Галицький економічний вісник https://doi.org/10.33108/galicianvisnyk_tntu
Galician economic journal, No 4 (95) 2025
https://doi.org/10.33108/galicianvisnyk_tntu2025.04
ISSN 2409-8892. Web: **http://galicianvisnyk.tntu.edu.ua**

PUBLIC ADMINISTRATION

ПУБЛІЧНЕ УПРАВЛІННЯ ТА АДМІНІСТРУВАННЯ

УДК 004.056.5:35.07:351.74

ЦИФРОВА ГІГІЄНА ПУБЛІЧНИХ СЛУЖБОВЦІВ ЯК ВАЖЛИВА СКЛАДОВА НАЦІОНАЛЬНОЇ БЕЗПЕКИ

Михайло Дубель

Донецький національний університет імені Василя Стуса,
Вінниця, Україна
ORCID: https://orcid.org/0000-0003-2229-0419

Резюме. *Присвячено визначенню базових правил дотримання цифрової гігієни для публічних службовців з метою підтримання національної безпеки. Для досягнення поставленої мети визначено такі наукові завдання: визначити перелік базових правил дотримання цифрової гігієни для публічних службовців, а саме, розкрити питання надійності паролів на акаунтах, витоків інформації на сторонніх сайтах, специфіки фішінгу, особливостей протоколів з'єднання, розкрити механізм cookie файлів, проаналізувати практику вірусів та антивірусів. У дослідженні цифрова гігієна публічного службовця поділено на умовні блоки: безпечне користування поштою (управління паролями, розпізнавання фішингових атак), грамотне поводження на сторонніх сайтах (звертання уваги на протокол з'єднання сайтів, розгляд cookie файлів, перевірка сайту на віруси). У якості прикладу фішинговх атак у дослідженні наведено виток пошти комітету Демократичної партії США у 2016 році та атаку на голову президентської кампанії Гілларі Клінтон Джона Подесту шляхом підробки електронного листа, на пошту останнього із проханням змінити пароль. У якості прикладу витоку інформації зі стороннього сайту наведено випадок Facebook Marketplace у 2024 році. Витік бази даних містив широкий спектр персональної інформації, включаючи імена, номери телефонів, адреси електронної пошти, ідентифікатори Facebook та інформацію про профіль Facebook. Зловмисники можуть використовувати адреси електронної пошти, що витікають в Інтернет під час фішингових атак та мобільних фішингових атак на номери користувачів Facebook Marketplace. Зразком використання вірусу у геополітичних цілях можна вважати SUNBURST. SUNBURST була атакою на ланцюг поставок, яка використовує бекдор, імплантований у постачальника, для атаки та опосередкованого компрометування організацій по всьому світу. Orion, програмне забезпечення SolarWinds, яке було скомпрометовано злочинцями, використовувалося близько 33 000 державних та приватних клієнтів. Підсумовуючи дослідження, потрібно відзначити те, що, в першу чергу, працівник публічного органу влади має відрізняти свою особисту та корпоративну пошту, що знаходиться в екосистемі установи. Реєструватися на різних сайтах з корпоративної пошти потенційно небезпечно для цілісності системи, бо будь-який сайт зі значною кількістю користувачів можуть зламати з метою комерційної реалізації масиву інформації. Важливо розуміти, що національна безпека є складної системою, а, як відомо, цілісність системи визначається цілісністю найслабкішого елемента. В рамках дослідження – необережного публічного службовця.*

Ключові слова: *цифрова гігієна, публічні службовці, витоки інформації, фішинг, національна безпека, cookie файли.*

