Важливу роль у міжнародній системі протидії дезінформації відіграє Європейський Союз, зокрема проєкт EUvsDisinfo, який здійснює системний моніторинг і фіксацію дезінформаційних кампаній. Накопичені дані дозволяють аналізувати типові наративи інформаційних атак та формувати контрзаходи на рівні держав-партнерів.

Перспективним напрямом розвитку розвідувально-аналітичної діяльності є впровадження технологій штучного інтелекту та машинного навчання для автоматизованого виявлення інформаційних загроз. За оцінками аналітичного центру RAND Corporation, використання AI-систем у сфері інформаційної безпеки дозволяє значно підвищити швидкість і точність виявлення дезінформаційних кампаній. Водночас це потребує належного нормативного регулювання, щоб уникнути порушення прав людини та забезпечити баланс між безпекою і свободою інформації.

Отже, розвідувально-аналітичне забезпечення протидії дезінформації та інформаційно-психологічним операціям є ключовим елементом сучасної системи національної безпеки, особливо в умовах гібридної війни. Практика показує, що інформаційний вплив стає рівнозначним за значенням із військовими та політичними засобами боротьби, а інколи навіть визначає їх ефективність. Умови збройної агресії Російської Федерації проти України продемонстрували високу інтенсивність і технологічну складність інформаційних атак, що потребує постійного вдосконалення методів їх виявлення, аналізу та нейтралізації.

Сучасний стан цієї сфери характеризується переходом до цифрових та автоматизованих систем моніторингу інформаційного простору, використанням OSINT-інструментів та технологій штучного інтелекту. Водночас існують проблеми, пов’язані з швидкістю поширення дезінформації, недостатньою координацією між суб’єктами безпеки та необхідністю вдосконалення нормативно-правового регулювання.

Перспективи розвитку полягають у подальшій інтеграції інноваційних технологій, посиленні міжнародного співробітництва та формуванні комплексної системи інформаційної безпеки, здатної не лише реагувати на загрози, але й прогнозувати їх виникнення. Таким чином, ефективне розвідувально-аналітичне забезпечення є необхідною умовою стійкості держави в умовах сучасних інформаційних війн.

Пристінський Роман Володимирович
начальник кафедри тактики
доктор філософії,
підполковник
Навчально-науковий інститут забезпечення державної безпеки
Національної академії Національної гвардії України

OSINT ЯК СКЛАДОВА СУЧАСНОЇ РОЗВІДКИ: ПОБУДОВА СИСТЕМИ ЗБОРУ, ВЕРИФІКАЦІЇ ТА АНАЛІТИКИ ВІДКРИТИХ ДАНИХ

У тезі-доповіді досліджено роль розвідки з відкритих джерел (OSINT) у системі сучасного військового розвідувального забезпечення в умовах гібридних загроз, цифровізації інформаційного простору та повномасштабної збройної агресії проти України.

У контексті стрімкого розвитку цифрових технологій та інформаційних потоків зростає значущість відкритих джерел як джерела розвідувальної інформації. Відкрита розвідка (OSINT - Open Source Intelligence) дедалі частіше виступає повноцінним інструментом збору, аналізу та використання даних у військовій, правоохоронній, кібербезпековій, аналітичній та журналістській діяльності. OSINT дозволяє отримувати цінну інформацію з широкого спектра відкритих джерел, включаючи цифрові ЗМІ, соціальні мережі, відеохостинги, форуми, бази даних, супутникові знімки та інші ресурси, доступні без спеціального доступу.

Мета публікації – обґрунтування ролі OSINT у сучасній розвідці та визначення підходів до побудови системи збору, верифікації й аналітики відкритих даних.

Інформація, добута через OSINT, базується на публічно доступних джерелах - соціальних мережах, супутникових знімках, форумах, ЗМІ, офіційних документах, картах тощо. Цей підхід дозволяє виявити переміщення ворожих військ, визначити місце розташування техніки, зібрати візуальні докази атак, відстежити логістичні маршрути противника або навіть ідентифікувати окремих військовослужбовців. Сьогодні OSINT перестає бути допоміжною функцією - він перетворюється на один з ключових елементів сучасної військової розвідки. Цифровий слід, який залишає супротивник, може бути перетворений на бойову перевагу. А зібрані з різних джерел дані дозволяють сформувати цілісну оперативну картину, іноді навіть точнішу, ніж традиційні розвідувальні дані.

