УДК 343.8:004.77
DOI https://doi.org/10.24144/2307-3322.2025.91.4.59

OSINT У ЗАБЕЗПЕЧЕННІ НАЦІОНАЛЬНОЇ БЕЗПЕКИ

Рибка Д.,
старший викладач
Національної академії Служби безпеки України,
доктор філософії
ORCID: 0000-0002-8824-0089

Рибка Д. OSINT у забезпеченні національної безпеки

В статті доведено, що OSINT є передовою методикою збирання та аналізу інформації з відкритих джерел, що активно використовується органами безпекового спрямування. Це концепція, методологія і технологія добування і використання військової, політичної, економічної та іншої інформації з відкритих джерел без порушення законів – для підтримки прийняття рішень у сфері національної оборони і безпеки. Акцентовано, що на OSINT припадає 80-95% усіх даних, які використовуються розвідувальною спільнотою в усьому світі. Його застосування дозволяє більш комплексно підійти до вирішення завдань із забезпечення національної безпеки, більш оптимально використовувати людські та фінансові ресурси, пришвидшити процес прийняття організаційних рішень, підвисити ефективність боротьби зі злочинністю тощо. Проаналізовано методологію OSINT, що включає в себе: пошук інформації, реєстрацію та облік інформації, аналіз інформації і синтез повідомлень з різних відкритих джерел, адміністрування та розповсюдження інформації та має низку переваг: доступність джерел інформації; обсяг джерел інформації; різносторонність; оперативність отримання; легкість подальшого використання; вартість отримання інформації. Також окреслено позитивні сторони OSINT: глобальність оформлення інформації та її використання в режимі реального часу; сприяння розумінню контексту подій, які підлягають аналізу; його використання не вимагає додаткових фінансових витрат на придбання спеціальної техніки; не потрібна тривала підготовка певних спеціалістів; його джерела є у вільному доступі, а тому може бути використана не лише суб'єктами правоохоронної діяльності (представниками державної влади), а й приватними детективами, волонтерами та ін.; його використання (за певних умов) не порушує прав громадян. Доведено, що ефективність OSINT обумовлюється її раціональним плануванням, чітким дотриманням певних принципів, залучення до його проведення кваліфікованих працівників, оперативним формулюванням отриманих висновків та їх вчасною передачею зацікавленим особам, а також розробленням на їх основі оптимальних заходів із забезпечення національної безпеки.

Ключові слова: інформація, збирання інформації, аналіз інформації, відкриті джерела інформації, протидія злочинності.

Rybka D. OSINT in ensuring national security.

The article proves that OSINT is an advanced method of collecting and analyzing information from open sources, which is actively used by security agencies. This is a concept, methodology and technology of obtaining and using military, political, economic and other information from open sources without violating laws - to support decision-making in the field of national defense and security. It is emphasized that OSINT accounts for 80-95% of all data used by the intelligence community worldwide. Its use allows for a more comprehensive approach to solving national security tasks, more optimal use of human and financial resources, speed up the process of making organizational decisions, increase the effectiveness of the fight against crime, etc. The OSINT methodology is analyzed, which includes: information search, registration and accounting of information, information analysis and synthesis of messages from various open sources, information administration and dissemination and has a number of advantages: availability of information sources; volume of information sources; versatility; speed of receipt; ease of further use; cost of obtaining information. The positive aspects of OSINT are also outlined: the global nature of information

processing and its use in real time; facilitating understanding of the context of events to be analyzed; its use does not require additional financial costs for the purchase of special equipment; does not require long-term training of certain specialists; its sources are freely available, and therefore can be used not only by law enforcement agencies (representatives of state authorities), but also by private detectives, volunteers, etc.; its use (under certain conditions) does not violate the rights of citizens. It has been proven that the effectiveness of OSINT is determined by its rational planning, strict adherence to certain principles, the involvement of qualified employees in its implementation, the prompt formulation of the conclusions obtained and their timely transfer to interested parties, as well as the development of optimal measures to ensure national security on their basis.

Key words: information, information collection, information analysis, open sources of information, combating crime.