https://doi.org/10.33108/galicianvisnyk_tntu2025.04.183 *Отримано 07.05.2025*

Corresponding author: Mykhailo Dubel; e-mail: m.dubel@donnu.edu.ua

UDC 004.056.5:35.07:351.74

DIGITAL HYGIENE OF PUBLIC SERVANTS AS AN IMPORTANT COMPONENT OF NATIONAL SECURITY

Mykhailo Dubel

Vasyl' Stus Donetsk National University, Vinnytsia, Ukraine

Summary. *The article is devoted to determining the basic rules of digital hygiene for public servants in order to support national security. To achieve the set goal, the following scientific tasks were defined: to determine a list of basic rules of digital hygiene for public servants, namely – to reveal the issues of password reliability on accounts, information leaks on third-party sites, the specifics of phishing, the features of connection protocols, to reveal the mechanism of cookie files, to analyze the practice of viruses and antiviruses. In the study, the digital hygiene of a public servant is divided into conditional blocks: safe use of mail (password management, recognition of phishing attacks), competent behavior on third-party sites (paying attention to the site connection protocol, considering cookie files, checking the site for viruses). As examples of phishing attacks, the study cites the 2016 Democratic National Committee email leak and the attack on Hillary Clinton's presidential campaign chairman John Podesta by forging an email to his email address asking him to change his password. As an example of a third-party information leak, the Facebook Marketplace incident in 2024 is cited. The database leak contained a wide range of personal information, including names, phone numbers, email addresses, Facebook IDs, and Facebook profile information. Attackers can use email addresses leaked to the Internet in phishing attacks and mobile phishing attacks on Facebook Marketplace user numbers. An example of the use of a virus for geopolitical purposes is SUNBURST. SUNBURST was a supply chain attack that used a backdoor implanted in a supplier to attack and indirectly compromise organizations around the world. Orion, the SolarWinds software that was compromised by criminals, was used by about 33,000 government and private customers. Summing up the study, it should be noted that, first of all, an employee of a public authority should distinguish between their personal and corporate mail located in the institution's ecosystem. Registering on different sites from corporate mail is potentially dangerous for the integrity of the system, because any site with a significant number of users can be hacked for commercial sale of an array of information. It is important to understand that national security is a complex system, and, as is known, the integrity of the system is determined by the integrity of the weakest element, in the framework of the study – a careless public employee.*

Key words: *digital hygiene, public servants, information leaks, phishing, national security, cookies.*

https://doi.org/10.33108/galicianvisnyk_tntu2025.04.183 *Received 07.05.2025*

Постановка проблеми. Однією з важливих вимог до публічних працівників як в Україні, так і, тим паче, державах Європейського Союзу є базові знання з користування інформаційно-комунікаційними технологіями. Серед переліку цифрових компетентностей слід відзначити ті, що можна охарактеризувати як знання цифрової гігієни – базові вміння, що можуть допомогти зберегти цільність і конфіденційність інформації користувача. У більшості випадків зламати цілісність пристрою намагаються знайомі люди. З публічними службовцями ситуація інша через те, що інформація про них знаходиться у відкритому доступі на сайтах установ, що робить достатньо зручною мішенню для злочинців, особливо в умовах війни. Це спонукає до того, що публічні службовці мають володіти хоча б базовим умінням дотримання правил безпечного поводження в інтернеті, особливо з робочого пристрою або з робочої (корпоративної) пошти.

Аналіз останніх досліджень і публікацій. Питанням цифрових компетентностей публічних службовців присвячено праці В. В. Наместніка [1], К. В. Копняк, В. В. Покиньчереди [2], В. В. Фостікової [3]. Специфіка цифрової гігієни розкрито у дослідженнях М. В. Гуцалюк [4], О. Ж. Скибуна [5], проте розглядалася більше у вигляді кібергігієни. Саме тому виникає актуальність дослідження саме питання цифрової гігієни та шляхів дотримання її публічними службовцям для підвищення національної безпеки.

Метою дослідження є визначення базових правил дотримання цифрової гігієни для публічних службовців.

Постановка завдання. Для досягнення поставленої мети визначено такі наукові завдання: визначити перелік базових правил дотримання цифрової гігієни для публічних службовців, а саме – розкрити питання надійності паролів на акаунтах, витоків інформації на сторонніх сайтах, специфіки фішингу, особливостей протоколів з'єднання, розкрити механізм cookie файлів, проаналізувати практику вірусів та антивірусів. Для виконання цих завдань використано аналіз досвіду випадків з практики, сайти, де можна скористатися різними технологіями для дотримання цифрової гігієни.

Для вирішення поставлених завдань використано такі методи: аналіз, синтез, узагальнення, аналогія.

Результати дослідження. Слід зазначити, що підняття актуальності підвищення цифрової грамотності загалом публічних службовців у нашій державі призвело до появи сервісу «Цифрограм для державних службовців» [6]. Проте, попри всі його очевидні переваги, хотілося б також розкрити кілька сервісів за напрямком основ цифрової гігієни у цій публікації.

