https://doi.org/10.15407/np.77.322
УДК 061.1:342.511]:316.77-047.34:303.717OSINT]“36”

Денис Павленко,
кандидат юридичних наук, старший науковий співробітник,
Національна бібліотека України імені В. І. Вернадського
Голосіївський просп., 3, Київ, 03039, Україна
e-mail: pavlenko_dv@ukr.net
ORCID: https://orcid.org/0000-0003-4073-7106

ІНСТИТУТ ПРЕЗИДЕНТСТВА В ЕПОХУ ВІДКРИТИХ ДАНИХ: МОЖЛИВОСТІ OSINT ДЛЯ АНАЛІЗУ КРИЗОВИХ СИТУАЦІЙ

Сучасний інститут президентства зазнає істотних трансформацій під впливом розвитку відкритих даних, цифрової прозорості та глобальної інформаційної динаміки. У XXI ст. діяльність глав держав відбувається в умовах постійного публічного спостереження, миттєвого доступу до інформації та гібридних медіасистем, що виходять за межі національних кордонів. Це зумовлює потребу в переосмисленні функціонування президентської влади в умовах інформаційної відкритості, особливо під час кризових ситуацій політичного, соціального чи безпекового характеру. У статті досліджується роль Open Source Intelligence (OSINT) – розвідки з відкритих джерел – як аналітичного інструмента для вивчення діяльності президентських інститутів у добу відкритих даних. OSINT-технології дають змогу системно збирати, перевіряти та інтерпретувати відкриту інформацію з медіа, соціальних мереж, державних платформ і користувацького контенту, що дає змогу виявляти закономірності прийняття рішень, комунікаційні стратегії та поведінкові моделі президентів під час криз. У статті наведено приклади застосування OSINT-інструментів для аналізу президентської комунікації під час надзвичайних подій – воєн, пандемій, політичних конфліктів. Висновки дослідження свідчать, що в умовах відкритих даних інститут президентства має адаптуватися до нової реальності прозорості, оперативності та аналітичної підготовленості. Інформаційна відкритість розглядається не як ризик, а як стратегічний ресурс, який за належного управління може зміцнювати довіру суспільства до влади та стійкість демократичних інституцій.

Ключові слова: інститут президентства, відкриті дані, OSINT, війна, прозорість, управління, інформаційна безпека, демократична підзвітність

Постановка проблеми. Сучасний інститут президентства функціонує та розвивається в унікальному середовищі, яке поєднує динамічну цифровізацію та глобальну відкритість державних процесів, відповідно, якість держуправління залежить від масиву доступних даних і швидкості обміну цією інформацією. З одного боку, це породжує нові виклики для президентських структур, з іншого – створює безліч потенційних можливостей для модернізації підходів та методик кризового менеджменту. В умовах кризи ефективний аналіз інформації стає не просто завданням, а необхідністю та критично важливим ресурсом для побудови стратегії запобігання ризикам, пошуку актуальних рішень, і безпосереднє використання OSINT-інструментів дає змогу отримувати швидкі та верифіковані дані з відкритих джерел. Для України ці питання набувають особливої актуальності, адже в умовах війни питання безпеки держави та її кіберпростору стали базовими в спектрі загальної боротьби за свободу й незалежність. Відповідно, інститут президентства став ключовим суб'єктом формування довгострокових безпекових стратегій та підтримки комунікації із суспільством і зовнішнім світом, що потребує постійної актуалізації підходів та інструментів роботи з масивами даних. З огляду на це дедалі більшу увагу дослідників привертають технології відкритої розвідки (OSINT) як засіб підсилення інституційної спроможності президентської влади. Незважаючи на зростання кількості аналітичних матеріалів про OSINT, комплексних досліджень щодо взаємодії інституту президентства і відкритих даних у контексті кризового аналізу залишається недостатньо. Особливо відчутною є прогалина в оцінці того, як відкриті дані можуть бути інтегровані в процеси стратегічних комунікацій, сценарного моделювання, швидкого реагування та суспільної легітимації рішень глави держави.

Аналіз останніх досліджень і публікацій. Теоретичні розробки науковців щодо впливу відкритих даних і процесів диджиталізації на оновлення інструментарію інституту президентства в аналізі сучасного інфополя залишаються недостатньо розробленими. Лише окремі дослідники, зокрема З. Аврахамі [1], Л. Блок [2], Т. Вейкман, С. Лечелер [4], звертають увагу на взаємозв'язок між відкритими даними та прийняттям рішень на найвищому державному рівні.

