УДК 351.746.1:004.738.5(477)(1991/2024)

КУЛЬЧИЦЬКА Л. аспірантка Державної наукової установи "Інститут інформації, безпеки і права НАПрН України", співробітник Служби безпеки України
ORCID: https://orcid.org/0009-0008-7182-7976

ІСТОРИКО-ПРАВОВИЙ ОГЛЯД СТАНОВЛЕННЯ ТА РОЗВИТКУ РОЗВІДКИ З ВІДКРИТИХ ДЖЕРЕЛ ІНФОРМАЦІЇ ЯК САМОСТІЙНОЇ СПРОМОЖНОСТІ З ДОБУВАННЯ ТА АНАЛІЗУ ДАНИХ В УКРАЇНІ

DOI: https://doi.org/10.37750/2616-6798.2025.4(55).346483

***Анотація**. У статті досліджується становлення та розвиток розвідки з відкритих джерел (англ. Open-Source Intelligence – OSINT) як самостійної спроможності з добування, обробки та аналізу даних в Україні.*

Доводиться, що сьогодні для України характерними є глобальні та євроатлантичні тенденції розвитку OSINT: розробка специфічної методології, спроби уніфікації тактики і процедур проведення цієї діяльності, запровадження окремого правового регулювання та вирішення етичних проблем. Звертається увага на те, що розвиток OSINT в Україні відбувався за власним, багато в чому унікальним сценарієм, обумовленим історичним контекстом та факторами військового і політичного характеру.

У статті вперше проведено періодизацію історико-правового розвитку розвідки OSINT в інтересах національної безпеки України. Автором виокремлено чотири етапи такого: 1) інституційне становлення в "аналогову" еру (1991-2005 рр.); 2) цифровізація OSINT та поява недержавних акторів (2005-2014 р.р.); 3) професіоналізація OSINT та правове визнання (2014-2022 рр.); 4) нова архітектура OSINT: великі дані, ШІ та глобальне партнерство (2022 р. – донині). Для кожного етапу визначено характерні його особливості та специфічні ознаки.

Авторкою наголошено, що шлях розвитку OSINT в інтересах національної безпеки України пройшов шлях від закритої, "аналогової" державної монополії, що спиралася на застарілі радянські практики, до гнучкої, професійної та юридично визнаної цифрової спроможності, яка сьогодні стоїть на трьох стовпах: синергії держави і суспільства, технологіях штучного інтелекту та міжнародному партнерстві.

***Ключові слова:** інформація, дані, збір та обробка інформації, дані з відкритих джерел, OSINT, оперативно-розшукова діяльність, контррозвідувальна діяльність, інформаційно-аналітична діяльність, інформаційна діяльність, штучний інтелект, національна безпека України.*

***Summary**. This article explores genesis and development of Open-Source Intelligence (OSINT) in Ukraine as an intelligence discipline derived from open data collection, processing, and analysis.*

Nowadays Ukraine shares global and Euro-Atlantic tendencies in OSINT development, namely: design of the specific methodology, attempts to unify tactics and techniques, introduce legal framework and solve some ethical problems. Particular attention is given to the fact that OSINT in Ukraine developed in its own way, sometimes unique, due to the historical context and both political and military reasons.

This article offers the first periodization of historical and legal stages of development of OSINT in the interests of national security of Ukraine, namely: 1) institutional development in the "analog" era (1991-2005); 2) digitalization of OSINT and emergence of the non-state actors (2005-2014); 3) professionalization of OSINT and its legal recognition (2014-2022); 4) the new architecture of OSINT:

big data, AI and global partnership (2022- till now). Specific features and particularities of every stage are established.

The author emphasizes that OSINT for the national security of Ukraine developed from the closed, "analog" state monopoly, which relied on the old soviet practices, to the modern flexible, professional, and legally recognized digital capacity. Today it relies on three pillars: synergy of state and society, Artificial Intelligence technologies, and international partnership.

***Keywords**: information, data, data collection and processing, open-source data/information, OSINT, Open-Source Intelligence, operational-investigative activities, counter-intelligence, information and analytical activities, Artificial Intelligence, national security of Ukraine.*

Постановка проблеми. Такий вид діяльності як одержання даних з відкритих джерел (англ. Open-Source Intelligence – OSINT) в інтересах забезпечення національної безпеки проводився буквально з моменту появи держави, видозмінюючись та структуруючись під її потреби. Однак як самостійна спроможність державних інституцій, у тому числі спеціальних служб, з добування, обробки та аналізу даних ця діяльність оформилась значно пізніше – у ХХ столітті. Такою часовою віхою науковці називають Другу світову війну, і з тих пір розвідка з відкритих джерел визнається окремим напрямом діяльності із забезпечення національної безпеки, що змінюється синхронно до розвитку технологій роботи з інформацією.

Зараз абревіатура OSINT є загальновизнаною і зрозумілою серед науковців та практиків управління, права, інформаційних технологій та інших галузей знань багатьох країн й часто не потребує перекладу. Однак становлення і розвиток OSINT в Україні має свої відмінності та специфічні риси, зумовлені історичним, політичним, військовим контекстом, вплив якого доповнювався розвитком інформаційних. Розкриття таких особливостей вимагає розуміння як практичних аспектів діяльності зі здобування інформації з різних джерел в інтересах національної безпеки, так і загально-політичних і правових умов такої діяльності.

Аналіз останніх досліджень і публікацій. Питання добування, обробки, аналізу, використання даних з відкритих джерел розглядаються в наукових дослідженнях фахівців різних галузей, зокрема управління, права, інформаційних технологій.

Зміст, характерні особливості, класифікація, історія появи та застосування OSINT досліджуються такими українськими науковцями, як Д. Ланде, О. Довгань, Н. Жмур, М. Землянікіна, Т. Ткачук, Д. Зоренко, М. Пашковський, О. Торбас, Р. Радейко, Н. Юрх, Р. Ширшов, Б. Косохатько. Серед закордонних вчених, які розкривають проблематику OSINT, слід відзначити роботи М. Баззеля, Н. Хассана, Дж. Едісона, Р. Хіджазі, М. Глассмана, М. Канг, Е. Брайянт та інших. Незважаючи на наявність суттєвих наукових напрацювань щодо змісту та методів OSINT, досі не було здійснено комплексного історико-правового аналізу етапів його формування та інституалізації в інтересах національної безпеки України, що і зумовило актуальність та предмет цього дослідження.

Мета статті полягає у здійсненні історико-правового аналізу етапів становлення та розвитку OSINT як самостійної спроможності з добування і аналізу інформації для забезпечення національної безпеки України.

Виклад основного матеріалу.

Науковці і практики стверджують, що у сучасному суспільстві найціннішим активом є інформація, яка відіграє ключову роль у створенні економічних благ [1, с. 140] та дає стратегічну перевагу у забезпеченні національної безпеки. Бріттані Кайзер, колишня директорка з розвитку бізнесу компанії "Cambridge Analytica", назвала відзнаку сучасності: цінність даних перевершила вартість нафти [2].

У цифрову еру технологічні здобутки мультиплікували джерела інформації та зробили більш поширеним цифровий спосіб фіксації даних, відсунувши на другий план традицію збереження на аналогових носіях. Названа тенденція повною мірою стосується і змін, які тривають у зборі, обробці та аналізі даних з відкритих джерел інформації. У цій царині спецслужби перейшли від роботи з текстами, зображеннями у пресі, паперових довідниках і картах до роботи з цифровими масивами даних найрізноманітніших форматів у хмарних середовищах соціальних медіа, архівів чи інших віртуальних просторів.

