КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 3 (27), 2025
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2025.27.734
УДК 004.738.8

Прокопович-Ткаченко Дмитро Ігорович
кандидат технічних наук, доцент, з
авідувач кафедри кібербезпеки та інформаційних технологій
Університет митної справи та фінансів, Дніпро, Україна
ORCID ID: 0000-0002-6590-3898
omega2417@gmail.com

Звєрєв Володимир Павлович
кандидат технічних наук, старший науковий співробітник,
доцент кафедри інженерії програмного забезпечення та кібербезпеки
Державний торговельно-економічний університет, Київ, Україна
ORCID ID: 0000-0002-0907-0705
zvieriev_vp@knute.edu.ua

Бушков Валерій Генадійович
аспірант кафедри інженерії програмного забезпечення та кібербезпеки
Державний торговельно-економічний університет, Київ, Україна
ORCID ID: 0009-0005-5097-2689

Хрушков Борис Сергійович
аспірант кафедри кібербезпеки та інформаційних технологій
Університет митної справи та фінансів, Дніпро, Україна
ORCID ID: 0009-0002-3978-5012

ФІШИНГОВІ АТАКИ НА ЗАШИФРОВАНІ МЕСЕНДЖЕРИ: МЕТОДИ, РИЗИКИ ТА РЕКОМЕНДАЦІЇ ЗАХИСТУ (НА ПРИКЛАДІ МЕСЕНДЖЕРА SIGNAL)

Анотація. У даній статті проаналізовано методи фішингових атак, що становлять серйозну загрозу для зашифрованих мобільних месенджерів, зокрема Signal. Особливу увагу приділено новітнім технікам, які застосовують російські хакери, пов'язані з ГРУ РФ, із використанням підроблених QR-кодів. Продемонстровано, яким чином зловмисники можуть несанкціоновано прив'язувати додаткові пристрої до облікових записів, здобуваючи можливість відстежувати комунікацію користувачів у режимі реального часу. Досліджено ефективність різних заходів безпеки, включно з оновленнями безпеки від розробників Signal, двофакторною автентифікацією, застосуванням комплексного захисту операційних систем та використанням інструментів на зразок Google Play Protect. Наведені результати дозволяють дійти висновків про необхідність підвищеної уваги до верифікації QR-кодів та постійної перевірки списку прив'язаних пристроїв. Практичні рекомендації, запропоновані в цій роботі, спрямовано на зниження ризику компрометації облікових записів, захист конфіденційної інформації та підвищення загального рівня кібербезпеки користувачів. Представлено також перспективи удосконалення системи безпеки месенджерів, які можуть бути корисними для розробників, державних органів та фахівців з інформаційної безпеки. Додатково розглянуто потенційні виклики, пов'язані з інтеграцією новітніх технологій безпеки, а також можливості адаптації традиційних підходів до сучасних кіберзагроз. Таким чином, проведене дослідження робить вагомий внесок у формування сучасної методології протидії фішинговим атакам, визначає напрями подальших робіт у галузі розробки та впровадження захисних технологій для мобільних платформ, що гарантуватимуть вищий рівень приватності та безпеки користувачів у цифровому середовищі.

Ключові слова: кібербезпека; фішинг; зашифровані месенджери; Signal; прив'язка пристроїв; QR-коди; двофакторна автентифікація; захист даних.

ВСТУП

Сучасний розвиток засобів цифрової комунікації значно змінює парадигму інформаційної безпеки. Зашифровані месенджери, такі як Signal, Telegram, WhatsApp, стають основним інструментом обміну повідомленнями завдяки високому рівню конфіденційності та зручності користування. Проте, навіть найбільш захищені платформи не є повністю убезпеченими від кібератак, що використовують соціальну інженерію, шкідливе програмне забезпечення та, зокрема, фішинг.

