навчання здатні адаптуватися до змін у режимі реального часу, що особливо важливо для ведення бойових дій у складних та нестабільних умовах.

Дослідження також виявило необхідність перегляду підходів до підготовки фахівців розвідки в умовах воєнного стану. На думку авторів, підготовка повинна включати оволодіння сучасними інформаційними технологіями, знання основ ШІ, вміння аналізувати відкриті джерела інформації (OSINT), а також розуміння специфіки міжвідомчої взаємодії в умовах комплексної оборони.

На підставі результатів дослідження автори дійшли висновку, що система розвідувального забезпечення формувань НГ України має розвиватися в напрямі створення гнучкої, децентралізованої моделі, здатної адаптуватися до загроз як регулярного, так і асиметричного характеру. У межах такої моделі інтеграція цифрових платформ, систем підтримки прийняття рішень, кіберзахисту та прогнозної аналітики є запорукою її ефективності.

Таким чином, реалізація запропонованих напрямів удосконалення РЗ дозволить посилити спроможності Національної гвардії України в контексті виконання завдань у рамках сектора безпеки і оборони. Надалі доцільним є створення експериментальної платформи для тестування елементів ШІ у взаємодії з підрозділами розвідки, що стане основою для формування концептуальної моделі РЗ в умовах воєнного стану.

Єрьоміна Людмила,
старший викладач
кафедри інформаційної безпеки держави,
Навчально-науковий інститут інформаційної безпеки
та стратегічних комунікацій НА Служби безпеки України

ПОТЕНЦІАЛ OSINT У СИСТЕМІ НАЦІОНАЛЬНОЇ БЕЗПЕКИ УКРАЇНИ

Аналіз потенціалу OSINT (розвідки з відкритих джерел) у вітчизняній системі інформаційної безпеки потребує комплексного розгляду технологічних, організаційних, кадрових, нормативних і стратегічних чинників, які визначають можливості ефективного використання відкритих джерел в інтересах національної безпеки України. У світлі гібридних загроз, інформаційної війни, посиленої активності ворожих спецслужб і кібердиверсій, що набули особливої гостроти в умовах повномасштабної агресії з 2022 року, саме OSINT виступає одним із найважливіших і водночас найменш витратних інструментів стратегічної аналітики та оперативного моніторингу інформаційного простору.

Унікальна особливість OSINT полягає в тому, що збирання даних здійснюється з відкритих, загальнодоступних джерел, що значно знижує потребу у спеціальному технічному обладнанні та дозволяє легально акумулювати інформацію з тисяч джерел у реальному часі.

Розглянемо найважливіші напрями, в яких відкриті джерела інформації (OSINT) можуть ефективно застосовуватись в українській системі національної безпеки, з урахуванням реалій гібридної війни, кіберзагроз і системної дезінформації (табл.1).

Найвищий потенціал спостерігається у сфері кібербезпеки, де OSINT використовується для виявлення цифрових вразливостей, фішингових кампаній, аналізу цифрових слідів хакерських угруповань. Державна служба спеціального зв'язку та захисту інформації, кіберпідрозділи поліції та CERT-UA активно використовують відкриті джерела для виявлення загроз до їх безпосередньої реалізації, що дозволяє діяти превентивно, а не реактивно [1].

Таблиця 1. **Основні сфери застосування OSINT у системі національної безпеки України**

Сфера застосування	Приклади використання OSINT	Відомства / структури, що застосовують	Потенціал ефективності
Кібербезпека	Виявлення витоків, фішинг-кампаній, цифрових слідів хакерів, сканування вразливостей	Держспецзв'язку, CERT-UA, кіберполіція	Високий
Воєнна розвідка	Геолокація техніки, моніторинг супутникових знімків, розпізнавання військових об'єктів	ГУР МОУ, ЗСУ, Сили спецоперацій	Високий
Контррозвідка та ідентифікація	Аналіз акаунтів, профілів, зв'язків осіб, цифрових слідів, поведінки в соцмережах	СБУ, ДБР, підрозділи Нацполіції	Середній–високий
Інформаційна протидія	Виявлення фейкових наративів, інформаційних атак, спростування дезінформації	РНБО, Центр стратегічних комунікацій, СБУ	Високий
Розслідувальна журналістика	Збір доказів злочинів, аналіз метаданих, супутникові знімки, виявлення замовників кампаній	Bellingcat, Texty.org.ua, Molfar, Слідство.Інфо	Високий
Громадянське спостереження	Моніторинг дій ворога, фіксація злочинів, геолокація обстрілів, аналіз публічних баз	OSINT-волонтери, Myrotvorets, InformNapalm	Високий

Джерело: складено автором

Не менш значущою є роль OSINT у воєнній розвідці. За допомогою супутникових знімків, фотографій у соціальних мережах, відео з відкритих платформ та цифрової геолокації аналітики виявляють пересування ворожої техніки, підтверджують обстріли цивільних об'єктів, фіксують сліди воєнних злочинів. У цьому контексті OSINT суттєво доповнює класичні розвідувальні

методи, зменшуючи залежність від закритих джерел. Підрозділи ГУР МОУ, Збройних Сил України та Сил спеціальних операцій застосовують OSINT-інструменти для оперативної оцінки обстановки та зменшення невизначеності в бойових умовах.