Як влучно зауважують американські науковці Nihad Hassan та Rami Hijazi, точну дату навіть терміну "розвідка з відкритих джерел" (англ. Open Source Intelligence – OSINT) встановити неможливо, однак такий вид діяльності очевидно практикувався спеціальними службами сотні років [3, с. 1]. Олексій Швидкий визначив еволюцію розвідки з відкритих джерел як послідовні переходи від ранніх початків до сьогодні таким чином:

"1) ранні початки OSINT (OSINT 1.0) сягають початку XIX століття – від використання газет країн-противників для прийняття рішень у секторі оборони;

2) кінець XIX століття – початок XX століття (OSINT 2.0) – поява систематичної практики збору інформації з відкритих джерел з появою генеральних штабів та державних (національних) розвідувальних управлінь;

3) кінець XX століття (OSINT 3.0) – поява інформаційно-комунікаційних технологій сприяла розширенню сфери охоплення та формуванню ширшої розвідувальної діяльності;

4) сучасна ера (OSINT 4.0) – моніторинг інформації у соціальних мережах, поява нових рівнів інформації шляхом використання супутників, відбулось розмиття меж між традиційним збором розвідданих та обміном публічною інформацією" [4, с. 227-228].

Однак, загальновизнаною серед науковців умовною стартовою точкою розвідки з відкритих джерел як окремої спроможності з добування інформації є Друга світова війна. Michael Glassman та Min Ju Kang доводять, що саме в цей період були винайдені чи створені методики обробки інформації, окремі компоненти яких залишаються релевантними донині, як зокрема:

1) створення зрозумілого для кінцевого споживача звіту з чіткою аргументацією і посиланнями на джерела;

2) формування таблиць посилань, в яких одиниці даних оцінені за їх важливістю, значенням для сфери аналізу та проблеми, якої стосуються; це дозволяє кінцевому споживачеві за необхідності самостійно перевірити релевантність отриманих даних і обґрунтованість висновку, а також застосувати добуті відомості до інших пов'язаних сфер зацікавленості.

Ці компоненти, як і інші складові методик, що створювалися, мали на меті розвиток здатності тих, хто збирає (добуває) дані, знайти і виокремити з певного масиву релевантні, обробити їх, провести аналіз та зробити висновок. За визначенням Michael Glassman та Min Ju Kang, це були ранні форми OSINT у сучасному розумінні цієї спроможності [5, p. 675].

Д. Ланде [6, с. 13], О. Довгань [7, с. 8-9], Н. Жмур [8, с. 96], Т. Ткачук [9, с. 8-9] та інші автори називають дві знакові події на підтвердження оформлення нової спроможності здобування інформації. Йдеться про створення у США у грудні 1941 року Служби моніторингу іноземного мовлення (англ. Foreign Broadcast Information Service – FBMS) та підготовка також у США так званого "Єльського звіту" 1951 року. Н. Жмур та

М. Землянікіна запропонували періодизацію розвідки з відкритих джерел на основі досвіду США таким чином:

“1) кінець 1941 р. – створення в США Служби моніторингу зарубіжних трансляцій задля дослідження радіо програм…;

2) 2005-2009 рр. – у США був створений центр із аналізу розвідувальних матеріалів з відкритих джерел. Відбулося це внаслідок зростання кількості інформації, що розміщувалась на просторах інтернету;

3) 2009-2016 рр. – стрімкий розвиток Інтернету, його ролі та впливу на людське життя;

4) 2017 р. – сьогодення – поступове введення концепції OSINT не лише в сферу оборони, але й в інші сфери життєдіяльності людини” [8, с. 96].

Якщо говорити про подальше лідерство США в сфері OSINT, то з часом у звітах розвідорганів саме цієї країни відкриті дані, належним чином оброблені та проаналізовані, поступово стали визнаватися як пріоритетні.

У 1995-1996 роках так звана Комісія Аспіна-Брауна – Комісія Конгресу США з визначення ролі і спроможностей розвідувальної спільноти США (англ. Commission on the Roles and Capabilities of the United States Intelligence Community) працювала над переглядом змісту розвіддіяльності у зв’язку із закінченням "холодної війни". Комісія розробила відповідні рекомендації для Президента і Конгреса США, визначивши розвідку з відкритих джерел як перспективний і пріоритетний напрям отримання інформації. За висновками Комісії, розвідувальна діяльність – це діяльність, що включає в себе здобування інформації з публічно доступних джерел інформації, у тому числі іноземних та радіо, телебачення та друкованих медіа, офіційних чи приватних публікацій та даних з комп’ютерних мереж. У звіті багаторазово Комісія підкреслила факт зростання обсягів публічно доступних даних та визначила необхідність зосередити зусилля на розвитку навичок та експертності співробітників розвідорганів, щоб забезпечити можливість використання “цілого всесвіту інформації, наразі доступної з відкритих джерел” [10], аналітичного поєднання її з даними з інших джерел для забезпечення процесу прийняття рішень урядом.

Наступних суттєвих змін розвідспільнота США та системи збору й аналізу інформації, включаючи розвідку з відкритих джерел, зазнала після теракту 9/11 у 2001 році: спочатку було анонсовано створення Центру відкритих джерел (англ. Open Source Center – OSC) на основі та замість функціонуючої ще з 1941 року Служби моніторингу іноземного мовлення (FBMS). У складі Офісу Директора національної розвідки, але на базі ЦРУ, OSC покликаний був здійснювати збір і аналіз даних “з Інтернету, баз даних, преси, радіо, телебачення, відео, геопросторових даних і комерційних зображень” [11], а також проводити дослідження, підготовку і управління інформаційними технологіями в інтересах всієї розвідспільноти. У 2015 OSC перетворився на Підприємство відкритих джерел (англ. Open Source Enterprise – OSE), яке стало частиною Директорату цифрових інновацій уже у складі ЦРУ. Стратегічне призначення OSE, як і OSC – збір, аналіз та поширення інформації з відкритих джерел, а також розробка методик проведення OSINT в інтересах усіх членів розвідспільности – залишилися незмінними [12].

Сьогодні для України характерні основні тенденції змін правових та організаційних підходів до OSINT, які спостерігаються у західних партнерів. Це виокремлення OSINT як окремої спроможності збору, обробки, аналізу даних, розробка специфічної методології, уніфікація тактики і процедур, а також запровадження правового регулювання. Однак така синхронізація трендів сталася не одразу.

Перший період становлення розвідки з відкритих джерел тривав з 1991 – рік відновлення незалежності – по 2004 рік.

Збір інформації та її аналіз визначався обов'язком Служби безпеки України, без конкретизації джерел. Так, Закон України "Про Службу безпеки України" у редакції від 25 березня 1992 року зобов'язав СБУ "здійснювати розвідувальну та інформаційно-аналітичну роботу в інтересах ефективного проведення органами державної влади та управління України внутрішньої і зовнішньої діяльності, вирішення проблем оборони, соціально-економічного будівництва, науково-технічного прогресу, екології та інших питань, пов'язаних з національною безпекою України" [13].

Коли СБ України (а до неї — Служба національної безпеки, що працювала лише півроку [14]) почала збирати інформацію з відкритих джерел, вона значною мірою спиралася на досвід радянських спецслужб, наприклад в організації повсякденних обов'язків. Це чинило стримуючий вплив, бо не передбачало активне сприйняття передових практик і досвіду іноземних спецслужб, які розвивали власні методики роботи з відкритими даними, підкреслюючи їх перспективність.

Водночас, отримання даних з відкритих джерел інформації вже отримало визначення як окремий вид спеціальної діяльності. Суть заходів щодо відкритих джерел інформації в СБУ полягала в "аналітичному опрацюванні преси та публікацій …. з метою отримання розвідувальної інформації, яка може бути використана в інтересах безпеки суспільства і держави" [15].