Щодо технологій відкритої розвідки (OSINT) наявна значна кількість наукових і прикладних досліджень, присвячених методології збору, аналізу та верифікації інформації з відкритих джерел. Теоретичні засади OSINT заклали такі автори, як Г. Вільямс [5], І. Блум [5], М. Фам [3], А. Фам-Нгуєн [3], а також дослідницькі групи "Bellingcat", "CIR", "DFRLab", які практично демонструють можливості технології у сфері безпеки, воєнної аналітики, розслідувань і кризового моніторингу. В українському контексті значний внесок зробили Б. Аганін [6], В. Іващенко [8], О. Кулабухов [9], В. Майданюк [7], М. Нечипорук [7], В. Новічков [9], О. Романюк [7], В. Товстик, К. Чукалов [8], В. Шульга [9]; медіаорганізації "Texty.org.ua", Українська OSINT-спільнота, які адаптують методи відкритої розвідки до умов війни та інформаційних загроз.

Попри значний масив досліджень більшість праць зосереджена на технічних або безпекових аспектах OSINT. Значно менше уваги приділено тому, як інструменти відкритої розвідки можуть бути інституціоналізовані в системах публічного управління, зокрема в діяльності інституту президентства. Недостатньо вивченими залишаються такі питання: інтеграція OSINT у процеси кризового менеджменту на рівні глави держави; роль OSINT у стратегічних комунікаціях Президента в умовах інформаційних атак; стандарти верифікації інформації для ухвалення політичних рішень на основі відкритих даних; використання OSINT для оцінювання ризиків і прогнозування розвитку кризових ситуацій; етичні, правові та інституційні обмеження застосування відкритої розвідки президентськими структурами; зв'язок між відкритими даними й легітимністю рішень Президента в умовах високої суспільної турбулентності тощо. Отже, хоча наукова література частково висвітлює окремі складові теми, цілісне дослідження функціонування інституту президентства в епоху відкритих даних через призму OSINT залишається недостатньо розробленим. До того ж підходи OSINT-аналізу традиційно застосовувалися у військовій та розвідувальній сферах, але недостатньо досліджувалися в контексті політичного управління.

Метою статті є комплексний аналіз OSINT-інструментів як сучасного засобу трансформації інституту президентства в умовах епохи відкритих даних і визначення потенціалу OSINT для прийняття

політичних рішень у кризових ситуаціях. Дослідження спрямоване на виявлення того, яким чином відкриті джерела інформації можуть підвищити ефективність кризового менеджменту на рівні президентської влади, які можливості вони створюють для оперативного отримання релевантних даних, а також які ризики, обмеження й інституційні виклики супроводжують інтеграцію OSINT у державне управління.

Виклад основного матеріалу. Сучасне цифрове середовище та комунікації вже давно перестали сприйматися як набір персоналізованих майданчиків для поширення даних, сьогодні це глобальний простір, у якому правда та дезінформація переплітаються настільки щільно, що відрізнити їх іноді практично неможливо. І це створює величезну нішу для розвитку маніпулятивних методик та інструментів, які впливають на життя не лише окремих особистостей, а й держав і міжрегіональних об'єднань. Під інформаційною загрозою опиняються численні державні інститути та ключові владні структури, серед яких інститут президентства, стратегічне значення якого особливо посилюється в кризових умовах. Тому впровадження OSINT-інструментів у сферу сучасного держуправління дедалі більше стає нагальною вимогою національної безпеки та невід'ємним вектором моніторингових програм функціонування президентської влади.