Перш за все потрібно розпочати з того, що публічні службовці мають усвідомлювати, чи були вже зламані його дані, у тому числі й особисті пошта або акаунти на інших сайтах. Один з подібних варіантів – це перевірити паролі на Менеджері паролів від Google [7]. На основі перевірки знаходяться три категорії, що потенційно можуть допомогти у визначенні надійності своїх акаунтів. Перша позиція – кількість зламаних паролів та сайт, де відбувся злам, друга – кількість повторюваних паролів, третя – ненадійні паролі. Тут важливо відзначити, що більшість користувачів сильно тяжіють до автоматизації процесу користування інтернетом. Відповідно, паролі не просто зберігають, коли сайт пропонує подібне зробити, а використовують однакові паролі для різних сайтів. Відповідно, злам одного сайту може, за інерцією, призвести до зламу відразу ряду сайтів, а у випадку публічних службовців – до зламу сайту установи. Дещо схожий аспект недотримання цифрової гігієни мало історичний аналог у випадку витоку пошти комітету Демократичної партії США у 2016 році. 22 липня 2016 року, під час президентської кампанії у США 2016 року, WikiLeaks опублікував серію приватних електронних листів, що належать Національному комітету Демократичної партії [8]. Цей витік включав майже 20 000 електронних листів і 8 000 вкладень, які належали семи вищим посадовим особам Національного комітету Демократичної партії. Хоча більшість електронних листів були нешкідливими, деякі з них підтверджували, що Національний комітет Демократичної партії віддає перевагу кандидату в президенти Гілларі Клінтон, а не Берні Сандерсу, що викликало обурення через заявлений нейтралітет щодо кандидата від Демократичної партії. У цьому випадку атака включала метод соціальної інженерії фішингу, який спрямований на певну особу, спонукаючи її встановити шкідливе програмне забезпечення. Потім програмне забезпечення забезпечує вибірковий віддалений доступ до комп'ютерних систем цільової програми.

Тут відзначимо певний нюанс – далеко не всі користувачі зберігають паролі саме у Google, а деякі не зберігають взагалі. Проте це ще не дає гарантії, що виток з пошти не був допущений. Тут може бути корисним сервіс від haveibeenpwned [9]. На ньому можна подивитися, чи був виток даних з сайту, на якому зареєстровано публічного службовця, навіть з його особистої пошти. Подібна викрадена інформація з сайтів спрямована на спамерів та шахраїв. Шахраї використовують імена користувачів та паролі, що витікають з одного сайту, для входу в облікові записи на інших вебсайтах, де користувачі використовували ті самі облікові дані. Відповідно, це альтернативний спосіб отримання даних про користувачів.

Прикладом витоку даних з сайту популярної компанії є Facebook Marketplace у 2024 році [10]. Витік бази даних містив широкий спектр персональної інформації, включаючи імена, номери телефонів, адреси електронної пошти, ідентифікатори Facebook та інформацію про профіль Facebook. Зловмисники можуть використовувати адреси електронної пошти, що витікають в інтернет, під час фішингових атак та мобільних фішингових атак на номери користувачів Facebook Marketplace. Розкриті номери мобільних телефонів та особиста інформація також можуть бути використані в атаках на заміну SIM-карт, що дозволить їм викрасти коди багатофакторної автентифікації, надіслані через SMS, та захопити облікові записи своїх жертв.

Відзначимо, що витік даних з Facebook Marketplace – не перший подібний інцидент, з яким Meta зіткнулася за останні роки. У листопаді 2022 року Meta була оштрафована на 265 мільйонів євро (275,5 мільйона доларів) за нездатність захистити особисту інформацію користувачів Facebook від парсерів після того, як у квітні 2021 року на хакерському форумі було оприлюднено дані, пов'язані з понад 533 мільйонами облікових записів Facebook. Викрадені дані вперше з'явилися в хакерській спільноті в червні 2020 року. Вони містили інформацію, яку можна було витягти з публічних профілів та приватних номерів мобільних телефонів постраждалих облікових записів. Стався витік даних понад 533 мільйонами користувачів Facebook, зокрема їхніх номерів мобільних телефонів, ідентифікаторів Facebook, імен, статі, місцезнаходження, сімейного статусу, професій, дат народження та адрес електронної пошти. Майже кожен запис користувача Facebook, що витік у квітні 2021 року, містив номери мобільних телефонів, ідентифікатори Facebook та імена користувачів.

