УДК 355.4

В. Ю. Бутузов

Д. О. Ковтонюк

І. С. Луговський

ОСОБЛИВОСТІ ОРГАНІЗАЦІЇ ТА ВЕДЕННЯ ОСОБОВОЇ РОЗВІДКИ ОРГАНАМИ РОЗВІДКИ ФОРМУВАНЬ НАЦІОНАЛЬНОЇ ГВАРДІЇ УКРАЇНИ ПІД ЧАС УЧАСТІ У ВІДСІЧІ ЗБРОЙНОЇ АГРЕСІЇ

На підставі аналізу досвіду виконання розвідувальних завдань під час відсічі повномасштабної збройної агресії російської федерації розглянуто особливості організації та ведення особової розвідки силами оборони України, уточнено перелік основних завдань особової розвідки в сучасних умовах. Наведено проблемні питання зі збору розвідувальної інформації, що мали місце у ході отримання відомостей від місцевого населення. Описано загальні підходи з добування відомостей шляхом аналізу соціальних медіа та сервіси, які використовуються для їх моніторингу. Окреслено шляхи подальшого розвитку спроможностей особової розвідки Національної гвардії України.

Ключові слова: *збройна агресія, розвідувальна інформація, особова розвідка, розвідувальне забезпечення операцій, мережева розвідка.*

Постановка проблеми. Військові конфлікти та збройна агресія завжди становили серйозну загрозу для міжнародної безпеки та стабільності. Досвід ведення сучасних бойових дій неодноразово підтверджував важливість організації усіх можливих видів розвідки та використання способів її ведення. Крім того, спостерігалися закономірні одночасні зміни у способах ведення збройної боротьби та організації розвідки в її інтересах. Зміщення способів протистояння у бік комплексної боротьби, відповідно, спрямовує в цьому напрямку і розвиток способів ведення розвідки.

Разом з тим досвід організації та ведення розвідки під час відсічі збройної агресії російської федерації вказує на можливість використання результатів розвідки тактичного рівня для забезпечення позитивного впливу на хід і результати операції угруповання військ сил оборони держави.

З початком повномасштабного вторгнення російських військ на територію України неабиякої актуальності набуло питання добування розвідувальних відомостей від місцевого населення, а також з відкритих джерел інформації, таких як ЗМІ, соціальні мережі та громадські джерела. Зазначені способи добування розвідувальної інформації відносять до заходів особової розвідки, які є важливою складовою стратегії забезпечення безпеки та захисту національних інтересів у воєнний період. Розвідка від місцевого населення та з відкритих джерел інформації дає змогу отримувати цінні дані про дії противника, його розташування, зброю та наміри, що є необхідним для ефективного планування бойових операцій (дій) та прийняття відповідних рішень командування.

Аналіз останніх досліджень і публікацій. На цей час розгляду питання з визначеної тематики приділено увагу в низці наукових праць [1–5].

Так, автором статті [1] розглянуто розвідувальну діяльність у контексті методів збору розвідувальних даних. Прикладом такої діяльності представлено розвідку на основі аналізу відкритих джерел інформації – OSINT (Open Source Intelligence), її регламентацію та організацію як компонента інформаційної роботи розвідувальних служб США.

Зміст роботи [2] присвячено аналізові досвіду організації розвідки з відкритих джерел інформації в розвідувальних службах окремих європейських країн.

Автором праці [3] проведено огляд теоретичних та практичних аспектів військової розвідки, сучасного стану нормативно-правового забезпечення розвідувальної діяльності в Україні, а також

додаткових та альтернативних форм отримання стратегічних і тактичних даних. Наголошено на визначенні факторів здійснення військової розвідки, умов, переваг і недоліків стратегічної, тактичної та оперативної розвідки. Водночас сформульовано висновок про поточну ситуацію щодо стану військової розвідки в Україні в контексті побудови системи заходів боротьби з гібридною війною.

У дослідженні [4] розкрито сутність діяльності з отримання розвідувальної інформації з відкритих джерел (OSINT) та визначено перспективи використання сучасних розвідувальних технологій у Національній гвардії України (НГУ).

Робота [5] окреслює подальший розвиток теорії та практики розвідки; містить результати дослідження щодо виявлення невідповідностей між ефективністю та вимогами до розвідки частин і підрозділів НГУ, а також обґрунтовує основні напрямки підвищення її ефективності в антитерористичній операції.

Однак наведені наукові праці не повною мірою розкривають питання особливостей організації та ведення особової розвідки розвідувальними підрозділами формувань НГУ в інтересах підготовки і ведення бойових (спеціальних) дій у складі угруповань військ сил оборони держави в умовах воєнного стану під час відсічі та стримування військової агресії.

Метою статті є проведення аналізу особливостей організації та ведення особової розвідки органами розвідки формувань Національної гвардії України під час участі у відсічі повномасштабної збройної агресії російської федерації.

