УДК 342
DOI https://doi.org/10.32782/yuv.v4.2025.9

Ю. Кардашевський,
доктор філософії у галузі права,
керівник відділу внутрішнього контролю
Національного агентства з питань запобігання корупції

МІЖДИСЦИПЛІНАРНІ ЗАСАДИ РОЗВІДУВАЛЬНОЇ АНАЛІТИКИ В СЕКТОРІ БЕЗПЕКИ УКРАЇНИ

Постановка проблеми. Розвідувальна аналітика є ключовим елементом системи національної безпеки, що забезпечує своєчасне виявлення загроз, прогнозування ризиків і формування ефективних рішень у сфері безпеки. В умовах глобалізації та інформаційної турбулентності вона виконує функцію «мозкового центру», що інтегрує розвідувальні дані, аналітичні методи й правові інструменти для підтримки стратегічного та оперативного управління.

Її місце визначається не лише функціональним навантаженням, а й взаємодією з іншими суб'єктами сектору безпеки – спецслужбами, правоохоронними органами, аналітичними центрами. Аналітика створює інформаційне підґрунтя для протидії гібридним загрозам, тероризму, кібератакам і підтримує прийняття рішень у критичних ситуаціях.

Метою наукової публікації є дослідження сучасних аспектів функціонування розвідувальної аналітики через такі напрями як: функціональна роль у багаторівневому ухваленні рішень; інституційна структура та механізми міжвідомчої взаємодії; правове регулювання діяльності аналітичних підрозділів; застосування технологій (big data, AI, кіберінструментів); а також участь у виявленні та аналізі актуальних загроз – від гібридних війн до інформаційних атак.

Даний комплексний підхід до аналізу означених проблемних питань дозволить осмислити розвідувальну аналітику як системний елемент управління безпекою в умовах сучасних викликів.

Виклад основного матеріалу. Говорячи про *функціональну роль розвідувальної аналітики в системі національної безпеки*, зауважимо, що розвідувальна аналітика є центральним елементом системи національної безпеки, що виконує критично важливі функції в ідентифікації, аналізі та прогнозуванні загроз. Вона базується на інтеграції розвідувальних даних, методів аналізу та технологічних рішень, забезпечуючи формування об'єктивної картини безпекового середовища.

На с*тратегічному рівні* аналітика сприяє формуванню державної політики у сфері безпеки, розробці сценаріїв розвитку загроз і визначенню пріоритетів реагування. *Оперативна аналітика* забезпечує швидке реагування на загрози, підтримує міжвідомчу координацію та інтегрується з оперативно-розшуковою діяльністю. *Тактична аналітика* орієнтована на підтримку безпекових операцій, ґрунтуючись на точних, спеціалізованих даних з технічних та агентурних джерел [1; 2; 3].

Комплексна роль аналітики охоплює як традиційні загрози (тероризм, військові конфлікти), так і новітні – кіберзлочинність, гібридні війни, інформаційні атаки. Прогнозування ризиків ґрунтується на експертному

аналізі, математичних моделях, штучному інтелекті та big data [4]. Разом з тим, аналітичні продукти мають бути своєчасними, достовірними та релевантними для всіх рівнів управління. При цьому важливими залишаються питання якості даних, правового регулювання та інтеграції інформації з різних джерел [5; 6].

У провідних державах світу (США, Велика Британія) аналітика функціонує в межах чітко структурованих моделей з єдиною системою збору й аналізу даних [7; 8]. В Україні розвідувальна аналітика розвивається у відповідь на нові виклики, зокрема через впровадження технологій, розвиток міжвідомчої взаємодії та професійного середовища. Водночас актуальними залишаються проблеми нормативного забезпечення та обмежених ресурсів [9].

Тож функціональна роль розвідувальної аналітики в системі національної безпеки є багатовимірною і комплексною. Вона охоплює виявлення загроз, формування об'єктивної інформаційної бази, прогнозування ризиків і підтримку прийняття управлінських рішень на різних рівнях. Ефективність цієї ролі визначається якістю аналітичних методів, рівнем технологічного забезпечення, правовим регулюванням та ступенем координації між суб'єктами безпеки.