Актуальність проблеми зумовлена тим, що фішингові атаки — один із найпоширеніших методів компрометації облікових записів та отримання доступу до конфіденційних даних. Під впливом активного розвитку технологій фішингові сценарії набули нових форм, пов’язаних з мобільними пристроями та застосунками для безпечного обміну повідомленнями. Зокрема, використанням підроблених QR-кодів зловмисники можуть перехоплювати комунікацію в реальному часі, отримувати контроль над обліковим записом жертви та розширювати спектр кібератак, включно з поширенням шкідливого програмного забезпечення.

Постановка проблеми. У сучасному інформаційному середовищі кібербезпека набуває все більшої актуальності через стрімкий розвиток технологій та зростання кількості кібератак. Однією з найнебезпечніших загроз є фішингові атаки, спрямовані на зашифровані мобенджери, зокрема Signal, який користується великою популярністю завдяки високому рівню конфіденційності. Проблема полягає у використанні зловмисниками новітніх методів соціальної інженерії, таких як підроблені QR-коди, що дозволяють несанкціоновано прив’язувати додаткові пристрої до облікових записів. Це створює серйозні ризики для збереження конфіденційної інформації користувачів та порушує основні принципи безпеки цифрового простору. Проблематика даного дослідження має безпосередній зв’язок з важливими науковими та практичними завданнями, серед яких розробка ефективних методів захисту інформації, вдосконалення систем аутентифікації та зниження ризику компрометації даних [10]. Врахування людського чинника, що часто стає слабким місцем у системах безпеки, також є важливим аспектом, оскільки незнання або необережність користувачів може стати вирішальним фактором успіху фішингової атаки [3, с. 35].

Аналіз останніх досліджень і публікацій. Огляд сучасних наукових робіт показує, що проблема фішингових атак у мобільних додатках привертає значну увагу дослідників. Ранні роботи [3] – [6] висвітлювали загальні підходи до протидії електронному викраденню особистих даних, однак новітні публікації зосереджують увагу на специфіці атак через зашифровані канали зв’язку, зокрема в Signal. Автори [4] зазначають, що традиційні методи безпеки часто не враховують нюанси соціальної інженерії, яка застосовується для обходу технічних заходів. Більш детальний аналіз, проведений у дослідженнях [5] та [6], демонструє, що використання підроблених QR-кодів стає все більш популярним інструментом для компрометації мобільних месенджерів, що вимагає розробки нових методологій захисту. Незважаючи на успішні результати попередніх досліджень, залишається кілька невирішених питань, зокрема — визначення оптимальних алгоритмів верифікації підключених пристроїв та інтеграція мультифакторної автентифікації для мінімізації ризиків [3] – [6]. Ці аспекти стають основою для подальших досліджень, що мають на меті розробку комплексних систем безпеки, здатних ефективно протидіяти новітнім формам фішингу.

Мета статті полягає у вивченні технічних і соціальних аспектів фішингових атак на прикладі месенджера Signal, аналізі можливостей компрометації облікових записів через механізм прив'язки додаткових пристроїв та розробці рекомендацій для підвищення рівня безпеки користувачів. Основними завданнями є:

- розглянути наявні у літературі та звітах методи фішингу, що застосовуються проти зашифрованих месенджерів;
- проаналізувати сценарій атаки із використанням підроблених QR-кодів для Signal;
- запропонувати практичні рекомендації для користувачів та розробників з метою мінімізації ризиків компрометації.

Наукова новизна отриманих результатів полягає у деталізації механізму фішингових дій щодо функції прив'язки додаткових пристроїв у Signal та формуванні цілісного підходу до захисту від таких атак. Практична цінність роботи полягає в інтегрованому описі кроків захисту, застосовних не лише до Signal, а й інших зашифрованих месенджерів і мобільних додатків.

МЕТОДИКА ДОСЛІДЖЕННЯ

Дослідження проведено з урахуванням сучасних підходів у галузі кібербезпеки, що базуються на системному аналізі, методах експериментального моделювання та емпіричному зборі даних про фішингові кампанії. У межах роботи було виокремлено кілька методологічних аспектів.