Актуальність дослідження. Як відомо, ніщо не має значення окрім фактів. Саме на фактах ґрунтується різноманітна діяльність, зокрема, й у сфері забезпечення національної безпеки. У сучасному світі існує безліч джерел інформації, як відкритих, так і з обмеженим доступом. Найбільшим джерелом, з якого можна отримати інформацію, є мережа Internet, як її поверхнева частина, так і dark net. Але інформацію важливо як знайти, так і якісно проаналізувати. При цьому, як зазначено у стандарті НАТО АРР-6: «Аналіз – це вивчення цілого, детальне дослідження його частин та їхньої взаємодії».

Збирання та аналіз інформації з відкритих джерел в умовах сьогодення має назву OSINT (Open Source Intelligence) та набуває все більшої актуальності. За оцінками фахівців на OSINT припадає 80-95% усіх даних, які використовуються розвідувальною спільнотою в усьому світі. Очікується, що до 2026 року ринок OSINT досягне майже 12 мільярдів доларів.

Застосування досліджуваного інструменту дозволяє більш комплексно підійти до вирішення завдань із забезпечення національної безпеки, більш оптимально використовувати людські та фінансові ресурси, пришвидшити процес прийняття організаційних рішень тощо. OSINT дозволяє забезпечити інформаційну підтримку осіб, які приймають стратегічні рішення; отримання актуальної інформації про поточні події; надходження важливої інформації, яку неможливо отримати іншими способами; може бути використаний у специфічних випадках, наприклад, фішинг, криптовалюта, події, що відбуваються у dark net тощо.

Аналіз останніх досліджень і публікацій. Зважаючи на подальшу актуалізацію використання OSINT широке коло науковців займається дослідженням його особливостей та розробляє шляхи використання, зокрема, в інтересах забезпечення національної безпеки. У своїх працях зазначеним питанням приділяли увагу К.В. Власов, А.В. Білоборов, Б. Денисенко, Д.С. Зоренко, О.Ю. Іохов, О.Є. Користін, П.С. Клімушин, Л.О. Кульчицька, Р.В. Лех, С.О. Мартинюк, О.В. Миньо, В.Т. Оленченко, Н.П. Свиридюк, О.І. Червяков, Т.С. Яровой тощо. Водночас, проблематика використання OSINT і досі не висвітлена у повному обсязі.

Метою статті є висвітлення особливостей використання OSINT в забезпеченні національної безпеки.

Виклад основного матеріалу. OSINT – це те, що як пересічні громадяни, так і ті, хто залучені до забезпечення безпеки суспільства у різних сферах, роблять фактично щодня з різних причин (наприклад, дивляться, бачать або чують новини, переглядають соціальні мережі або досліджують когось перед тим, як найняти на роботу, вивчають інформацію, що утворюється в ході професійної діяльності). Загалом, OSINT як відокремлена практика зародилася в США у 40-х рр. минулого століття із заснуванням Служби моніторингу закордонних трансляцій. Якщо ж говорити про Україну, то з відновленням державності у 1991 році отримання даних з відкритих джерел також було повсякденною практикою оперативно-службової діяльності, однак без такого структурного виділення як в США. До появи інтернету це було також дослідження друкованих ЗМІ, документів, звітів, матеріалів конференцій, наукових робіт, різноманітних довідників, списків тощо. Після виникнення глобальної мережі зміст OSINT змінився [1, с. 4].

OSINT – це концепція, методологія і технологія добування і використання військової, політичної, економічної та іншої інформації з відкритих джерел без порушення законів – для підтримки прийняття рішень у сфері національної оборони і безпеки. Він будується на певних принципах, якими є закріплені основоположні ідеї, засади, найбільш загальні положення, що визначають сутність, зміст і спрямованість діяльності суб'єктів, які здійснюють OSINT, спосіб і форму їх ді-

яльності. Кожен з принципів відрізняється своєю специфікою. Зокрема, до загальних принципів OSINT віднесено:

– законність – людина, її права та свободи визнаються найвищими цінностями та визначають зміст і спрямованість діяльності держави;

– дотримання прав і свобод людини – обмеження прав і свобод людини допускається виключно на підставах та в порядку, визначених Конституцією і законами України, за нагальної необхідності і в обсязі, необхідному для виконання завдань відповідних державних органів;

– науковість – методи, що використовуються в ході OSINT мають враховувати сучасні досягнення науки (у тому числі у сфері комп'ютерних технологій) та бути такими, що дозволять відтворити цей процес під час іншого схожого аналізу;