Водночас інституційне закріплення розвідувальної аналітики та механізми її взаємодії в державних органах є важливою складовою забезпечення національної безпеки. У сучасних умовах, які характеризуються складністю та багатовимірністю загроз, інтеграція аналітичних ресурсів і міжвідомча координація є запорукою оперативності, повноти та достовірності аналітичної інформації.

Розвідувальна аналітика традиційно функціонує в межах спеціалізованих державних структур, серед яких важливі місця належать розвідувальним органам, службам безпеки, оборонним відомствам і правоохоронним органам. Кожен із цих суб'єктів має власні функції, аналітичні підрозділи, методології та інформаційні ресурси. Проте їх співпраця ускладнюється великою кількістю завдань і інформаційних потоків [2; 8].

З розвитком концепції комплексної безпеки та інформаційної інтеграції з'явилися нові інституційні форми, що підвищили ефективність аналітики – аналітичні центри (think tanks), центри з обміну інформацією (fusion centers) та міжвідомчі координаційні платформи. Аналітичні центри, як незалежні або напівдержавні установи, забезпечують науково-експертний супровід національної безпеки, залучаючи експертів для мультидисциплінарного аналізу. Прикладом є RAND Corporation (американська некомерційна дослідницька організація, що спеціалізується на аналізі та консалтингу в галузі державної політики, а також проводить дослідження та розробки в різних галузях, включаючи національну безпеку), Royal United Services Institute for Defence and Security Studies (RUSI) (британський аналітичний центр, що спеціалізується на проблемах міжнародної безпеки та військової справи) або Український інститут майбутнього (незалежний аналітичний центр, що прогнозує зміни у країні та світі та моделює можливі сценарії розвитку подій).

Ф'южн-центри функціонують як практичні інструменти інтеграції інформації від різних державних і недержавних суб'єктів, об'єднуючи дані розвідки, правоохоронних органів, митниці, прикордонної охорони та інших. Їх мета – забезпечити обмін інформацією, ідентифікацію загроз та координацію заходів реагування. Така модель активно застосовується в США та ЄС для боротьби з тероризмом, організованою злочинністю та кіберзагрозами [10; 11].

Особливої актуальності набувають механізми міжвідомчої координації, які включають нормативно-правове

регулювання, створення робочих груп, обмін інформацією на основі договорів про конфіденційність і технічні засоби інтеграції даних. В міжнародній практиці використовуються стандартизовані протоколи обміну інформацією, такі як STIX/TAXII [12] для кіберрозвідки, а також платформи (SIEM-системи), що забезпечують автоматизоване сповіщення про інциденти [4].

Наразі в Україні питання інституційного закріплення розвідувальної аналітики активно розвиваються і основними суб'єктами в даному аспекті є Служба безпеки України, Міністерство оборони України, Національна поліція України, Державна служба спеціального зв'язку, Служба зовнішньої розвідки, а також органи при Раді національної безпеки і оборони. Сучасні виклики, такі як кібервійна, гібридні загрози та інформаційні атаки, вимагають створення більш гнучких структур, зокрема ф'южн-центрів, що здатні оперативно акумулювати інформацію та приймати скоординовані рішення.

Важливим елементом ефективної взаємодії є міждержавне співробітництво (NATO, EUROPOL тощо), завдячуючи якому спільні аналітичні платформи та інформаційний обмін дозволяють своєчасно виявляти транснаціональні загрози та реагувати на них на ранніх стадіях. [13; 14]

Недостатня координація та відсутність уніфікованих підходів можуть призвести до дублювання функцій, втрати інформації та сповільнення реакцій на загрози. Тому модернізація інституційної системи аналітики повинна бути одним із пріоритетів державної політики у сфері національної безпеки.

Усе більшого значення в межах розвідувальної аналітики набуває *правове забезпечення ролі розвідувальної аналітики*, а саме нормативно-правового регулювання повноважень, відповідальності та меж діяльності аналітичних підрозділів у сфері безпеки. Разом з тим, правове забезпечення діяльності розвідувальної аналітики є основою ефективного функціонування національної безпеки. Воно вимагає чіткого нормативного регулювання, що визначає повноваження, відповідальність та межі роботи аналітичних підрозділів, забезпечуючи баланс між державними інтересами, правами людини та громадянина.

