ОСНОВИ ЦИФРОВОЇ ГІГІЄНИ ДЕРЖАВНИХ СЛУЖБОВЦІВ

Дубель Михайло
PhD, старший викладач кафедри політології та державного управління,
Донецький національний університет імені Василя Стуса
ORCID: 0000-0003-2229-0419

В умовах повномасштабного вторгнення на територію нашої держави переважна кількість суспільства існування загрози сприймає у фізичному вимірі. Відповідно вектор джерел небезпеки інформаційно-технологічного виміру привертає до себе набагато менше уваги. Необхідно більш точно сформулювати напрям загроз, аналізу яких буде приділена увага у цьому дослідженні. Цифрова гігієна не є часто вживаним у повсякденному, або навіть науковому, спілкуванні. Тому варто зазначити, що цифрова гігієна не тотожна інформаційній гігієні, якій приділяється значна увага у стратегії інформаційної безпеки. У першому напрямі увага приділяється безпечному користуванню своїми пристроями, у другому – саме безпечному розпорядженню своїм інформаційним простором, тобто, інакше кажучи, засадам фільтрації інформації на достовірну та підроблену. Отже, основи цифрової гігієни набагато ближчі до спрощеної версії кібербезпеки.

Аспекти дослідження можуть бути корисними для звичайних користувачів, а також для працівників державної служби. Проте акцент саме на другій категорії у зв'язку з їх публічністю та доступом до важливої державної інформації. Справа у тому, що коли хтось бажає отримати доступ до інформації пересічного громадянина, то зазвичай це буде людина з оточення. У випадку державних службовців ситуація є складнішою – їм необхідно подавати декларації, робоча пошта знаходиться у вільному доступі, значна частина інформації набагато легше відстежується у публічному просторі. Водночас важливо зазначити, що державні працівники пов'язані у процесі робочого листування корпоративною мережею, унаслідок чого злам одного працівника призводить до ланцюгової реакції.

Щоб зрозуміти актуальність цього дослідження, варто навести випадки, коли недотримання засад цифрової гігієни призводило до витоків інформації, що впливало на політичну ситуацію як у окремій державі, так і навіть мало певний потенціал для впливу на міждержавні відносини. Розповсюдження конфіденційної інформації у публічному просторі, внаслідок зламу певних працівників, у науковій літературі привело до появи терміну – «злам та виток» – схеми, у якій відбувається спочатку отримання інформації, а потім її подальше розповсюдження. Звісно, варто враховувати, що зазвичай люди, які стоять за зламами, є непублічними, тому для успіху схеми необхідно мати майданчик, що буде основою для так званої дистрибуції витоку. По-перше, варто згадати за класичного представника, що пов'язаний з витоками – WikiLeaks, що ще з 2006 року займа-

ється публікацією витоків [7]. Найбільш відомі випадки, що пов'язані з подібним джерелом – виток пошти Демократичної партії США у 2016 році та штабу Макрона у 2017 році. У першому випадку це частково призвело до падіння рейтингу Сандерса, певного удару по репутації Клінтон, та, як наслідок, перемоги Трампа. У другому випадку особливого результату не було досягнуто, тобто виток не став ефективним. Звісно, виникає думка, що подібні витоки мають вплив лише під час передвиборчих перегонів, проте, це дещо хибне твердження. По-друге, потенціал зламів та витоків досить значний і тут варто також навести кейси з вітчизняного середовища. Наприклад, під час повномасштабного вторгнення російські загарбники далеко не завжди були обережними під час користування цифровим середовищем, що яскраво розкривається у матеріалах розслідувань каналу Телебачення Торонто [2].

