EUROPEAN OPEN SCIENCE SPACE

DOI 10.70286/EOSS-19.01.2026.002.81-84

ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ПЕРСОНАЛЬНИХ ДАНИХ МЕШКАНЦІВ ЖИТЛОВОГО КОМПЛЕКСУ ПРИ ВИКОРИСТАННІ СТОРОННІХ API (НА ПРИКЛАДІ TELEGRAM)

Пашкевич Тетяна
бакалавр
Бабич Юлія
к.т.н., доцент
Кафедра інформаційних технологій проєктування та дизайну
Національний університет «Одеська політехніка», Україна

Анотація. У роботі досліджується проблема забезпечення безпеки персональних даних мешканців при використанні сторонніх API у цифрових системах управління житловими комплексами. Розглянуто особливості інтеграції Telegram Bot API як популярного інструменту комунікації між управляючими компаніями та мешканцями. Проаналізовано архітектурні вразливості API, основні вектори атак і ризики витоку інформації, пов'язані з обробкою персональних та фінансових даних. Запропоновано багаторівневу модель захисту, що поєднує технічні та організаційні заходи безпеки та відповідає вимогам національного і європейського законодавства у сфері захисту персональних даних.

Ключові слова: персональні дані, сторонні API, інформаційна безпека, Telegram Bot API, захист інформації.

Вступ. Цифрова трансформація сфери управління житловими комплексами супроводжується активним впровадженням месенджерів як основних каналів комунікації з мешканцями. Сервіси миттєвих повідомлень забезпечують оперативне інформування про нарахування платежів, технічні роботи, аварійні ситуації та зворотний зв'язок із користувачами. Водночас інтеграція сторонніх API, зокрема Telegram Bot API, у CRM-системах управляючих компаній створює нові виклики для захисту персональних даних мешканців. За результатами галузевих досліджень, понад 60% інцидентів витоку інформації пов'язані з неналежним захистом API та помилками конфігурації серверної інфраструктури.

Актуальність дослідження зумовлена необхідністю дотримання вимог Закону України «Про захист персональних даних» та Загального регламенту захисту даних (GDPR), які встановлюють підвищену відповідальність за обробку конфіденційної інформації через сторонні платформи. Особливу складність становить той факт, що частина даних передається і зберігається в інфраструктурі, яка не перебуває під повним контролем управляючої організації. Як зазначає Б. Шнайєр, безпека не є статичним станом або продуктом, а

безперервним процесом, що потребує системного підходу та постійного вдосконалення.

Метою дослідження є розробка комплексного підходу до забезпечення безпеки персональних даних мешканців при інтеграції Telegram Bot API в CRM-системи управління житловими комплексами. Для досягнення поставленої мети визначено такі задачі: проаналізувати архітектурні особливості та потенційні вразливості Telegram Bot API; визначити критичні точки компрометації персональних даних; дослідити основні вектори атак на системи зі сторонніми API; розробити багаторівневу модель захисту персональних даних; сформулювати практичні рекомендації щодо безпечної імплементації месенджерів у системах управління житловими комплексами.

Результати дослідження Telegram Bot API надає HTTP-інтерфейс для автоматизації комунікації між сервісами та користувачами без необхідності використання складних криптографічних протоколів. Ключовим елементом безпеки в даній архітектурі є токен доступу, отриманий через сервіс BotFather. Компрометація цього токена надає зловмиснику повний контроль над ботом, включаючи можливість читання та відправлення повідомлень, а також доступ до історії взаємодії з користувачами.

На відміну від приватних чатів, у яких застосовується наскрізне шифрування, взаємодія з ботами не гарантує end-to-end encryption. Повідомлення зберігаються на серверах Telegram у зашифрованому вигляді, проте через API передається значний обсяг метаданих, зокрема унікальні ідентифікатори користувачів, часові мітки та типи контенту. Це формує розподілену модель довіри, у межах якої управляюча компанія залежить як від безпеки власної серверної інфраструктури, так і від політик сторонньої платформи.

