НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ПОЛТАВСЬКА ПОЛІТЕХНІКА
ІМЕНІ ЮРІЯ КОНДРАТЮКА

ЗБІРНИК МАТЕРІАЛІВ

77-Ї НАУКОВОЇ КОНФЕРЕНЦІЇ ПРОФЕСОРІВ, ВИКЛАДАЧІВ, НАУКОВИХ ПРАЦІВНИКІВ, АСПІРАНТІВ ТА СТУДЕНТІВ УНІВЕРСИТЕТУ

16 травня – 22 травня 2025 р.

1. IT ARMY of Ukraine [Електронний ресурс]. – Режим доступу: https://itarmy.com.ua. – Назва з екрана. – Дата звернення: 05.05.2025.

2. Шахрайство, фішинг та кібератаки: як вберегти себе від зловмисників у мережі [Електронний ресурс]. – Режим доступу: https://euneighbourseast.eu/uk/news/stories/shahrajstvo-fishyng-ta-kiberataky-yak-vberegty-sebe-vid-zlovmysnykiv-u-merezhi/. – Назва з екрана. – Дата звернення: 05.05.2025.

3. Васильєва О.В. Розбудова національної системи кібербезпеки в умовах війни / О.В. Васильєва // Law and Safety. – 2023. – №12. – С. 100–108. – [Електронний ресурс]. – Режим доступу: http://lsej.org.ua/12_2023/100.pdf. – Дата звернення: 05.05.2025.

4. Живило Є.О. Тестування на проникнення: навч. посіб. Ч.1 / Є.О. Живило; за ред. Є.О. Живило. – Полтава: ПНТУ «Полтавська політехніка ім. Юрія Кондратюка», 2024. – 134 с.

5. Живило Є.О. Тестування на проникнення: навч. посіб. / Є.О. Живило; за ред. Є.О. Живило. – Полтава: ПНТУ «Полтавська політехніка ім. Юрія Кондратюка», 2024. – 239 с.

УДК 004.492.2

Є.О. Живило, к.держ.упр.
Н.Є. Ландик, студент 102 КБ
Національний університет
«Полтавська політехніка імені Юрія Кондратюка»

ПРОТОКОЛ MATRIX ТА ЙОГО МЕТОДИ ШИФРУВАННЯ

Matrix – це відкритий децентралізований протокол та програмне забезпечення, призначене для обміну повідомленнями, передачі даних і голосової комунікації в режимі реального часу. Його архітектура базується на моделі федеративної мережі, що дозволяє користувачам різних серверів обмінюватися інформацією без централізованого посередника. При цьому, головною метою є забезпечення приватності повідомлень та надійності при зваємодії між різними комунікаційними платформами. Завдяки відкритій архітектурі, користувачі мають змогу самостійно хостити сервера та створювати автономні мережі, не прив’язані до центрального сервера чи конкретного постачальника [1, 2].

Головною перевагою Matrix є наскрізне шифрування (E2EE), яке забезпечує конфіденційність переданих даних. Це означає, що доступ до даних має тільки відправник та отримувач. Основні протоколи шифрування це криптографічні бібліотеки Olm та Megolm, які гарантують безпеку як для індивідуальних, так і для групових чатів.

Olm – це криптографічна бібліотека, розроблена для забезпечення

наскрізного шифрування в децентралізованому протоколі Matrix. Вона створена за зразком протоколу Signal і реалізує механізм Double Ratchet, що забезпечує високу ступінь конфіденційності завдяки властивості прямої секретності – кожне нове повідомлення шифрується унікальним ключем, який недоступний навіть у разі компрометації попередніх ключів.

У криптографічній основі Olm використовуються наступні алгоритми: еліптична крива (Curve25519) – для асиметричного обміну ключами; AES-256 (у режимі CBC) – для симетричного шифрування вмісту повідомлень; SHA-256 – для хешування та перевірки цілісності.

Ця комбінація забезпечує три базові властивості інформаційної безпеки [3]:

1. Конфіденційність, завдяки шифруванню повідомлень таким чином, що їх можуть прочитати лише учасники розмови.