У сучасному цифровому середовищі дезінформація та неправдива інформація швидко поширюються через мультимедійний контент на різних платформах і мовах та, як правило, пов'язана з кібербезпекою й розвідкою. Тому історично OSINT, як підхід до збору відкритої інформації, з'явився у військових і розвідувальних структурах США ще всередині XX ст., але цілеспрямоване застосування OSINT до аналізу діяльності глав держав, у тому числі президентів, сформувалося значно пізніше – у 1990–2000-х роках [2, с. 96]. Це пов'язано з розвитком цифрових медіа, появою великих масивів відкритих даних та соціальних мереж. Перші системні спроби аналізувати відкриті джерела було здійснено під час Другої світової війни: Foreign Broadcast Monitoring Service (FBMS) у США (створений у 1941 р.) займався моніторингом відкритих радіотрансляцій Німеччини, Японії та Італії; BBC Monitoring Service (Велика Британія) аналізував

відкриті новинні потоки, газети та інші медіа країн-суперників. FBMS ще до появи терміна "OSINT" збирала й аналізувала відкриту інформацію про політичних лідерів інших держав. Вони моніторили пресу, радіо- й телетрансляції, офіційні заяви глав держав. Це був перший системний прообраз OSINT-аналізу лідерів, включно з президентами.

Під час Холодної війни розвідка США й НАТО використовувала відкриті джерела для регулярного аналізу: ЗМІ СРСР, дипломатичні публікації, наукові журнали, офіційні статистичні дані, публічні виступи радянської еліти. Проте OSINT залишався другорядним порівняно з HUMINT [розвідка, що базується на людських джерелах (агентурна розвідка)] і SIGINT (радіо- та електропередачі). Після 1989 р. і зростання кількості відкритої інформації OSINT отримав офіційне визнання. У 1992 р. було створено Open Source Center (OSC) у США при CIA; NATO створює окремі OSINT-доктрини (перші керівні документи – середина 1990-х років). Саме в цей час OSINT стає повноцінною дисципліною, а не допоміжним методом.

З розвитком інтернету в 2000-х роках OSINT починають активно застосовувати журналісти, аналітичні центри, приватні розвідники (наприклад, Stratfor), правоохоронні органи, військові аналітики під час війн в Іраку, Афганістані та ін. Події в Україні (2014 р. та особливо після 2022 р.) також спричинили стрімкий розвиток OSINT: Bellingcat – один з найвідоміших колективів, який довів роль OSINT у міжнародних розслідуваннях (MH17, отруєння Скрипалів, війна РФ проти України), українські волонтерські спільноти (InformNapalm, Molfar, Центр стратегічних комунікацій та ін.) стали світовими лідерами в практичному застосуванні OSINT. Наприклад, за даними відкритих джерел, Molfar – українська OSINT-агенція, яка з початком повномасштабного вторгнення приєдналася до кіберспротиву російській агресії. З 2022 р. спільнота розслідувачів "Molfar" провела 1 тис. 271 розслідування та опрацювала інформацію з 720 відкритих і закритих світових реєстрів даних. Основні теми їхніх розслідувань – ідентифікація воєнних злочинів та спростування російської пропаганди.

Таким чином, хоча фактчекери вже давно виконують завдання аналізу відкритих даних, в еру надлишку інформації цей процес став

дедалі більш трудомістким і ресурсоємним. У 2025 р. обсяг даних, які генеруються, зберігаються та споживаються, уже перевищує 180 зеттабайт, що значно ускладнює їх обробку і використання. Для порівняння, у 2020 р. цей показник становив 64,2 зеттабайта [9, с. 73].

Тому закономірно вдосконалюються підходи й методики роботи з даними, а також виникають нові інструменти верифікації. Загалом, зарубіжні дослідники зазвичай визначають відкриті джерела інформації (OSINT) як збір, обробку та кореляцію загальнодоступної інформації з відкритих джерел, таких як засоби масової інформації, соціальні мережі, форуми, блоги, публічні урядові дані, комерційні публікації або набори даних. Це системи збору даних з різних джерел, які використовують передові методи збору та аналізу, що дає змогу отримати більш широку картину про об'єкт спостереження, при цьому зібрана інформація, як правило, повертається в процес збору для уточнення й наближення до кінцевої мети [1, с. 154232]. Засоби OSINT охоплюють широкий спектр цифрових технологій, що дають можливість збирати, систематизувати, перевіряти й аналітично опрацьовувати інформацію з відкритих джерел. Вони включають пошукові системи, бази даних, соціальні мережі, геопросторові сервіси, інформаційні агрегатори, спеціалізовані онлайн-інструменти та аналітичні платформи. Ряд українських дослідників наводять приклади та порівняння функцій OSINT-інструментів: SHODAN [пошук підключених до інтернету пристроїв за різними параметрами (IP-адреса, порти, сервіси), виявлення вразливостей у підключених пристроях]; Maltego (збір та аналіз великих обсягів даних з різних джерел, виявлення зв'язків між різними об'єктами, візуалізація проаналізованих даних); Recon-Ng (збір інформації з різних джерел, таких як соціальні мережі, пошукові системи тощо, аналіз зібраної інформації для виявлення загроз і вразливостей); Spiderfoot (збір інформації з різних джерел в інтернеті, аналіз зв'язків між об'єктами, виявлення загроз безпеці та вразливостей) [8, с. 221].