Алгоритмічний аналіз вразливостей

Для виявлення та опису характерних ознак фішингових атак на зашифровані месенджери застосовувався алгоритмічний аналіз:

- Оцінювалися основні процедури автентифікації та шифрування повідомлень, що реалізовані в протоколі Signal Protocol.
- Виокремлювалися вразливі точки, зокрема механізм прив'язки додаткових пристроїв та автентифікація через QR-код.
- Порівнювалися результати аналізу з аналогічними результатами для месенджерів Telegram і WhatsApp.

Аналіз здійснювався за допомогою тестових сценаріїв, що імітують дії потенційного зловмисника: завантаження підробленого зображення QR-коду, звернення до фішингового веб-сервера та інші дії соціальної інженерії.

Моделювання атак

Щоб оцінити реальні ризики та ймовірність успішної компрометації, застосовано моделювання різних сценаріїв. Формалізуємо ймовірність успішної атаки як:

$$P_{attack} = P_{phish} \times P_{malware} \times P_{human\_error}, \quad (1)$$

де P_{phish} — ймовірність успішного фішингового впливу (тобто, що користувач просканує підроблений QR-код або перейде за шкідливим посиланням);

$P_{malware}$ — імовірність успішного встановлення чи запуску шкідливого програмного коду (експлойтів, троянів тощо);

P_{human_error} — показник людського чинника, що відображає необережність чи брак знань у користувача.

Для кращої оцінки факторів ризику використовувалася низка емпіричних даних, зібраних із публічних звітів компаній-розробників антивірусного ПЗ, а також з академічних джерел. Крім того, передбачалася кореляція між цими складовими: наприклад, при високій ймовірності людської помилки (P_{human_error}) одночасно зростає ризик фішингових дій.

Статистичний аналіз даних безпеки

Дослідження також включало статистичний аналіз:

$$\Delta R_i = R_{i,\ захищ} - R_{i,\ базов}, \quad (2)$$

де $R_{i,\ захищ}$ — залишковий ризик після застосування захисних заходів;

$R_{i,\ базов}$ — базовий ризик без додаткових засобів безпеки;

ΔR_i — ефект (зниження або підвищення) рівня ризику для і-го сценарію атаки.

Згідно з отриманими даними, впровадження двофакторної автентифікації може зменшувати вірогідність успішного фішингу на 30–40%, а регулярна перевірка прив'язаних пристроїв у обліковому записі здатна знизити успішність атаки ще на 10–15%.

Вибірка даних і параметри дослідження

Для комплексного аналізу було сформовано тестову вибірку з різних сценаріїв, що охоплюють:

- атаки на новостворені акаунти Signal;
- атаки на акаунти користувачів, які нехтують оновленнями безпеки;
- атаки з використанням зламаних APK-файлів або підроблених веб-версій Signal.

У табл. 1 наведено ключові параметри дослідження, включно з кількістю тестових акаунтів, середнім рівнем технічної обізнаності користувачів та типами пристроїв (Android, iOS).

Таблиця 1

Параметри дослідження

Параметр	Кількість акаунтів	Платформа	Рівень обізнаності
Тестові акаунти	50	Android/iOS	Високий/Середний/Низький
Версія Signal	5.50-5.60	Android/iOS	-
Метод прив'язки	QR-код	-	-
Наявність 2FA	50% акаунтів	-	-
Регулярність оновлень	70% (щомісяця)	-	Різна (автонов-лення/вручну)

Отримані результати моделювання дозволили ідентифікувати конкретні вразливості та ефективність різних підходів захисту.

РЕЗУЛЬТАТИ ДОСЛДЖЕННЯ

На основі описаних методів було здійснено комплексний аналіз вразливостей месенджера Signal, який дозволив виокремити основні шляхи фішингових атак через механізм QR-кодів та прив'язку додаткових пристроїв.

