УДК 004.056.5:351.862
DOI https://doi.org/10.32782/tnv-pub.2025.2.8

ЦИФРОВІ ВИТОКИ ІНФОРМАЦІЇ ЯК ЗАГРОЗА ДЛЯ НАЦІОНАЛЬНОЇ БЕЗПЕКИ

Дубель М. В. – *доктор філософії з міжнародних економічних відносин, старший викладач кафедри політології та державного управління Донецького національного університету імені Василя Стуса*
ORCID: 0000-0003-2229-0419

Стаття присвячена визначенню особливостей категорії цифрових витоків інформації як загрози для системи національної безпеки. Підкреслюється, що операції злому та витоку можна розділити на два чітких етапи: отримання даних і контенту за допомогою кібератак («злом») і їх поширення за допомогою різних стратегій («витік»). Витоки інформації стали особливо популярні протягом десятиліття 2010–2020 років, коли у публічному середовищі трапилася серія значних випадків. У статті розглядаються приклади з досвіду інших держав. Особлива увага у дослідженні приділяється хакерському втручанню у виборчі процеси у США в 2016 році та у Франції у 2017 році. У першому випадку подібний злам пошти Національного комітету Демократичної партії призвело до дискредитації політичної сили та поразки на виборах. У другому випадку політична партія En Marche змогли довести підробку інформації витоку та перемогти на виборах. Крім визначених випадків, також аналізуються витоки, таких як The Drone Papers, Panama Papers та Panama Papers. У статті приділяється визначенню різних мотивів, пов'язані з витоком інформації, конкретних практик або технологій витоків. Отже, можна визначити основні способи потенційної боротьби з витоками інформації, що може нести потенційну загрозу національній безпеці. В першу чергу, працівники державного сектору, представники різних політичних сил мають розрізняти особисту та публічну пошту, не використовуючи однакові паролі, бо, у випадку зламу пошти працівника, злочинці отримують доступ до конференційної установи місця роботи. Крім того, важливу роль грає довіра при обміні інформації через електронні способи зв'язку – працівники мають знати, що доступ до свого акаунту не потрібно надавати техпідтримці без доказу їхньої участі в організації. Не менш важливо й те, що важливу інформацію взагалі краще не надсилати поштою.

Ключові слова: *цифрові витоки, злам пошти, кібератака, національна безпека, фішинг.*

Dubel M. V. Digital information leaks as a threat to national security

The article is devoted to defining the features of the category of digital information leaks as a threat to the national security system. It is emphasized that hacking and leaking operations can be divided into two clear stages: obtaining data and content through cyberattacks ("hacking") and their distribution using various strategies ("leaking"). Information leaks became especially popular during the decade of 2010–2020, when a series of significant cases occurred in the public environment. The article considers examples from the experience of other states. Particular attention in the study is paid to hacker interference in the electoral processes in the USA in 2016 and in France in 2017. In the first case, a similar hack of the Democratic National Committee's mail led to the discrediting of the political force and defeat in the elections. In the second case, the political party En Marche was able to prove the falsification of the leaked information and win the elections. In addition to the specific cases, leaks such as The Drone Papers, Panama Papers and Panama Papers are also analyzed. The article focuses on identifying various motives associated with information leakage, specific practices or technologies of leaks. Thus, it is possible to identify the main ways to potentially combat information leaks, which may pose a potential threat to national security. First of all, public sector employees, representatives of different political forces should distinguish between personal and public mail, not using the same passwords, because, in the event of hacking an employee's mail, criminals gain access to the conference facility of the workplace. In addition, trust plays an important role in the exchange of information via electronic means of communication – employees should know that access to their account should not be provided to technical support without proof of their participation in the organization. No less important is the fact that it is better not to send important information by mail at all.

Key words: *digital leaks, email hacking, cyberattack, national security, phishing.*

Постановка проблеми. Питання витоків інформації розглядається представникам різних напрямків досліджень з одного боку, як можливість отримання сенсаційних публікацій (журналісти), так і з боку загрози національній безпеці держав (фахівці з державного управління, політологи). В умовах повномасштабного вторгнення російських агресорів в Україну на перший план, на думку дослідника, має виходити питання саме національної безпеки. У зв'язку з тим, що російські загарбники діють не лише методами безпосередньо фізичної агресії, так і шляхом зламу поштових адрес та, як наслідок, витоку інформації, яка може висвітлити конфіденційну інформацію. Крім того, навіть по відношенню до держав, які не ведуть війну з Росією, злочинці втручаються у процес проведення виборів, з метою приведення до влади «зручних кандидатів».

