УДК 004.056:004.7

ПРОСТІ ПРАВИЛА КІБЕРГІГІЄНИ ЯК ОСНОВА ЗАХИСТУ КОРИСТУВАЧА В ЦИФРОВОМУ СЕРЕДОВИЩІ

Діденко Т.В.[1]; Ткачук А.С.[2]
[1,2]Національний університет «Одеська політехніка»
[1,2]Україна, Одеса
[1]https://orcid.org/0009-0006-7880-2638; [2]a.s.tkachuk@op.edu.ua

Анотація. *У роботі розглянуто актуальну науково-практичну проблему низького рівня кібергігієни пересічних користувачів як головної причини успішних інцидентів у цифровій сфері. Обґрунтовано, що більшість порушень виникає через людські помилки: перехід за неперевіреними посиланнями, повторне використання паролів та передавання одноразових кодів. Наведено статистичні дані CERT-UA та Verizon DBIR 2025. Узагальнено п'ять базових правил кібергігієни, визначено нейтралізовані ними загрози та оцінено часові витрати на їх впровадження. Показано, що виконання цих правил суттєво знижує ризики.*

Ключові слова: *кібербезпека; кібергігієна; двофакторна автентифікація; паролі; соціальна інженерія.*

Вступна частина. Цифрові сервіси стали невід'ємною частиною повсякденного життя: через смартфон людина керує банківським рахунком, навчається, отримує державні послуги в застосунку «Дія» та спілкується в месенджерах. Разом із цим зростає кількість інцидентів, спрямованих на звичайних користувачів. За даними урядової команди CERT-UA, у 2025 році було опрацьовано 5927 кіберінцидентів проти 4315 у 2024 році (зростання приблизно на 37,4 %), а кількість зафіксованих фішингових випадків зросла з 843 до 1727 [1].

Особливість ситуації полягає в тому, що більшість успішних випадків компрометації відбувається не через складні технічні вразливості, а через людські помилки: перехід за підробленим посиланням, повторне використання пароля або повідомлення одноразового SMS-коду. Найнадійніші технічні засоби захисту втрачають сенс, якщо користувач сам передає доступ до свого облікового запису. Водночас більшість рекомендацій написані для фахівців і містять десятки складних пунктів. Тому актуальним є визначення мінімального набору простих правил кібергігієни для будь-якої людини без технічної освіти.

Правові засади кібербезпеки в Україні визначено Законом «Про основні засади забезпечення кібербезпеки України» [2]. У звіті Verizon Data Breach Investigations Report 2025 (12 195 підтверджених витоків) зафіксовано, що людський фактор присутній приблизно в 60 % випадків, а викрадені облікові дані є найпоширенішим способом початкового доступу (22 %) [3].

Дослідження Microsoft показало, що багатофакторна автентифікація (MFA) знижує ризик компрометації облікового запису на 99,22 % [4]. У рекомендаціях NIST SP 800-63B-4 (2025) акцентовано увагу на довжині пароля та його перевірці за списками скомпрометованих баз [5]. Психологічні механізми соціальної інженерії детально описано К. Хеднеді [6] та Р. Андерсоном [7], а соціотехнічні аспекти – вітчизняними науковцями [8]. Спробу звести захист до базових дій робить агенція CISA у програмі Secure Our World [9].

Мета роботи полягає у формулюванні мінімального набору простих правил кібергігієни для пересічного користувача на основі аналізу міжнародних рекомендацій та оцінці часових витрат на їх впровадження.

Основна частина. Аналіз статистики дає змогу виділити чотири основні загрози: підроблені повідомлення та соціальна інженерія, компрометація облікових записів, шкідливе ПЗ і втрата даних. За даними CERT-UA, у 2025 році зафіксовано 2058 випадків поширення шкідливого ПЗ, 1727 фішингових випадків, 988 інфікувань і 425 зламів акаунтів [3]. Для їх нейтралізації сформульовано п’ять базових правил.

Правило 1. Довгі унікальні паролі та менеджер паролів. Головна характеристика надійного пароля – його довжина. NIST рекомендує не менше 15 символів для єдиного фактора автентифікації [5]. Зручно застосовувати парольні фрази з кількох випадкових слів. Паролі доцільно зберігати в менеджері паролів (Bitwarden, 1Password або менеджер браузера).

Правило 2. Двофакторна автентифікація (2FA). Навіть у разі компрометації пароля другий фактор не дає змоги увійти в акаунт. Увімкнення 2FA знижує ризик компрометації більш ніж на 99 % [4]. Насамперед її слід увімкнути для пошти, месенджерів, соцмереж та банківських застосунків.