Виклад основного матеріалу. Організація та ведення особової розвідки під час відсічі збройної агресії є складним завданням, яке вимагає високої підготовки, ефективного планування та використання сучасних технологій. Аналіз наявного досвіду показує, що успіх за таких умов залежить від злагодженої роботи розвідувальних підрозділів, використання передових засобів збору розвідувальних відомостей та швидкого аналізу даних.

До розвідувальних відомостей належать усі зведення, які характеризують діючого або ймовірного противника, а також місцевість та погоду в районі майбутніх бойових дій. Розвідувальні відомості, що добуваються, збираються і обробляються, перетворюються на розвідувальні дані [6]. Шляхи їх отримання можуть охоплювати різноманітні джерела, такі як аналітичні звіти, супутникові знімки, розвіддані від спеціальних служб та інші джерела. Збір, аналіз та обробка цих даних допомагають всебічно оцінити обстановку, попередити можливі загрози та визначити подальші кроки.

Однак для більш повного розуміння ситуації та отримання конкретної інформації про противника або його об’єкти використовується особова розвідка.

Під особовою розвідкою у цій статті слід розуміти комплекс заходів і дій, що здійснюються визначеними підрозділами з використанням способів добування відомостей від людських ресурсів (джерел) з метою забезпечення органів військового управління (штабів) розвідувальною інформацією в інтересах підготовки і ведення бойових (спеціальних) дій військовими частинами (підрозділами) сил оборони України. Особова розвідка ведеться шляхом використання особових та неособових джерел інформації (відкриті джерела інформації, документи та зразки озброєння і військової техніки противника). Вона надає деталізовану інформацію, яка допомагає підтвердити чи спростувати розвідувальну інформацію, дає змогу отримати відповіді на конкретні питання та збільшує ступінь достовірності інформації, яку використовують органи управління сил оборони для прийняття рішень.

Основними завданнями особової розвідки є:

– добування розвідувальної інформації про сили і засоби противника та його наміри з метою забезпечення ведення бойових (спеціальних) дій військовими частинами та підрозділами;

– добування розвідувальної інформації про об’єкт, зону (район) бойових (спеціальних) дій з метою забезпечення заходів безпеки застосування військових частин та підрозділів, в інтересах яких вони діють;

– збір розвідувальної інформації з метою оцінювання результатів бойових (спеціальних) дій;

– розвідка місцевості та інфраструктури в районах дій військ;

– отримання розвідувальної інформації з відкритих джерел;

– проведення аналізу добутої первинної розвідувальної інформації, тенденцій змін обстановки в зоні (районі) ведення бойових (спеціальних) дій;

– пошук та виявлення перспективних осіб.

Одним із ключових питань особової розвідки у ході ведення бойових (спеціальних) дій військовими частинами (підрозділами) сил оборони держави є отримання відомостей від місцевого населення в інтересах прийняття рішень органами управління Збройних Сил України (ЗСУ) та НГУ зокрема.

Ведення особової розвідки шляхом отримання відомостей від місцевого населення є одним з ефективних методів збору розвідувальної інформації в умовах динамічності ведення бойових дій. Цей підхід відбувається у взаємодії з людьми, які проживають на території, зайнятій ворогом, або мають доступ до цінної інформації, що стосується ворожих дій, настроїв населення, важливих подій та інших розвідувально значущих аспектів.

В умовах швидкого просування військ противника, але збереженого національного мобільного зв'язку, доступу до мережі Інтернет у поєднанні з великою кількістю абонентських термінальних пристроїв (мобільних телефонів, ПЕОМ, камер відеоспостереження тощо), зберігається можливість здійснювати збір та передачу інформації від місцевого населення дистанційно.

Варто зазначити, що на початковому етапі повномасштабного вторгнення рф отримання інформації про знаходження та пересування противника було дещо ускладнене. З одного боку, інформації про пересування військ противника було достатньо, та разом з тим вона надходила із запізненням, або час на перевірку достовірності нівелював її важливість. У більшості випадків йдеться про передачу фотографій та відео техніки противника за допомогою месенджерів Viber, WhatsApp та Signal. Водночас більшість місцевого населення не володіла інформацією про те, куди необхідно надавати подібні матеріали, тому здебільшого їх розміщували у групах та соціальних мережах або надсилали знайомим військовослужбовцям ЗСУ, НГУ, представникам Служби безпеки України та співробітникам правоохоронних органів.

Також слід зазначити активізацію населення суміжної держави – Республіки Білорусь, яке почало повідомляти в соціальних мережах про залізничні та автомобільні перевезення сил і засобів противника на своїй території, рух колон військової техніки у бік нашої держави, про час, місце та кількість пусків ракет, злети з військових аеродромів літаків (вертольотів) та прямування їх у бік державного кордону України.