Як видно з переліку, завдання OSINT-інструментів – отримати максимально повну картину події або об'єкта аналізу на основі легально доступних джерел. Найбільш поширені з них можна деталізувати:

1. Інструменти загального пошуку (пошук документів, згадок, новин, офіційної інформації):

– Google Advanced Search, Bing, DuckDuckGo;

– оператори пошуку: site:, filetype:, intitle:, inurl:, cache:, related:;

– розширені оператори: inurl, filetype, site та ін. для отримання більш точних і глибоких результатів, ніж при звичайному пошуку (Google dorks).

2. Аналіз соціальних мереж і платформ контенту (відстеження медіаактивності, аналіз поведінки користувачів, виявлення дезінформації, геолокація через публікації):

– Facebook, Twitter/X, Instagram, TikTok, LinkedIn;

– аналітичні сервіси: CrowdTangle, Twint, Hoaxy, Social Bearing.

3. Геолокаційні інструменти (визначення місця подій, руху техніки, оцінка наслідків надзвичайних ситуацій, верифікація відео):

– Google Maps, Google Earth Pro, Bing Maps;

– Satellite imagery: Sentinel Hub, Maxar, NASA Worldview;

– EXIF-аналітика: exif.tools, Jeffrey's Image Metadata Viewer.

4. Аналіз відеоматеріалів і зображень (перевірка автентичності відео, встановлення хронології подій, підтвердження місця та часу зйомки, виявлення підробок):

– YouTube Data Viewer, InVid, Amnesty Media Verification Toolkit;

– витяг фреймів, пошук збігів через зворотний пошук зображення;

– зворотний пошук: Google Images, Yandex Images, TinEye;

– аналіз тіней, об'єктів, погодних умов;

– витяг EXIF-даних.

5. Бази даних і реєстри (ідентифікація структури власності, фінансових схем, відстеження логістики):

– державні реєстри (ЄДРПОУ, кадастрові карти, судові реєстри);

– бази літаків / кораблів: ADS-B Exchange, MarineTraffic;

– реєстри компаній: OpenCorporates, D&B Hoovers;

– бази доменів: Whois Lookup, DNSlytics.

6. Оцінювання кіберпростору (аналіз кіберризиків, атрибуція кібератак, профілювання цифрових об'єктів):

– аналіз доменів і IP: Shodan, Censys, FOFA;

– пошук витоків даних: Have I Been Pwned;

– трекінг активності в даркнеті (через спеціальні агрегатори).

При цьому до переліку найбільш поширених інструментів, як правило, застосовуються й алгоритми машинного навчання та аналізу мереж, що дає можливість використовувати штучний інтелект (ШІ) для ідентифікації патернів у поведінці користувачів, які часто сприяють поширенню дезінформації [7, с. 111]. Наприклад, це може включати певні ключові слова, фрази, хештеги або навіть специфічні способи взаємодії між користувачами. За допомогою розроблених моделей ШІ може прогнозувати, де та коли можливий наступний спалах дезінформації, що дає змогу організаціям й інституціям, які борються з дезінформацією, підготуватися та вжити превентивних заходів заздалегідь.

У контексті роботи із владними структурами західними дослідниками запропоновано також підхід із формування критичних звітів, що дає змогу в стислі терміни формувати верифіковану аналітику для прийняття політичних рішень. Наприклад, розроблено Ægis як напівавтоматизоване рішення для перевірки мультимедійного контенту (зображень, відео) впливових осіб та пов'язаних з ним тверджень, що створює структуровані звіти про перевірку. Технологія приймає як вхідні дані необроблені медіафайли та контекст, обробляє їх для вилучення підказок і доказів щодо деталей джерела, місця, часу, особи, причини, аналізу. Зібрані докази потім об'єднуються в перевірену інформацію, яка надається як вхідні дані для синтезу остаточного звіту про перевірку [3, с. 14043]. Як зазначає О. Романюк, такі підходи корисні, але мають посилюватися інтероперабельністю та співпрацею між різними ШІ-системами, що також дасть їм змогу ефективно обмінюватися даними й аналітикою, особливо на міжнародному рівні, що є критично важливим у контексті побудови стратегічних комунікацій між державами [7, с. 205].