Водночас аналітичні підрозділи державних структур мають законодавчо визначені повноваження для збору, обробки та аналізу інформації, зокрема через спеціальні методи і технічні засоби [15 – 18]. Законодавство регламентує доступ до різних інформаційних ресурсів, включаючи відкриті джерела та обмежену інформацію. Важливим є дотримання принципу законності, особливо при обробці персональних даних відповідно до Закону України «Про захист персональних даних» [19].

У цьому контексті важливим стає дотримання відповідальності та контролю за діяльністю аналітичних підрозділів, яка регулюється не лише законами, але й механізмами контролю, що передбачають кримінальну, адміністративну та дисциплінарну відповідальність за порушення. Зокрема, Кримінальний кодекс України [20] передбачає відповідальність за зловживання службовим становищем (ст. 365), насильницьке зникнення (ч. 1 ст. 146-1), вимагання (ч. 4 ст. 189), перевищення влади та інші правопорушення.

З розвитком кіберпростору й зростає актуальність правового регулювання діяльності аналітичних підрозділів у сфері кібербезпеки. Закон України «Про основні засади забезпечення кібербезпеки України» [21] визначає правові основи захисту інформаційних ресурсів та регламентує повноваження органів, відповідальних за кіберзахист, зокрема аналітичних служб. Особливу увагу приділено регулюванню моніторингу

та аналізу кіберзагроз, а також міжвідомчій і міжнародній взаємодії (NATO Cooperative Cyber Defence Centre of Excellence, 2020).

Разом з тим правове забезпечення розвідувальної аналітики в Україні враховує міжнародні стандарти, такі як рекомендації Ради Європи, ОБСЄ, НАТО щодо прав людини та координації міжвідомчих структур, що сприяє інтеграції українських аналітичних систем у міжнародний простір безпеки. В умовах глобалізації та посилення транснаціональних загроз роль міжнародно-правових стандартів у регулюванні розвідувальної аналітики стає критично важливою. Вони визначають принципи діяльності аналітичних структур, встановлюючи межі співпраці та захисту прав людини в міжнародному контексті. Україна, як держава, що інтегрується в європейські та світові системи безпеки, орієнтується на численні міжнародні документи, що регламентують діяльність розвідувальних підрозділів.

В даному аспекті *Європейська конвенція з прав людини (ЄКПЛ)* [22] є основою для забезпечення прав і свобод громадян у розвідувальній діяльності. Статті 8 – 11 ЄКПЛ гарантують право на приватність та свободу вираження думок, що вимагає від аналітичних структур дотримання принципу пропорційності при зборі та обробці інформації. Впровадження цих положень в національне законодавство України здійснюється через Конституцію та спеціальні закони.

Водночас Україна, як країна, що прагне до інтеграції в європейські та міжнародні механізми безпеки, керується положеннями резолюцій та рекомендацій, ухвалених Радою Європи, яка, своєю чергою, розробляє нормативні підходи у сферах захисту персональних даних, протидії тероризму та кібербезпеки. Зокрема, Рекомендація CM/Rec (2010) 13 визначає стандарти для роботи розвідувальних служб з дотриманням прав людини та основних свобод, а також встановлює норми обміну інформацією для запобігання злочинам та тероризму [23].

У сфері розвідувальної аналітики міжнародні стандарти, ухвалені авторитетними організаціями, відіграють ключову роль у формуванні національної нормативної бази та забезпеченні балансу між безпекою і правами людини. Зокрема, *Організація Об'єднаних Націй* у своїх Резолюціях 68 сесії (68/178 «Захист прав людини і основоположних свобод в умовах боротьби з тероризмом» та 68/167 «Право на недоторканність особистого життя в цифрове століття») підкреслює необхідність забезпечення прозорості, підзвітності та законності у розвідувальній діяльності, особливо в умовах цифровізації [24].