Збір відкритої інформації у військовому контексті передбачає цілеспрямовану та організовану діяльність із виявлення, відбору й фіксації релевантних даних із публічно доступних джерел. До таких джерел належать соціальні мережі, відкриті комунікаційні платформи, супутникові знімки, геоінформаційні сервіси, публікації засобів масової інформації, офіційні повідомлення органів влади, електронні реєстри, а також цифрові сліди, що залишаються в інформаційному просторі внаслідок діяльності особового складу, підрозділів чи військової техніки. Організаційно система збору вибудовується відповідно до визначених розвідувальних потреб. Початковим етапом є формулювання інформаційного запиту або розвідувального завдання (наприклад, уточнення дислокації підрозділів противника, виявлення маршрутів переміщення техніки, аналіз стану військової інфраструктури). Далі здійснюється ідентифікація потенційних джерел, визначення методів моніторингу та добору технічних інструментів. Важливою складовою є безперервність процесу збору, що дозволяє забезпечити актуальність інформації в умовах швидкої зміни бойової обстановки.

З огляду на визначальну роль інформаційної переваги, ключовим чинником ефективності військового OSINT стає належна організація процесу збору відкритої інформації, що повинна відповідати умовам бойової діяльності, інформаційного протиборства та інтегруватися в загальну систему розвідувального забезпечення військ.

Військове значення OSINT для Національної гвардії України полягає також у можливості підвищення рівня ситуаційної обізнаності на тактичному та

оперативному рівнях. Підрозділи НГУ, які залучаються до охорони громадської безпеки чи несення служби у бойових умовах, завдяки відкритим джерелам отримують додаткові дані щодо настроїв серед населення, потенційних осередків напруження, маршрутів переміщення ворожих сил, що дозволяє своєчасно адаптувати дії до змін обстановки. Це, своєю чергою, сприяє зменшенню ризиків, підвищенню ефективності використання ресурсів і збереженню життя особового складу.

Суттєвим є також аспект міжвідомчої взаємодії. Отримана в результаті OSINT-діяльності інформація може бути використана не лише для потреб самих підрозділів НГУ, а й передаватися до суміжних структур — зокрема Служби безпеки України, Головного управління розвідки Міністерства оборони України, Державної прикордонної служби тощо. Таким чином, НГУ виконує не лише споживацьку, а й аналітико-інформаційну функцію у загальнодержавній системі безпеки.

Таким чином у контексті повномасштабної збройної агресії проти України система OSINT набуває особливої значущості для підрозділів Національної гвардії України. Її використання сприяє підвищенню рівня ситуаційної обізнаності, своєчасному виявленню загроз, протидії дезінформації та інформаційно психологічним впливам, а також забезпечує інформаційну підтримку управлінських рішень на тактичному й оперативному рівнях.

Перспективи подальших досліджень доцільно пов’язувати з розробленням комплексних моделей функціонування військових OSINT-систем, удосконаленням механізмів автоматизації аналітичних процесів і форму міжвідомчих стандартів обміну та верифікації відкритої інформації. Реалізація зазначених напрямів сприятиме зміцненню інформаційної переваги України та підвищенню ефективності діяльності суб’єктів сектору безпеки і оборони в умовах сучасних викликів.

Савранський Валерій Петрович
старший викладач кафедри тактики – начальник служби РЕБ
полковник
Київський інститут Національної гвардії України
Корень Денис Олександрович
курсант 123 навчальної групи
факультет забезпечення державної безпеки
Київський інститут Національної гвардії України

ВПЛИВ ВОЄННОГО СТАНУ НА РОЗВИТОК ЕЛЕКТРОННОГО УРЯДУВАННЯ В УКРАЇНІ

Згідно з дослідженнями University Taubman Center for Public Policy, перехід від традиційного державного управління до «електронного урядування» припускає послідовне проходження п’яти основних етапів.