Звісно, це спонукає державу до розробки стандартів та програм навчання, що могли б допомогти держслужбовцям виконувати багатогранний функціонал. З Професійних стандартів Реєстру Кваліфікацій значна кількість професії потребують диплому спеціальності 281 (за новим стандартом D4) «Публічне управління та адміністрування» [1]. Зі стандарту цієї спеціальності можна визначити наступні програмні результати навчання «РН9 Знати основи електронного урядування»; «РН10 Уміти користуватися системою електронного документообігу» [2]. Але, окрім цих напрямків потрібно відзначити дотримання цифрової гігієни. Особливо важливо використовувати інструментарій цифрових навиків у державній службі в умовах воєнного стану, коли кожен з працівників такого напрямку може бути мішенню для ворога.

Аналіз останніх досліджень і публікацій. Питанню витоків інформації з конфіденційного у публічне середовище, а також розгляду наслідків подібних дій присвячено праці таких вітчизняних вчених, як М. Стрельбіцького, В. Мазура, і В. Лемешка [3], О. Берназюк [4], О. Кіпішинова, Л. Сметаніна [5], М. Дмитришин, М. Жураківська [6]. Проте, тема не втрачає свою актуальність через різноманіття цифрових викликів.

Метою статті є визначення особливостей цифрових витоків конфіденційної інформації як загрози для системи національної безпеки.

Виклад основного матеріалу. Одним з найбільш розповсюджених напрямків загроз для діяльності державних службовців є потенціальні витоків конференційної інформації. Окрім досвіду з вітчизняної практики актуальним буде також розглянути випадки з міжнародної практики, особливо враховуючи, що більшість ініціаторів загроз російські хакери.

Витоки конференційної державної інформації стають все більш вагомими для динамічного цифрової публічного середовища, що пов'язано з діями різних акторів, яким притаманні різноманітні цілями. З одного боку, витоки виступають драйвером для критичних журналістських розслідувань. З іншого боку, витоки також стали загальною стратегією, пов'язаною з кампаніями впливу, фінансованими державою хакерствами та кібертактикою в умовах сучасних, у тому числі і гібридних війн. Витоки інформації також використовувалися як стратегія в рамках інформаційного хаосу, зокрема в акціях «дезінформації», часто з явними пропагандистськими цілями. Операції злому та витоку передбачають два чітких етапи: отримання даних і контенту за допомогою кібератак («злом») і їх поширення за допомогою різних стратегій («витік»).

Витоки інформації стали особливо популярні протягом десятиліття 2010–2020 років, коли у публічному середовищі трапилася серія значних випадків.

Типовим прикладом операції зі злому та витоку є оприлюднення інформації, отриманої від Національного комітету Демократичної партії і пов'язаних організацій і людей перед виборами в США 2016 року.

22 липня 2016 року, під час президентської кампанії у США 2016 року, WikiLeaks опублікував серію приватних електронних листів, що належать Національному комітету Демократичної партії. Цей витік включав майже 20 000 електронних листів і 8 000 вкладень, які належали семи вищим посадовим особам Національного комітету Демократичної партії (подія, яку ця стаття буде називати «зломом 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 [7].

Злам Національного комітету Демократичної партії став темою президентських виборів і поштовхом для розслідування Федеральним бюро розслідувань. Кілька чиновників із національної безпеки США назвали це «проблемою національної безпеки та контррозвідки». Події після Зламу Національного комітету Демократичної партії включали організовані протести проти Національного комітету Демократичної партії і відставку голови Деббі Вассерман Шульц.

Аналітики CrowdStrike виявили двох противників, які постійно проживають у мережі Національного комітету Демократичної партії: «Fancy Bear» і «Cozy Bear», які раніше були причетні до інших кіберінцидентів, включаючи проникнення в несекретні мережі Білого дому, Державного департаменту США та інших американських і міжнародних цілей. Витонченість злому – і його схожість із проникненням в інші чутливі політичні цілі, раніше організовані Cosy Bear і Fancy Bear – викликали підозру, що до цього причетна іноземна держава. 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.

