6. Ступак О. Т. Інформаційно-цифрова компетентність як складова освітнього процесу сучасної школи. *Сучасні аспекти модернізації науки: стан, проблеми, тенденції розвитку :* матеріали XXIII-ої Міжнар. науково-практ. конф. (7 серп. 2022 р., м. Дікірх). С. 220–224.
7. Тітова Л. О. Онлайн-засоби формування інформаційно-цифрової компетентності майбутніх педагогів в умовах дистанційного навчання. *Věda a perspektivy*. 2022. № 5(12). С. 132–143.
8. Тітова Л. О., Ковтанюк М. С., Ямковенко В. О. Цифрові засоби розвитку медіаграмотності здобувачів освіти. *Українські студії в європейському контексті.* 2024. № 8. С. 305–311.
9. Ткачук Г. В., Медведєва М. О. ІКТ як засіб формування інформаційно-цифрової компетентності студентів педагогічних університетів. *Молодь і ринок.* 2023. № 1/209. С. 74–80.

Мірошниченко М.Ю.
кандидат технічних наук, доцент,
доцент кафедри комп'ютерних наук
Таврійський державний агротехнологічний університет
імені Дмитра Моторного

АЛГОРИТМ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ В СОЦІАЛЬНИХ МЕРЕЖАХ

Анотація*. З розвитком соціальних мереж зростає кількість персональних даних, що стають доступними для третіх осіб. Сучасні платформи, такі як Facebook, Instagram обробляють мільйони даних щоденно, що створює серйозні виклики для захисту приватності користувачів. Ця стаття аналізує існуючі методи захисту даних у соціальних мережах та пропонує використовувати алгоритм, який включає комбінацію криптографічних методів, багатоетапну автентифікацію та аналіз поведінки для забезпечення захисту персональної інформації.*

Ключові слова: *персональні дані, захист даних, соціальні мережі, алгоритм, шифрування.*

Miroshnichenko M. Algorithm for protection of personal data in social networks*. With the development of social networks, the amount of personal data that becomes available to third parties is increasing. Modern platforms such as Facebook, Instagram process millions of data every day, which creates serious challenges for protecting user privacy. This article analyzes the existing methods of data protection in social networks and proposes to use an algorithm that includes a combination of cryptographic methods, multi-step authentication and behavior analysis to ensure the protection of personal information.*

Key words*: personal data, data protection, social networks, algorithm, encryption.*

Актуальність. Соціальні мережі, такі як Facebook, Instagram, TikTok та інші, вже давно стали невід'ємною частиною нашого повсякденного життя [2, с. 388]. Вони функціонують як універсальні платформи для комунікації, обміну інформацією та створення соціальних зв'язків на основі використання технології Web 2.0 [10, с. 28]. Користувачі активно діляться своїми думками, фотографіями, відео, місцезнаходженням та іншими особистими даними, створюючи величезний масив інформації, яка стає доступною для різних категорій користувачів. Водночас, персональна інформація може потрапити до сторонніх осів та може бути неправомірно використана. Зважаючи на це, виникає потреба в алгоритмах, що могли б ефективно захищати персональні дані в соціальних мережах від несанкціонованого доступу.

Метою статті є аналіз причин втрати персональної інформації в соціальних мережах, висвітлення існуючих методів захисту даних у соціальних мережах.

Виклад основного матеріалу. Соціальні мережі перетворилися на глобальні платформи для обміну інформацією, що призводить до зберігання великих обсягів особистих даних, у тому числі персональної інформації, що включає дані про контакти, інтереси користувачів тощо. Окрім базової інформації про ім'я, вік, стать та місцезнаходження, соціальні мережі аналізують інтереси, перегляди контенту, взаємодії з іншими користувачами та навіть моделі поведінки в Інтернеті.

Така інформація є не просто індивідуальними даними кожного користувача, а цінним ресурсом для рекламодавців, аналітичних

компаній і навіть державних установ. Через це обсяги інформації, яку соціальні мережі збирають, обробляють та зберігають, зростають неймовірними темпами. Така інформація дає змогу створювати профілі користувачів з високим рівнем деталізації, що підвищує ефективність таргетованої реклами.