У 1992 році прийнято Закон України "Про інформацію", який, в контексті розвідки з відкритих джерел зокрема визначив основні терміни, принципи інформаційних відносин, їх суб'єкти і об'єкти, напрями державної інформаційної політики, право на інформацію, види інформаційної діяльності, а також види інформації та інші наріжні поняття [16].

У подальшому, Конституцією України встановила і право на збір інформації в цілому, і обмеження при проведенні збору даних приватного характеру. Стаття 34 визначає право кожного "вільно збирати, зберігати, використовувати і поширювати інформацію усно, письмово або в інший спосіб – на свій вибір", а частина друга статті 32 – можливість збирання, зберігання, використання інформації про особу як виняток – за умови визначення законом і лише в інтересах національної безпеки, економічного добробуту та прав людини [17].

У цей період були прийняті й інші закони, що визначили правові умови та допустимі межі проведення заходів зі збору, обробки та аналізу інформації в інтересах національної безпеки України загалом:

"Про оперативно-розшукову діяльність" 1992 року, стаття 1 якого відносила до завдань пошук і фіксацію фактичних даних про протиправні діяння окремих осіб та груп, відповідальність за які передбачена Кримінальним кодексом України, розвідувально-підривну діяльність спеціальних служб іноземних держав та організацій з метою припинення правопорушень та в інтересах кримінального судочинства, а також отримання інформації в інтересах безпеки громадян, суспільства і держави [18];

"Про розвідувальні органи України" 2001 року, одним із завдань яких визначалося добування, аналітична обробка та надання визначеним законом органам державної влади розвідувальної інформації (стаття 4). До розвідувальних органів були віднесені СБУ та розвідорган Міноборони й органу виконавчої влади з питань захисту державного кордону України (стаття 6) [19];

Кримінальний кодекс України, який встановив відповідальність за порушення права недоторканності приватного життя (стаття 182), незаконне втручання в роботу

електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку (стаття 361) [20];

"Про контррозвідувальну діяльність" 2003 року, який визначав серед її завдань добування, аналітичну обробку та використання інформації, що містить ознаки або факти розвідувальної, терористичної та іншої діяльності спеціальних служб іноземних держав, а також організацій, окремих груп та осіб на шкоду державній безпеці України (стаття 2), а серед принципів визначав поєднання гласних та негласних форм та методів діяльності (стаття 4); для виконання визначених законом завдань підрозділам та співробітникам надавалося право здійснювати контррозвідувальний пошук, розвідувальні і оперативно-розшукові заходи з використанням оперативних та оперативно-технічних сил і засобів, виявляти, фіксувати і документувати гласно і негласно розвідувальні, терористичні та інші посягання на державну безпеку України, вести їх оперативний облік, а також здійснювати іншу діяльність [21];

"Про основи національної безпеки" 2003 року, який визначив основні засади державної політики, спрямованої на захист національних інтересів, а також поняття національної безпеки [22].

Історично певний час частина сучасних органів сектору безпеки перебували в межах одного відомства як окремі підрозділи, і це визначило співпадіння в підходах до процедур отримання, обробки та аналізу даних з відкритих джерел. Організаційно розвідку з відкритих джерел здійснювали самі співробітники спецслужби, практично не користуючись можливостями третіх сторін – фізичних осіб, громадських організацій тощо – та обмежуючись не цифровими відкритими джерелами інформації, а так званими традиційними – друкованими статтями в медіа, довідниками, матеріалами конференцій, зустрічей тощо.

Причиною був технологічний рівень розвитку суспільства, за якого у загальнодоступному цифровому обігу не було значної кількості даних – у 1997 році кількість користувачів Інтернету в Україні складало всього 1% дорослого населення [23].

Водночас, слід визнати, що інституційна інерція, відсутність люстрації та абсолютна централізація державного управління в 90-х роках XX століття стримували в Україні розвиток OSINT як окремої розвідувальної спроможності зі здобування та аналізу даних. Негативний ефект мала тривала фактична політична орієнтація нашої держави на російську федерацію за декларованого курсу багатовекторності, що обмежувало вивчення і застосування передового досвіду західних спецслужб.

У 2005 році в Україні почався наступний етап розвитку OSINT як окремої спроможності здобування даних. Цей етап визначили чинники технологічного та організаційно-правового характеру, зумовлені стрімким зростанням кількості користувачів всесвітньої мережі Інтернет і появою соціальних медіа. Як зауважують іноземні науковці, OSINT як спроможність зі здобування даних у вузькому, цифровому значенні з'явився саме з розвитком Інтернету і затим соціальних медіа, що уможливило пошук і виявлення інформації у великих масивах даних [5, p. 674].

У 2005 році число користувачів Інтернету у світі перевищило 1 млрд осіб, що складало на той час 17% населення [24, с. 73]. В Україні в цей же час темпи приросту користувачів інтернету теж суттєво зросли: у 2004 році відбувся перший стрибок – з 8% до 13% дорослого населення, з подальшим постійним зростанням у середньому на 3-4%. У 2012 році ситуація змінилася особливо різко – за рік кількість користувачів зросла на 11% і сягнула 43% дорослого населення [23].

З’явилися найбільші соціальні медіа: у 2004 році в США – перша соціальна мережа Facebook [25], яка тривалий час не була надто поширеною в Україні, та у 2006 році – російські "Одноклассники" й "ВКонтакте" [26], які стали і тривалий час залишалися найбільш популярними в Україні [27].

Саме тому протягом 2005-2014 років, з доступністю Інтернету як системи вільної циркуляції даних, що не має фізичних кордонів та є загальнодоступним джерелом інформації, OSINT швидко видозмінювався.

Якщо до 2004 року добування даних з відкритих джерел інформації стосувалося переважно перебігу подій, виокремлення тенденцій розвитку ситуації тощо, то тепер значною мірою йшлося також і про збір відомостей про особу. Саме соціальні медіа стали загальнодоступним джерелом інформації особистого характеру – люди оприлюднювали свої особисті дані: прізвища та імена, дати народження, місця проживання, контакту інформацію та факти зі своєї біографії, а також фото і відео. Загалом дані соціальних медіа тих часів давали можливість отримати три види інформації щодо особи:

1) дані, які особа оприлюднювала самостійно;

2) метадані контенту, який оприлюднює особа, тобто дані про дані, поширювані особою;

3) зв’язки і взаємодії різних осіб (точніше, їх акаунтів) у соціальних медіа.

Крім інформації про особу, збільшилась кількість даних про події, які оприлюднювали і поширювали користувачі соціальних медіа, тим самим даючи можливість встановити факт настання події, її характеристики, сприйняття, можливий вплив на розвиток ситуації тощо.

З організаційно-правової точки зору в Україні відбулися такі зміни: у 2005 році ліквідований розвідувальний орган у складі СБ України й створено Службу зовнішньої розвідки України [28]. На відміну від СБУ, яка на той час була “правоохоронним органом зі спеціальними функціями” [29], Служба зовнішньої розвідки, відповідно до Закону, визначалася виключно як розвідувальний орган (стаття 1) та мала стати, за визначенням, найбільшим рушієм використання розвідки з відкритих джерел як окремого виду діяльності зі здобування інформації з метою сприяння реалізації та захисту національних інтересів і протидії загрозам національній безпеці України.

Закон України "Про захист персональних даних", прийнятий у 2010 році, був покликаний врегулювати правові відносини, пов’язані із захистом і обробкою персональних даних, і спрямований на захист основоположних прав і свобод людини і громадянина, зокрема права на невтручання в особисте життя у зв’язку з обробкою персональних даних (стаття 1). Закон також містив положення, що стосувалися обмеження його дії у випадках, передбачених законом, наскільки це необхідно у демократичному суспільстві в інтересах національної безпеки, економічного добробуту або захисту прав і свобод суб’єктів персональних даних чи інших осіб (стаття 25) [30].