Тепер можна перейти до розкриття практичних або техніко-комунікаційних аспектів дослідження. Спочатку потрібно розглянути основні загрози, що пов'язані з користуванням цифровим середовищем державними службовцями, мається на увазі поняття фішинг. Варто зазначити, що значна кількість листів, що приходять сучасному користувачу на електронну пошту є спамом. Спам та фішинг мають досить фундаментальні відмінності – до першої категорії належить будь-яка інформація, на яку ми не розраховуємо, коли отримуємо, тоді як друга категорія має прямий намір нанести шкоду отримувачу. Тому спам, зокрема політичний, не несе ніякої прямої загрози державним службовцям, якщо не враховувати те, що будь-яка зайва інформація несе перенавантаження на користувача. Так виникає певний виклик у вигляді того, що необхідно відрізнити фішинг та побудувати стратегію поводження себе з подібними повідомленнями. Зазвичай основна задача фішингу – імітуватися під звичайні листи, тобто, під знайомі користувачу організації. Отже, здебільшого середньостатистичний держслужбовець буде отримувати фішингові листи, що будуть мати вигляд повідомлень від технічної підтримки або від колег із проханням допомоги, або повідомлення від інших відділів. Так формуються декілька основних правил поводження із фішиногом – не переходити за посиланнями у підозрілих листах (тих, які не очікувалися); не завантажувати файли з подібних листів собі на пристрій та, взагалі, зв'язуватися з колегами, у разі отримання подібних листів телефоном чи навіть особисто, а не лише на пошту. Взагалі, досить універсальним та зручним у використанні є інтерактивний тест, що пропонує Google, для перевірки вміння розпізнавати фішинг [3].

Наступна категорія класичних загроз основ цифрової гігієни пов'язана з використанням паролів. Банально буде говорити, але створення якісного та, водночас, зручного паролю, є досить поширеним викликом для будь-якого користувача, зокрема для державного службовця. Завдяки даним сайту Nordpass можемо

розглянути не лише перелік найбільш часто зламаних паролів по світу, але й для нашої країни теж [6]. На основі подібного аналізу бачимо, що досі, на жаль, вітчизняні користувачі використовують паролі на кшталт 123456 або password. Тому загальними порадами під час створення акаунту будуть такі – не використовувати подібні легкі паролі, не застосовувати прості слова, імена, прізвища, не обирати лише цифри або літери. Для створення якісних паролів можна використовувати або спеціалізовані сайти, або західний спосіб поєднання декількох слів, або ж шифрування латиницею слова, яке пишеться кирилицею. Деякі користувачі намагаються облегшити користування сайтами за допомогою збереження паролів у Менеджерах паролів в браузерах [1]. З одного боку це зручно, з іншого – призведе до потенційного забування паролів. Проте, завдяки Менеджеру паролів можна подивитися, чи були зламані паролі, або наскільки вони за системою аналізу паролів вважаються легкими.

Наступний та останній напрям цифрової гігієни у межах цього дослідження пов'язаний із наслідками витоків, але не конкретних користувачів, а цілого великого сайту. Наприклад, злам Internet Archive призвів до витоку даних 31 мільйону користувачів, це були адреси пошти, ім'я користувачів та, що найбільш шкідливо у цій ситуації – паролі користувачів [5]. Це повертає нас у дослідженні до тієї інформації, що звучить навіть у вінницьких трамваях – не використовувати однакові паролі на різних сайтах, у першу чергу – на особистих сайтах та тих, що пов'язані з роботою. Проте, якщо подібний виток вже трапився, потрібно спробувати це виявити та змінити паролі на усіх сайтах, де використовувався ідентичний пароль. Для розв'язання подібних ситуацій може сприяти сайт haveibeenpwned.com, де можна проглянути інформацію про зафіксовані витоки та перевірити свою пошту на наявні витоки [4].

Отже, усі перелічені засади цифрової гігієни не охоплюють увесь інструментарій. Проте для повсякденного використання зазначені напрями і поради є достатньо корисними. У подальших дослідженнях можна визначити специфіку дотримання безпеки використання файлів кукі, протоколів безпечного з'єднання тощо.

Список використаних джерел

1. Менеджер паролів. *Google.* URL: https://passwords.google.com/?hl=uk (дата звернення: 01.04.2026).

2. Телебачення Торонто. *Youtube.* URL: https://www.youtube.com/@uttoronto (дата звернення: 01.04.2026).

3. Тест «Ви вмієте розпізнавати фішинг?» *Google.* URL: https://phishingquiz.withgoogle.com/?hl=uk (дата звернення: 01.04.2026).

4. Haveibeenpwned. URL: https://haveibeenpwned.com/ (дата звернення: 01.04.2026).

5. Internet Archive hacked, data breach impacts 31 million users. *Bleeping Computer.* 2024. URL: https://www.bleepingcomputer.com/news/security/internet-archive-hacked-data-breach-impacts-31-million-users/ (дата звернення: 01.04.2026).

6. Top 200 Most Common Passwords: Generations change, password habits remain. *NordPass.* URL: https://nordpass.com/most-common-passwords-list/ (дата звернення: 01.04.2026).
7. WikiLeaks. URL: https://wikileaks.org/ (дата звернення: 01.04.2026).