Організація з безпеки і співробітництва в Європі (ОБСЄ) у своїх звітах та документах акцентує на дотриманні міжнародних стандартів при використанні новітніх технологій для протидії кіберзагрозам і транскордонній злочинності [25]. У свою чергу, *Північноатлантичний альянс (НАТО)* у межах діяльності Центру передового досвіду з кібероборони (Cooperative Cyber Defence Centre of Excellence) окреслює принципи інтеграції національних систем у спільну мережу обміну розвідувальною інформацією, наголошуючи на важливості юридично обґрунтованого підходу до інформаційної безпеки та співпраці між державами [26].

Міжнародно-правові стандарти створюють фундамент для функціонування розвідувальної аналітики, гармонізуючи національні інтереси з міжнародними зобов'язаннями. Їхнє впровадження сприяє розвитку прозорої, ефективної та гуманної системи розвідувальної аналітики, що відповідає вимогам сучасних загроз і викликів.

Тож особливо в останні роки важливим для держави є роль *координації міжнародних стандартів*

із національним законодавством. Інтеграція міжнародних стандартів у національне законодавство України сприяє розвитку механізмів контролю та підзвітності у сфері розвідувальної аналітики. Це дозволяє зменшити ризики зловживань, покращити якість аналітичної роботи та зміцнити довіру громадськості. Важливими є також навчання кадрів та застосування міжнародних практик для зміцнення інституцій, що контролюють діяльність аналітичних підрозділів.

Отже, цілком логічним є висновок, що нормативно-правове забезпечення діяльності розвідувальної аналітики є складним комплексом законів, підзаконних актів та міжнародних договорів. Визначення повноважень, меж діяльності та відповідальності аналітичних підрозділів гарантує їх ефективність і законність. Особлива увага приділяється забезпеченню прав і свобод громадян, а також координації між суб'єктами безпеки, зокрема в кіберсфері та економічній безпеці.

Особливе значення мають технологічне забезпечення та виклики в розвідувальній аналітиці. Сучасна розвідувальна аналітика активно інтегрує цифрові технології, такі як великі дані (Big Data), штучний інтелект (ШІ), машинне навчання та засоби кіберзахисту. Ці інструменти значно підвищують обсяг, швидкість і глибину обробки інформації, що є критично важливим для національної безпеки в умовах глобальних загроз. Проте зростають і нові технологічні ризики, пов'язані з кіберзагрозами, етичними та правовими проблемами.

Цифрові технології автоматизують традиційні аналітичні процеси, зокрема пошук інформації, кластеризацію, візуалізацію та прогнозування тенденцій. Алгоритми обробки природної мови (NLP), геоінформаційні системи (GIS), а також аналітичні платформи типу Palantir та Analyst's Notebook дозволяють здійснювати багатовимірний аналіз подій у режимі реального часу. Окрему роль відіграє аналіз даних з відкритих джерел (OSINT), що дозволяє здійснювати моніторинг соціальних медіа та інших індикаторів загроз [27].

Разом з тим, обробка великих даних відкриває нові можливості для виявлення прихованих взаємозв'язків і прогнозування криз. Джерела таких даних включають супутникові знімки, перехоплення трафіку, фінансові транзакції та поведінку в кіберпросторі. Системи, такі як Hadoop, Apache Spark та Cassandra, дозволяють обробляти пета-байти даних, класифікуючи та оцінюючи їх на предмет достовірності [28]. Для України інтеграція Big Data є важливим напрямом, закріпленим у Доктрині інформаційної безпеки України.

Штучний інтелект як рушій аналітичної еволюції автоматизує аналітичні процеси, дозволяючи генерувати висновки на основі великих обсягів даних. Алгоритми deep learning, графові нейронні мережі та методи предиктивної аналітики здатні виявляти незвичні зв'язки і прогнозувати кризові ситуації. У країнах НАТО ШІ вже інтегрований у механізми інформаційного синтезу та прийняття рішень у сфері безпеки, з акцентом на етичне регулювання автономних систем [29].

Водночас проблемним є процес впровадження новітніх технологій, що стикається: з дефіцитом кваліфікованих кадрів для роботи з комплексними системами; фрагментацією інфраструктури та відсутністю єдиних стандартів обміну інформацією; правовою невизначеністю щодо використання ШІ у прийнятті управлінських рішень; а також натикається на загрозу «технологічного шуму» – надлишок даних може перевищити аналітичні можливості систем [29].