Інші дослідники, зокрема Б. Аганін, застерігають, що застосування і вдосконалення тих чи інших OSINT-інструментів часто призводить до використання інформації з відкритих джерел з різною метою. На прикладі інституту президентства в Україні більшість інформації, яка продукується главою держави та Офісом Президента, є джерелом OSINT-звітів для іноземних агентств, проте в перекрученому вигляді активно використовується і ЗМІ РФ для створення

інформаційно-пропагандистських завдань [6, 8]. Тому використання стандартизованих підходів у такому аналізі є ключовою вимогою до оперування перевіреними даними.

Незважаючи на глобальну популярність OSINT, повноцінної, єдиної міжнародної стандартизації не існує. Наразі сформовано системи рекомендацій, методологічні моделі й секторальні стандарти, які частково виконують роль стандартів і можуть вважатися регуляторними для окремих OSINT-процесів у сфері державного управління. Найвідоміші методології, які активно використовуються у військовій сфері та діяльності владних інститутів, але офіційно все ж не є повноцінними стандартами: модель "OSINT Framework", методологія NATO OSINT Handbook, методологія американської розвідки (CIA Tradecraft + ODNI ICD 203/ICD 301), Bellingcat Methodology (Verification Standards) [4, с. 1517]. Також разом з уніфікацією для президентських структур особливо актуальним залишається питання подальшої інтеграції в ці процеси, адже потік даних стрімко зростає й масштабується, що потребує актуального реагування та пошуку нових підходів до їх опрацювання. Уже понад десятиліття експерти з технологій говорять про еволюцію до Web 3.0 – «семантичного вебу», який включатиме пряму та непряму машинну обробку даних, машинне навчання й автоматизоване мислення. Тому інституційні структури в подальшому матимуть справу не просто з генерованою інформацією – це буде симбіоз ШІ, доповненої реальності та психометрії [5, с. 23], що несуть в собі ще більший пласт даних, і лідери держав мають розуміти, що саме в здатності ефективно опанувати цей ресурс полягатиме безпека держави й суспільства.

Висновки. Отже, проведене дослідження сприяє переосмисленню ролі президентських інститутів у цифрову добу, пропонує нові методологічні підходи до аналізу політики, підкреслює важливість розвитку національних компетенцій у сфері OSINT для зміцнення державної стійкості та забезпечення ефективного публічного управління. OSINT, як метод збору та інтерпретації відкритих джерел, дедалі частіше стає ключовим елементом систем кризового реагування, забезпечуючи оперативність, багатовимірність і доказовість даних, доступних для ухвалення стратегічних рішень на найвищому

політичному рівні. Тому потенціал OSINT у діяльності Президента може охоплювати як раннє виявлення загроз, так і моніторинг розвитку криз, а також підтримку стратегічних комунікацій, що набуває особливого значення в умовах війни та постійних інформаційних атак. Інтеграція відкритих даних у процеси державного управління здатна підвищити прозорість, адаптивність і легітимність президентських рішень.

Водночас невирішеними залишаються питання відсутності стандартизованих протоколів роботи з OSINT у структурах, що забезпечують діяльність Президента; ризики маніпуляцій, дезінформації та помилок інтерпретації; етичні й правові обмеження; також проблеми інституційної спроможності до використання великих масивів відкритих даних у режимі реального часу. Недостатня кількість комплексних досліджень на перетині політології, data science та кризового менеджменту свідчить про актуальність подальших міждисциплінарних підходів.

OSINT може стати одним із ключових інструментів модернізації інституту президентства та підвищення ефективності управління кризовими ситуаціями. Перспективними напрямами подальших досліджень є розробка моделей OSINT-підтримки прийняття рішень Президентом, вивчення інституційних механізмів інтеграції відкритих даних і розробка нормативних рамок, що забезпечують баланс між безпекою, ефективністю та демократією в добу цифрової відкритості.