OSINT у контррозвідувальній сфері демонструє здатність виявляти приховані зв'язки осіб, аналізувати їхню присутність у відкритому цифровому середовищі, профілювати за поведінкою в соцмережах. Служба безпеки України та інші правоохоронні органи використовують ці дані для ідентифікації підривної діяльності, спроб вербування, а також розкриття ворожої агентурної мережі. Особливу цінність має поєднання OSINT із HUMINT, коли інформація з відкритих джерел підтверджує або спростовує дані з агентурної мережі, дозволяючи обґрунтовано приймати рішення.

У сфері інформаційної протидії OSINT відіграє ключову роль у боротьбі з дезінформаційними кампаніями. Завдяки постійному моніторингу соціальних мереж, платформ новин і виявленню синхронних вкидів, можливо своєчасно виявляти фейки, аналізувати ворожі наративи, виявляти координаторів інформаційних атак та формувати контрнаративи. Центр стратегічних комунікацій та інформаційної безпеки, що функціонує при РНБО, разом із відповідними підрозділами СБУ, уже реалізують комплексні підходи до OSINT-аналізу з метою інформаційного захисту.

Розслідувальна журналістика в Україні також активно використовує OSINT-інструменти для викриття корупції, воєнних злочинів, незаконної діяльності або маніпуляцій. Проєкти на кшталт Bellingcat, Molfar, Texty.org.ua, «Слідство.Інфо» за допомогою аналітики відкритих джерел і супутникових даних створюють докази, які потім використовуються в судових процесах, міжнародних розслідуваннях та адвокаційних кампаніях. Їхня діяльність доводить, що OSINT — це не лише інструмент держави, а й інструмент громадянського контролю й підзвітності [2].

Окрема категорія — ***громадянське спостереження та волонтерський OSINT.*** Ініціативи типу Myrotvorets, InformNapalm, DeepState, GeoConfirmed здійснюють щоденний моніторинг фронту, фіксують обстріли, локалізують наслідки воєнних дій, відстежують переміщення ворожих сил. Ці структури часто співпрацюють з офіційними органами, передаючи верифіковану інформацію для подальших оперативних дій. Унікальність української ситуації полягає в тому, що велика частина OSINT-активностей здійснюється не лише на рівні держави, а й «знизу», що створює ефект гнучкої мережевої безпеки.

Українські ініціативи та проєкти, що використовують OSINT, зокрема: аналітична група Molfar, інформаційно-аналітична платформа Texty.org.ua, проєкт InformNapalm, Державна структура — Центр стратегічних комунікацій та інформаційної безпеки, бази Myrotvorets, DeepStateMap.live, Антикорупційне розслідувальне бюро Bihus.Info. Ці структури демонструють, що OSINT в Україні є не лише інструментом державної розвідки, але й потужним громадянським та журналістським ресурсом, який здатний конкурувати з традиційними службами збору інформації за швидкістю, точністю та гнучкістю реагування.

Отже, потенціал OSINT в українській системі інформаційної безпеки є надзвичайно значним, але його реалізація вимагає системного підходу: нормативного врегулювання, інституційного зміцнення, технічного переоснащення, кадрової підготовки й інтеграції міжвідомчого обміну. За наявності політичної волі, координації із західними партнерами та підтримки цифрових ініціатив знизу, OSINT може перетворитися з фрагментарного інструменту в один із ключових елементів національної інформаційної оборони, що забезпечить гнучкість, превентивність і прозорість дій у сфері державної безпеки.

Заєць Наталія,
викладач кафедри №23,
Військовий інститут телекомунікацій та інформатизації імені Героїв Крут

Жилінський Ігор,
Військовий інститут телекомунікацій та інформатизації імені Героїв Крут

Коваленко Іван,
Військовий інститут телекомунікацій та інформатизації імені Героїв Крут

РОЛЬ ШТУЧНОГО ІНТЕЛЕКТУ У РОЗВІДУВАЛЬНО-АНАЛІТИЧНІЙ ДІЯЛЬНОСТІ: СУЧАСНІ МОЖЛИВОСТІ ТА МАЙБУТНІ ВЕКТОРИ РОЗВИТКУ

У сучасних умовах змін глобального безпекового середовища, коли традиційні підходи до ведення розвідки підсилюються інформаційними та кіберзагрозами, особливої актуальності набуває використання високотехнологічних рішень. Однією з провідних технологій, що визначає перспективи розвитку оборонного сектору, є штучний інтелект (ШІ). Його здатність до швидкої обробки великих обсягів даних, виявлення прихованих закономірностей і формування прогнозів надає розвідувальній діяльності нового виміру.

Сьогодні провідні країни світу вже впроваджують ШІ для реалізації таких завдань, як обробка відкритих джерел інформації (OSINT), аналіз контенту соціальних мереж, відео- та аудіозаписів; класифікація об’єктів на зображеннях, отриманих із супутників і БПЛА; автоматизований переклад, транскрипція і аналіз мовлення; виявлення відхилень у поведінці інформаційних суб’єктів; оцінка ризиків та підтримка ухвалення рішень у режимі реального часу.

Системи глибокого навчання (Deep Learning) і нейронні мережі забезпечують розпізнавання образів, класифікацію подій і моделювання сценаріїв розвитку ситуацій, що суттєво підвищує рівень ситуаційної обізнаності. Особливо важливими такі можливості є в умовах бойових дій, де критичною є оперативна перевірка достовірності отриманої інформації з метою мінімізації ризику впливу дезінформації.