Перебуваючи в комп'ютерній системі Національного комітету Демократичної партії, Fancy Bear і Cozy Bear викрали значні обсяги інформації на інші сервери, включаючи електронні листи офіційних осіб Демократичної партії, які вказували на те, що вони віддають перевагу Гілларі Клінтон над Берні Сандерсом, обома кандидатами на висування в президенти від партії в 2016 році. Крім того, багато електронних листів містили інформацію про донорів партії, дані їхніх кредитних карток, номери соціального страхування та іншу особисту інформацію. Ці електронні листи були опубліковані на WikiLeaks у дві хвилі, і час кожної хвилі виглядав стратегічним. Перша партія (20 000 електронних листів і 8 000 вкладень) була опублікована 22 липня 2016 року, за кілька днів до з'їзду Демократичної партії у Філадельфії, де існували чутки, що вже незадоволені прихильники Берні Сандерса можуть спробувати зірвати офіційний процес висунення. Друга партія (8000 електронних листів) була оприлюднена 6 листопада 2016 року, у неділю перед виборами. Обидві дати публікації точно відповідали відомим точкам перелому кампанії, коли увага громадськості була в зеніті, і незадоволені демократи були найбільш схильні до впливу негативної інформації про Клінтон і маніпуляції Національного комітету Демократичної партії на первинних виборах.

Крім того, важливо зазначити, що деякі операції зі злому та витоку також містять підроблені елементи. Це було особливо очевидно під час кампанії Клінтон

і витоків інформації Демократичної партії, які відбулися в контексті президентських виборів у США 2016 року і були здійснені хакерами, пов'язаними з російськими спецслужбами. У цьому випадку російські хакери, які стояли за цією операцією, створили веб-сайти фейкових новин, щоб оприлюднити інформацію, отриману ними в результаті кібератак. Вони також використовували підроблену особу «Guccifer 2.0», яка представила себе незалежним румунським хакером, який бере на себе відповідальність за операцію злому та витоку. Ця персона зіграла вирішальну роль у передачі вкраденої інформації WikiLeaks і, наприклад, американським журналістам. Створення підроблених персонажів, таких як Guccifer 2.0, було навмисною стратегією приховування справжніх осіб і намірів злочинців. Guccifer 2.0 також виступив публічним обличчям операції, сприяючи охопленню журналістів і інформаційних організацій для популяризації витоків, зберігаючи видимість легітимності.

Національного комітету Демократичної партії був не єдиною метою російської операції. Третя партія електронних листів, опублікованих WikiLeaks, належала Джону Подесті, голові президентської кампанії Клінтон і колишньому голові апарату Білого дому. Електронні листи були отримані шляхом надсилання фішингового листа на обліковий запис Gmail Подести в березні 2016 року. Електронні листи Подести містили докази суперечливих зауважень, які Клінтон робила різним аудиторіям Уолл-стріт, включаючи банкірів Goldman Sachs, надаючи довіри згубним звинуваченням у тому, що вона підтримувала тісні стосунки з фінансовим сектором. Цей витік стався через день після того, як Білий дім звинуватив Росію в організації злому Національного комітету Демократичної партії [8].

Потенційно важливий характер навіть найменшої помилки демонструє витік даних Подести. Коли помічник Подести спробував автентифікувати фішинговий електронний лист у ІТ-персоналу Національного комітету Демократичної партії, йому сказали, що воно «законне», що виявилося опечаткою, оскільки ця відповідь також містила рекомендацію змінити пароль Gmail Подести. Кампанія Трампа та розчаровані прихильники Сандерса широко використовували електронні листи Національного комітету Демократичної партії і Podesta, щоб атакувати та делегітимізувати Клінтон. Ці напади могли вплинути на результати президентських виборів у США.

