зображення, маскуванням, пошкодженням техніки або недостатністю навчальних даних.

Для практичного використання результатів OSINT доцільно фіксувати рівень достовірності висновку: попередня, імовірна або підтверджена ідентифікація. Попередня ідентифікація ґрунтується на окремих візуальних ознаках; імовірна – на поєднанні кількох ознак і частковій перевірці; підтверджена – на узгоджених незалежних джерелах, що збігаються за місцем, часом, типом об'єкта та контекстом.

Висновки. OSINT є важливим інструментом ідентифікації військової техніки та підрозділів рф за відкритими цифровими джерелами. Його ефективність ґрунтується на поєднанні візуальної ідентифікації, аналізу маркувань, геолокації, хронолокації, крос-верифікації, аналізу цифрового сліду та сучасних цифрових інструментів.

Найбільш обґрунтованим є підхід, за якого OSINT розглядається не як набір окремих інструментів, а як послідовний процес перевірки інформації: від аналізу джерела та візуальних ознак до зіставлення з незалежними даними й оцінювання достовірності висновку.

Для сектору безпеки і оборони OSINT-методи мають практичне значення як засіб документування, аналітичного узагальнення, протидії дезінформації та підготовки особового складу до критичного аналізу відкритих цифрових матеріалів. Їх використання має здійснюватися з урахуванням правових, етичних і безпекових обмежень.

Примітка. Дослідження виконано згідно з планом роботи науково-дослідного гуртка «Актуальні питання бойового та логістичного забезпечення» кафедри бойового та логістичного забезпечення Київського інституту Національної гвардії України на 2025–2026 навчальний рік.

Пристанський Дмітрій Олексійович
Курсант 3 курсу Військово-юридичного інституту
Національно-юридичного університету
Імені Ярослава Мудрого
Гашенко Сергій Васильович,
старший викладач кафедри загальновійськових дисциплін, підполковник
Військово-юридичного інституту
Національного юридичного університету імені Ярослава Мудрого

РОЗВІДУВАЛЬНО-АНАЛІТИЧНЕ ЗАБЕЗПЕЧЕННЯ ПРОТИДІЇ ДЕЗІНФОРМАЦІЇ ТА ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНИМ ОПЕРАЦІЯМ У СУЧАСНИХ УМОВАХ: СТАН ТА ПЕРСПЕКТИВИ РОЗВИТКУ

В умовах збройної агресії Російської Федерації проти України інформаційний компонент війни набув особливого значення, оскільки поряд із застосуванням військової сили активно використовуються інструменти пропаганди, маніпуляції фактами, поширення панічних настроїв, дискредитації органів державної влади та

підриву довіри до сектору безпеки й оборони. У зв'язку з цим зростає роль розвідувально-інформаційної роботи як системи збору, обробки, аналізу та прогнозування даних щодо джерел, каналів і методів ворожого інформаційного впливу. Саме своєчасне виявлення загроз, оцінка їх масштабу та вироблення ефективних рішень щодо нейтралізації інформаційних операцій є важливою умовою забезпечення стійкості держави.

Разом із тим сучасний стан розвідувально-інформаційної діяльності потребує подальшого вдосконалення з урахуванням нових технологічних викликів, розвитку кіберпростору та зростання обсягів інформації, що потребує оперативного аналізу. Особливого значення набуває впровадження штучного інтелекту, автоматизованих систем моніторингу інформаційного середовища, міжвідомчої координації та сучасних методів прогнозування інформаційних загроз. У зв'язку з цим дослідження сучасного стану та перспектив розвитку розвідувально-аналітичного забезпечення протидії дезінформації є важливим як у теоретичному, так і у практичному аспекті.

Розвідувально-аналітичне забезпечення протидії дезінформації та інформаційно-психологічним операціям є важливою складовою системи національної безпеки, що спрямована на своєчасне виявлення, аналіз та нейтралізацію інформаційних загроз. У сучасних умовах інформаційний простір перетворився на самостійний театр гібридного протиборства, де поряд із традиційними військовими діями активно застосовуються методи психологічного впливу, інформаційного маніпулювання та стратегічної пропаганди. Особливої актуальності це набуває в умовах збройної агресії Російської Федерації проти України, де інформаційні операції використовуються як інструмент підриву державної стійкості, деморалізації населення та дискредитації органів державної влади.

Сучасні інформаційно-психологічні операції характеризуються високим рівнем технологічності, використанням соціальних мереж, бот-мереж, алгоритмів штучного інтелекту та технологій створення синтетичного контенту. Як зазначається у Стратегії інформаційної безпеки України, затвердженій Указом Президента України, інформаційні загрози визначаються як один із ключових факторів впливу на національну безпеку держави, що потребує системного моніторингу та розвідувально-аналітичного реагування.

У цих умовах розвідувально-аналітична робота трансформується від класичного збору інформації до комплексної обробки великих масивів даних у режимі реального часу. Згідно з аналітичними матеріалами NATO Strategic Communications Centre of Excellence, сучасні інформаційні операції РФ та інших акторів характеризуються автоматизацією поширення дезінформації, використанням штучного інтелекту та глибокою персоналізацією впливу на аудиторії. Це зумовлює необхідність застосування алгоритмічних систем аналізу інформаційного середовища та впровадження інструментів OSINT-аналітики.

В умовах війни проти України інформаційна складова набула системного характеру. За даними Центру протидії дезінформації при РНБО України, основними напрямами ворожого впливу є поширення фейкових новин, маніпуляція фактами бойових дій, дискредитація мобілізаційних процесів та спроби підриву міжнародної підтримки України . Такі дії формують постійну потребу в оперативному розвідувально-аналітичному супроводі інформаційного простору та швидкому реагуванні на загрози.

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.