Не зважаючи на всі перелічені сприятливі для розвитку розвідки з відкритих джерел фактори технологічного і правового характеру, слід констатувати, що прориву у розвитку OSINT в секторі безпеки України у той період не сталося. Пошук і здобування інформації здійснювався значною мірою хаотично – без розробки методик, уніфікації підходів тощо. Банально не передбачалося і не було достатньої кількості комп’ютерів, підключених до мережі Інтернет. Організаційно виокремлення підрозділів чи створення посад, посадові яких передбачали би проведення такого виду діяльності, не відбулося. Причини лежали в політичній площині, де панували непослідовність відходу від російського вектору у зовнішній політиці, загравання з російським бізнесом і

політикумом, що агресивно проникали у внутрішні справи нашої країни. Зближення з Заходом відбувалося нерівномірно, окремі практики, у тому числі при роботі з інформацією, формальне сприймалися, але не впроваджувалися.

Натомість у приватному секторі України, за участі колишніх працівників спецслужб та правоохоронних органів і науковців, з'явилися окремі компанії або підрозділи у складі фінансово-промислових груп, що провадили так звану "конкурентну розвідку", "корпоративну розвідку", "бізнес-розвідку", яка визначалася як система збору, обробки та аналізу інформації про внутрішнє та зовнішнє середовище компанії з метою підтримки прийняття управлінських рішень [31], та модель роботи якої відтворювала розвідувальний цикл спеціальних служб [32, с. 25].

Наступний період становлення розвідки з відкритих джерел інформації починається у 2014 році. Історично склалося, що надзвичайні події часто стають поштовхом до нового етапу організаційного оформлення і правового регулювання використання інформації, у тому числі з відкритих джерел, в інтересах національної безпеки. При цьому зміни відбуваються настільки безпрецедентні за своїм змістом, що суттєво впливають на весь подальший розвиток ситуації.

Як Друга світова війна стала умовною точкою початку розвідки з відкритих джерел в історії органів сектору безпеки і оборони й у сучасному її розумінні, так і російська агресія 2014 року вивела на абсолютно новий рівень роботу з відкритими джерелами інформації в інтересах національної безпеки України. Анексія Автономної Республіки Крим та окупація частини Донецької і Луганської областей підштовхнула українські органи сектору безпеки і оборони до рішучих дій – швидких та ефективних, у тому числі зі здобування й аналізу інформації.

Саме тому у 2014 році відбувся сплеск OSINT і особливо SOCMINT (пошук, збір інформації з соціальних медіа) в Україні. Місцеві сепаратисти в Автономній Республіці Крим, Донецькій, Луганській областях за російського кураторства використовували соціальні медіа для поширення антиукраїнських ідей. Водночас, в цих же медіа з'явилася значна кількість даних, що підтверджували факти перебування російських військовослужбовців на території України. Ця інформація не залишилася поза увагою українських громадян, держави, зокрема органів сектору безпеки і оборони України, і світової спільноти, а робота з відкритою інформацією перетворилася зі спорадичного пошуку й фіксації відокремлених даних на напрацювання методик їх системного добування, обробки, аналізу, у тому числі з використанням спеціального програмного забезпечення.

Розвідкою з відкритих джерел результативно та в інтересах національної безпеки почали займатися громадські організації та волонтери, співпрацюючи з вітчизняними органами сектору безпеки та оборони. Зокрема, у 2014 році створено спільноти "Інформнапалм" [33] та "Миротворець" [34], присвячені саме висвітленню перебігу подій у Криму та на Сході України й викриттю причетності росії до розв'язування військових дій, встановленню учасників збройного конфлікту з російської сторони та з числа громадян України, що перейшли на бік ворога. Здобуті дані оприлюднювалися на сайтах зазначених спільнот для широкого загалу та надавалися для потреб органів сектору безпеки і оборони, у тому числі за окремим протоколом доступу.

Важливим юридичним аспектом стало визнання отримуваних з відкритих джерел даних доказами у кримінальних провадженнях.

Слідчі Служби безпеки України та Генеральної прокуратури України ввійшли до складу Спільної слідчої групи (англ. Joint Investigation Team), створеної за ініціативи української сторони для розслідування збиття Боїнгу777 рейсу МН17 "Амстердам -

Куала-Лумпур" у липні 2014 року російським ЗРК "Бук" поблизу села Грабове Донецької області [35]. Серед іншого, Слідча група проаналізувала 5,5 млрд сторінок інформації в інтернеті. 17.11.2022 року Окружний суд в Гаазі виніс вирок у справі, яким визнав винними 3 з 4 обвинувачених [36].

Справа стала знаковою для всієї світової OSINT-спільноти з двох причин: по-перше, зібрані в інтернеті дані були визнані доказами; по-друге, до складу таких доказів ввійшли дані не тільки зафіксовані слідчими, а й зібрані громадськими організаціями, зокрема, британською дослідницькою групою Bellingcat та українською "Інформнапалм". Як зазначив засновник і керівник Bellingcat Еліот Гіггінс, саме з цієї справи аматори-осінтери перейшли від збору розрізнених фактів до формування цілісної сукупності доказів, а керівник групи вперше був запрошений міжнародними слідчими як свідок, будучи не безпосереднім учасником подій, а координатором збору даних з відкритих джерел інформації [37].

Що стосується організаційного оформлення розвідки з відкритих джерел в органах сектору безпеки і оборони України, то у 2016-2017 роках в органах системи МВС України (Національній поліції, Державній прикордонній службі) запроваджено підрозділи кримінального аналізу, одним із елементів якого було визначено пошук інформації у відкритих джерелах [38, с. 105-106]. До Закону України "Про оперативно-розшукову діяльність" внесені зміни щодо права підрозділів, які здійснюють ОРД, безпосередньо проводити або ініціювати проведення кримінального аналізу (пункт 21 статті 8) [39].

Суттєво змінилися інші правові умови діяльності та сам сектор безпеки і оборони України: прийнято закони України "Про національну безпеку" [40], "Про Національне антикорупційне бюро України" [41], "Про розвідку" [42] та інші й внесені зміни до тих законів, що визначали допустимі межі діяльності зі збору, обробки, аналізу інформації.

Зокрема зміни 2015 року до Закону України "Про доступ до публічної інформації" збільшили доступність даних державних реєстрів України для широкого загалу вітчизняних осінтерів. Зокрема, принципи забезпечення доступу до публічної інформації відтепер передбачали можливість вільного отримання, поширення та будь-якого іншого використання інформації, що була надана або оприлюднена відповідно до цього Закону, крім обмежень, встановлених законом (пункт 2 статті 4 Закону), а доступ до цієї інформації у тому числі передбачався на державному веб-порталі відкритих даних (стаття 5 Закону) [43]. На виконання приписів цього закону, розпорядники інформації зобов'язувалися оприлюднити та оновлювати дані згідно з вимогами "Положення про набори даних, які підлягають оприлюдненню у формі відкритих даних", затвердженого постановою Кабінету Міністрів України [44]. Запровадження системи електронних закупівель та електронного декларування осіб, уповноважених на виконання функцій держави або місцевого самоврядування, з прийняттям відповідних законів суттєво підвищили рівень прозорості та доступності даних про витрати бюджетів і статки чиновників.