З огляду на менеджер паролів Google, також можна проаналізувати третій показник, а саме – надійність паролю. Справа в тому, що більшість людей, як правило, розробляють паролі, які найзручніші для запам’ятовування. З одного боку, – зручно, бо не треба втрачати багато часу, щоб ввести, з іншого, – використання загальновідомої інформації, такої, як ім’я своє або близьких, дат народження, назв місць – все це буде відомо з поверхневого аналізу профіля держслубовця у соціальних мережах. Саме тому актуальним можна вважати використання різних сервісів, де можна як перевірити потенційний пароль (не вводячи свій), так і скористатися запропонованим. Наприклад, можна скористатися зв’язкою від вітчизняного розробника антивірусів Zillya! та Кіберполіції України. Zillya! Показує, наскільки надійним є пароль, при цьому наголошено, що не потрібно вводити справжній пароль [11]. Кіберполіція ж пропонує згенерувати пароль, який потім можна перевірити на сайті Zillya! [12]. Проте, навіть без використання подібних сайтів, можна спробувати метод зворотного перекладу кирилиці та латини. Наприклад, слово переклад перетворюється на gthtrkfl.

Ми вже згадували про фішингові атаки, тому можемо розкрити деталі щодо сутності фішингу. Фішинг відрізняється від спаму тим, що друга категорія спрямована на те, щоб розповсюдити інформацію для стимулювання збуту, то перша категорія несе загрозу, бо не пропонує у відповідь певні послуг або товар. З різних видів фішингу в дослідженні акцентуємо увагу саме на фішинг у пошті. Публічним управлінцям на пошту можуть приходити фішингові лист з метою зламу корпоративних акаунтів або особистої пошти. Тут корисним може стати певний інструмент у вигляді тесту від Google, у якому перелічено шляхом інтерактивних зображень найбільш типові випадки фішингових листів – маскування під бренди, підробка послань, пропозиції грошей [13].

Фішинг мав місце у політичній практиці, упродовж згаданого випадку зі США у 2016 році. Російські хакери успішно атакували голову президентської кампанії Гілларі Клінтон Джона Подесту у 2016 році не за допомогою потужного програмного забезпечення-вимагача. Натомість росіяни застосували один із найстаріших засобів у хакерській історії – фішинг електронною поштою. Російські хакери надіслали Подесту

електронного листа , який виглядав так, ніби він надійшов з Gmail, із проханням змінити пароль. Коли Подеста натиснув кнопку в листі, ввів своє ім'я користувача та пароль, ненавмисно розкривши росіянам свої облікові дані для входу. Після цього зламу російське агентство військової розвідки атакувало щонайменше 109 співробітників передвиборчого штабу Клінтон за допомогою 214 унікальних фішингових електронних листів [14].

Окрім пошти, загроз працівникам публічних установ несе відвідування сайтів, у першу чергу, сторонніх сайтів. Тут може бути корисним розрізняти сайт з протоколам з'єднання http та https, де друга категорія відрізняється наявністю протоколу з'єднання безпеки. У першому випадку протоколу з'єднання користування сайтом не є конфіденційним – інформація, що вводиться, не захищається власниками цього інтернет-ресурсу, тобто не шифрується від сторонніх користувачів [15]. Крім того, є момент, що інформація на незахищеному сайті може подаватися трішки швидше. Відповідно, конфіденційну інформацію, навіть паролі та логіни, як вже згадувалося, потрібно вводити лише на сайтах з другим варіантом протоколу з'єднання.