Інші операції зі злому та витоку продемонстрували ще більш явні верстви підробки. У 2017 році осіб, пов'язаних із політичною партією Еммануеля Макрона En Marche!, було зламано, а їхні електронні листи згодом злили в спробі підірвати кампанію Макрона за кілька днів до загальних виборів у Франції [9]. Витік і розповсюдження матеріалів збіглися з початком виборчої тиші, або медіа-блек-хауту. Це передбачено Виборчим кодексом Франції, який забороняє трансляцію «будь-яких повідомлень, що мають характер виборчої пропаганди», починаючи з опівночі напередодні виборів, тобто між п'ятницею та суботою 2017 року. У ЗМІ було вікно, щоб повідомити про публікацію витоку, але не було часу переглянути, перевірити та відповідально повідомити про вміст через крайній термін відключення та 15 ГБ розпакованих даних. Кампанія Макрона оприлюднила заяву, в якій пов'язала витік інформації з хакерськими атаками, спрямованими проти кампанії, підтвердивши законність деяких документів, наголосивши, що інші були підробленими. Заява також містила критику щодо часу публікації, стверджуючи, що це частина спроби демократичної дестабілізації, як це було видно під час президентських виборів у США роком раніше. Час витоку інформації був «прямою спробою маніпулювати виборчим процесом через вразливість, створену періодом виборчої тиші» [10].

Французький виборчий комітет у суботу вранці оприлюднив заяву про те, що кампанія Макрона повідомила його про витік, який також містить підроблені документи, і нагадав ЗМІ «про відповідальність, яку вони повинні нести, коли на карту поставлено вільне волевиявлення виборців і щирість голосування», і «просить органи преси, і зокрема їхні веб-сайти, не повідомляти про зміст цих даних» [11]. Приблизно в січні та лютому 2017 року, коли Макрон отримав перевагу в опитуваннях, цілеспрямовані інформаційні кампанії проти нього стали більш агресивними з двох основних джерел: кремлівських ЗМІ та американських альтернативних правих. Крім того, кампанія Макрона показала, що вони були ціллю кількох кібератак протягом виборчого періоду, деякі з яких можна було приписати Росії та були успішними. Незважаючи на те, що уряд Франції ніколи офіційно не приписував ні злом, ні витік інформації підтримуваним Росією акторам, аналіз, проведений дослідниками та компаніями з кібербезпеки, стверджує, що докази свідчать про зацікавленість Росії у підриві виборів у Франції. У зломі були схожі на російські шаблони, докази, які також були підтримані Агентством національної безпеки США, а також значна участь і вплив американських альтернативних правих у маніпулятивному дискурсі щодо витоку.

Витік інформації про Макрона полягав у зломі та розповсюдженні в Інтернеті 150 000 електронних листів і документів, які походять з кампанії Макрона та належать п'яти особам, пов'язаним з партією La République En Marche і близьким до її кандидата Еммануеля Макрона. Витоки були поєднанням справжніх електронних листів і підробок. Близько 9 ГБ даних було опубліковано користувачем під назвою EMLEAKS на сайті для обміну документами Pastebin, який дозволяв анонімну публікацію. Викрадені документи були опубліковані під назвою #MacronLeaks у соціальних мережах у форматі .eml із посиланням на Pastebin. У січні 2017 року охоронна фірма Trend Micro приписала Pawn Storm багато початкових фішингових атак. Останній вважався спецслужбами США інструментом Головного розвідувального управління Росії. Ці кібератаки були спричинені співучастю внутрішніх опонентів Макрона у Франції, особливо в ультраправих групах, які поширювали фейкові новини в соціальних мережах і перефразували та адаптували їх відповідно до французького культурного та політичного контексту. Серед осіб, які транслювали фейкові новини, створені Sputnik або Russia Today під час першого туру президентських виборів, більшість були прихильниками Франсуа Фійона та Марін Ле Пен [11]. Модель маніпуляції почалася з поширення інформації про Macron Leaks на 4Chan, потім у більш звичайних соціальних мережах, таких як Twitter, перш ніж її поширили американські альтернативно-праві та французькі ультраправі спільноти. Відразу після оприлюднення інформації про Макрона виборча комісія Франції опублікувала заяву, в якій закликала всі ЗМІ дотримуватися періоду припинення кампанії та взагалі не коментувати витоки до дня виборів, щоб захистити чесність виборчого процесу та його результатів. У той же час глава відділу кібероперацій Макрона Мунір Маджубі заявив, що витоки містять фейкову інформацію, що змусило WikiLeaks дистанціюватися від Macron Leaks.