– своєчасність – OSINT має бути проведений у найкоротший строк з моменту визначення його необхідності, з тим, щоб його результати не втратили актуальність та могли бути ефективно використані при забезпеченні національної безпеки;

– цілеспрямованість – OSINT має бути спрямований на отримання відповіді на запитання, що його ініціювали, формування висновків, які мають якомога вищу ймовірність ступеня достовірності їх істинності, та розроблення рекомендацій, найбільш доцільних для впровадження, виходячи зі змісту інформації, яка підлягала аналізу;

– безперервність – в ході OSINT має бути охоплена інформація за весь період, у якому відбувались події, що прямо або опосередковано відносяться до відповіді на запитання, що обумовило необхідність збирання та аналізу інформації з відкритих джерел;

– ефективність – висновки, сформульовані за результатами проведення кримінального аналізу, та засоби візуалізації, які їх супроводжують мають бути безпосередньо застосовані для прийняття ефективних управлінських рішень під час досудового розслідування або оперативно-розшукової діяльності.

Спеціальними принципами OSINT є принципи достовірності; об'єктивності; конкретності та ясності; реальності; контролю; обов'язкового встановлення причини та наслідку; обов'язкової чіткості, логічності і якості формулювання висновків.

Методологія OSINT включає в себе: пошук інформації, реєстрацію та облік інформації, аналіз інформації і синтез повідомлень з різних відкритих джерел, адміністрування та розповсюдження інформації.

Термін «інформація» унормований в законі України «Про інформацію», у якому наводиться його визначення та надається класифікація доступу до інформації. Так, «інформація» – це будь які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді. За порядком доступу інформація поділяється на відкриту інформацію та інформацію з обмеженим доступом, причому, будь-яка інформація вважається відкритою, крім тієї, що віднесена законом до інформації з обмеженим доступом [2]. Цим же законом дається визначення терміну «масова інформація», під якою розуміється інформація, що поширюється з метою її доведення до необмеженого кола осіб. Інформація будь-якого виду має свою самостійну цінність, специфічні закономірності функціонування та розвитку, вона здатна до випереджального впливу на державну політику, часто визначає вибір варіанта політичного розвитку, поведінки різноманітних соціальних груп та окремих громадян.

Крім того, інформація служить найважливішим видом забезпечення законодавчої діяльності, адже саме вона лежить в основі ухвалення рішення щодо регулювання тих або інших суспільних відносин. Інформація в органах державної влади класифікується за різними ознаками. Так, інформація в системі публічної політики та управління поділяється на офіційну та неофіційну, загальнодержавну та регіональну, горизонтальну або вертикальну, змістовну й цільову, загальнодоступну та з обмеженим доступом тощо. У цілому ж інформація державних органів та органів місцевого самоврядування – це передусім офіційна документована інформація, яка створюються в процесі діяльності державних органів та органів місцевого самоврядування.

З поняттям «інформація» тісно пов'язані такі поняття, як «інформаційний процес» та «інформаційний шум». Інформаційний процес – це сукупність носіїв інформації, самої інформації та аудиторії, яка отримує цю інформацію. У свою чергу, інформаційний шум – це повідомлення, які непотрібні користувачу інформації, незалежно від того, відомі вони йому чи ні. Інформаційні шуми часто створюють інформаційні бар'єри – різноманітні перешкоди, які заважають поширенню інформації та її ефективному використанню.

У сфері міжнародної інформації використовуються терміни «джерела інформації» та його різновид «відкриті джерела інформації». Так, під терміном джерела інформації розуміються встановлені законом бази і банки даних із широким типом представництва, які використовуються у дипломатичній практиці, діяльності міжнародних організацій, у регулюванні міжнародних конфліктів, у передачі особистої інформації.

У межах OSINT терміни «відкрите джерело» та «загальнодоступна інформація» використовуються у значеннях:

– відкрите джерело – особа або група осіб, які надають інформацію без вимоги збереження її конфіденційності – інформація або відносини, незахищені від публічного розкриття. Відкриті джерела належать до сфери загальнодоступної інформації і не мають обмеження в доступі для фізичних осіб;

– загальнодоступна інформація – дані, факти, інструкції або інші матеріали, опубліковані чи розміщені для широкого використання, які доступні для громадськості, законно побачені або почуті випадковими спостерігачами, представлені на відкритих зустрічах для громадськості.