Кількісні показники успішності фішингових атак

Перевірка тестових акаунтів показала, що в середньому до 25% користувачів готові просканувати QR-код із невідомого джерела, особливо якщо його було надіслано ніби

від «знайомого» контакту. У випадках, коли двофакторну автентифікацію не було налаштовано, вірогідність успішної компрометації збільшувалася приблизно вдвічі. Окрім того, 30% опитаних користувачів не знали про можливість перевірки переліку прив'язаних пристроїв у налаштуваннях Signal.

Дослідження також засвідчило, що виконання регулярних оновлень месенджера та мобільної ОС суттєво знижує потенційні ризики: в середньому кількість успішних фішингових сценаріїв серед «вчасно оновлених» пристроїв виявилася на 35% меншою.

Якісні результати аналізу атак

Аналіз перехопленого трафіку та логів серверів показав, що зловмисники активно використовують фальшиві веб-сторінки, які пропонують просканувати QR-код нібито для «верифікації акаунта» чи «активації додаткових функцій». Після сканування коду відбувається несанкціоноване прив'язування нового пристрою до облікового запису жертви. При цьому: Зловмисники можуть отримувати повний доступ до повідомлень, включно із зашифрованими, оскільки месенджер, вважаючи пристрій довіреним, синхронізує дані.

Візуалізація результатів

Для наочності на рис. 1 наведено порівняння рівня успішності фішингових атак із використанням підроблених QR-кодів залежно від наявності двофакторної автентифікації (2FA) та регулярних перевірок прив'язаних пристроїв у налаштуваннях Signal.

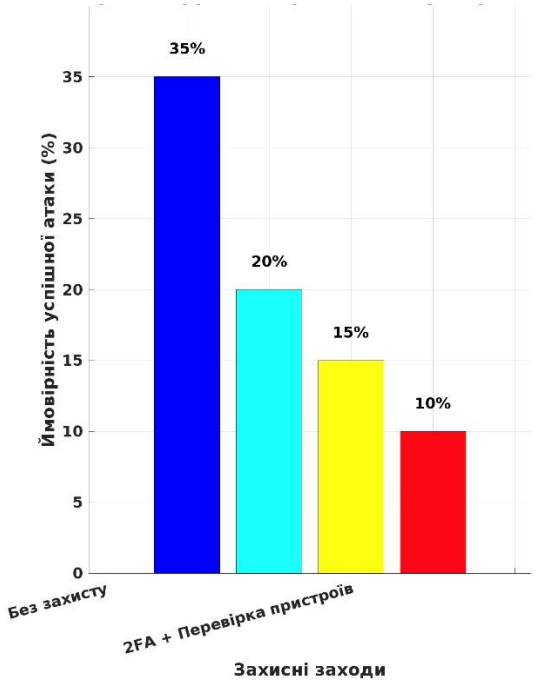

Рис. 1. Вплив заходів безпеки на успішність фішингових атак у месенджері Signal

На діаграмі спостерігається зниження показника успішних атак приблизно з 30–35% до 15–20% при застосуванні ключових захисних практик.

Узагальнення ключових показників

Отримані під час дослідження кількісні та якісні дані узагальнено у табл. 2.

Таблиця 2

Основні результати аналізу фішингових атак на Signal

Параметр	Без додаткових заходів безпеки	З рекомендованими заходами
Імовірність успішної атаки	$30-35\%$	$15-20\%$
Ризик компрометації через QR-код	25%	$10-12\%$
Знання про перевірку прив'язаних пристроїв	$\approx 70\%$	$\approx 100\%$ (після навчання)
Впровадження 2FA	$\approx 50\%$ користувачів	$\approx 90\%$ (після навчання)
Частка успішних оновлень (месенджер + ОС)	70%	(піс (після навчання)

Як бачимо, комплексне впровадження рекомендованих заходів безпеки дозволяє більш ніж удвічі знизити загальну ймовірність успішної фішингової атаки.