Розглянемо більш коротко ще деякі приклади витоків, пов'язаного з публічними діячами.

The Drone Papers у 2015 році. Американське інформаційне видання The Intercept опублікувало розгорнуте розслідування секретних військових програм безпілотників США. Публікація базувалася на кеш-пам'яті витоку документів, отриманих журналістом The Intercept. У 2021 році колишнього співробітника розвідки Деніела Хейла засудили до 45 місяців в'язниці за розголошення матеріалів.

Після висунення перших звинувачень у 2019 році Хейл визнав себе винним у збереженні та передачі інформації про національну оборону [12].

Panama Papers у 2016 році. Панамські документи – це спільне розслідування офшорної економіки, проведене Süddeutsche Zeitung та Міжнародним консорціумом журналістів-розслідувачів у 2016 році. Розслідування викрило діяльність панамської компанії Mossack Fonseca, яка спеціалізується на наданні офшорних послуг. Спільне розслідування ґрунтувалося на 1,5 мільйонах фінансових і юридичних записів, проаналізованих групою з 370 міжнародних журналістів під керівництвом ICIJ. У 2017 році це розслідування отримало Пулітцерівську премію за роз'яснювальну репортажність і вважається одним з найбільш визначальних прикладів журналістики даних і транскордонних спільних розслідувань [13].

BlueLeaks у 2020 році. BlueLeaks – це назва, дана витоку 269 ГБ внутрішніх даних правоохоронних органів США, отриманих хакерським колективом Anonymous і оприлюднених групою прозорості DDoSecrets на своєму веб-сайті за допомогою однорангової технології обміну файлами BitTorrent у 2020 році. Витік виявив раніше недоступну інформацію про операції правоохоронних органів у США разом із особистою інформацією про офіцерів [14].

Ці приклади жодним чином не є вичерпними, коли йдеться про складність і різноманітність сучасних витоків інформації. Однак разом вони утворюють потенційно велику вибірку того, як витоки набули форми за останні роки.

Огляд вибраних тематичних досліджень показує, що витоки можуть відбуватися в різних режимах і діях. Наприклад, Drone Papers є відвертим випадком інформування. Тут викривач із розвідувального співтовариства розкрив інсайдерську інформацію, щоб висвітлити справи, що становлять суспільний інтерес, зовнішнім третім сторонам і спонукати до дій. Panama Papers характеризуються величезним обсягом залученої інформації та є яскравим прикладом «мегаловитоку», включаючи той факт, що вона була предметом широкомасштабного міжнародного журналістського розслідування. «Мегавитоки» можна віднести до інформування (якщо джерело є інсайдером), але журналістська практика, яку вони зазвичай включають – від журналістики даних до транскордонних розслідувань – робить їх чітко ідентифікованою категорією в екосистемі витоків [15]. Витік Національного комітету Демократичної партії також був для суспільних інтересів, оскільки внутрішні електронні листи Національного комітету Демократичної партії були викрадені зовнішніми хакерами, а потім оприлюднені за допомогою різних стратегій. Вся операція була частиною акції політичного впливу на державному рівні, яка не мала ані інформаційного, ані активістського характеру.

Про мотиви, пов'язані з витоком інформації, важко здогадуватися або тлумачити, особливо враховуючи той факт, що вони можуть не бути оприлюдненими чи повідомленими. Однак, принаймні у випадках, про які тут йдеться, деякі елементи доступні. Ймовірне джерело Drone Papers, Деніел Хейл, визнав себе винним у «збереженні та передачі інформації про національну оборону» репортеру, фактично підтверджуючи свою роль інформатора [16]. Для BlueLeaks джерелом даних було виявлено групу хактивістів Anonymous; однак, враховуючи ефемерний і децентралізований характер групи, офіційних заяв про відповідальність немає. Тим не менш, деякі спостерігачі включили злам BlueLeaks до ширшого набору цифрових дій у відповідь, увічнених членами Anonymous після вбивства Джорджа Флойда [17] . Стосовно Panama Papers викривач Джон Доу опублікував маніфест про обґрунтування витоків, стверджуючи, що вони були вмотивовані «не якоюсь конкретною політичною метою, а просто тому, що я достатньо розумів їхній