Специфічність такої інформації пов'язана з тим, що вона є результатом аналітичної обробки великого обсягу відкритого, загальнодоступного інформаційного потоку, яким є:

– ЗМІ: друковані газети, журнали, радіо та телебачення;

– всесвітня мережа «Інтернет»: онлайн-публікації, блоги, дискусійні групи (форуми), медіа громадян (наприклад, відео з мобільних телефонів, контент, створений користувачами), YouTube, RuTube та інші відеохостинги, вікі-довідники та інші вебсайти соціальних медіа (фейсбук, твітер, інстаграм, телеграм та ін.), dark net. Ці джерела також випереджають безліч інших джерел через своєчасність і легкість доступу;

– офіційні державні джерела: публічні урядові звіти, бюджети, слухання, телефонні довідники, пресконференції, вебсайти та виступи. Хоча ці джерела походять з офіційних джерел, вони є публічно доступними і можуть використовуватися відкрито і вільно;

– професійні та академічні публікації: інформація, отримана з журналів, конференцій, симпозіумів, наукових праць, дипломів та дисертацій;

– комерційні дані: комерційні зображення, фінансові та промислові оцінки, бази даних;

– інша література: технічні звіти, патенти, робочі документи, ділові документи, неопубліковані роботи та інформаційні бюлетені.

Отже, особливістю OSINT в професійній діяльності, та фактором, що його ускладнює, є те, що кількість та самі джерела для постійно змінюються, тому для його проведення необхідно чітке планування процесу, використання різноманітних підходів, методів та засобів, а також особливих підходів для аналізу отриманої інформації.

OSINT має низку переваг, до яких відносять:

– доступність джерел інформації – для використання джерел інформації OSINT не потрібно проводити спеціальних заходів або створювати складні технічні розвідувальні системи, потрібно тільки знати, де і що шукати;

– обсяг джерел інформації – OSINT обробляє величезний обсяг інформаційних ресурсів, який продовжує інтенсивно зростати;

– різносторонність – враховуючи постійне збільшення доступних інформаційних ресурсів в світі, за допомогою OSINT можна задовольнити більшість інформаційних потреб споживачів розвідувальної інформації;

– оперативність отримання – високий ступінь відновлення інформаційних ресурсів, відстеження змін обстановки, об'єктів розвідки в реальному масштабі часу;

– легкість подальшого використання – будь-які таємниці прийнято оточувати бар'єрами грифів секретності, принципів ізоляції інформації і особливих режимів доступу. Все це надзвичайно ускладнює взаємодію та передачу інформації у зацікавлені структури. Що ж стосується OSINT, то її без проблем можна передавати будь-яким зацікавленим інстанціям;

– вартість отримання – робота фахівців з OSINT потребує лише доступу до мережі Internet та окремого програмного забезпечення, для оптимізації їх роботи з пошуку інформації та аналізу великих її обсягів.

Узагальнено, проведення OSINT полягає у пошуку значущої інформації, її систематизації, аналізі та розробленні відповідних висновків, що можуть бути використані при забезпеченні безпеки суспільства від кримінальних протиправних посягань. Для ефективної його організації варто враховувати, що цикл OSINT містить низку етапів, а саме:

– створення онлайн-запитів для пошуку або моніторингу інформації;

– попереднє оцінювання – щоб уникнути надмірного збору даних і дотримуватися принципів мінімізації обсягу даних і сфокусованості дослідження;

– збір інформації – вилучення цифрових даних з Інтернету (вручну або з використанням відповідного програмного забезпечення), до яких відноситься документація, URL-адреса, вихідний код HTML, захоплення повної сторінки тощо;

– збереження – забезпечення того, щоб зібрана інформація зберігалася та була відновною, зокрема, хешування;

– верифікація – процеси оцінювання достовірності інформації, яке полягає в оцінюванні надійності джерела інформації та змісту інформації, контенту (наприклад, верифікація акаунту в соціальних мережах;

– аналіз отриманої інформації, формулювання висновків та рекомендацій – інтерпретація даних, формулювання висновків та рекомендацій для подальшої діяльності із забезпечення національної безпеки.