Інші аспекти, пов'язані з відвідуванням сайтів та пов'язаними з цим загрозами торкаються cookie файлів. Файли cookie являють собою невеликі фрагменти тексту, які відвіданий сайт використовує для зв'язку з користувачем. Завдяки подібним файлам сайт запам'ятовує потрібну інформацію, щоб користувачам було легше відвідувати сайт наступного разу. Без використання подібних файлів нове відвідування сайту було б, як у перший раз, у браузерах не було б збереження, корзина теж не працювала б. Водночас, cookie файли допомагали працювати таргетованій рекламі як у Google відображається портрет користувача. Проте, окрім цієї монетизації, є інші неодностайні моменти, що пов'язані з подібними файлами. Конфіденційність в інтернеті достатньо важлива як публічним службовцям, так і звичайним користувачам. Хоча файли cookie за своєю суттю не є шкідливими, їх увімкнення може призвести до різних ризиків щодо конфіденційності та безпеки. Оскільки файли cookie можуть відстежувати та записувати онлайн-активність користувачів, їх можна використовувати для створення профілю поведінки, інтересів та звичок перегляду веб-сторінок. Проблема полягає не в самому відстеженні, а в тому, що компанії можуть робити з цією інформацією. Деякі можуть використовувати її для цільової реклами для онлайн-покупок, тоді як інші можуть продавати цю інформацію стороннім рекламним та веб-аналітичним компаніям без згоди користувача. Викрадення сеансу теж характерна файлам – хакери можуть використовувати файли cookie для перехоплення сеансів перегляду веб-сторінок і, по суті, отримання доступу до облікових записів користувачів. Перехоплення сеансу часто відбувається, коли сайт не шифрує файли cookie, що робить їх вразливими до перехоплення. Але це питання більше до використання https. Крім цього характерно зловживання сторонніми файлами cookie – якщо недобросовісний рекламодавець або маркетингове агентство має доступ до даних відстеження, вони можуть використовувати їх для зловмисних цілей, таких, як створення цільових фішингових шахрайств або розгортання шкідливого програмного забезпечення, що також відоме як шкідлива реклама.

Для публічних службовців важливою є перевірка сайтів на дотримання умов користування cookie файлам. Одним із сайтів, що можуть у цьому допомогти, назвемо cookiemetrix – визначає, чи сайт відповідає Закону ЄС про файли cookie, і дає інформацію про файли cookie, встановлені з веб-сайту, до того, як відвідувачі дадуть згоду [16]. Окрім цього сайту можна також на сайтах переглядати, натискаючи на місце протоколу з'єднання, які файл використовує сайт, та чи можна відключити файли.

Наприкінці напрямків загроз для дотримання цифрової гігієни потрібно назвати віруси, що частково переходять на сферу кібербезпеки. Тематика вірусів, напевно,

найпопулярніша серед перелічених тем у цьому дослідженні. Прикладом вірусу, що був спрямований на держустанови, можна назвати SUNBURST. SUNBURST була атакою на ланцюг поставок, яка використовує бекдор, імплантований у постачальника, для атаки та опосередкованого компрометування організацій по всьому світу. Orion, програмне забезпечення SolarWinds, яке було скомпрометовано злочинцями, використовувалося близько 33 000 державних та приватних клієнтів. Багато з них були компаніями зі списку Fortune 500 та федеральними урядовими установами. Атаку виявлено у грудні 2020 року, через вісім місяців після першого порушення. Вона вплинула на урядові установи США, технологічні компанії та країни, включаючи Канаду, Бельгію, Велику Британію та Ізраїль. Джерелом був фрагмент шкідливого програмного забезпечення, доставлений у вигляді DLL-файлу Windows (SolarWinds.Orion.Core.BusinessLayer.dll), імплантованого в пакет оновлення SolarWinds [17].

Торкаючися тем вірусів, потрібно розглянути також антивіруси. Серед антивірусів теж є ті, що несуть небезпеку. До подібних можна назвати антивіруси від російських розробників. Крім того, антивіруси оновлюються з певним часовим лагом, який потрібен на підтягування свіжих сигнатур. Як варіант, що не потребує встановлення на пристрій, є Вірус Тотал, на якому можна перевірити як сайт, так і файл [18].

Висновки. Звісно, це лише базові елементи безпечного користування поштою для державного службовця. У дослідженні цифрова гігієна публічного службовця поділяється на умовні блоки: безпечне користування поштою (управління паролями, розпізнавання фішингових атак), грамотне поводження на сторонніх сайтах (звернення уваги на протокол з'єднання сайтів, розгляд cookie файлів, перевірка сайту на віруси). Підсумовуючи дослідження, потрібно відзначити, що, в першу чергу, працівник публічного органу влади має відрізняти свою особисту та корпоративну пошту, що знаходиться в екосистемі установи. Реєструватися на різних сайтах з корпоративної пошти потенційно небезпечно для цілісності системи, бо будь-який сайт зі значною кількістю користувачів можуть зламати з метою комерційної реалізації масиву інформації. Важливо розуміти, що національна безпека є складною системою, а, як відомо, цілісність системи визначається цілісністю найбільш слабкого елементе, в рамках дослідження – необережного публічного службовця.