Остання з наведених змін правових умов роботи з інформацією дала поштовх до появи нового виду бізнесу, суть якого полягала у наданні послуг доступу до агрегованих даних з публічно доступних державних реєстрів, довідників, наборів даних, матеріалів державних закупівель через зручний клієнто-орієнтований інтерфейс. Це суттєво економило час для збору інформації та гарантувало її вищу повноту і достовірність. Так з'явилися сервіси-агрегатори даних з відкритих джерел – YouControl, Opendatabot, Vkursipro, Feodal, Scanbe.io, Clarity Project та інші. Цією можливістю активно користувалися журналісти-розслідувачі, громадські організації та приватний бізнес.

Технологічно доступність Інтернету, яким на 2014 рік користувалося уже половина дорослого населення України [45], та масове поширення смартфонів, які давали можливість фіксувати і миттєво поширювати великі обсяги даних (фото, відео, текстових тощо), гарантували їх експоненційне зростання в публічному інформаційному просторі.

Однак, у цей же період, з 2014 року, з'явилася і тенденція до контролю і обмеження доступу до цифрового контенту в мережі Інтернет. У 2014 році росія почала поетапно запроваджувати на державному рівні заходи контролю поведінки користувачів у мережі Інтернет та обов'язкову їх ідентифікацію, тим самим посилюючи можливості своїх спецслужб [46].

З метою захисту населення від шкідливих пропагандистських впливів для користувачів в Україні були заблоковані російські соціальні мережі, пошуковий сервіс "Яндекс" та деякі інші російські інтернет-ресурси, відповідно до Указу Президента України №133/2017 [47]. У 2020 році змінами до Закону України "Про інформацію" передбачено, що право на інформацію може бути обмежене законом в інтересах національної безпеки, територіальної цілісності або громадського порядку та з іншою названою у цьому законі метою [48].

І в цей же період, у 2018 році розгорівся міжнародний скандал у справі Cambridge Analytica – британської аналітичної компанії, яка використовувала аналіз та профілювання користувачів соцмереж, насамперед Facebook, для маркетингу та впливу на їх електоральні вподобання [49]. За словами колишньої директорки з розвитку бізнесу компанії Brittany Kaiser, політики вперше визнали "воєнізацію даних" (англ. weaponization of data), тобто перетворення даних (чи роботу з ними) на зброю, а викривач Cambridge Analytica Christopher Wylie визнав створену методику збору даних, їх обробки і використання, глибоко неетичною [2]. Розгляди справи Cambridge Analytica парламентами Великобританії і США та урядами Німеччини, Австралії, Індії мали наслідком посилення захисту персональних даних та пов'язаних з цим заходів регуляції діяльності соціальних медіа.

Як висловилася в своїх свідченнях Конгресу США Emma L Briant з University of Essex "використання даних не є саме по собі проблемою, справа в тому, як саме вони використовуються, і саме це має бути врегульоване щонайменше запровадженням вимоги щодо підвищення прозорості" [50]. Інші вимоги, на думку Emma L Briant, мають включати питання відповідальності за роботу з даними та пропорційність їх використання.

Саме ці вимоги були втілені в прийнятих у той період основних актах ЄС у сфері захисту персональних даних та технічного захисту інформації: Директиві ЄС 2016/679 "Загальний регламент захисту даних" (англ. General Data Protection Regulation – GDPR) і Директиві ЄС 2016/680 про захист фізичних осіб щодо обробки персональних даних компетентними органами з метою запобігання, розслідування, виявлення або переслідування кримінальних правопорушень чи виконання кримінальних покарань, а також про вільний рух таких даних.

Ці акти визначили можливість обробки персональних даних з обмеженням права суб'єкта на отримання інформації про факт обробки, коли це необхідно для захисту національної безпеки, захисту прав і свобод інших осіб, охорони громадської безпеки, уникнення завдання шкоди запобіганню, виявленню, розслідуванню, судовому переслідуванню кримінальних правопорушень або виконанню покарань. До такої обробки висувалися вимоги дотримання принципів: законність та справедливість,

прозорість мети, мінімізація обсягу даних, обмеженість строку зберігання, забезпечення безпеки та конфіденційності [51].

У рамках НАТО були прийняті стандарти проведення розвідки з відкритих джерел силами оборони, які визначили основні узгоджені для членів Альянсу поняття щодо OSINT: стандарт 6522 “Спільна союзна доктрина з питань розвідки з відкритих джерел” (AJP-2.9, 2019) і стандарт 6537 ”Тактика, техніки та процедури розвідки з відкритих джерел ” (AIntP-22, 2022).

Зазначені міжнародні документи не містили норм прямої дії стосовно України, однак визначили вимоги до регулювання діяльності зі збору, обробки та аналізу даних, у тому числі з відкритих джерел інформації, на міжнародному і національному рівнях з огляду на стратегічний курс на євроатлантичну інтеграцію.

У 2022 році розпочався поточний етап розвитку розвідки з відкритих джерел в інтересах національної безпеки України.

Більшість тенденцій розвитку розвідки з відкритих джерел інформації в Україні, характерних для періоду, що почався у 2014 році, продовжують свою дію: зростання рівня діджиталізації суспільства, експоненційне зростання кількості доступних вікритих даних, співпраця органів сектору безпеки з громадськістю, спроби врегулювання правових умов розвідки з відкритих джерел тощо. Однак декілька факторів технологічного, правового та організаційного характеру стали новими, і саме тому цей період визначається для України як окремий.

Повномасштабне вторгнення російської федерації в Україну викликало вибухове збільшення обсягів відкритих даних, що потрапляють в Інтернет. За підрахунками Matthew Ford зі Swedish Defence Institute, процитованими The Economist, у 2022 році за 80 днів з початку повномасштабного вторгнення в Інтернет потрапило відео подій загальною тривалістю понад 10 років (для порівняння – такий обсяг відеоданих про події війни в Сирії потрапив в інтернет за 10 років) [52].

Також, різко зросла і кількість даних особистого характеру, які продаються або оприлюднюються, найчастіше в темному Інтернеті (даркнеті) – частині інтернету, яка не індексується стандартними пошуковими системами та вимагає спеціального програмного забезпечення для доступу [53]. Поява таких даних зумовлена як скоординованою діяльністю ворожих спецслужб, які переслідують мету підриву довіри громадян до своєї держави, так і індивідуальними злочинними діями хакерів, які діють з корисливою метою, продаючи дані. Зібрані так звані злиті бази даних призвели до появи телеграм-ботів чи андроїд-застосунків, які за плату або в обмін на надання власних даних надають користувачеві персональні дані інших осіб. З’явився неформальний термін, який означав швидке отримання ідентифікуючих, але неверифікованих даних особи за уривчастими даними (номером телефону, електронною-поштою, телеграм-ідентифікатором тощо) з відповідного телеграм-боту або андроїд-застосунку. Тобто, закритість і захищеність персональних даних почала масово нівелюватися.

Ці характеристики найбільше ілюструють ключову відмінність збору інформації з відкритих джерел від попередніх періодів, а саме: доступність величезних обсягів даних (big data), у тому числі неетичних за змістом, без визначеного правового статусу та захисту, і потребу у відборі з них релевантних даних програмними засобами, у тому числі із застосуванням технологій штучного інтелекту (ШІ).

Якщо у випадку Cambridge Analytica технологія ШІ застосовувалася виключно спеціалістами всередині компанії, то з появою у 2022 році генеративних моделей на кшталт Chat GPT, Perplexity, Claude, Deep Seek та інших, їх можливості з автоматизації пошуку, обробки, аналізу інформації почали використовувати величезна кількість

людей, включаючи осінтерів. Слід відзначити, що одразу з запуском цих моделей держави почали намагатися впровадити стосовно їх діяльності заходи регулюючого впливу, вимагаючи запровадження обмежень щодо роботи з інформацією особистого характеру.