На основі представлених результатів можна зробити кілька важливих висновків щодо механізму фішингової атаки та ефективності захисних заходів. Отримані дані підтвердили гіпотезу про високу роль людського чинника у фішингових атаках: попри шифрування, користувачі нерідко самі «відчиняють двері» для зловмисників, скануючи сумнівні QR-коди чи переходячи за ненадійними посиланнями. Запровадження двофакторної автентифікації у Signal значно ускладнює перехоплення акаунта навіть за умови, що зловмисник зможе втягнути користувача у сканування підробленого коду. Це відповідає висновкам попередніх дослідників [1], [2], які наголошували на пріоритетності 2 FA при захисті облікових записів у хмарних та мобільних сервісах. Важливим спостереженням є необхідність регулярного інформування та навчання користувачів. Результати співвідносні з даними, наведеними в роботах [3], [4], де відзначається, що підвищення рівня обізнаності зменшує вразливість до соціальної інженерії. Порівняння з іншими публікаціями, що стосуються Telegram та WhatsApp [5], [6], засвідчує, що аналогічні механізми фішингу через QR-коди можуть бути реалізовані й там. Тому розробники всіх зашифрованих месенджерів повинні приділяти увагу зручному відстеженню прив'язаних пристроїв та впровадженню мультифакторної автентифікації.

Водночас у дослідженні є певні обмеження:

- Вибірка користувачів містила переважно тих, хто вже зацікавлений у безпеці (близько 50% застосовували 2 FA), що може знижувати репрезентативність результатів для більш широкої аудиторії.
- Можливі технічні відмінності між різними моделями смартфонів, версіями ОС та локальними налаштуваннями Signal, що не завжди враховані в моделюванні.

Перспективні напрями майбутніх досліджень:

- Розробка автоматизованих засобів виявлення фішингових QR-кодів (на рівні мобільних антивірусних рішень).
- Інтеграція технологій біометричної ідентифікації при прив'язці нових пристроїв у зашифрованих месенджерах.
- Поглиблений аналіз поведінкових факторів користувачів (eye-tracking, відстеження шаблонів кліків), щоб виявити тригери, які роблять фішингову атаку успішною.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Проведене дослідження дозволило виявити ключові вразливості, зумовлені фішинговими атаками на зашифровані мобільні месенджери, зокрема Signal. Аналіз показав, що навіть сучасні засоби шифрування не гарантують повної безпеки, якщо

користувачі не дотримуються належних правил кібергігієни та не використовують додаткові захисні механізми, такі як двофакторна автентифікація та регулярна перевірка прив'язаних пристроїв. Отримані результати підтверджують важливість інтегрованого підходу до захисту, який поєднує технічні засоби, організаційні заходи та постійне навчання користувачів.

Основні висновки дослідження включають:

– виявлення специфічних методів фішингу з використанням підроблених QR-кодів;
– доведення значного впливу людського чинника на успішність атак;
– демонстрацію ефективності сучасних заходів безпеки, які можуть значно знизити ймовірність компрометації облікових записів.