Водночас для підвищення ефективності аналітичної діяльності національної безпеки доцільно: створити єдину міжвідомчу аналітичну платформу з відкритою архітектурою, розробити нормативні акти для

регулювання використання ШІ та аналітики Big Data, інвестувати в освіту аналітиків нового покоління, зокрема, у галузі data science та інформаційної безпеки, та забезпечити аудит технологічних рішень, зокрема, в контексті етики та публічної підзвітності [30].

Тому важливим є розуміння, що інформаційні технології, великі дані, штучний інтелект і кібербезпека – це основа розвідувальної аналітики в цифрову епоху. Вони змінюють парадигму аналізу загроз, роблячи його глибшим і адаптивним. Однак для забезпечення ефективного використання цих технологій необхідно вирішити проблеми нормативного регулювання, інтеграції між відомствами та етичного використання даних.

Сучасна розвідувальна аналітика функціонує як системоутворюючий елемент архітектури безпеки, що активно взаємодіє з оперативно-розшуковою, правоохоронною, превентивною діяльністю та зовнішньою розвідкою. Важливість такої взаємодії зростає у контексті економічної безпеки, де основним завданням є не лише виявлення правопорушень, але й попередження деструктивних процесів у фінансовій, енергетичній та інституційній сферах.

Оперативно-розшукова діяльність, згідно з українським законодавством, забезпечує отримання інформації про правопорушення, що дозволяє формувати доказову базу для кримінальних справ. Розвідувальна аналітика інтегрує ці результати з відкритими джерелами, контррозвідувальною інформацією, фінансовим моніторингом та іншими даними, що допомагає оперативним підрозділам у виборі цілей і напрямів дій. Зокрема, виявлення загроз економічного характеру, таких як транснаціональні фінансові правопорушення чи банківські схеми, є важливою частиною цієї взаємодії.

Розвідувальна аналітика також використовується для прогнозування та упередження загроз. У сфері економічної безпеки це включає виявлення ознак легалізації капіталу, концентрації контролю над критичними інфраструктурами або змін у поведінці ринків. Для цього застосовуються аналітичні моделі, що виявляють тренди та формують індикатори ризику. В ЄС подібні системи працюють в аналітичних центрах міністерств фінансів для попередження економічних криз чи спекуляцій на фінансових ринках.

Висновки. Економічна безпека України передбачає захист від загроз, зокрема у фінансовій, технологічній та інституційній сферах. Розвідувальна аналітика відіграє роль «сенсора загроз», виявляючи ризики у сферах державних закупівель, банківського сектору та інвестицій. У відповідь на ці загрози оперативно-розшукові та правоохоронні органи реалізують превентивні заходи, а зовнішня розвідка доповнює картину зовнішнім економічним впливом. Така модель взаємодії вимагає створення єдиної платформи даних та уніфікованих стандартів обміну інформацією.

Отже, інтеграція розвідувальної аналітики з оперативно-розшуковою, превентивною, правоохоронною та зовнішньою розвідкою є ключем до ефективного забезпечення економічної безпеки. Важливими складовими є не тільки обмін даними, а й глибока інформаційно-аналітична інтеграція, що дозволяє своєчасно виявляти загрози та стратегічно керувати ризиками. Це вимагає модернізації нормативної бази, вдосконалення інституційної архітектури та підготовки нової генерації аналітиків, здатних працювати на перетині юриспруденції, економіки та безпеки.

У статті розглядається розвідувальна аналітика як ключовий елемент національної безпеки в умовах цифрової трансформації та глобальних загроз. Проаналізовано функціональну роль аналітики на стратегічному, оперативному та тактичному рівнях, з урахуванням багаторівневого ухвалення рішень,

правового регулювання та інституційної взаємодії. Особливу увагу приділено впровадженню сучасних технологій – Big Data, штучного інтелекту (ШІ), алгоритмів машинного навчання, SIEM-систем, STIX/TAXII-протоколів – у процес аналітичної діяльності. Акцентовано на проблемах кібербезпеки, фрагментації інфраструктури, дефіциті кадрів та правовій невизначеності щодо використання ШІ. Показано значення міжвідомчої координації, ф'южн-центрів і міжнародних стандартів (НАТО, ООН, ОБСЄ, Рада Європи) у забезпеченні ефективності аналітики.