На жаль, конфіденційні дані часто стають мішенню кіберзлочинців. І це не є новиною, адже поряд з можливістю вільного доступу до інформації, розташованої в мережі Інтернет, збільшились ризики втрати персональної інформації сторонніми особами [8, с. 347]. Вразливість користувацьких даних стає значним питанням, оскільки кіберзлочинці можуть використовувати ці дані для шантажу, фішингу, крадіжки особистості та інших видів шахрайства. До прикладу, інформація про місцезнаходження дозволяє відстежувати переміщення користувачів, що може становити ризик для їхньої фізичної безпеки, особливо якщо така інформація стає доступною в режимі реального часу. Персоналізована інформація може бути використана для негативних інформаційних впливів на особисту думку користувачів [3, с. 82]. Особисті контакти та інформація про соціальне оточення можуть бути використані для проведення атак соціальної інженерії, коли зловмисники маніпулюють користувачем, аби отримати доступ до ще більшого обсягу конфіденційної інформації.

У таких умовах особливо важливо впроваджувати алгоритми, що можуть ефективно захищати дані користувачів від несанкціонованого доступу, використання та розповсюдження. Такі алгоритми повинні поєднувати сучасні технології шифрування для захисту даних під час зберігання і передачі, багатофакторну автентифікацію для забезпечення надійного доступу та інноваційні підходи для виявлення та запобігання кібератак. Наприклад, аналітичні алгоритми та машинне навчання можуть використовуватися для виявлення аномальної активності в облікових записах, що дозволяє оперативно реагувати на можливі загрози.

Існує декілька підходів, що вже використовуються для захисту персональних даних у соціальних мережах: шифрування даних, автентифікація користувачів, аналіз поведінки. Більшість платформ використовує алгоритми шифрування, такі як AES [9, с. 88] та RSA [4, с. 90], для зберігання особистих даних у зашифрованому вигляді. Це робить

інформацію недоступною для сторонніх осіб без відповідного ключа. Соціальні мережі застосовують двофакторну або багатоетапну автентифікацію, яка підвищує рівень безпеки. Наприклад, під час входу користувача платформи запитують одноразовий пароль, що відправляється на телефон. Деякі соціальні мережі, такі як Facebook, використовують машинне навчання для більш глибокого розуміння користувачів [7, с. 132] та відстеження підозрілої активності, аналізуючи, наприклад, з якого пристрою чи географічного місця виконується вхід.

Попри всі переваги, існуючі підходи не є ідеальними. Наприклад, шифрування даних забезпечує безпеку лише на етапі зберігання, але не захищає від витоків, що можуть статися в процесі передачі. Автентифікація може бути зламаною, зокрема, за допомогою методів соціальної інженерії. Аналіз поведінки має обмеження у відстеженні складних атак, наприклад, з використанням VPN чи анонімайзерів.

Для підвищення рівня захисту персональних даних пропонується комбінований алгоритм, який включає такі етапи: модуль шифрування з використанням гібридного підходу, трьохетапна автентифікація, аналіз поведінки та машинне навчання, інтеграція блокчейну для децентралізації зберігання. Слід зазначити, що мультифакторна автентифікація вважається ключовим елементом кібербезпеки, що знаходить широке застосування в електронній комерції, банківській сфері, корпоративних мережах, де захист даних є критичним. Цей метод вимагає від користувачів підтвердження своєї особи не тільки через стандартний спосіб (логін та пароль), але й за допомогою додаткових факторів ідентифікації користувача [6, с 301].

Модуль шифрування з використанням гібридного підходу передбачає поєднання симетричного та асиметричного шифрування (AES та RSA) підвищує безпеку як при зберіганні, так і при передачі даних. Наприклад, симетричне шифрування за стандартом AES забезпечує швидку та ефективну обробку даних, а асиметричне шифрування RSA використовується для надійного обміну ключами. Такий гібридний підхід знижує ризик компрометації даних на етапах як зберігання, так і передачі, забезпечуючи їхню конфіденційність і цілісність.

Трьохетапна автентифікація пропонує використовувати персональну інформацію, яка включає: пароль, одноразовий код,

біометричні дані (відбитки пальців або розпізнавання обличчя). Ця комбінація мінімізує ризик несанкціонованого доступу навіть у випадках компрометації одного з рівнів захисту, забезпечуючи високу надійність підтвердження особи користувача.