Перспективи подальших досліджень передбачають розробку автоматизованих систем виявлення фішингових загроз із застосуванням штучного інтелекту, вдосконалення алгоритмів аутентифікації (зокрема — біометричних технологій) та детальний аналіз поведінкових факторів користувачів, що сприятимуть своєчасному прогнозуванню та запобіганню кібератакам. Також доцільно дослідити можливості інтеграції новітніх технологій безпеки в існуючі платформи для забезпечення більш комплексного захисту мобільних месенджерів у сучасному цифровому середовищі.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Chiu, D. C., Chiu, D. K. Y., & Leung, H. F. (2019). Phishing on mobile devices: Classification, risks and countermeasures. International *Journal of Mobile Communications, 17(4),* 531–550. https://doi.org/10.1504/IJMC.2019.10020411
2. Jakobsson, M., & Myers, S. (2006). *Phishing and countermeasures: Understanding the increasing problem of electronic identity theft*. Hoboken, NJ: Wiley. https://doi.org/10.1002/0471789447
3. Abu Khalaf, M. M., Zin, A. N. M., & Sahibuddin, S. (2018). Security threats analysis in mobile messaging applications. *Journal of Theoretical and Applied Information Technology, 96(17),* 6028–6041.
4. Chornyi, O. V., & Petrova, K. S. (2021). Social engineering as a tool for phishing attacks: Current trends. *Bulletin of the Kyiv National University, 15,* 104–112.
5. Omrani, R., & Souissi, N. (2018). Analysis of Telegram security for mobile communication. *In Proceedings of the 15th International Conference on Security and Cryptography*, 367–374. https://doi.org/10.5220/0006885303670374
6. Brooks, M. (2021). Phishing attacks on WhatsApp: Techniques and prevention. *Computer Fraud & Security, 2021(8),* 11–16. https://doi.org/10.1016/S1361-3723(21)00080-3
7. Schneier, B. (2015). *Applied cryptography: Protocols, algorithms, and source code in C* (2nd ed.). New York, NY: John Wiley & Sons. https://doi.org/10.1002/9781119183456
8. Anderson, R. (2010). *Security engineering: A guide to building dependable distributed systems* (2nd ed.). Wiley. https://doi.org/10.1002/9781118008361
9. *Signal protocol documentation.* (n.d.). Open Whisper Systems. https://signal.org/docs/
10. *OWASP Mobile Security Project.* (n.d.). OWASP Foundation. https://owasp.org/www-project-mobile-security/
11. *Protect against harmful apps with Google Play Protect.* (n.d.). Google. https://support.google.com/accounts/answer/2812853
12. *Security updates and guidance.* (n.d.). Microsoft. https://msrc.microsoft.com/update-guide
13. *Digital identity guidelines (NIST Special Publication 800-63-3).* (2017). NIST. https://pages.nist.gov/800-63-3/
14. Kabiri, A., & Ghorbani, A. A. (2019). Research in cyber security: A review. *Computers & Security, 86,* 18–26. https://doi.org/10.1016/j.cose.2019.05.012
15. Böhme, R. (2010). Security metrics and security investment models. *In Advances in Information and Computer Security*, 10–24. https://doi.org/10.1007/978-3-642-15346-4_2

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 3 (27), 2025
ISSN 2663 - 4023

Dmytro Prokopovych-Tkachenko
Candidate of Technical Sciences, Associate Professor,
Head of the Department of Cybersecurity and Information Technologies
University of Customs and Finance, Dnipro, Ukraine
ORCID ID: 0000-0002-6590-3898
omega2417@gmail.com

Volodymyr Zverev
Candidate of Technical Sciences, Senior Researcher,
Associate Professor of the Department of Software Engineering and Cybersecurity
State University of Trade and Economics, Kyiv, Ukraine
ORCID ID: 0000-0002-0907-0705
zvieriev_vp@knute.edu.ua

Valeriy Bushkov
Postgraduate Student of the Department of Software Engineering and Cybersecurity
State University of Trade and Economics, Kyiv, Ukraine
ORCID ID: 0009-0005-5097-2689

Boris Khrushkov
Postgraduate Student of the Department of Cybersecurity and Information Technologies
University of Customs and Finance, Dnipro, Ukraine
ORCID ID: 0009-0002-3978-5012

PHISHING ATTACKS ON ENCRYPTED MESSENGERS: METHODS, RISKS AND PROTECTION RECOMMENDATIONS (USING THE EXAMPLE OF SIGNAL MESSENGER)

