ГРИНЧУК ОЛЕКСАНДР
магістр права, магістр військового управління, начальник управління з питань запобігання, виявлення та припинення правопорушень – заступник начальника Головного управління Військової служби правопорядку у Збройних Силах України

ЗАХАРЧУК РОМАН
магістр права, магістр психології, аспірант, Київський університет права Національної академії наук України

ПРАВОВІ ЗАСАДИ ЗАСТОСУВАННЯ OSINT У ДІЯЛЬНОСТІ ВІЙСЬКОВОЇ ПОЛІЦІЇ: МІЖНАРОДНИЙ ДОСВІД ТА УКРАЇНСЬКІ ПЕРСПЕКТИВИ

Сучасні умови ведення збройних конфліктів, цифровізація суспільства та поширення відкритих інформаційних джерел зумовлюють необхідність використання новітніх аналітичних інструментів у діяльності органів сектору безпеки і оборони. Одним із таких інструментів є розвідка з відкритих джерел (OSINT – Open Source Intelligence), яка забезпечує можливість збору, аналізу та використання інформації з публічно доступних ресурсів для прийняття управлінських і правозастосовних рішень.

У діяльності військової поліції, зокрема Військової служби правопорядку у Збройних Силах України (далі – Служба правопорядку), OSINT може застосовуватися для моніторингу дисциплінарних ризиків, виявлення правопорушень, підтримки службових розслідувань та забезпечення інформаційної безпеки військових формувань. Міжнародний досвід свідчить, що у країнах-членах НАТО OSINT є невід'ємним елементом інформаційно-аналітичного забезпечення військових операцій, інтегрованим у загальний розвідувальний цикл відповідно до Посібника НАТО з розвідки з відкритих джерел (NATO Open Source Intelligence Handbook) [11].

У Збройних Силах США правові та організаційні засади застосування OSINT визначаються, зокрема, Армійською публікацією з техніки і тактики ATP 2-22.9 «Розвідка з відкритих джерел» [12], яка закріплює її статус як повноцінної розвідувальної дисципліни, а також документом «Порядок здійснення та нагляд за діяльністю розвідки Армії США» (AR 381-10) [13], що встановлює обмеження щодо збору інформації та забезпечує дотримання прав людини.

Водночас застосування OSINT пов'язане з низкою правових викликів, насамперед у сфері захисту персональних даних та дотримання права на приватність. В Україні відповідні правовідносини регулюються Конституцією України, зокрема статтею 32, яка гарантує невтручання в особисте і сімейне життя [1], Законом України «Про захист персональних даних», який визначає правові підстави та порядок обробки персональних даних (зокрема статті 6, 7, 8) [2], а також Законом України «Про інформацію», що встановлює правовий режим інформації, включаючи відкриту інформацію та інформацію з обмеженим доступом (зокрема статті 20, 21) [3].

На міжнародному рівні ключове значення мають положення Конвенції про захист прав людини і основоположних свобод [7], а також стандарти, закріплені у Регламенті (ЄС) 2016/679 Європейського Парламенту і Ради (Загальний регламент про захист даних – GDPR) [8], Конвенції Ради Європи №108+ про захист осіб у зв'язку з автоматизованою обробкою персональних даних [9] та Директиві (ЄС) 2016/680 Європейського Парламенту і Ради щодо захисту персональних даних у сфері правоохоронної діяльності [10].

Правовий аналіз свідчить, що використання OSINT у діяльності військової поліції повинно здійснюватися з дотриманням принципів законності, необхідності та пропорційності відповідно до міжнародних стандартів захисту прав людини [7].

У контексті діяльності Служби правопорядку особливого значення набуває використання OSINT у межах проведення перевірок та службових розслідувань. Відповідно до Інструкції про організацію та проведення перевірок у Збройних Силах України, затвердженої наказом Генерального штабу Збройних Сил України від 13.12.2014 № 262 [6], перевірка розглядається як діяльність, спрямована на отримання та аналіз фактичних даних для встановлення обставин правопорушення.

Своєю чергою, відповідно до Порядку проведення службового розслідування у Збройних Силах України, затвердженого наказом Міністерства оборони України від 21.11.2017 № 608, службова перевірка це «комплекс заходів, які здійснюються з метою перевірки інформації про вчинення правопорушення, з'ясування наявності підстав для призначення службового розслідування, обставин порушення виконавської дисципліни, встановлення осіб, які вчинили правопорушення», а службове розслідування визначається як «комплекс заходів, які проводяться з метою уточнення причин і умов, що сприяли вчиненню правопорушення, а також встановлення ступеня вини особи (осіб), чиї дії або бездіяльність стали причиною вчинення правопорушення» [5].

Практичне значення застосування OSINT у межах службових розслідувань службових перевірок та перевірок, які проводить Служба правопорядку полягає у можливості оперативного отримання первинної інформації про подію, її обставини або причетних осіб без необхідності негайного виїзду на місце події. Аналіз відкритих джерел (зокрема соціальних мереж, засобів масової інформації, відкритих реєстрів та інших цифрових ресурсів) дає змогу сформувати попередню інформаційно-аналітичну модель ситуації або профіль особи.

Наявність такої попередньої картини дозволяє оптимізувати процес прийняття рішень, підвищити адресність заходів перевірки та службового розслідування, а також забезпечити більш ефективне використання ресурсів. У підсумку це сприяє підвищенню результативності діяльності Служби правопорядку.

З огляду на це, OSINT може виступати ефективним інструментом первинної перевірки інформації, збору додаткових фактичних даних у межах службових розслідувань та перевірок, документування обставин подій (у тому числі цифрових слідів) та встановлення причинно-наслідкових зв'язків між діями військовослужбовців та їх наслідками.