Правило 3. Своєчасне оновлення програмного забезпечення. Оновлення ОС, браузера та застосунків закривають відомі вразливості. Достатньо увімкнути автоматичне оновлення. Програми слід встановлювати виключно з офіційних джерел.

Правило 4. Розпізнавання підроблених повідомлень. Небезпечні повідомлення мають ознаки: тиск часом, підозрілі посилання, обіцянку виплат. Просте правило: не переходити за посиланнями, а відкривати сервіс самостійно через офіційний сайт чи застосунок.

Правило 5. Резервне копіювання. Програми-вимагачі фігурували в 44 % підтверджених витоків даних у 2025 році [3]. Резервна копія дає змогу відновити файли без виплати викупу. Рекомендується правило «3-2-1»: три копії даних, на двох різних носіях, одна з яких зберігається в хмарі.

Зв’язок між загрозами та заходами захисту подано в таблиці 1.

Таблиця 1

Відповідність загроз і базових правил кібергігієни

Загроза	Правило захисту	Час на впровадження
Підбір і витік паролів	Довгі унікальні паролі, менеджер паролів	30–60 хв
Злам облікового запису	Двофакторна автентифікація (2FA)	5–10 хв на сервіс
Шкідливе ПЗ, вразливості	Автооновлення, ПЗ лише з офіційних джерел	5 хв
Соціальна інженерія	Перевірка джерела, вхід лише через офіційний застосунок	Постійна звичка
Втрата даних, вимагачі	Резервне копіювання за правилом «3-2-1»	30 хв

Як видно з таблиці 1, жодне з п'яти правил не потребує спеціальних технічних знань чи суттєвих витрат. Загальний час на їх впровадження становить 1–2 години, а захисний ефект зберігається постійно.

Висновки. Аналіз показав, що головною причиною успішних інцидентів є людський фактор (присутній приблизно в 60 % витоків даних). Запропоновано п’ять базових правил кібергігієни, кожне з яких нейтралізує конкретну загрозу без додаткових фінансових витрат. Подальші дослідження доцільно спрямувати на розробку коротких курсів для студентів.

Використання інструментів ШІ. Під час виконання дослідження та підготовки матеріалів тез доповідей інструменти штучного інтелекту не використовувалися.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

[1] *У 2025 році кількість кібератак зросла на 37 %: дані CERT-UA.* (2026). dev.ua. https://dev.ua/news/u-2025-rotsi-kilkist-kiberatak-zrosla-na-37-1767858414

[2] Про основні засади забезпечення кібербезпеки України № 2163-VIII. (2017) https://zakon.rada.gov.ua/laws/show/2163-19

[3] Verizon. (2025). *2025 Data Breach Investigations Report.* https://www.verizon.com/business/resources/reports/dbir/

[4] Meyer, L. A., Romero, S., Bertoli, G., Burt, T., Weinert, A., & Lavista Ferres, J. M. (2023). *How effective is multifactor authentication at deterring cyberattacks*? Microsoft Research.

[5] National Institute of Standards and Technology. (2025). *Digital Identity Guidelines: Authentication and Authenticator Management*. https://doi.org/10.6028/NIST.SP.800-63B-4

[6] Hadnagy, C. (2018). *Social Engineering: The Science of Human Hacking* (2nd ed.). Wiley.

[7] Anderson, R. (2020). *Security Engineering: A Guide to Building Dependable Distributed Systems* (3rd ed.). Wiley.

[8] Бурячок, В. Л., Толубко, В. Б., Хорошко, В. О., & Толюпа, С. В. (2015). *Інформаційна та кібербезпека: соціотехнічний аспект*. ДУТ.

[9] Cybersecurity and Infrastructure Security Agency. (2024). *Secure Our World*. https://www.cisa.gov/secure-our-world

Didenko T.V., Tkachuk A.S.

Simple cyber hygiene rules as a basis for user protection in the digital environment

Abstract. *The paper addresses the topical scientific and practical problem of poor cyber hygiene among ordinary users, which remains the main cause of successful cyber incidents. It is substantiated that most incidents are caused not by complex technical vulnerabilities but by human errors: clicking phishing links, reusing passwords, or handing one-time codes to attackers. Five basic cyber hygiene rules are summarized: long unique passwords and a password manager, two-factor authentication, timely software updates, phishing recognition, and data backup.*

Key words: *cybersecurity; cyber hygiene; two-factor authentication; passwords; social engineering.*