зміст, щоб усвідомити масштаб описаної в них несправедливості» [18]. Нарешті, оскільки витік Національного комітету Демократичної партії був частиною таємної операції, здійсненої державним діячем, немає чітких деталей про мотивацію та обґрунтування. Однак було доведено, що російські агенти розвідки використовували підроблену особу на прізвисько Guccifer 2.0, щоб зімітувати підробленого румунського хактивіста як актора, відповідального за злом і витік, щоб операція могла виглядати як спроба хактивіста, тим самим маскуючи свої геополітичні мотиви [7].

Коли справа доходить до конкретних практик або технологій, пов'язаних із витоком, тематичні дослідження пропонують різне уявлення про те, як витоки можуть бути передані визначеним одержувачам або опубліковані, особливо з точки зору використання спеціальних технологій або практик інформаційної безпеки [19]. Хоча подібні висновки були надані не у всіх досліджуваних випадках, деякі з них проливають світло на те, як криптографія може бути безпосередньо пов'язана з витоками та як використання інструментів шифрування може підтримувати або навіть визначати певні випадки витоків. В інших випадках, чи використовувалося шифрування взагалі, залишилося нерозкритим. Незрозуміло, чи The Drone Papers почалося з витоку через платформу витоку The Intercept, але Міністерство юстиції Сполучених Штатів цитує в заяві посилання на невизначену «платформу обміну зашифрованими повідомленнями», через яку ймовірне джерело витоку спілкувалося з репортером [12]. У випадку з Панамськими документами відомо, що Джон Доу анонімно зв'язався з Süddeutsche Zeitung через невизначені зашифровані канали та попросив журналістів спілкуватися лише в Інтернеті та через безпечні канали [18]. За даними Міністерства юстиції Сполучених Штатів, WikiLeaks, перша платформа для розповсюдження інформаторів, отримала електронні листи, пов'язані з витоком Національного комітету Демократичної партії, «через зашифровані канали, у тому числі, можливо, через приватну комунікаційну систему WikiLeaks», що – хоча це не зазначено – могло бути посиланням на анонімну зашифровану систему подання WikiLeaks [19]. Навпаки, DDoSecrets не опублікував інформацію про те, як вони опинилися у володінні документами BlueLeaks, але на веб-сайті колективу вказані різні форми зашифрованого зв'язку як потенційні джерела.

Висновки. З початку російського повномасштабного військового вторгнення на територію нашої держави в 2022 році проблеми витоків конфіденційної інформації постали на абсолютно новому рівні у зв'язку з кібератаками. В той ж час історичні приклади витоків інформації зі світової практики так само як і витоки Національного комітету Демократичної партії або партії Макрона у Франції вказують нам на те, що російські хакери спрямовують свою діяльність на підрив демократичних процесів.

Отже, можна визначити основні способи потенційної боротьби з витоками інформації, що може нести потенційну загрозу національній безпеці. В першу чергу, працівники державного сектору, представники різних політичних сил мають розрізняти особисту та публічну пошту, не використовуючи однакові паролі, бо, у випадку зламу пошти працівника, злочинці отримують доступ до конференційної установи місця роботи. Крім того, важливу роль грає довіра при обміні інформації через електронні способи зв'язку – працівники мають знати, що доступ до свого акаунту не потрібно надавати техпідтримці без доказу їхньої участі в організації. Не менш важливо й те, що важливу інформацію взагалі краще не надсилати поштою.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ:

1. Відомості про Професійні стандарти. URL: https://register.nqa.gov.ua/profstandarts?profession_id=523

2. Стандарт вищої освіти рівень вищої освіти перший (бакалаврський) рівень ступінь вищої освіти «Бакалавр» галузь знань 28 «Публічне управління та адміністрування». URL: https://mon.gov.ua/static-objects/mon/sites/1/vishcha-osvita/zatverdzeni%20standarty/12/21/281-Publ.upr.ta.administruvannya-bakalavr.21.01.22.pdf

3. Стрельбіцький М., Мазур В., Лемешко В. Протоколи обміну 'агрегованої' інформації в інформаційно–телекомунікаційній системі. *Сучасні інформаційні технології у сфері безпеки та оборони*. 2023. Вип. 46(1), с. 51–55.