Аналіз загроз дозволив виділити три основні вектори атак. Перший вектор пов’язаний із компрометацією токенів доступу внаслідок їх зберігання у відкритому коді або конфігураційних файлах. Другий вектор реалізується через атаки типу Man-in-the-Middle при використанні polling-режиму замість більш захищеного webhook-підходу. Третій вектор базується на соціальній інженерії та фішингових атаках, спрямованих на отримання доступу до Telegram-акаунтів мешканців.

Для мінімізації зазначених ризиків у роботі запропоновано багаторівневу модель захисту персональних даних, що ґрунтується на принципі defense-in-depth. Перший рівень моделі передбачає захист токенів доступу та конфігурацій системи шляхом використання спеціалізованих систем управління секретами, автоматизованої ротації ключів і детального журналювання доступу. Другий рівень спрямований на забезпечення безпечної передачі даних із використанням webhook-механізму, протоколу TLS 1.3, перевірки джерела запитів та мережевих обмежень. Третій рівень реалізує принципи мінімізації та псевдонімізації персональних даних за рахунок обмеження обсягу інформації, що передається через месенджер. Четвертий рівень включає впровадження багатофакторної автентифікації для доступу до чутливої інформації. Архітектура обробки

персональних даних мешканців при використанні Telegram Bot API представлена на рис. 1, де відображено основні компоненти системи, канали передачі інформації та зони відповідальності між сторонньою платформою й серверною інфраструктурою управляючої компанії, а також визначено ключові точки потенційної компрометації даних, що потребують додаткових механізмів захисту.

