МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ХЕРСОНСЬКИЙ ДЕРЖАВНИЙ АГРАРНО-ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ

Економічний факультет

МАТЕРІАЛИ

Всеукраїнської студентської науково-практичної конференції

МІЖДИСЦИПЛІНАРНІ НАУКОВІ СТУДІЇ 2026

10 квітня 2026 року

м. Кропивницький, Україна

Капрелова А. Р. – здобувачка вищої освіти другого (магістерського) рівня Херсонського державного аграрно-економічного університету

Башинський І. А. – к. наук з державного управління, доцент, доцент кафедри публічного управління, права та гуманітарних наук Херсонського державного аграрно-економічного університету

ОСОБИСТА ЦИФРОВА ГІГІЄНА У ВІРТУАЛЬНОМУ СЕРЕДОВИЩІ: МЕТОДИ ТЕХНІЧНОГО ЗАХИСТУ

У 2026 році особисті заходи цифрової безпеки у віртуальному просторі стають життєво важливими. З огляду на зростання кількості онлайн-послуг, віддаленої праці, цифрових розрахунків та мережевого зберігання даних, користувачі стають об'єктами посягань з боку фішингу, спроб зламу облікових записів та витоків даних, що може призвести до фінансових та приватних втрат. У цьому матеріалі розглядаються приклади хакерських атак, методи їх нейтралізації та превентивні кроки, які необхідно вжити для збереження конфіденційності й мінімізації збитків від подібних інцидентів.

У 2017 році програму-шифрувальник WannaCry розробила північнокорейське кіберзлочинне угруповання Lazarus, використовуючи експлойт EternalBlue, викрадений у Агентства національної безпеки США. Ця кампанія зачепила комп'ютери на базі Windows у понад 150 країнах, зашифрувавши файли на 200–500 тисячах машин – від медичних закладів Великої Британії до підприємств та фабрик в Іспанії.

Першочерговим завданням було отримання викупу в розмірі 300–600$ у біткойнах за дешифрування файлів на заражених комп'ютерах.

Зловмисники прагнули швидко отримати прибуток від жертв по всьому світу. Окрім того, масове зараження мало на меті формування ботнету – потужної армії скомпрометованих пристроїв під контролем хакерів, яку можна було б задіяти для подальших атак, шпигунства або продажу доступу. Однак, найголовнішим наслідком став колапс: параліч роботи лікарень, виробництв та банків у більш ніж 150 державах.

Для зупинки поширення атаки компанія Microsoft випустила оновлення ще до початку масового зараження; було знайдено “стоп-кран” (зареєструвавши специфічний домен), організації блокували та виводили з експлуатації застарілі системи. Збитки оцінюються у 4–8 мільярдів доларів, що призвело до зупинки роботи медичних закладів та комерційних структур, вимагаючи викуп. Попри те, що поширення вдалося стримати протягом 1–2 тижнів, процес відновлення зайняв місяці [1].

Зловмисники, імовірно пов’язані з китайськими спецслужбами, скористалися вразливістю в системі безпеки сайту Equifax – великого американського бюро кредитних історій, що обробляє дані мільйонів громадян. Їхньою метою була крадіжка даних для подальшого продажу на нелегальних ринках або використання для шахрайства з ідентифікаційними даними та кредитами. Вони отримали доступ через вразливість у програмному забезпеченні Apache Struts, розташованому на сторінці для оскарження кредитної інформації, і протягом 2,5 місяців викрали дані 147 мільйонів американців, 15 мільйонів британців та 19 тисяч канадців. Серед викраденого були також номери платіжних карток понад 209 тисяч осіб.

Equifax зафіксувала інцидент 29 липня 2017 року, того ж дня встановивши патч, але найняла експертів Mandiant для розслідування та оголосила про витік публічно лише 7 вересня – через шість тижнів. Компанія посилила мережевий захист, запровадила моніторинг та сегментацію. Наслідки були руйнівними: штрафи, що перевищили $575 мільйонів, відставки топ-менеджерів, падіння акцій на 35%, а також тисячі судових

позовів. Відновлення безпекової інфраструктури тривало багато місяців [2].