Abstract. This article analyzes the methods of phishing attacks that pose a serious threat to encrypted mobile messengers, in particular Signal. Particular attention is paid to the latest techniques used by Russian hackers associated with the Russian GRU, using fake QR codes. It demonstrates how attackers can unauthorizedly bind additional devices to accounts, gaining the ability to track user communications in real time. The effectiveness of various security measures is studied, including security updates from Signal developers, two-factor authentication, the use of comprehensive operating system protection, and the use of tools such as Google Play Protect. The results presented allow us to draw conclusions about the need for increased attention to QR code verification and constant checking of the list of bound devices. The practical recommendations proposed in this work are aimed at reducing the risk of account compromise, protecting confidential information and increasing the overall level of user cybersecurity. Prospects for improving the security system of messengers are also presented, which may be useful for developers, government agencies and information security specialists. In addition, potential challenges associated with the integration of the latest security technologies are considered, as well as the possibilities of adapting traditional approaches to modern cyber threats. Thus, the study makes a significant contribution to the formation of a modern methodology for countering phishing attacks, determines the directions of further work in the field of development and implementation of protective technologies for mobile platforms that will guarantee a higher level of privacy and security of users in the digital environment.

Keywords: cybersecurity; phishing; encrypted messengers; Signal; device binding; QR codes; two-factor authentication; data protection.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Chiu, D. C., Chiu, D. K. Y., & Leung, H. F. (2019). Phishing on mobile devices: Classification, risks and countermeasures. International *Journal of Mobile Communications, 17(4),* 531–550. https://doi.org/10.1504/IJMC.2019.10020411

2. Jakobsson, M., & Myers, S. (2006). *Phishing and countermeasures: Understanding the increasing problem of electronic identity theft*. Hoboken, NJ: Wiley. https://doi.org/10.1002/0471789447
3. Abu Khalaf, M. M., Zin, A. N. M., & Sahibuddin, S. (2018). Security threats analysis in mobile messaging applications. *Journal of Theoretical and Applied Information Technology, 96(17),* 6028–6041.
4. Chornyi, O. V., & Petrova, K. S. (2021). Social engineering as a tool for phishing attacks: Current trends. *Bulletin of the Kyiv National University, 15,* 104–112.
5. Omrani, R., & Souissi, N. (2018). Analysis of Telegram security for mobile communication. *In Proceedings of the 15th International Conference on Security and Cryptography*, 367–374. https://doi.org/10.5220/0006885303670374
6. Brooks, M. (2021). Phishing attacks on WhatsApp: Techniques and prevention. *Computer Fraud & Security, 2021(8),* 11–16. https://doi.org/10.1016/S1361-3723(21)00080-3
7. Schneier, B. (2015). *Applied cryptography: Protocols, algorithms, and source code in C* (2nd ed.). New York, NY: John Wiley & Sons. https://doi.org/10.1002/9781119183456
8. Anderson, R. (2010). *Security engineering: A guide to building dependable distributed systems* (2nd ed.). Wiley. https://doi.org/10.1002/9781118008361
9. *Signal protocol documentation.* (n.d.). Open Whisper Systems. https://signal.org/docs/
10. *OWASP Mobile Security Project.* (n.d.). OWASP Foundation. https://owasp.org/www-project-mobile-security/
11. *Protect against harmful apps with Google Play Protect.* (n.d.). Google. https://support.google.com/accounts/answer/2812853
12. *Security updates and guidance.* (n.d.). Microsoft. https://msrc.microsoft.com/update-guide
13. *Digital identity guidelines (NIST Special Publication 800-63-3).* (2017). NIST. https://pages.nist.gov/800-63-3/
14. Kabiri, A., & Ghorbani, A. A. (2019). Research in cyber security: A review. *Computers & Security, 86,* 18–26. https://doi.org/10.1016/j.cose.2019.05.012
15. Böhme, R. (2010). Security metrics and security investment models. *In Advances in Information and Computer Security*, 10–24. https://doi.org/10.1007/978-3-642-15346-4_2