Отже, збирання інформації з відкритих джерел розпочинається з визначення архітектури завдання (вимог), визначення запитань, на які необхідно відповісти, формулювання завдання для виконання окреслених вимог. У подальшому від вивчення вхідних даних, які окреслюватимуть шуканий об'єкт або декілька об'єктів. На цьому етапі аналізуються можливі напрямки пошуку та логічні зв'язки між вхідними даними, які здатні підвищити ефективність застосовуваних рішень. Аналіз вхідних даних передбачає послідовне вивчення їх ознак (атрибутів), додаткових відомостей (метаданих) та змісту. В процесі пошуку інформації важливо користуватися різними інформаційно-пошуковими системами та спеціально-призначеними системами пошуку інформації про об'єкти за різними ідентифікаторами.

Під час збирання та узагальнення інформації необхідно спрямовувати зусилля на своєчасне виявлення прихованих суспільно-небезпечних процесів та явищ, що посягають на національну безпеку і публічний порядок та порушують інтереси держави та суспільства, зокрема, особливу увагу приділяти інформації щодо:

– діяльності та рішень органів державної влади, які викликають негативний суспільний резонанс та її критика;

– політичного життя;

– діяльності та процесів, пов'язаних з громадськими, у тому числі радикальними організаціями;

– ситуації в релігійному середовищі, національні, сексуальні меншини;

– інформації щодо діяльності профспілкових та правозахисних організацій та заходів за їх участі;

– щодо діяльності можливих агентів рф тощо.

Серед можливостей OSINT особливий інтерес становить технологія автоматичної ідентифікації особи людини за елементами зовнішності, за її відображенням на фотографії або відеозаписі. Дана технологія цікава тому, що може здійснюватися без контакту з об'єктом пошуку. У всесвітній мережі є онлайн-сервіси пошуку осіб за елементами зовнішності серед масиву фотозображень, що містяться у популярних соціальних мережах (наприклад, «Search4faces») на особистих сторінках осіб. За результатами пошуку сервіси надають користувачу масив, що складається з переліку максимально схожих осіб, із відсотковим зазначенням збігу зовнішності обличчя знайденої особи з досліджуваною. Тобто отримані результати не містять інформацію про індивідуально-конкретну тотожність осіб, оскільки до такого висновку можна дійти або шляхом суб'єктивної оцінки співпадаючих ознак зовнішності людини, або використовуючи спеціальні методи портретної експертизи. При цьому важливо розуміти, що візуальне сприйняття ознак зовнішності особами, які не є спеціалістами в галузі судово-портретної експертизи, ґрунтується лише на підставі суб'єктивної оцінки окремих ознак та внутрішнього переконання. І навпаки, спеціалісти оцінюють збіг зовнішності порівнюваних осіб, застосовуючи науково-обґрунтовані спеціальні методи портретної експертизи, що дає змогу об'єктивно проаналізувати результати пошуку.

Також доволі змістовним та цікавим виявляється пошук в глибинних шарах Internet – Dark net. Здійснюючи пошук в dark net варто враховувати, що він використовується як платформа для розповсюдження нелегальних послуг, наприклад, послуг замовних вбивць або послуг з виготовлення вибухових пристроїв тощо. Він являє собою частину Інтернету до якого можна отримати доступ тільки використовуючи специфічне програмне забезпечення або технології peer-to-peer.

При цьому контент dark net не індексується звичайними пошуковими системами. Тому інформація, отримана з його сторінок, становить особливу цінність та дозволяє підвисити ефективність забезпечення національної безпеки як від внутрішніх, так і від зовнішніх загроз.

Під час верифікації відомостей необхідно порівняти зібрані відомості між собою на предмет їх релевантності та логічності. При цьому варто враховувати джерела надходження відповідної інформації, а також час її потенційного створення. Окремі дані, актуальні в один період часу, у подальшому можуть не становити інтересу або взагалі дезорієнтувати загальний напрям роботи. Для порівняння відповідних даних краще скласти таблицю із фактичними даними, які підтверджують ту або іншу гіпотезу. Факти, які суперечать один одному, потребують додаткової перевірки та пояснень.

Після того, як зібрана інформація візуалізована та проаналізована, здійснюється формування висновків , яких виділяють чотири види:

– гіпотеза – пробний висновок, який потребує додаткової інформації для підтвердження або спростування;

– прогноз – висновок про щось, що трапиться у майбутньому;

– розрахунок – висновок, зроблений щодо цілого за частиною з використанням кількісних методів;

– умовивід – добре обґрунтоване пояснення[1].