Аналіз поведінки та машинне навчання дозволяє забезпечити побудову поведінкових моделей на основі попередніх дій користувача. Наприклад, алгоритм аналізує звичну модель поведінки користувача, включаючи параметри, такі як географічне розташування, час активності, використовувані пристрої тощо. У разі виявлення значних відхилень від звичайної поведінки система може автоматично призупинити доступ до облікового запису або вимагати додаткову автентифікацію, що знижує ризики несанкціонованого проникнення.

Використання блокчейну для розподіленого зберігання особистих даних підвищить їхню безпеку. Блокчейн може забезпечити прозорість і контроль доступу до інформації, дозволяючи користувачам керувати своїми даними незалежно від централізованих серверів [1, с. 163].

Слід зазначити, що несанкціоноване втручання у роботу соціальних мереж, у тому числі кібератаки, є одним з напрямків злочинних дій з боку хакерів та шахраїв. Значна увага приділяється захисту інформаційних систем [5, с. 121], у тому числі онлайн сервісів, що забезпечують роботу підприємств, державний установ тощо. В цьому контексті захищена інформаційна система повинна мати механізми захисту від зовнішніх та внутрішніх загроз, використовувати шифрування даних та трьохфакторну аутентифікацію тощо.

Висновки. Комбінований алгоритм захисту персональних даних для соціальних мереж є відповіддю на зростаючі загрози безпеці, з якими стикаються користувачі сучасних платформ. Алгоритм спрямований на інтеграцію кількох передових технологій для досягнення комплексного захисту конфіденційної інформації. Поєднання новітніх методів шифрування, багатоетапної автентифікації, аналізу поведінки користувачів та блокчейн-технологій дозволяє ефективно захищати особисті дані як на етапі зберігання, так і при передачі.

Представлений алгоритм забезпечує не тільки захист від зломів і несанкціонованого доступу, але й формує високий рівень прозорості та контролю користувачем своїх даних. Комплексний захист, що включає багатофакторну автентифікацію, шифрування та блокчейн, дозволяє

створити стійку до атак систему, що адаптується до нових загроз і потреб користувачів у захисті персональної інформації.

Література

1. Андрущак І. Є., Кошелюк В. А. Особливості захисту хмарного середовища на основі blockchain. *The 10 th International scientific and practical conference "Science, innovations and education: problems and prospects"* (May 4-6, 2022, Tokyo, Japan). 2022. С. 161–167.
2. Гаврилюк О. Статистика і тенденції функціонування соціальних мереж. *Цифрова платформа: інформаційні технології в соціокультурній сфері*. 2023. № 2(6). С. 383–397.
3. Колмакова В. О., Шаров С. В. Використання МВОК для формування імунітету від інформаційних загроз. *Українські студії в європейському контексті*. 2023. № 6. С. 80–87.
4. Коробейнікова Т. І., Копач А. І. Сучасні алгоритми шифрування: детальний аналіз та перспективи розвитку. *SWorldJournal*. 2024. № 25-01. С. 89–95.
5. Мірошниченко М. Ю. До проблеми захисту інформаційних систем. *Сучасний стан та перспективи розвитку електротехнічних систем: матеріали IV Всеукр. наук.-практ. інтернет-конференції пам'яті В.В. Овчарова* (04-18 листопада 2021 р., м. Мелітополь). 2021. С. 120–122.
6. Назаров Є.М. Захист на рівні додатків: сучасні виклики та технології. *Українські студії в європейському контексті*. 2023. №7. С. 300–307.
7. Проскурніна Н. В. Штучний інтелект у маркетинговій діяльності. Зовнішня торгівля: економіка, фінанси, право. 2020. № 4. С. 129–140.
8. Сергієнко Т. І. Роль інформаційних технологій у житті сучасної людини. *Українські студії в європейському контексті*. 2023. №7. С. 344–349.
9. Шаповал І. В., Лебедев Д. Ю. Алгоритм роботи пристрою AES шифратора. *Problems of Informatization and Management*. 2016. № 53(1). С. 87–91.
10. Sharov S., Rassokha I. Specific features of using Web 2.0 technology in the educational process. *Вісник Черкаського національного університету імені Богдана Хмельницького*. Серія: Педагогічні науки. 2022. № 3. С. 26–33.