Conclusions. Of course, these are only the basic elements of safe use of mail for a civil servant. In the study, the digital hygiene of a public employee is divided into conditional blocks: safe use of mail (password management, recognition of phishing attacks), competent behavior on third-party sites (paying attention to the site connection protocol, considering cookie files, checking the site for viruses). Summing up the study, it should be noted that, first of all, an employee of a public authority should distinguish between their mail and corporate mail located in the institution's ecosystem. Registering on different sites from corporate mail is potentially dangerous for the integrity of the system, because any site with a significant number of users can be hacked for commercial sale of an array of information. It is important to understand that national security is a complex system, and, as is known, the integrity of the system is determined by the integrity of the weakest element, in the framework of the study – a careless public employee.

Список використаних джерел

1. Наместнік В. В. Цифрова компетентність публічних службовців: сутність поняття. *Інституціоналізація публічного управління в Україні в умовах євроінтеграційних та глобалізаційних викликів* : матеріали щоріч. Всеукр. наук.-практ. конф. за міжнар. участю (Київ, 24 трав. 2019 р.) : у 5 т. Київ, 2019. Т. 4. С. 67–86.
2. Копняк К. В., Покиньчереда В. В. Формування цифрової компетентності державних службовців у процесі фахової підготовки. *Державне управління: удосконалення та розвиток*. 2021. № 10. DOI: https://doi.org/10.32702/2307-2156-2021.10.31

3. Фостікова В. Сучасні вимоги до цифрових компетентностей державних службовців. *Аспекти державного управління.* 2020. Т. 8. Спецвип. № 1. С. 133–135. DOI: https://doi.org/10.15421/152061
4. Гуцалюк М. В. Окремі аспекти боротьби з організованою кіберзлочинністю. *Актуальні проблеми управління інформаційною безпекою держави* : зб. тез наук.-практ. конф. (м. Київ, 4 квітня 2019 р.). Київ: Нац. акад. СБУ, 2019. С. 199–201.
5. Скибун О. Ж. Кібергігієна як складова формування цифрової держави. *Вісник Національної академії державного управління при Президентові України. Серія «Державне управління»*. 2021. № 2 (101). С. 39–46.
6. Цифрограм для держслужбовців. URL: https://osvita.diia.gov.ua/digigram (дата звернення: 07.05.2025).
7. Менеджер паролів Google. URL: https://passwords.google.com/ (дата звернення: 07.05.2025).
8. WikiLeaks releases thousands of documents about Clinton and internal deliberations. URL: https://www.washingtonpost.com/news/post-politics/wp/2016/07/22/on-eve-of-democratic-convention-wikileaks-releases-thousands-of-documents-about-clinton-the-campaign-and-internal-deliberations/ (дата звернення: 07.05.2025).
9. Have i been pwned? URL: https://haveibeenpwned.com/ (дата звернення: 07.05.2025).
10. 200,000 Facebook Marketplace user records leaked on hacking forum. URL: https://www.bleepingcomputer.com/news/security/200-000-facebook-marketplace-user-records-leaked-on-hacking-forum/ (дата звернення: 07.05.2025).
11. Ваш пароль, як сейф. Перевір його надійність. Zillya! URL: https://zillya.ua/check-password (дата звернення: 07.05.2025).
12. Генератор Кіберполіції України. URL: https://cyberpolice.gov.ua/generate-password/ (дата звернення: 07.05.2025).
13. Can you spot when you're being phished? URL: https://phishingquiz.withgoogle.com/?hl=en (дата звернення: 07.05.2025).
14. Phishing for political secrets: Hackers take aim at midterm campaigns. URL: https://www.cbsnews.com/news/campaign-2018-email-phishing-hackers-take-aim-at-midterm-elections/ (дата звернення: 07.05.2025).
15. Is enabling cookies a security risk? Best practices for users and businesses. URL: https://www.dsolutionsgroup.com/is-enabling-cookies-a-security-risk-best-practices-for-users-and-businesses/ (дата звернення: 07.05.2025).
16. Determines if your website is not comply with EU Cookie Law. URL: https://www.cookiemetrix.com/ (дата звернення: 07.05.2025).
17. SUNBURST backdoor malware: What it is, how it works, and how to prevent it | Malware spotlight. URL: https://www.infosecinstitute.com/resources/malware-analysis/sunburst-backdoor-malware-what-it-is-how-it-works-and-how-to-prevent-it-malware-spotlight/ (дата звернення: 07.05.2025).
18. Virustotal. URL: https://www.virustotal.com/gui/home/upload (дата звернення: 07.05.2025).