4. Берназюк О.О. Електронне урядування як особлива форма публічного управління: поняття та проблеми запровадження. *Наук. вісник Ужгород. нац. ун-ту. Серія Право*. 2019. Вип. 55. Том 2. С. 32–35.

5. Кіпішинова О., Сметаніна Л. Цифровізація управління персоналом в органах державної влади. *Актуальні проблеми державної служби*. 2021. No 3 (84). С. 202–205.

6. Витік персональних даних в електронному урядуванні: реалії та проблеми державних вебсайтів і порталів. *Публічне управління і адміністрування в Україні*. 2020. № 20. С. 111–119.

7. Kilovaty, I. (2018). Doxfare: politically motivated leaks and the future of the norm on non-intervention in the era of weaponized information. *Harv. Nat'l Sec. J.*, *9*, 146.

8. Briant, E. L. (2023). Hack attacks. How cyber intimidation and conspiracy theories drive the spiral of "secrecy hacking". In J. Steel & J. Petley (Eds.), *The Routledge companion to freedom of expression and censorship* (pp. 285–296).

9. Orban, F. (2024). Sowing the Seeds of Distrust? Foreign Cyber Interference in the French Presidential Election in 2017 and 2022. *Trust under Threat*, 157.

10. Downing, J., & Ahmed, W. (2019). # MacronLeaks as a "warning shot" for European democracies: challenges to election blackouts presented by social media and election meddling during the 2017 French presidential election. *French Politics*, *17*, 257–278.

11. Bollmann, H. S., & Gibeon, G. (2022). *The spread of hacked materials on Twitter: A threat to democracy? A case study of the 2017 Macron Leaks* (Doctoral dissertation, Hertie School).

12. Barnes, J.E. (2021). Ex-Intelligence Analyst Is Sentenced for Leaking to a Reporter. *The New York Times*. URL: https://www.nytimes.com/2021/07/27/us/politics/daniel-hale-leaksentence.html.

13. Cabra, M. and Kissane, E. (2016). Wrangling 2.6TB of data: The people and the technology behind the Panama Papers. *ICIJ.org*. URL: https://www.icij.org/investigations/panamapapers/data-tech-team-icij/

14. Lee, M. (2020). Hack of 251 Law Enforcement Websites Exposes Personal Data of 700,000 Cops. *The Intercept*. URL: https://theintercept.com/2020/07/15/blueleaks-anonymous-ddoslaw-enforcement-hack/.

15. Woodall, A. (2018). Media capture in the era of megaleaks. *Journalism*, 19(8), 1182–1195.

16. United States Department of Justice. (2021). Former Intelligence Analyst Pleads Guilty to Disclosing Classified Information. URL: https://www.justice.gov/usao-edva/pr/former-intelligenceanalyst-pleads-guilty-disclosing-classified-information.

17. Beran, D. (2020). The Return of Anonymous. *The Atlantic*. URL: https://www.theatlantic.com/technology/archive/2020/08/hacker-group-anonymousreturns/615058/

18. Süddeutsche Zeitung. (2016). John Doe's Manifesto. URL: https://panamapapers.sueddeutsche.de/articles/572c897a5632a39742ed34ef/

19. Di Salvo, P. (2024). A Typology of Digital Leaks as Journalistic Source Materials. In *The Palgrave Handbook of Everyday Digital Life* (pp. 469–488). Cham: Springer International Publishing.

REFERENCES:

1. Vidomosti pro Profesiyni standarty. https://register.nqa.gov.ua/profstandarts?profession_id=523 [in Ukrainian]/

2. Standart vyshchoyi osvity riven′ vyshchoyi osvity pershyy (bakalavrs′kyy) riven′ stupin′ vyshchoyi osvity «Bakalavr» haluz′ znan′ 28 «Publichne upravlinnya ta administruvannya». https://mon.gov.ua/static-objects/mon/sites/1/vishcha-osvita/zatverdzeni%20standarty/12/21/281-Publ.upr.ta.administruvannya-bakalavr.21.01.22.pdf [in Ukrainian]/

3. Strel′bits′kyy, M., Mazur, V. i Lemeshko, V. (2023) «Protokoly obminu ‘ahrehovanoyi″ informatsiyi v informatsiyno–telekomunikatsiyniy systemi» [Protocols for the exchange of «aggregated» information in the information and telecommunication system], *Suchasni informatsiyni tekhnolohiyi u sferi bezpeky ta oborony*, 46(1), 51–55 [in Ukrainian].