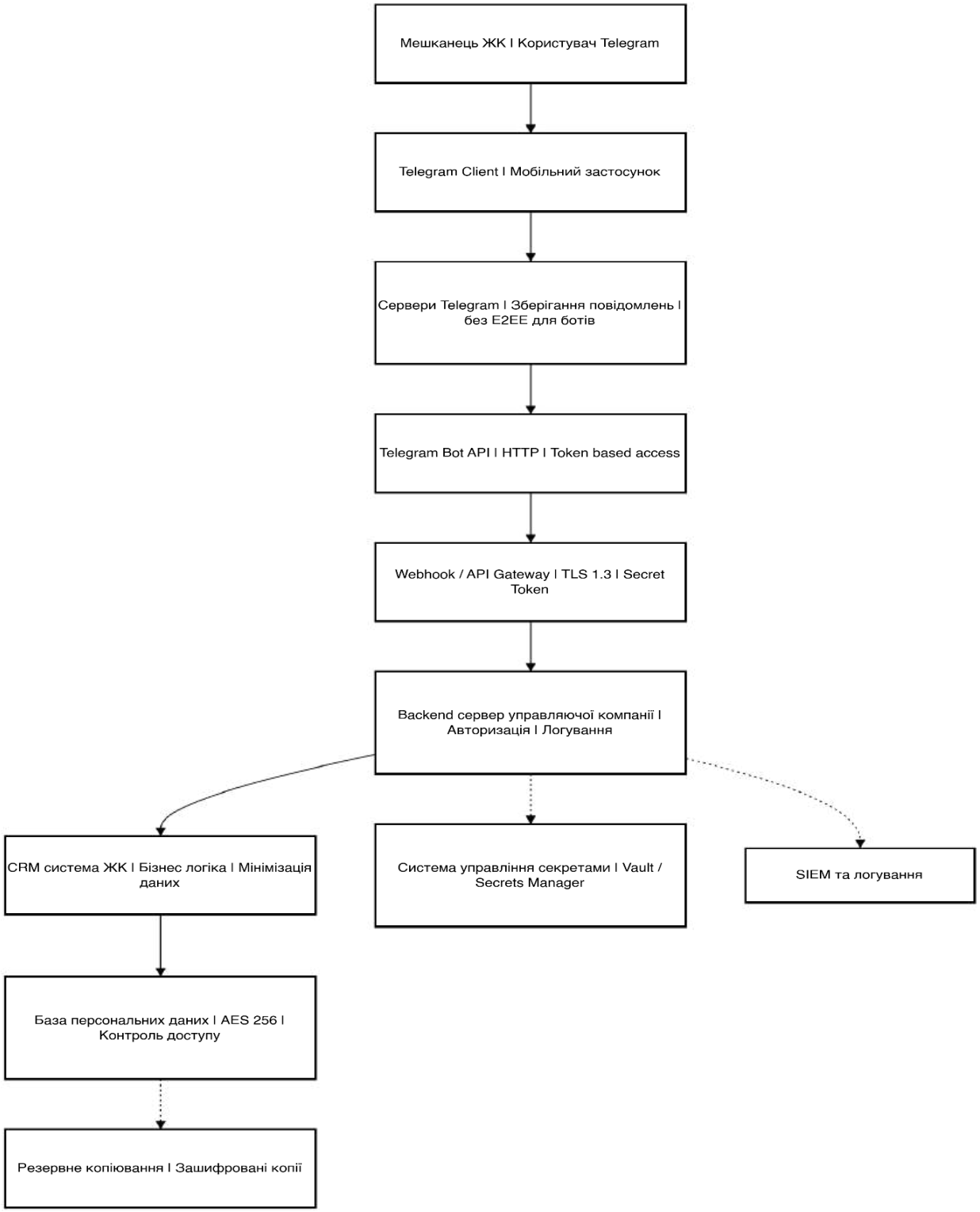

Рисунок 1. Архітектура обробки персональних даних мешканців житлового комплексу при використанні Telegram Bot API

Важливим доповненням до технічних заходів є організаційні процедури, зокрема регулярний аудит безпеки, навчання персоналу та розробка внутрішніх політик роботи з персональними даними. Детальне логування операцій без фіксації чутливого контенту та інтеграція з SIEM-системами дозволяють своєчасно виявляти аномальну активність і реагувати на потенційні інциденти безпеки.

Висновки. Проведене дослідження показало, що інтеграція Telegram Bot API у CRM-системи управління житловими комплексами супроводжується підвищеними ризиками для безпеки персональних даних мешканців. Водночас використання сторонніх API не обов'язково означає компроміс у рівні захисту за умови впровадження багаторівневої моделі безпеки, яка поєднує технічні та організаційні заходи. Запропонований підхід може бути адаптований для інших месенджерів і сторонніх сервісів, що робить результати дослідження актуальними для широкого кола організацій. Перспективи подальших досліджень пов'язані з автоматизацією аудиту безпеки API-інтеграцій та застосуванням сучасних криптографічних технологій для підвищення рівня конфіденційності.

Список використаних джерел

1. European Parliament and Council. (2016). General Data Protection Regulation (EU) 2016/679. https://eur-lex.europa.eu/.
2. OWASP Foundation. (2023). OWASP API Security Top 10. https://owasp.org/.
3. Schneier, B. (2015). Secrets and lies: Digital security in a networked world. Wiley.
4. Верховна Рада України. (2010). Закон України «Про захист персональних даних» № 2297-VI. https://zakon.rada.gov.ua/.

DOI 10.70286/EOSS-19.01.2026.003.84-87

СТВОРЕННЯ РОЗПОДІЛЕНИХ СИСТЕМ НА ОСНОВІ ТЕХНОЛОГІЇ REMOTE METHOD INVOCATION

Рибак Ольга
к.т.н., доцент
ORCID: 0000-0002-0250-3037
Кафедра інформаційних технологій проєктування та дизайну
Національний університет «Одеська політехніка», Україна

Розподілені системи використовуються для роботи з великими обсягами даних, віддаленого доступу до ресурсів та побудови масштабованих сервісів. Такі системи дозволяють кільком комп'ютерам працювати як одна обчислювальна структура, користувачі якої залишаються пов'язаними, а процеси