Щодо факторів правового характеру, то в Україні правовий режим воєнного стану, запроваджений з 24.02.2022 року, створив принципово інші умови роботи насамперед з персональними даними, передбачаючи можливість правомірного обмеження права на їх захист.

З організаційної точки зору оформилася тенденція до врегулювання не лише інформаційної діяльності в цілому, а й окремо розвідки з відкритих джерел. У 2023 році в Україні імплементовані стандарти НАТО 6522 “Спільна союза доктрина з питань розвідки з відкритих джерел” (AJP-2.9, 2019) і 6537 “Тактика, техніки та процедури розвідки з відкритих джерел OSINT” (AIntP-22, 2022) [54]. Стратегія розвитку СБ України на 2025-2030 роки визначає необхідність використання розвідки з відкритих джерел серед інших напрямів здобування інформації для оцінки масштабу і характеру загроз та пріоритетність використання у тому числі OSINT серед для оперативного виявлення і знищення ворожих цілей за будь-яких умов [55].

Виходячи із викладеного, періодизація історико-правового розвитку розвідки з відкритих джерел в інтересах національної безпеки України є такою:

ЕТАП І.
ІНСТИТУЦІЙНЕ СТАНОВЛЕННЯ В "АНАЛОГОВУ" ЕРУ
(1991–2005 рр.)

Цей початковий етап характеризується процесами формування нормативно-правової бази функціонування сектору безпеки незалежної України. Розвідка з відкритих джерел (OSINT) у цей період мала такі ключові риси:

1) Невизначеність правових основ OSINT.

Діяльність у сфері розвідки регулювалася новоствореними законами, що визначали загальні засади інформаційно-аналітичної діяльності, проте спеціалізоване правове поле для OSINT було відсутнє.

2) Переважання нецифрових форматів.

Основна діяльність з розвідки з відкритих джерел велася переважно з фізичними носіями інформації: періодичними виданнями, офіційними довідниками, архівами, бібліотечними фондами, даними, отриманими в ході оперативно-розшукової діяльності, що визначало методологію роботи як переважно "аналогову".

3) Державна монополія та інституційна інерція.

OSINT як професійна діяльність була виключною прерогативою державних акторів, насамперед Служби безпеки України. Ця інформаційно-аналітична діяльність передбачалася посадовими обов’язками окремих співробітників і регламентувалася відомчими інструкціями, водночас не виокремлюючись в самостійний напрям діяльності, і значною мірою спиралася на застарілі радянські практики.

4) Повільний розвиток OSINT.

Прогрес стримувався низьким рівнем проникнення сучасних інформаційних технологій в діяльність спецслужб та їхньою інституційною консервативністю, що призвело до відставання від передових світових напрацювань.

5) Зародковий стан недержавного OSINT.

Робота недержавних акторів зі збору та обробки інформації з відкритих джерел була фрагментарною та не мала значного впливу на забезпечення національної безпеки.

Ця діяльність була представлена переважно окремими розслідуваннями журналістів, науковими дослідженнями чи спробами бізнес-аналізу.

ЕТАП ІІ.
ЦИФРОВІЗАЦІЯ OSINT ТА ПОЯВА НЕДЕРЖАВНИХ АКТОРІВ
(2005–2014 рр.)

Цей часовий проміжок відзначений технологічними змінами в суспільстві та першими кроками до диверсифікації акторів, що провадять збір та аналіз інформації з відкритих джерел, хоча в державному секторі якісного прориву не відбулося. Його характерними ознаками є:

1) Технологічна революція та зародження "цифрового" OSINT.

Стрімке зростання кількості інтернет-користувачів та поява соціальних медіа стали ключовими факторами, що відкрили можливості збору та аналізу великих масивів даних у цифровому середовищі та зумовили поступовий перехід від аналізу статичних джерел до моніторингу динамічних онлайн-ресурсів та неструктурованих даних (форуми, блоги, соціальні медіа).

2) Структурування сектору безпеки і оборони України.

Виокремлюються нові спеціальні служби, що раніше існували як підрозділи у складі Служби безпеки України.

3) Поява і активізація діяльності недержавних акторів.

Методи OSINT почали активно використовувати в інтересах бізнесу, а не лише для потреб національної безпеки. Відбулося становлення так званої "корпоративної розвідки", що використовує OSINT для бізнес-аналітики.

4) Поступова синхронізація з глобальними трендами.

Український OSINT-дискурс починає поступово синхронізуватися із західним, зокрема американським. Розвиток відбувається переважно в комерційному секторі, тоді як державний сектор залишається відносно інертним через неналежне матеріальне та забезпечення та ідеологічну непослідовність органів сектору безпеки.

ЕТАП ІІІ.
ПРОФЕСІОНАЛІЗАЦІЯ OSINT ТА ПРАВОВЕ ВИЗНАННЯ
(2014 – 2022 рр.)

Початок збройної агресії Російської Федерації у 2014 році став потужним каталізатором для якісної трансформації OSINT. Цей етап характеризується перетворенням OSINT на одну з ключових інформаційних технологій сектору безпеки і оборони та включає такі складові:

1) Операціоналізація та бойове застосування.

Збройна агресія російської федерації проти України, що створила гострий запит на оперативну, точну та доказову інформацію для протидії збройній та гібридній загрозам. OSINT перестав бути лише інструментом пасивного аналізу і став інструментом активного впливу, підтримки бойових дій, збору доказів у злочинах проти основ національної безпеки та порушень міжнародного гуманітарного права. Він утверджується як високоефективна інформаційна технологія, здатна вирішувати широкий спектр завдань – від тактичних до стратегічних. Відбувається його інтеграція в операційні процеси всіх складових сектору безпеки і оборони.

2) Стрімка професіоналізація та спеціалізація.

В органах сектору безпеки і оборони України з'являється спеціалізація зі збору даних, формуються унікальні методики, що відповідають напрямам розвідувальної, контррозвідувальної, оперативно-службової, оперативно-бойової діяльності.

3) Формування OSINT-екосистеми.

Виникає синергетична взаємодія між органами сектору безпеки і оборони та недержавними аналітичними центрами, волонтерськими спільнотами (наприклад InformNapalm), міжнародними партнерами в інтересах національної безпеки України.

4) Правова легітимізація.

Вперше у світовій практиці дані, отримані з відкритих джерел, почали використовуватись як докази в кримінальних провадженнях за фактами воєнних злочинів, вчинених російськими загарбниками.

5) Актуалізація викликів захисту і безпеки даних.

Розробка глибоко неетичних протоколів збору й обробки особистої інформації засвідчили зростаючу важливість регулювання цифрового простору та захисту громадян від маніпулятивного використання персональних даних, впровадження вимог прозорості, відповідальності та пропорційності використання даних.

6) Поглиблення міжнародної співпраці.

Посилюється міжнародне співробітництво органів сектору безпеки і оборони із західними спецслужбами та правоохоронними органами у сфері OSINT.

ЕТАП IV.
НОВА АРХІТЕКТУРА OSINT:
ВЕЛИКІ ДАНІ, ШІ ТА ГЛОБАЛЬНЕ ПАРТНЕРСТВО
(2022 р. –донині)

Повномасштабне вторгнення росії на територію України започаткувало новий етап, що характеризується експоненційним зростанням обсягів даних, застосуванням новітніх технологій для їх обробки і аналізу та безпрецедентним рівнем співпраці. Цьому етапу характерні такі ознаки як:

1) Трансформація OSINT у воєнний час.

Повномасштабна військова агресія рф супроводжується масштабними кібератаками, зламами державних систем накопичення даних, маніпуляціями відкритою інформацією та використанням даних як зброї.