2. Цілісність, гарантія того, що дані не були змінені або пошкоджені під час передачі.

3. Автентичність, підтвердження справжності джерела повідомлення і захист від атак типу «людина посередині» (Man-in-the-Middle).

Таким чином, Olm є ключовим компонентом безпечної цифрової комунікації, який поєднує сучасні криптографічні технології з децентралізованою архітектурою, забезпечуючи високий рівень захисту користувацьких даних.

Megolm – це криптографічний протокол, розроблений як оптимізована версія Olm для забезпечення наскрізного шифрування в групових чатах системи Matrix [4]. На відміну від Olm, який реалізує механізм Double Ratchet для захисту приватних розмов, Megolm використовує симетричне шифрування з попередньо згенерованим ключем сеансу. Це дозволяє ефективно шифрувати повідомлення у великих чатах без значного навантаження на обчислювальні ресурси. Хоча Megolm не забезпечує повної прямої секретності, він гарантує достатній рівень захисту конфіденційності, цілісності та автентичності даних завдяки використанню сучасних криптографічних алгоритмів, таких як AES для шифрування та HMAC для перевірки цілісності.

Таким чином, Megolm доповнює Olm у загальній архітектурі Matrix, забезпечуючи баланс між продуктивністю та безпекою в умовах багатокористувацького спілкування.

Крім наскрізного шифрування, Matrix підтримує автентифікацію користувачів, перевірку ключів вручну або через QR-коди, а також федеративну структуру. Це дає змогу надсилати повідомлення між різними приватними доменами користувачів та іншими месенджерами.

Популярність протоколу Matrix постійно зростає у світі завдяки його відкритості, гнучкості та прозорості. Його впроваджують державні органи, військові структури, IT-компанії та користувачі що піклуються про свою приватність. Наприклад, уряд Франції створив на базі протоколу власний

мессенджер Tchap, а Німеччина використовує Matrix у державному секторі [5].

Отже, протокол Matrix є потужним інструментом для захищеного спілкування в умовах постійно зростаючих кіберзагроз. Його методи шифрування відповідають сучасним вимогам до конфіденційності та стійкості до атак, що його робить його перспективним стандартом у сфері в безпечних мессенджерів.

Література:

1. Живило Є.О. Тестування на проникнення: навч. посіб. Ч.1 / Є.О. Живило; за ред. Є.О. Живило. – Полтава: ПНТУ «Полтавська політехніка ім. Юрія Кондратюка», 2024. – 134 с.

2. Живило Є.О. Тестування на проникнення: навч. посіб. / Є.О. Живило; за ред. Є.О. Живило. – Полтава: ПНТУ «Полтавська політехніка ім. Юрія Кондратюка», 2024. – 239 с.

3. Довжиков О. Penetration Testing Learning / О. Довжиков. – \[Електронний ресурс]. – Режим доступу: https://dou.ua/lenta/articles/penetration-testing-learning/. – Дата звернення: 08.05.2025.

4. Що таке тестування на проникнення? / \[Електронний ресурс]. – Режим доступу: https://datami.ee/ua/blog/what-is-penetration-testing/. – Дата звернення: 08.05.2025.

5. Тестування на проникнення: від А до Я / \[Електронний ресурс]. – Режим доступу: https://kr-labs.com.ua/blog/testuvannya-na-pronyknennya-pentest-vid-a-do-ya/. – Дата звернення: 08.05.2025.

УДК 004.492.2

Т.М. Фесенко, к.т.н., доцент
Ю.П. Топчій, студент групи 201 КБ
Л. Ю. Копійка студент групи 201 КБ
Національний університет
«Полтавська політехніка імені Юрія Кондратюка»

ТЕСТУВАННЯ НА ПРОНИКНЕННЯ ЯК ІНСТРУМЕНТ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ: МЕТОДОЛОГІЯ, ІНСТРУМЕНТИ, РОЗВИТОК

У сучасному цифровому середовищі, де зростає кількість кіберзагроз, забезпечення інформаційної безпеки стає пріоритетним завданням для організацій усіх рівнів. Одним із найефективніших методів оцінки та зміцнення захищеності інформаційних систем є тестування на