4. Bernaziuk O.O. (2019). Elektronne upravlinnia yak osoblyva forma publichnogo upravlinnia: ponyattia ta problemy zaprovadzhennia [E-government as a Special Form of Public Administration: Concepts and Implementation Issues]. *Nauk. visnyk Uzhhorod. nats. un-tu. Seriia Pravo*. Vyp. 55. Tom 2. S. 32–35 [in Ukrainian].

5. Kipishynova O.V., Smetanina L.S. Cyfrovizacija upravlinnja personalom v organah derzhavnoi’ vlady [Digitalization of personnel management in public authorities]. *Aktual’ni problemy derzhavnoi’ sluzhby*. 2021. № 3(84). S. 202–205 [in Ukrainian].

6. Dmytryshyn, M.V., & Zhurakivs′ka, M.I. (2020). Vytik personal′nykh danykh v elektronnomu uryaduvanni: realiyi ta problemy derzhavnykh vebsaytiv i portaliv [Leakage of personal data in e-government: realities and problems of state websites and portals]. Publichne upravlinnya i administruvannya v Ukrayini. 20. S. 111–119 [in Ukrainian].

7. Kilovaty, I. (2018). Doxfare: politically motivated leaks and the future of the norm on non-intervention in the era of weaponized information. *Harv. Nat’l Sec. J.*, *9*, 146.

8. Briant, E. L. (2023). Hack attacks. How cyber intimidation and conspiracy theories drive the spiral of “secrecy hacking”. In J. Steel & J. Petley (Eds.), *The Routledge companion to freedom of expression and censorship* (pp. 285–296).

9. Orban, F. (2024). Sowing the Seeds of Distrust? Foreign Cyber Interference in the French Presidential Election in 2017 and 2022. *Trust under Threat*, 157.

10. Downing, J., & Ahmed, W. (2019). # MacronLeaks as a “warning shot” for European democracies: challenges to election blackouts presented by social media and election meddling during the 2017 French presidential election. *French Politics*, *17*, 257–278.

11. Bollmann, H. S., & Gibeon, G. (2022). *The spread of hacked materials on Twitter: A threat to democracy? A case study of the 2017 Macron Leaks* (Doctoral dissertation, Hertie School).

12. Barnes, J.E. (2021). Ex-Intelligence Analyst Is Sentenced for Leaking to a Reporter. *The New York Times*. https://www.nytimes.com/2021/07/27/us/politics/daniel-hale-leaksentence.html.

13. Cabra, M. and Kissane, E. (2016). Wrangling 2.6TB of data: The people and the technology behind the Panama Papers. *ICIJ.org*. https://www.icij.org/investigations/panamapapers/data-tech-team-icij/

14. Lee, M. (2020). Hack of 251 Law Enforcement Websites Exposes Personal Data of 700,000 Cops. *The Intercept*. https://theintercept.com/2020/07/15/blueleaks-anonymous-ddoslaw-enforcement-hack/.

15. Woodall, A. (2018). Media capture in the era of megaleaks. *Journalism*, 19(8), 1182–1195.

16. United States Department of Justice. (2021). Former Intelligence Analyst Pleads Guilty to Disclosing Classified Information. https://www.justice.gov/usao-edva/pr/former-intelligenceanalyst-pleads-guilty-disclosing-classified-information.

17. Beran, D. (2020). The Return of Anonymous. *The Atlantic*. https://www.theatlantic.com/technology/archive/2020/08/hacker-group-anonymousreturns/615058/

18. Süddeutsche Zeitung. (2016). John Doe's Manifesto. https://panamapapers.sueddeutsche.de/articles/572c897a5632a39742ed34ef/

19. Di Salvo, P. (2024). A Typology of Digital Leaks as Journalistic Source Materials. In *The Palgrave Handbook of Everyday Digital Life* (pp. 469–488). Cham: Springer International Publishing.