Окремої уваги потребує питання допустимості використання OSINT як доказової бази. Інформація з відкритих джерел може використовуватися як фактичні дані за умови дотримання критеріїв законності, достовірності, цілісності та можливості бути перевіреною. У цьому контексті доцільним є застосування міжнародних стандартів документування цифрових доказів, зокрема Берклійського протоколу щодо цифрових розслідувань із використанням відкритих джерел [14].

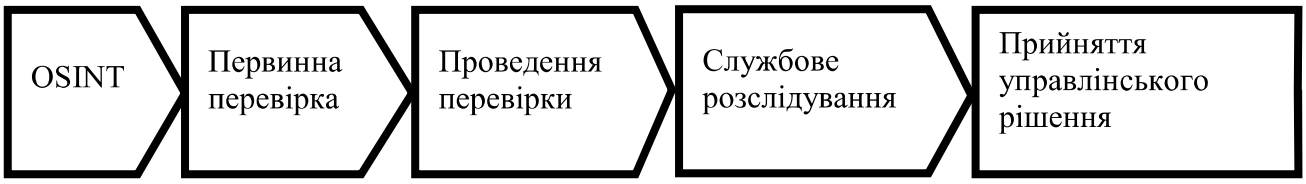

Схема 1. Модель застосування OSINT у діяльності Служби правопорядку

Запропонована модель демонструє, що OSINT виступає початковим елементом аналітичного циклу, який трансформується у процесуально оформлені результати перевірки та службового розслідування. Такий підхід забезпечує інтеграцію інформаційно-аналітичної діяльності у правозастосовну практику військової поліції та сприяє підвищенню ефективності прийняття управлінських рішень.

Інтеграція OSINT у процедури проведення перевірок службових перевірок і службових розслідувань сприяє підвищенню об'єктивності, повноти та оперативності встановлення

фактичних обставин правопорушень у Збройних Силах України. Водночас OSINT доцільно розглядати як перспективний інструмент підвищення ефективності діяльності військової поліції, використання якого потребує належного правового регулювання та адаптації міжнародного досвіду до національних умов.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Конституція України : Закон України від 28.06.1996 № 254к/96-ВР. URL: https://zakon.rada.gov.ua/laws/show/254к/96-вр#Text (дата звернення: 09.04.2026).
2. Про захист персональних даних : Закон України від 01.06.2010 № 2297-VI. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text (дата звернення: 09.04.2026).
3. Про інформацію : Закон України від 02.10.1992 № 2657-XII. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text (дата звернення: 09.04.2026).
4. Про Військову службу правопорядку у Збройних Силах України : Закон України від 07.03.2002 № 3099-III. URL: https://zakon.rada.gov.ua/laws/show/3099-14#Text (дата звернення: 09.04.2026).
5. Про затвердження Порядку проведення службового розслідування у Збройних Силах України : наказ Міністерства оборони України від 21.11.2017 № 608. URL: https://zakon.rada.gov.ua/laws/show/z1503-17#Text (дата звернення: 09.04.2026).
6. Про затвердження Інструкції про організацію та проведення перевірок у Збройних Силах України органами управління та підрозділами Військової служби правопорядку у Збройних Силах України : наказ Генерального штабу Збройних Сил України від 13.12.2014 № 262.
7. Конвенція про захист прав людини і основоположних свобод від 04.11.1950. URL: https://zakon.rada.gov.ua/laws/show/995_004#Text (дата звернення: 09.04.2026).
8. Регламент (ЄС) 2016/679 Європейського Парламенту і Ради від 27 квітня 2016 року (Загальний регламент про захист даних – GDPR). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation). URL: https://eur-lex.europa.eu/eli/reg/2016/679/oj (дата звернення: 09.04.2026).
9. Конвенція Ради Європи №108+ про захист осіб у зв'язку з автоматизованою обробкою персональних даних, 2018. URL: https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1 (дата звернення: 09.04.2026).
10. Директива (ЄС) 2016/680 Європейського Парламенту і Ради від 27 квітня 2016 року щодо захисту персональних даних у сфері правоохоронної діяльності. Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016. URL: https://eur-lex.europa.eu/eli/dir/2016/680/oj (дата звернення: 09.04.2026).
11. Посібник НАТО з розвідки з відкритих джерел NATO Open Source Intelligence Handbook. URL: https://ia801403.us.archive.org/32/items/NATOOSINTHandbookV1.2/NATO%20OSINT%20Handbook%20v1.2%20-%20Jan%202002.pdf (дата звернення: 09.04.2026).
12. Розвідка з відкритих джерел (Open Source Intelligence) : Армійська публікація з техніки і тактики ATP 2-22.9 / Міністерство армії США. Вашингтон, 2012. Open Source Intelligence : ATP 2-22.9. URL: https://irp.fas.org/doddir/army/atp2-22-9.pdf (дата звернення: 09.04.2026).
13. Діяльність розвідки Армії США : AR 381-10. Вашингтон : Міністерство армії США, 2007. U.S. Army Intelligence Activities : AR 381-10. URL: https://irp.fas.org/doddir/army/ar381-10.pdf (дата звернення: 09.04.2026).
14. Берклійський протокол щодо цифрових розслідувань із використанням відкритих джерел. Berkeley Protocol on Digital Open Source Investigations. URL: https://www.ohchr.org/sites/default/files/2024-01/OHCHR_BerkeleyProtocol.pdf (дата звернення: 09.04.2026).
15. Van Puyvelde D. The rise of open-source intelligence // European Journal of International Security. URL: https://www.cambridge.org/core/journals/european-journal-of-international-security/article/rise-of-opensource-intelligence/21122432399ECB8078BF0D89A76D0586 (дата звернення: 09.04.2026).