References

1. Namestnik V. V. (2019). Tsyfrova kompetentnist publichnykh sluzhbovtsiv: sutnist ponyattya. [Digital competence of public officials: the essence of the concept], materials of the Ukr. science-practice conf. *Instytutsionalizatsiya publichnoho upravlinnya v Ukrayini v umovakh yevrointehratsiynykh ta hlobalizatsiynykh vyklykiv*, Press NADU, Kyiv. Part 4, pp. 67–86.
2. Kopniak K. V., & Pokynchereda V. V. (2021) Formuvannia tsyfrovoi kompetentnosti derzhavnykh sluzhbovtsiv u protsesi fakhovoi pidhotovky. [Formation of digital competence of civil servants in the process of professional training] *Derzhavne upravlinnia: udoskonalennia ta rozvytok*, no. 10. DOI: https://doi.org/10.32702/2307-2156-2021.10.31
3. Fostikova V. (2020) Suchasni vymohy do tsyfrovykh kompetentnostei derzhavnykh sluzhbovtsiv [Modern requirements for digital competencies of civil servants]. *Aspekty derzhavnoho upravlinnia*, no. 8, vol. 1, pp. 133–135. DOI: https://doi.org/10.15421/152061
4. Gucaljuk M. V. (2019). Okremi aspekty borot'by z organizovanoju kiberzlochyn-nistju. *Aktual'ni problemy upravlinnja informacijnoju bezpekoju derzhavy* [Some aspects of the fight against organized cybercrime. Current issues of information security management of the state]. Zbirnyk tez naukovo-praktychnoi konferencii. Kyi'v: Nacional'na akademija SBU, pp. 199–201.
5. Skybun O. Zh. (2021) Kiberhihiiena yak skladova formuvannia tsyfrovoi derzhavy [Cybergigiena as a component of the formation of a digital state]. Bulletin of the National Academy of Public Administration under the President of Ukraine. Series "Public Administration", no. 2 (101), pp. 39–46.
6. Tsyfrohram dlya derzhsluzhbovtsiv. Available at: https://osvita.diia.gov.ua/digigram (accessed: 07 May 2025).
7. Menedzher paroliv Google. Available at: https://passwords.google.com/ (accessed: 07 May 2025).
8. WikiLeaks releases thousands of documents about Clinton and internal deliberations. Available at: https://www.washingtonpost.com/news/post-politics/wp/2016/07/22/on-eve-of-democratic-convention-wikileaks-releases-thousands-of-documents-about-clinton-the-campaign-and-internal-deliberations/ (accessed: 07 May 2025).

9. Have i been pwned? Available at: https://haveibeenpwned.com/ (accessed: 07 May 2025).
10. 200,000 Facebook Marketplace user records leaked on hacking forum. Available at: https://www.bleepingcomputer.com/news/security/200-000-facebook-marketplace-user-records-leaked-on-hacking-forum/ (accessed: 07 May 2025).
11. Vash parol′, yak seyf. Perevir yoho nadiynist′. Zillya! Available at: https://zillya.ua/check-password (accessed: 07 May 2025).
12. Henerator Kiberpolitsiyi Ukrayiny. Available at: https://cyberpolice.gov.ua/generate-password/ (accessed: 07 May 2025).
13. Can you spot when you're being phished? Available at: https://phishingquiz.withgoogle.com/?hl=en (accessed: 07 May 2025).
14. Phishing for political secrets: Hackers take aim at midterm campaigns. Available at: https://www.cbsnews.com/news/campaign-2018-email-phishing-hackers-take-aim-at-midterm-elections/ (accessed: 07 May 2025).
15. Is enabling cookies a security risk? Best practices for users and businesses. Available at: https://www.dsolutionsgroup.com/is-enabling-cookies-a-security-risk-best-practices-for-users-and-businesses/ (accessed: 07 May 2025).
16. Determines if your website is not comply with EU Cookie Law. Available at: https://www. cookiemetrix.com/ (accessed: 07 May 2025).
17. SUNBURST backdoor malware: What it is, how it works, and how to prevent it | Malware spotlight. Available at: https://www.infosecinstitute.com/resources/malware-analysis/sunburst-backdoor-malware-what-it-is-how-it-works-and-how-to-prevent-it-malware-spotlight/ (accessed: 07 May 2025).
18. Virustotal. Available at: https://www.virustotal.com/gui/home/upload (accessed: 07 May 2025).