У 2020 році група підлітків, очолювана 17-річним Гремом Іваном Маркасом Коннорсом із Флориди, використала методи соціальної інженерії, зокрема телефонні дзвінки та фішинг, для обману співробітників Twitter з метою отримання доступу до внутрішніх адміністративних панелей та фінансової вигоди. Удар прийшовся на понад 130 відомих акаунтів – від політичних лідерів (Обама, Байден, Трамп) та мільярдерів (Ілон Маск, Білл Гейтс, Джефф Безос) до корпорацій (Apple, Uber, Binance). Між 20:00 та 22:00 UTC 15 липня 2020 року хакери скомпрометували 45 акаунтів і опублікували твіти, закликаючи надсилати біткойни на певний гаманець, обіцяючи подвоїти суму протягом 20 хвилин.

Twitter оперативно заблокував верифіковані акаунти, вимкнув внутрішні інструменти та посилив процедури перевірки співробітників. Арешти відбулися 31 липня: Коннорс та двоє інших осіб були звинувачені у фінансовому шахрайстві та відмиванні грошей. Збитки від Twitter Bitcoin scam становили понад 120 000 доларів у біткойнах, зафіксовано понад 400 транзакцій за дві години [3].

Щоб знизити ймовірність стати жертвою хакерських атак, кожен користувач може здійснити декілька фундаментальних кроків у сфері цифрової гігієни:

1) Встановити менеджер паролів (наприклад, Bitwarden або 1Password) для генерації та зберігання унікальних складних паролів для кожної онлайн-платформи – це запобігає атакам типу “credential stuffing” після витоків даних;

2) Активувати двофакторну автентифікацію (2FA) через Google Authenticator або апаратний ключ типу YubiKey всюди, де це підтримується, щоб одного лише пароля хакерам було недостатньо;

3) Регулярно оновлювати операційні системи (Windows/macOS), а також налаштувати автоматичне створення резервних копій на зовнішній

носій або у хмарне сховище;

4) Користуватися VPN під час роботи з публічними мережами Wi-Fi, ретельно перевіряти URL-адреси перед переходом за посиланнями та уникати відкриття невідомих вкладень [4].

У 2026 році індивідуальна цифрова гігієна залишається основним захисним механізмом проти кіберінцидентів на кшталт WannaCry, злам Equifax та Twitter Bitcoin scam, які демонструють, як фішинг, слабкість паролів та застаріле програмне забезпечення призводять до катастрофічних наслідків – від паралічу медичних установ до викрадення персональних даних мільйонів осіб. Хоча зловмисники мають власні мотиви, прості дії користувачів – використання унікальних паролів через Bitwarden, 2FA з Google Authenticator, створення бекапів, застосування VPN та загальна обережність – могли б зменшити ризики на 90%. Ці технічні засоби є загальнодоступними, однак без усвідомлення їхньої критичної важливості вразливість залишається високою, отже, послідовне дотримання базових правил кібергігієни є невід'ємною складовою сучасного цифрового життя.

Використана література

1. WannaCry Ransomware Attack: All You Need to Know. *Kaspersky : web site*. URL: https://www.kaspersky.com/resource-center/threats/ransomware wannacry (дата звернення: 08.04.2026).

2. Equifax Data Breach FAQ. *CSO : web site*. URL: https://www.csoonline.com/article/567833/equifax-data-breach-faq-what-happened-who-was-affected-what-was-the-impact.html (дата звернення: 08.04.2026).

3. Twitter Investigation Report. *Department of Financial Services* : web site. URL: https://www.dfs.ny.gov/Twitter_Report (дата звернення: 08.04.2026).

4. NIST SP 800-63B Digital Identity Guidelines: Authentication and Lifecycle Management. *NIST : web site*. URL: https://pages.nist.gov/800-63-3/sp800-63b.html (дата звернення: 08.04.2026).