Досліджено нормативну базу України, зокрема закони «Про розвідку», «Про національну безпеку України», «Про основні засади кібербезпеки». Зазначено на критично важливій ролі міжнародно-правових стандартів у регулюванні розвідувальної аналітики, які визначають принципи діяльності аналітичних структур, встановлюючи межі співпраці та захисту прав людини в міжнародному контексті. Акцентовано, що Україна, як держава, яка інтегрується в європейські та світові системи безпеки, орієнтується на численні міжнародні документи, що регламентують діяльність розвідувальних підрозділів.

Обґрунтовано потребу у створенні єдиної міжвідомчої аналітичної платформи з відкритою архітектурою, розвитку кадрового потенціалу та впровадженні механізмів етичного і юридичного контролю за застосуванням технологій. У підсумку, стаття визначає аналітику як інструмент раннього попередження, стратегічного управління ризиками та сенсор загроз у сфері економічної безпеки.

Ключові слова: розвідувальна аналітика, національна безпека, big data, штучний інтелект, міжвідомча взаємодія, правове регулювання, ф'южн-центри.

Kardashevskyy Yu. Interdisciplinary principles of intelligence analytics in the security sector of Ukraine

The article explores intelligence analytics as a key component of national security amid digital transformation and global threats. It analyzes the functional role of analytics at strategic, operational, and tactical levels, considering multi-level decision-making, legal regulation, and institutional cooperation. Special attention is given to the integration of advanced technologies – Big Data, artificial intelligence (AI), machine learning algorithms, SIEM systems, and STIX/TAXII protocols – into the intelligence process. The article highlights critical issues such as cybersecurity challenges, infrastructure fragmentation, personnel shortages, and legal uncertainty in AI application. The role of interagency coordination, fusion centers, and international standards (NATO, UN, OSCE, Council of Europe) is examined in the context of enhancing analytical efficiency.

Ukraine's legal framework is analyzed, including the laws "On Intelligence," "On National Security of Ukraine," and "On Cybersecurity". The author emphasizes the critical role of international legal standards in regulating intelligence analytics, which define the principles of activity of analytical structures, establishing the boundaries of cooperation and protection of human rights in the international context. It is emphasized that Ukraine, as a state integrating into European and global security systems, is guided by numerous international documents regulating the activities of intelligence units.

The article substantiates the need to develop a unified interagency analytics platform with open architecture, invest in analytical human capital, and

implement ethical and legal oversight mechanisms for emerging technologies. In conclusion, the article identifies intelligence analytics as a key instrument for early warning, strategic risk management, and a threat sensor within economic security systems.

Key words: intelligence analytics, national security, big data, artificial intelligence, interagency cooperation, legal regulation, fusion centers.

Література:

1. Smith M. A Good Intelligence Analyst. International Journal of Intelligence and CounterIntelligence. 2017. Vol. 30. Pp. 181–185. URL: https://doi.org/10.1080/08850607.2016.1230708

2. Analyzing Intelligence: Origins, Obstacles, and Innovations. Georgetown University Press. 2008.

3. Ratcliffe J. H. Intelligence-Led Policing. Routledge. 2016.

4. Chen H.,ChianR. H. L.,Storey V. C. Business Intelligence and Analytics: From Big Data to Big Impact. MIS Quarterly. 2012. Vol. 36. No. 4. Pp. 1165–1188.

5. Klein G. Sources of Power: How People Make Decisions. MIT Press. 2017. DOI: 10.1061/(ASCE)1532-6748(2001)1:1(21)

6. Omand D. Securing the State: Reforming Intelligence. The RUSI Journal. 2019. № 164 (1). Pp. 12–26.

7. Gellman B. Dark Mirror: Edward Snowden and the Surveillance State. Bodley Head. 2020.

8. Lowenthal M. M. Intelligence: From Secrets to Policy (7th ed.). CQ Press. 2017.

9. Користін О. Є. Аналітична розвідка як елемент управління в системі кібербезпеки. Наука і правоохоронна. 2024. № 1. С. 10–18.