2) Зростання кількості витоків даних, у тому числі персональних.

Експоненційне зростання обсягів даних у відкритому доступі створює можливості для підвищення ефективності розвідки з відкритих джерел, однак з'являється виклик для здатності людини опрацювати ці дані без спеціального програмного забезпечення.

3) Big data і застосування штучного інтелекту.

Штучний інтелект став ключовим інструментом для автоматизованого пошуку, систематизації та аналізу великих обсягів даних, що дозволило суттєво підвищити ефективність та масштабувати розвідувальну діяльність. Технології штучного інтелекту стають важливим інструментом для виявлення неочевидних закономірностей та аналізу.

4) Формування національного інформаційного фронту.

Створюється модель загальнонаціональної OSINT-мобілізації, в рамках якої відбувається фактичне поєднання зусиль громадянського суспільства та державного сектору, що дозволяє досягти ефекту колективного розвідувального інтелекту.

5) Регуляція OSINT.

Початок формалізованого регулювання розвідки з відкритих джерел через імплементацію міжнародних стандартів, визначення стратегій її проведення та визначення місця серед інших розвідувальних спроможностей.

6) Інтенсивне міжнародне партнерство.

Співпраця сектору безпеки і оборони України з іноземними спецслужбами, правоохоронними органами та міжнародними організаціями перейшла від ситуативної взаємодії до системного та глибокого партнерства, перетворивши український OSINT на інтегрований елемент глобальної системи інформаційної взаємодії.

Таким чином, історія розвитку розвідки з відкритих джерел в секторі безпеки і оборони України пройшла еволюційний шлях, прискорений технологічним прогресом. Надзвичайні події, як російська агресія, дали поштовх до екстраординарних дій та парадоксальним чином сприяли інтенсифікації використання OSINT в інтересах національної безпеки. Цей шлях пролягав від закритої, "аналогової" державної монополії, що спиралася на застарілі радянські практики, до гнучкої, професійної та юридично визнаної цифрової спроможності, яка сьогодні стоїть на трьох стовпах: синергії держави і суспільства, технологіях штучного інтелекту та міжнародному партнерстві.

Список використаних джерел

1. Annie Maddison. Information and its management. *Managing Defence in a Democracy*/ Ed. By Laura R. Clearly. Cass Military Studies, 2010. 272 p.

2. Документальний фільм *The Great Hack* режисерів Jehane Noujaim і Karim Amer/ URL: https://www.netflix.com/watch/80117542?trackId=14277281&tctx=-97%2C-97%2C%2C%2C%2C%2C%2C%2CVideo%3A80117542%2CdetailsPagePlayButton (дата звернення 20.12.2021)

3. Nihad A. Hassan, Rami Hijazi. Open Source Intelligence Methods and Tools: A Practical Guide to Online Intelligence. Apress Media LLC, 2018. https://doi.org/10.1007/978-1-4842-3213-2.

4. Швидкий О. OSINT 4:0: Цифрові технології для зміцнення національної безпеки України. *Роль OSINT-досліджень у підвищенні рівня національної безпеки: матеріали круглого столу з міжнародною участю м. Львів, 7 травня 2025 року*, Львів: ЛьвДУВС, 2025. С. 227-232.

5. Michael Glassman, Min Ju Kang. Intelligence in the internet age: The emergence and evolution of Open Source Intelligence (OSINT) *Computers in Human Behavior.* 2012. № 28. P. 673-682.

6. Ланде Д.В. OSINT у кібербезпеці : навчальний посібник. Київ: ТОВ "Інжиніринг", 2024. 552 с.

7. Технологія OSINT в управлінні кризовими ситуаціями та попередженні кіберзагроз: науково-практичний посібник / О. Довгань, А. Старосєк, А. Тарасюк, Т. Ткачук. - КиївОдеса : Фенікс, 2024. 183 с.

8. Жмур Н., Землянікіна М. Історія становлення та сучасний стан технології пошуку інформації OSINT. *Юридичний вісник. 2022. 3 (64).* С. 95-101. DOI: 10.18372/2307-9061.64.16895

9. Технологія OSINT: інструменти та методи для захисту інформаційної безпеки: практичний посібник / Т. Ткачук, Н. Ткачук, І. Ничитайло, А. Старосєк. - Київ: НА СБУ, 2023. 180 с.

10. Preparing for the 21st Century - An Appraisal of U.S. Intelligence: Report of the Commission on the Roles and Capabilities of the United States Intelligence Community 1 March 1996. URL: https://www.govinfo.gov/app/details/GPO-INTELLIGENCE/context (Дата звернення 09.05.2025).

11. Публікація Офісу Директора національної розвідки від 08 листопада 2005 року. ODNI Announces Establishment of Open Source Center. URL:

https://web.archive.org/web/20060623072458/http://dni.gov/press_releases/20051108_release.htm (Дата звернення 09.05.2025).

12. Aftergood Steven. Open Source Center (OSC) Becomes Open Source Enterprise (OSE). URL: https://fas.org/publication/osc-ose/ (Дата звернення 09.05.2025).

13. Про Службу безпеки України: Закон України від 25.03.1992 р. N 2229-XII. URL: https://zakon.rada.gov.ua/laws/show/2229-12/ed19920325#Text (дата звернення 19.08.2023).

14. Постанова Верховної Ради України від 20 вересня 1991 року Про створення Служби національної безпеки України. URL: https://zakon.rada.gov.ua/laws/show/1581-12#Text (дата звернення 19.08.2023)

15. Витяг з Інструкції, затвердженої Наказом ЦУ СБУ № 0039 1992 року.

16. Про інформацію: Закон України від 02.10.1992 р. № 2658-XII. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text (дата звернення 19.08.2023)

17. Конституція України. URL: https://zakon.rada.gov.ua/laws/show/254к/96-вр?find=1&text=інформац#w1_7 (дата звернення 19.08.2023)

18. Про оперативно-розшукову діяльність: Закон України від 18.02.1992 р. № 2135-XII зі змінами в редакції від 09.08.2003 р. URL: https://zakon.rada.gov.ua/laws/show/2135-12/ed20030809#Text (дата звернення 19.08.2023).

19. Про розвідувальні органи України: Закон України від 22.03.2001 р. № 2331-III URL: https://zakon.rada.gov.ua/laws/show/2331-14/ed20010322#Text (дата звернення 19.08.2023).

20. Кримінальний кодекс України від 05.04.2001 р. № 2341-III зі змінами в редакції від 19.11.2003 р. URL: https://zakon.rada.gov.ua/laws/show/2341-14?ed=20031119&find=1&text=Стаття+361#w2_1 (дата звернення 19.08.2023).

21. Про контррозвідувальну діяльність : Закон України від 26.08.2002 р. № 374-IV в редакції від 01.08.2003. URL: https://zakon.rada.gov.ua/laws/show/374-15/ed20030801#Text (дата звернення 19.08.2023).

22. Про основи національної безпеки України: Закон України від 19.06.2003 р. № 964-IV. URL: https://zakon.rada.gov.ua/laws/show/964-15/ed20030619#Text (дата звернення 19.08.2023).

23. Публікація Київського міжнародного інституту соціології від 20.04.2012. Динаміка проникнення інтернету в Україну. URL: https://kiis.com.ua/?lang=ukr&cat=reports&id=80&page=1 (дата звернення 09.05.2025).

24. Горностай Н.І., Михальченкова О.Є. Стан галузі ІКТ в Україні і світі. *Інформаційні технології*. 2021. № 4. С. 71-77. DOI: 10.35668/2520-6524-2021-4-07.

25. Bellis Mary. The History of Facebook and How It Was Invented. URL: https://www.thoughtco.com/who-invented-facebook-1991791 (дата звернення 09.05.2025).

