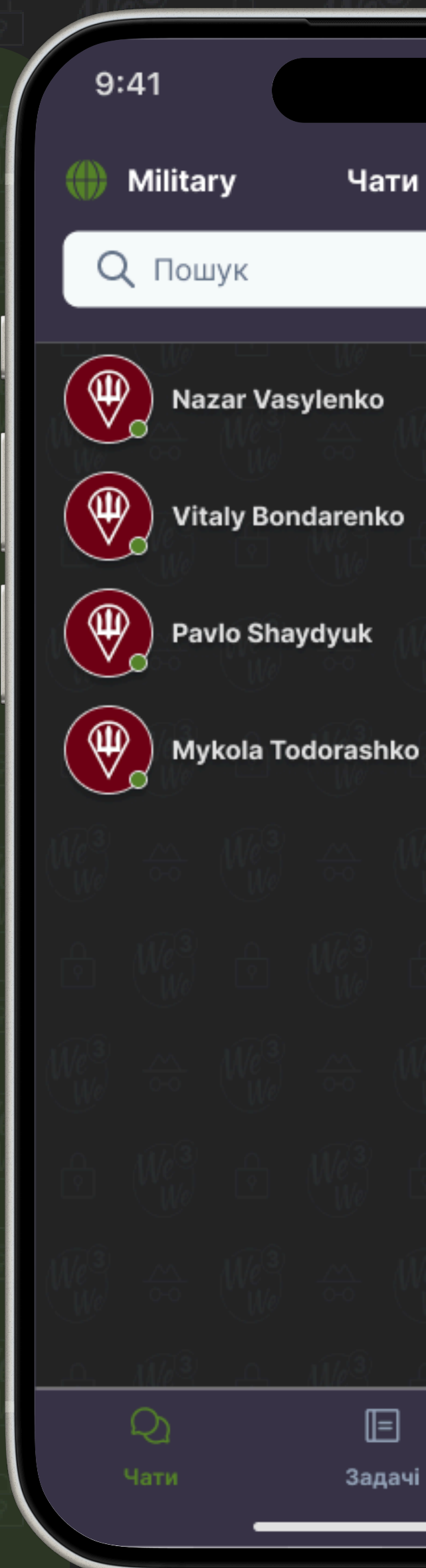
Активація користувачів без паролів: без SMS, без email — виключає ризики компрометації традиційних факторів.

Можливість white-label-випуску під іншим брендом (наприклад, STRUM).

Сквозне шифрування (E2E): AES-256 та RSA-4096 при коректній імплементації забезпечують криптостійкість, перевірену десятиліттями.

Повноцінні застосунки для iOS, macOS, Android та Windows.

Захист від соціальної інженерії та спроб примусового отримання доступу.



Родина WeWe3



WeWe3 Ядро
база з API для інтеграції в
корпоративні, військові
платформи, особисті
рішення



Особистості розробки



Захищений зв'язок останнього покоління,
створений українською командою з 25-річним
досвідом у наступальних та оборонних
кіберопераціях.

Команда, що працює над WeWe, має багаторічну
практику розробки та підтримки ІТ-продуктів
національного й міжнародного рівня поза
межами цього проєкту, з постійним акцентом на
безпеку даних.

Уся кодова база — власної розробки, без
використання open-source компонентів.

Це забезпечує повний контроль над безпекою,
можливість оперативних змін та швидку реакцію
на новітні виклики.

Стан розробки

Продукт отримав експертний висновок Фонду розвитку інновацій, де його визнано перспективним та необхідним для потреб Збройних Сил України, з позначкою високого рівня готовності.

Родина додатків WeWe постійно зростає: нині версії Global та Enterprise використовують тисячі користувачів по всьому світу. Це дозволяє глобально аналізувати та розвивати продукт, випереджаючи потенційні загрози.

Криптографічні стандарти та технічні вимоги погоджені з Державною службою спеціального зв'язку та захисту інформації України.



Зараз інформаційна безпека = життя.

Встановіть глобальну версію WeWe3 просто зараз — для себе та свого оточення.

Додатки доступні у відповідних магазинах AppStore та Google Play.

Не витрачайте час марно — ваше життя цінніше за все.

Шукайте WeWe3, і нехай ваше життя стане безпечнішим, спокійнішим і захищеним.



<https://weltwelle.com/>

Контакти