10. Fusion Centers' Support of National Strategies and Guidance. URL: https://www.dhs.gov/topic/fusion-centers-support-national-strategies-and-guidance

11. Gardner, Jeffrey Intelligence Fusion Centers for Homeland Security. Glasstree Academic Publishing. 2020. DOI: 10.20850/9781534299238

12. Goss, Adam STIX/TAXII: A Full Guide to Standardized Threat Intelligence Sharing. 2025. URL: https://surl.li/xuxcvq

13. North Atlantic Treaty Organization. Cyber Threats and NATO 2030 : Horizon Scanning and Analysis. 2022. URL: https://surl.li/vfcehr

14. Ertan A., Floyd K., Pernik P. & Stevens T. (Eds.) Cyber Threats and NATO 2030 : Horizon Scanning and Analysis. NATO CCDCOE Publications. 2020. URL: https://surl.li/xrcrec

15. Про розвідку : Закон України від 17 вересня 2020 року № 912-IX. URL: https://zakon.rada.gov.ua/laws/show/912-20#Text

16. Про національну безпеку України: Закон України від 21 червня 2018 року № 2469-VIII. URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text

17. Про оперативно-розшукову діяльність: Закон України від 18 лютого 1992 року № 2135-XII. URL: https://zakon.rada.gov.ua/laws/show/2135-12#Text

18. Про контррозвідувальну діяльність: Закон України від 26 грудня 2002 року № 374-IV. URL: https://zakon.rada.gov.ua/laws/show/374-15#Text

19. Про захист персональних даних: Закон України від 1 червня 2010 року № 2297-VI. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text

20. Кримінальний Кодекс України від 5 квітня 2001 року № 2341-III. URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text

21. Про основні засади забезпечення кібербезпеки України: Закон України від 5 жовтня 2017 року № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text

22. Конвенція про захист прав людини і основоположних свобод (з протоколами) (Європейська конвенція з прав людини), ратифікована Законом України від 17 липня 1997 року № 475/97-ВР. URL: https://zakon.rada.gov.ua/laws/show/995_004#Text

23. Рекомендація CM/Rec. 13 про захист осіб у зв'язку із застосуванням автоматизованої обробки персональних даних та у контексті використання таких даних (профайлінг). 2010. URL: https://surl.li/kvgmni

24. General Assembly of the United Nations. Resolutions 68th session. 2013. URL: https://www.un.org/en/ga/68/resolutions.shtml

25. OSCE: Organization for Security and Co-operation in Europe. URL: https://www.osce.org/

26. Stevens T., Ertan A., Floyd K., Pernik P. (Eds.) Cyber Threats and NATO 2030 : Horizon Scanning and Analysis. NATO Cooperative Cyber Defence Centre of Excellence. 2021. URL: https://surl.lu/lwgnbr

27. Користін О. Є., Свиридюк Н. П. Зарубіжний досвід антитерористичного використання OSINT. Науковий вісник Ужгородського національного університету. Серія: Право. 2024. Вип. 82. Т. 2. С. 177–181.

28. Mayer-Schцnberger V., Cukier K. Big Data: A Revolution That Will Transform How We Live, Work, and Think. Eamon Dolan/Houghton Mifflin Harcourt. 2013. URL: https://surl.li/ouqxbt

29. Khasawneh A. J., Mihus I., Svyrydiuk N., Zhyvko Z. Nature and purpose of artificial intelligence. Political, legal, and economic challenges in the 21st century. Naturaleza y finalidad de la inteligencia artificial. Retos polнticos, jurнdicos y econymicos en el siglo XXI. Clio. Revista de Historia, Ciencias Humanas y Pensamiento Critico. 2024. № 4 (8). Pp. 306–320. SCOPUS. DOI: https://www.scopus.com/authid/detail.uri?authorId=57208030041

30. An Artificial Intelligence Strategy for NATO. URL: https://surl.li/eadkar

Дата надходження статті: 11.07.2025
Дата прийняття статті: 18.07.2025
Опубліковано: 22.09.2025