Список використаних джерел

1. Avrahami Z., Zwilling M., Hajaj C. Leveraging OSINT for Advanced Proactive Cybersecurity: Strategies and Solutions. *IEEE Access.* 2025. Vol. 13. Pp. 154229-154250. https://doi.org/10.1109/ACCESS.2025.3603868

2. Block L. The long history of OSINT. *Journal of Intelligence History.* 2024. Vol. 23. No. 2. Pp. 95-109. https://doi.org/10.1080/16161262.2023.2224091

3. Pham M., Pham-Nguyen A., Le Ægis: AI-Enhanced OSINT for Multimedia Verification. *In Proceedings of the 33rd ACM International*

Conference on Multimedia (MM '25). (October 27-31, 2025. Dublin, Ireland) (pp. 14041-14047). https://doi.org/10.1145/3746027.3762034

4. Weikmann T., Lecheler S. Cutting through the hype: Un-derstanding the implications of deepfakes for the fact-checking actor-network. *Digital Journalism.* 2024. Vol. 12. Issue 10. Pp. 1505-1522. https://doi.org/10.1080/21670811.2023.2194665

5. Williams H. J., Blum I. Defining second generation open source intelligence (OSINT) for the defense enterprise. *RAND Corporation.* 2018. https://doi.org/10.7249/RR1964

6. Аганін Б. Ю. Окремі види небезпеки у процесі розміщення відкритої інформації у різноманітних джерелах та мережі інтернет. *Експерт: парадигми юридичних наук і державного управління.* 2025. № 1 (33). С. 6–11. https://doi.org/10.32689/2617-9660-2025-1(33)-6-11

7. Романюк О. Н., Майданюк В. П., Романюк О. В., Нечипорук М. Л. Використання штучного інтелекту для виявлення дезінформації. *Сучасні суспільні комунікації: міжнародний досвід та українські реалії* : матеріали Міжнар. наук.-практ. конф. Лубни : Вид-во ДЗ «ЛНУ ім. Т. Шевченка». 320 с. URL: https://ir.lib.vntu.edu.ua/bitstream/handle/123456789/46206/175150.pdf?sequence=2&isAllowed=y (дата звернення: 04.03.2026).

8. Товстик В. О., Чукалов К. Е., Іващенко В. Є., Чорненький К. А. Використання методу OSINT у кібербезпеці, зокрема під час воєнних конфліктів. *In The 9 th International scientific and practical conference "Scientific research: modern challenges and future prospects"(April 14-16, 2025).* MDPC Publishing, Munich, Germany. URL: https://sci-conf.com.ua/wp-content/uploads/2025/04/SCIENTIFIC-RESEARCH-MODERN-CHALLENGES-AND-FUTURE-PROSPECTS-14-16.04.2025.pdf#page=258 (дата звернення: 04.03.2026).

9. Шульга В. В., Новічков В. О., Нікора І. В., Кулабухов О. М., Дворський М. В. Інтелектуальна система аналізу відкритих джерел. *Збірник наукових праць Харківського національного університету Повітряних Сил*. 2025. № 3 (85). С. 70–78. https://doi.org/10.30748/zhups.2025.85.08

References

1. Avrahami, Z., Zwilling M., & Hajaj C. (2025). Leveraging OSINT for Advanced Proactive Cybersecurity: Strategies and Solutions. *IEEE Access, 13*, 154229-154250. https://doi.org/10.1109/ACCESS.2025.3603868

2. Block, L. (2024). The long history of OSINT. *Journal of Intelligence History*, *23*(2), 95-109. https://doi.org/10.1080/16161262.2023.2224091

3. Pham, M., Pham-Nguyen, A., & Le, A. (2025). Ægis:AI-Enhanced OSINT for Multimedia Verification. *In Proceedings of the 33rd ACM International Conference on Multimedia (MM'25), 27-31 October 2025* (pp. 14041-14047). Dublin, Ireland. https://doi.org/10.1145/3746027.3762034

4. Weikmann, T., & Lecheler, S. (2024). Cutting through the hype: Un-derstanding the implications of deepfakes for the fact-checking actor-network. *Digital Journalism, 12*(10), 1505-1522. https://doi.org/10.1080/21670811.2023.2194665