Здійснюючи OSINT при забезпеченні національної безпеки варто враховувати, що доцільно не обмежуватись лише інформацією з веб-сторінок. А зважаючи на те, що відсутня жорстка часова прив'язка це дає змогу відстежувати об'єкти в динаміці. При цьому власне OSINT не фішинг, доксинг чи зламування (хакінг), навіть якщо для цих дій використовуються такі самі інструменти чи методології, що й в OSINT.

Висновки. Отже, сьогодні OSINT є передовою методикою збирання та аналізу інформації з відкритих джерел. Її перевагою у забезпеченні національної безпеки, порівняно з іншими методами роботи з відомостями є загальнодоступний характер інформації, збір якої не потребує спеціального дозволу і може бути отримана законним шляхом без оформлення відповідної документації. До позитивних сторін OSINT доцільно віднести наступні фактори:

– глобальність оформлення інформації та її використання в режимі реального часу;

– дозволяє зрозуміти контекст подій, які підлягають аналізу;

– її використання не вимагає додаткових фінансових витрат на придбання спеціальної техніки та програмного забезпечення, адже достатньо мати лише доступ до всесвітньої мережі «Інтернет» та робочу станцію ПК (смартфон, планшет);

– не потрібна підготовка певних спеціалістів, оскільки технологія OSINT достатньо проста як в опануванні, так і в обробці вихідної та отриманні криміналістично значущої інформації;

– вона є у вільному доступі, а тому може бути використана не лише суб'єктами правоохоронної діяльності (представниками державної влади), а й приватними детективами, волонтерами та ін.;

– її використання (за певних умов) не порушує прав громадян.

Водночас, ефективність OSINT обумовлюється її раціональним плануванням, чітким дотриманням певних принципів, залучення до його проведення кваліфікованих працівників, оперативним формулюванням отриманих висновків та їх вчасною передачею зацікавленим особам, а також розробленням на їх основі оптимальних заходів із забезпечення національної безпеки.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Зоренко Д.С., Кульчицька Л.О., Лех Р.В., Червяков О.І. Використання інструментів та методів OSINT для отримання пошукової інформації: практичний порадник. 5-те вид., переробл. та доповн. Харків. Видавець: О.А. Мірошниченко, 2024. 80 с.
2. Про інформацію: Закон України від 02 жовт. 1992 р. № 2657-XII. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text.
3. Користін О.Є., Свиридюк Н.П. Зарубіжний досвід антитерористичного використання OSINT. *Науковий вісник Ужгородського національного університету.* Серія: Право. 2024. Вип. 82. Ч. 2. С. 177–181.

[1] Розвідка з відкритих джерел (OSINT) : наук.-метод. рек. / [Розроб.: Манжай О.В., Потильчак А.О.]; МВС України, Харків. нац. ун-т внутр. справ. Харків : ХНУВС, 2021. 30 с.

4. Користін О., Денисенко Б. Методологічні засади OSINT. Реалізація філософії «Intelligence-led Policing» в системі кримінального аналізу Національної поліції України: монографія / Користін О., Швець Д., Бутко Б., Денисенко Б. та ін., за заг. ред. Користіна О.Є. Київ: «ВАЙТ», 2024. 504 с.
5. Білобров А.В., Клімушин П.С. Використання технологій OSINT для отримання інформації. *Протидія кіберзлочинності та торгівлі людьми*: Збірник матеріалів Міжнародної науково-практичної конференції (м. Харків, 27 травня 2020 року). С. 135–137.
6. Яровой Т.С. OSINT як перспективний інструмент контролю за лобістською діяльністю в контексті державної безпеки. *Експерт: парадигми юридичних наук і державного управління*. 2019. № 4(6). С. 201–208.
7. Мартинюк С.О. Характеристика принципів функціонування OSINT у сфері національної безпеки. *Юридичний науковий електронний журнал*. 2021. № 9. С. 332–334.
8. Минько О.В., Іохов О.Ю., Оленченко В.Т., Власов К.В. Використання технологій OSINT для отримання розвідувальної інформації. *Експерт: парадигми юридичних наук і державного управління*. 2019. № 4(6). С. 201–208.