доступу до ресурсів (Web APIs). Access Token містить інформацію про клієнта і користувача, якщо вона наявна. Важливо розуміти, що є такі типи авторизації, в процесі яких користувач безпосередньої участі не бере (докладніше про це в наступній частині).

- Refresh Token (токен поновлення) – токен, за яким STS поверне новий Access Token. Залежно від режиму роботи, Refresh Token може бути багаторазовим і одноразовим. У випадку з одноразовим токеном, при запиті нового Access Token буде також сформований готовий Refresh Token, який слід використовувати при повторному оновленні. Очевидно, що одноразові токени більш безпечні.

При зверненні користувача до клієнта, той перенаправляє користувача на Open ID Connect Provider, який запитує у користувача логін і пароль. У разі успішного проходження перевірки параметрів аутентифікації він повертає назад identity toen і access token, з якими користувач може звертатися до захищеного ресурсу.

У реалізації OAuth2 використовується так званий jwt-токен, який складається з трьох частин. Припустимо, при зверненні до Identity provider ви відправляєте логін / пароль і у відповідь отримуєте токен. Він буде включати в себе: header (заголовок), payload (контент) і signature (підпис). На сайті jwt.io його можна декодувати і подивитися вміст у форматі JSON. На цьому сайті ви знайдете опис правил формування jwt-токенів.

Використання систем ідентифікації є важливим для будь-якої програми з різною архітектурою та потребує обґрунтування з урахуванням можливості підтримки її окремих блоків реалізації, масштабування та підтримки безпеки. Вивчення даних технологій дозволить розробникам здійснювати правильний вибір технологій безпеки та реалізовувати їх у власних проєктах.

Список використаних джерел:

1 Carnell J. Spring Microservices in Action / John Carnell., 2017. – 384 с.
2 Fowler M. Microservices. a definition of this new architectural term [Електронний ресурс] / Martin Fowler. – 2014. – Режим доступу до ресурсу: https://martinfowler.com/articles/microservices.html
3 Сабанов Алексей. Обзор технологий идентификации и аутентификации Режим доступу до ресурсу: https://www.aladdin-rd.ru/company/pressroom/articles/obzor_tehnologij_identifikacii_i_autentifikacii
4 Ресурс JWT – https://jwt.io.

Науковий керівник: Лозовик Ю. М.к.е.н., доцент

Панфілов Є. В.
Східноукраїнський національний університет імені Володимира Даля
panfilov.iflp@gmail.com

ЧАТ-БОТ ДЛЯ МЕСЕНДЖЕРА

Боти – це спеціальні програми, що виконують різні функції та спрощують життя їх користувачів. Написані для платформи Telegram, вони призначені для виконання самих різних функцій: від отримання новин до пошуку інформації та навіть торгівлі акціями. Головне завданням бота є автоматична відповідь після введеної йому користувачем команди. При цьому, працюючи безпосередньо через інтерфейс Telegram, програма імітує дії живого користувача, внаслідок чого користування таким ботом набагато зручно і зрозуміло.

Після бурхливих обговорень в IT-пресі з приводу ефективності чат-ботів, вони зайняли свою нішу в екосистемі користувачів і компаній. Наприклад, часто проєкти впроваджують ботів для оповіщення про будь-які події, а служби підтримки використовують їх для того, щоб швидко відповідати на запитання й відповіді клієнтів.

Алгоритм роботи бот-утиліт досить простий. Повідомлення, команди та запити, надіслані користувачами, передаються на програмне забезпечення, запущене на серверах

розробників. Посередницький анонімний сервер Telegram обробляє шифрування і здійснює зворотний зв’язок між утилітою і користувачем.

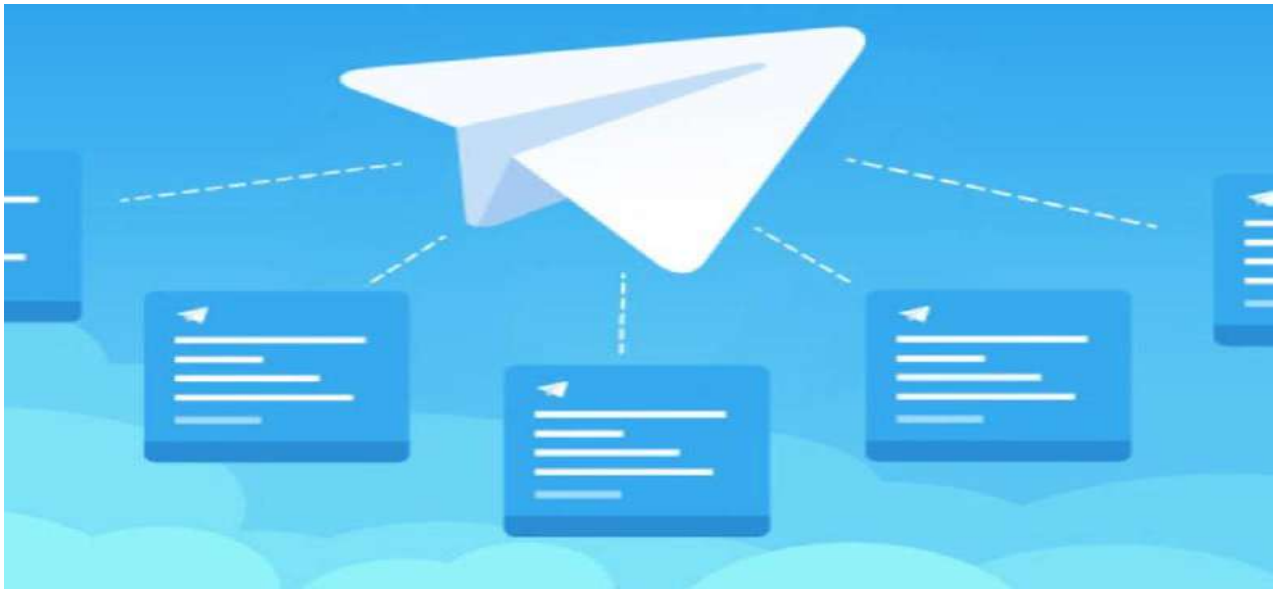

Рисунок 1 – Telegram та його боти

Науковий керівник: Іванов В. Г., к.т.н., доцент.