5. Williams, H. J., & Blum, I. (2018). Defining second generation open source intelligence (OSINT) for the defense enterprise. *RAND Corporation*. https://doi.org/10.7249/RR1964

6. Ahanin, B. Yu. (2025). Specific types of risks in the process of publishing open information in various sources and on the Internet. *Expert: Paradigms in Legal Studies and Public Administration, 1*(33), 6-11. https://doi.org/10.32689/2617-9660-2025-1(33)-6-11

7. Romaniuk, O. N., Maidaniuk, V. P., Romaniuk, O. V., & Nechyporuk, M. L. (2025). Vykorystannia shtuchnoho intelektu dlia vyiavlennia dezinformatsii [Using Artificial Intelligence to Detect Disinformation]. In *Modern Public Communication: International Experience and Ukrainian Realities. Proceedings of the International Scientific and Practical Conference*. Lubny [in Ukrainian]. Retrieved March 4, 2026, from https://ir.lib.vntu.edu.ua/bitstream/handle/123456789/46206/175150.pdf?sequence=2&isAllowed=y

8. Tovstyk, V. O., Chukalov, K. E., Ivashchenko, V. Ye., & Chornenkyi, K. A. (2025). Vykorystannia metodu OSINT u kiberbezpetsi, zokrema pid chas voiennykh konfliktiv [The Use of OSINT in Cybersecurity, Particularly During Armed Conflicts]. *In The 9 th*

International scientific and practical conference "Scientific research: modern challenges and future prospects", 14-16 April 2025. MDPC Publishing, Munich, Germany [in Ukrainian]. Retrieved March 4, 2026, from https://sci-conf.com.ua/wp-content/uploads/2025/04/SCIENTIFIC-RESEARCH-MODERN-CHALLENGES-AND-FUTURE-PROSPECTS-14-16.04.2025.pdf#page=258

9. Shulha, V. V., Novichkov, V. O., Nikora, I. V., Kulabukhov, O. M., & Dvorskyi, M. V. (2025). Intelligent System for Open-Source Intelligence Analysis. *Collection of Scientific Papers of Kharkiv National Air Force University, 3*(85), 70-78. https://doi.org/10.30748/zhups.2025.85.08

Отримано / Received 09.03.2026
Прийнято / Accepted 21.03.2026
Опубліковано онлайн / Published online 28.07.2026

Denis Pavlenko,
PhD (Juridic.), Senior Research Scientist,
V. I. Vernadskyi National Library of Ukraine
3 Holosiivskyi Ave., Kyiv 03039, Ukraine
e-mail: pavlenko_dv@ukr.net
ORCID: https://orcid.org/0000-0003-4073-7106

THE INSTITUTE OF PRESIDENCY IN THE AGE OF OPEN DATA: OSINT OPPORTUNITIES FOR CRISIS ANALYSIS

The institution of presidency is undergoing significant transformation partly reasoned by the influence of open data, digital transparency, and global information flows. In the 21st century, presidents operate under constant public scrutiny and within hybrid media ecosystems that transcend national boundaries. This reality requires rethinking how the presidency functions in an era of informational openness, particularly during political, social, or security crises. This article examines the role of Open-Source Intelligence (OSINT) as an analytical framework for studying presidential institutions in the age of open data. OSINT enables systematic collection, verification, and interpretation of publicly available information from various digital sources, including media content, social networks, governmental datasets, and user-generated materials. Through these tools, analysts can identify patterns of decision-making

and communication strategies employed by presidents during crisis situations. The research argues that applying OSINT methodologies enhances the understanding of the relationship between the presidency, media, and public opinion. Integrating open data into political analysis supports evidence-based policymaking, and strengthens democratic accountability. Case studies demonstrate how OSINT tools have been successfully used to analyze presidential communication during wars, pandemics, and political unrest. The article concludes that in the open-data environment, the presidency must evolve toward greater adaptability, transparency, and data-informed leadership. Information openness should be treated not as a vulnerability but as a strategic asset that reinforces public trust and institutional resilience. In the long run, this will not only enable a faster response to challenges but also allow for the anticipation of future developments, the formulation of proactive policies, the strengthening of communication with citizens, and the enhancement of transparency and efficiency in public administration.

Keywords: presidency, open data, OSINT, political crisis, transparency, governance, information security, democratic accountability