26. Архів публікації Павла Дурова у "ВКонтакте" від 3 лютого 2007 року. URL: https://archive.ph/20121225212654/https://vk.com/blog?nid=30 (дата звернення 09.05.2025).

27. Публікація ГО "Детектор медіа" від 18.01.2017. Кількість відвідувачів "ВКонтакте" в Україні досягла рекордної позначки - 15 мільйонів на добу. URL: https://ms.detector.media/sotsmerezhi/post/18220/2017-01-18-kilkist-vidviduvachiv-vkontakte-v-ukraini-dosyagla-rekordnoi-poznachky-15-milyoniv-na-dobu/ (дата звернення 09.05.2025) та стаття у Вікіпедії. VK (соцмережа). URL: https://uk.wikipedia.org/wiki/VK_(соцмережа)#cite_note-blog70-12 (дата звернення 09.05.2025).

28. Про Службу зовнішньої розвідки України: Закон України від 01.12.2005 р. № 3160-IV. URL: https://zakon.rada.gov.ua/laws/show/3160-15/ed20051201#Text (дата звернення: 19.08.2023).

29. Про Службу безпеки України: Закон України від 25.03.1992 р. N 2229-XII в редакції від 14.01.2006. URL: https://zakon.rada.gov.ua/laws/show/2229-12/ed20060114#Text (дата звернення: 19.08.2023).

30. Про захист персональних даних: Закон України № 2297-VI в редакції від 01.01.2014. URL: https://zakon.rada.gov.ua/laws/show/2297-17/ed20140101#Text (Дата звернення: 10.05.2025).

31. Корпоративна розвідка. URL: https://x-scif.info/articles-and-literature/korporatyvna-rozvidka/ (дата звернення 09.05.2025).

32. Погребной С., Герасимович І. Корпоративна безпека в Україні: як захистити бізнес. Короткий курс. - Київ: Кінцевий бенефіціар. 2024. 336 с.

33. Про спільноту. URL: https://informnapalm.rocks (Дата звернення 09.05.2025).

34. Про спільноту. URL: https://myrotvorets.center/about/ (Дата звернення 09.05.2025).

35. Повідомлення УНІАН. Міжнародна слідча група розпочала розслідування авіакатастрофи Boeing-777. URL: https://www.unian.ua/politics/amp-960721-mijnarodna-slidcha-grupa-rozpochala-rozsliduvannya-aviakatastrofi-boeing-777.html (дата звернення: 19.08.2023).

36. Публікація Центру протидії дезінформації РНБОУ від 18.11.2022. Що означає вирок по справі MH17 для України, росії та світу. URL: https://cpd.gov.ua/articles/shho-oznachaye-vyrok-po-spravi-mn17-dlya-ukrayiny-rosiyi-ta-svitu/ (дата звернення: 19.08.2023).

37. Гіггінз Е. Ми - Беллінгкет. Київ: Наш формат. 2022. 236 с.

38. Реалізація філософії "Intelligence-led Policing" в системі кримінального аналізу Національної поліції України: монографія / Користін О. та ін. Київ: "ВАІТЕ", 2024. 442 с.

39. Про Бюро економічної безпеки України: Закон України від 28.01.2021 р. № 1150-IX. URL: https://zakon.rada.gov.ua/laws/show/1150-20/ed20220101#n481 (Дата звернення 09.05.2025).

40. Про національну безпеку України: Закон України від 21.06.2018 № 2469-VIII. URL: https://zakon.rada.gov.ua/laws/show/2469-19/ed20180621#Text (Дата звернення 09.05.2025)

41. Про Національне антикорупційне бюро України: Закон України від 14.10.2014 р. № 1698-VII. URL: https://zakon.rada.gov.ua/laws/show/1698-18/ed20141014#Text (Дата звернення 09.05.2025).

42. Про розвідку: Закон України від 17.09.2020 р. № 912-IX URL: https://zakon.rada.gov.ua/laws/show/912-IX#Text (Дата звернення 09.05.2025).

43. Про внесення змін до деяких законів України щодо доступу до публічної інформації у формі відкритих даних: Закон України від 9 квітня 2015 року № 319-VIII. URL: https://zakon.rada.gov.ua/laws/show/319-19/ed20150409#Text (дата звернення: 19.08.2023).

44. Постанова Кабінету Міністрів України Про затвердження Положення про набори даних, які підлягають оприлюдненню у формі відкритих даних від 21.10.2015 № 835, URL: https://zakon.rada.gov.ua/laws/show/835-2015-п/ed20151021#Text (дата звернення: 19.08.2023)

45. Публікація Київського міжнародного інституту соціології 28.10.2013. Динаміка використання Інтернет в Україні. URL: https://kiis.com.ua/?lang=ukr&cat=reports&id=199&page=2&y=2013

46. Архів публікації від 30.07.2014 "ФСБ зможе черпати більше інформації зі соцмереж, про українців теж". URL: https://web.archive.org/web/20140730231217/http://www.pravda.com.ua/news/2014/07/30/7033461/ (Дата звернення 09.05.2025).

47. Указ Президента України №133/2017 "Про рішення Ради національної безпеки і оборони України від 28 квітня 2017 року "Про застосування персональних спеціальних економічних та інших обмежувальних заходів (санкцій)". URL: https://www.president.gov.ua/documents/1332017-21850 (Дата звернення 09.05.2025).

48. Про внесення змін до деяких законодавчих актів України у зв'язку з прийняттям Закону України "Про внесення змін до деяких законодавчих актів України щодо спрощення досудового розслідування окремих категорій кримінальних правопорушень": Закон України від 17 червня 2020 року № 720-IX. URL: https://zakon.rada.gov.ua/laws/show/720-20#n332 (Дата звернення 09.05.2025).

49. Cambridge Analytica Files on The Guardian. URL: https://www.theguardian.com/news/series/cambridge-analytica-files (Дата звернення 09.05.2025).

50. Evidence for the US Senate Judiciary Committee on Cambridge Analytica and SCL Group by Dr Emma L Briant, Senior Lecturer (equivalent to Associate Professor) at University of Essex. URL: https://www.judiciary.senate.gov/imo/media/doc/Professor%20Emma%20L.%20Briant%20Report%20on%20Cambrige%20Analytica.pdf (Дата звернення 09.05.2025).

51. Directive (EU) 2016/680 of the European Parliament and the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA. URL: https://eur-lex.europa.eu/eli/dir/2016/680/2016-05-04/eng (Дата звернення 09.05.2025).

52. Open Source Intelligence is piercing the fog of war in Ukraine. URL: https://www.economist.com/interactive/international/2023/01/13/open-source-intelligence-is-piercing-the-fog-of-war-in-ukraine (Дата звернення 09.05.2025).

53. Визначення терміну в онлайн-словнику Termin.in.ua. URL: https://termin.in.ua/darknet/ та онлайн-журналі Wired. URL: http://www.wired.com/2014/11/hacker-lexicon-whats-dark-web/ (Дата звернення 09.05.2025).

54. Перелік прийнятих чинних стандартів НАТО, передбачених Цілями партнерства, в Міністерстві оборони України, Збройних Силах України та інших складових сектору безпеки і оборони. [сайт] URL: https://www.mil.gov.ua/content/mil_standard/0752024_Perelik_standartiv_NATO.pdf (Дата звернення 09.05.2025).

55. Стратегія розвитку Служби безпеки України на 2025-2030 роки. URL: https://ssu.gov.ua/uploads/documents/2025/05/20/sbu-strategiya-2025-for-web.pdf (Дата звернення 19.08.2025)

~~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~~
~~~~~~~~~~~~~~