УДК 004.056.53

# ЗАСОБИ КОНТРОЛЮ БЕЗПЕКИ ОБЛІКОВИХ ЗАПИСІВ КОРИСТУВАЧІВ У СОЦІАЛЬНИХ МЕРЕЖАХ

**Пастух Я.Т.**
*Тернопільська Українська гімназія ім. І. Франка, учень*

## I. Вступ

Сьогодні кількість активних користувачів соціальних мереж наближається до 15 млрд [1]. Практично кожен користувач мережі Інтернет має, як мінімум, один профіль в соціальній мережі. Разом з тим, переважна більшість користувачів недооцінюють ризики інформаційної безпеки у соціальних мережах. Підтвердженням цього факту є масові повідомлення про злами та витік даних із облікових записів користувачів соціальних мереж [2-4]. Як правило, причиною цих інцидентів є незнання наявних засобів щодо контролю безпеки облікових записів, які реалізовані розробниками соціальних мереж. Також існує ряд рекомендованих та нереалізованих засобів, які суттєво впливають на рівень безпеки облікових записів.

Тому, актуальним є завдання аналізу відомих засобів контролю безпеки у популярних соціальних мережах. Отримані результати дозволять підвищити рівень безпеки облікових записів користувачів у соціальних мережах.

## II. Мета роботи

Метою роботи є аналіз відомих засобів контролю безпеки у популярних соціальних мережах.

## II. Аналіз засобів контролю безпеки у соціальних мережах

Безпека облікових записів користувачів соціальних мереж є взаємозв'язаною сукупністю засобів контролю безпеки, які реалізовані на стороні сервера соціальної мережі та ряду додаткових контролів, які необхідно періодично перевіряти/налаштовувати користувачу.

У роботі виділено наступні засоби контролю безпеки облікових записів користувачів у соціальних мережах:

- двоетапна перевірка – засіб контролю, який пропонує додатковий рівень безпеки для облікового запису користувача у соціальні мережі.
- приватний обліковий запис – засіб контролю, який дозволяє підвищити рівень конфіденційності облікового запису користувача у соціальні мережі.
- сповіщення про безпеку та конфіденційність – засіб контролю, який дозволяє сповістити користувача соціальної мережі про ймовірні порушення безпеки чи конфіденційності.
- перевірка авторизованих входів – засіб контролю, який дозволяє перевірити авторизовані входи та пристрої до облікового запису користувача соціальної мережі.
- формування довірених контактів – засіб контролю, який дозволяє внести в список кілька «друзів», які в разі порушення безпеки облікового запису стають поручителями для відновлення доступу.
- генерування кодів ідентифікації – засіб контролю, який дозволяє згенерувати коди ідентифікації, які можуть бути використані для двоетапної перевірки.
- підключення зовнішніх ключів безпеки - засіб контролю, який дозволяє використовувати зовнішні носії для зберігання ключів доступу до облікового запису користувача у соціальній мережі.
- перевірка складності пароля – засіб контролю, який дозволяє оцінити складність створеного користувачем пароля.
- перевірка витоків пароля – засіб контролю, який дозволяє оцінити пароль на предмет його витоку. Для перевірки витоків пароля можна скористатись інтернет-сервісом https://haveibeenpwned.com/. Пароль рекомендується змінити, якщо він є у базі даних зазначеного інтернет-сервісу.
- перевірка витоків даних для адреси електронної скриньки – засіб контролю, який дозволяє оцінити витоки пов'язані із адресою електронної поштової скриньки до якої прив'язаний обліковий запис користувача соціальної мережі. Для перевірки витоків даних для адреси

електронної скриньки можна скористатись інтернет-сервісом https://haveibeenpwned.com/. У випадку витоку даних для адреси поштової скриньки рекомендується її змінити.

- створення складного пароля – засіб контролю, який дозволяє автоматично згенерувати складний пароль для входу до облікового запису користувача у соціальній мережі. Для створення складного паролю можна скористатись інтернет-сервісом https://strongpasswordgenerator.com/.
- регулярна зміна паролю – засіб контролю, який нагадує користувачу соціальної мережі про необхідність регулярної зміни паролю відповідно до прийнятої парольної політики безпеки.
- перевірка доступу зовнішніх застосунків до облікового запису – засіб контролю, який дозволяє перевірити доступ зовнішніх застосунків до інформації із облікового запису користувача соціальної мережі.

Для аналізу засобів контролю безпеки, обрано найбільш популярні на сьогоднішній день соціальні мережі: Facebook, YouTube, Instagram.

Результати порівняльного аналізу засобів контролю безпеки облікових записів користувачів у соціальних мережах подано в таблиці 1.

Таблиця 1

Порівняльний аналіз засобів контролю безпеки облікових записів у соціальних мережах

| Засоби контролю безпеки | Реалізація у соціальній мережі | | |
|---|---|---|---|
| | Facebook | YouTube | Instagram |
| Двоетапна перевірка | + | + | + |
| Приватний обліковий запис | + | + | + |
| Сповіщення про безпеку та конфіденційність | + | + | - |
| Перевірка авторизованих входів | + | + | - |
| Формування довірених контактів | + | - | - |
| Генерування кодів ідентифікації | + | + | - |
| Підключення зовнішніх ключів безпеки | + | - | - |
| Перевірка складності пароля | + | + | - |
| Перевірка витоків пароля | - | - | - |
| Перевірка витоків даних для адреси електронної скриньки | - | - | - |
| Створення складного пароля | - | - | - |
| Регулярна зміна паролю | - | - | - |
| Перевірка доступу зовнішніх застосунків до облікового запису | + | + | - |

Аналіз табл. 1 показує, що жодна із соціальних мереж не має комплексного механізму захисту облікових записів, який би дозволив користувачу в автоматичному режимі перевірити та налаштувати засоби контролю безпеки облікових записів.

## III. Висновки

В рамках даної роботи виділено засоби контролю безпеки облікових записів користувачів у соціальних мережах Facebook, YouTube та Instagram. Проведено порівняльний аналіз виділених засобів, який дозволив встановити, що жодна із соціальних мереж не має комплексного механізму захисту облікових записів, який би дозволив користувачу в автоматичному режимі перевірити та налаштувати засоби контролю безпеки облікових записів.

Отримані результати планується використати при розробці математичного та програмного забезпечення для підвищення рівня безпеки персональних сторінок користувачів у соціальних мережах.

## Список використаних джерел


1. Most popular social networks worldwide as of October 2018, ranked by number of active users [Електронний ресурс]. Режим доступу – https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/.
2. До 50 млн акаунтів в Facebook зламані невідомими хакерами [Електронний ресурс] Режим доступу – https://znaj.ua/techno/176920-pid-zagrozoyu-50-mln-koristuvachiv-facebook-poperediv-pro-strashnu-nebezpeku.
3. Хакеры взломали тысячи каналов на Youtube [Електронний ресурс] Режим доступу – https://air.io/youtube/xakery-vzlomali-tysyachi-kanalov-na-youtube.
4. Up to six million Instagram accounts affected by data breach [Електронний ресурс] Режим доступу – https://thestack.com/security/2017/09/04/up-to-six-million-instagram-accounts-affected-by-data-breach/.