Частково, в телефонному режимі, через оперативно-чергову службу така інформація надходила до пунктів управління сил оборони держави, де уточнювалися деталі спостереження: час, місце, кількість, тип озброєнь тощо та передавалися далі для планування вогневого ураження противника. Це значно сприяло нарощуванню спроможностей сил оборони щодо виявлення, ідентифікації, розподілу цілей та ураження (знищення) сил противника. Проте можливості щодо процедури збору даних, їх аналізу та узагальнення не були автоматизованими, містили багато неточностей з причин значної кількості ланок передачі інформації та мали тенденцію швидко втрачати актуальність.

Отже, основними проблемами збору інформації на той час стали такі:

– спотворення інформації у процесі передачі через ланцюжок людей, а також її дублювання під час проходження через довгі ланцюжки;

– втрата актуальності інформації через швидкоплинність змін обстановки;

– продукування дезінформації, фейків та проведення заходів безпеки операції противником;

– потенційний доступ противника до відкритих даних соціальних мереж;

– значна увага кіберпідрозділів противника до контенту основних месенджерів і соціальних мереж та, як наслідок, перехоплення даних і вкидання дезінформації.

У зв'язку з цим почали вживати заходів щодо спрямування таких інформаційних потоків до розвідувальних органів, у тому числі створення відповідних чат-ботів на рівні держави. Подібний чат-бот «@stop_russian_war_bot» почав функціонувати 26.02.2022. Пізніше, 01.03.2022 на відповідних інформаційних ресурсах Служби безпеки України та загальнодержавних каналах була опублікована інструкція користування для щоденного інформування про обстановку шляхом заповнення формалізованої інтерактивної форми.

Це дало змогу підвищити якість інформації, що надходила, впорядкувати її та спростити опрацювання. Після первинної обробки інформації, що надходила, та оцінки її достовірності, вона доправлялася для подальшого використання в інтересах оборони держави.

На завершальному етапі була створена відповідна сторінка «єВорог» у застосунку «Дія».

Водночас варто згадати й негативний досвід, пов'язаний з недотриманням місцевим населенням елементарних правил «поводження» з інформацією про ворога, а саме розміщення в соціальних медіа

результатів вогневого ураження (ударів) противника, що вкрай спростило проведення заходів підтвердження результатів та корегування його вогню.

Один з таких найвідоміших випадків – це розміщення ТікТок відео про пересування техніки поблизу торговельно-розважального центру «Ретровіль» у м. Київ, внаслідок чого 20.03.2022 по ньому було нанесено удар [7].

Також до негативних прикладів можна віднести зберігання (невірне видалення) фото- та відеоматеріалів про противника в «гаджетах» місцевого населення. Як наслідок, у разі виявлення таких матеріалів у мобільних телефонах противник вдавався до жорстких заходів, що нерідко полягали в розстрілі цивільних осіб.

Поряд з отриманням відомостей від місцевого населення добування розвідувальних відомостей з відкритих джерел є особливим інструментом, який допомагає збирати цінні дані для ефективного виконання завдань розвідувального характеру органами розвідки формувань НГУ.

Добування розвідувальних відомостей з відкритих джерел або розвідка на основі відкритих джерел (за термінологією НАТО – OSINT) – це добування і використання військової, політичної, економічної, персональної та іншої інформації з відкритих джерел, без порушення законодавства [8].

OSINT, як правило, об'єднує в собі активні та пасивні заходи пошуку (збору), обліку й аналізу інформації. Джерелами зазначених відомостей є:

– ЗМІ;
– мережа Інтернет;
– державні дані;
– комерційні дані;
– академічні публікації тощо.

Крім того, широко використовуються загальнодоступні дані дистанційного зондування землі та аерофотозйомок (наприклад, Google Earth та мережа комерційних супутників Maxar Technologies Ltd).

Слід не плутати OSINT з «мережевою розвідкою», що являє собою комплекс заходів щодо отримання й обробки даних про віддалену інформаційну систему (об'єкт інформаційного дослідження), її ресурси, засоби захисту, використовувані пристрої і програмне забезпечення та їх уразливості.

Предметом дослідження мережевої розвідки є не побічні (небажані) ефекти, що неминуче супроводжують функціонування технічних засобів інформаційних систем (ІС) і утворюють неумисні канали витоку інформації, а різні види комп'ютерної інформації, що є результатом якраз штатного функціонування ІС та реалізації їх основного призначення – збору, аналізу, обробки, зберігання, передачі інформації тощо. Основним методом ведення мережевої розвідки є несанкціонований доступ до комп'ютерної інформації, що циркулює в ІС.

У мережевій розвідці, як і в технічній, можуть застосовуватися як пасивне перехоплення інформації (прийом і аналіз мережевого трафіка, сканування жорсткого диска та ін.), так і активні методи добування комп'ютерної інформації, за допомогою, наприклад, упровадження в об'єкти інформаційного дослідження вірусів, троянських програм або логічних бомб, що спрацьовують під час активізації певних умов або ініціюються сигналами зовні.

Найбільш широко як джерело OSINT використовуються соціальні мережі, оскільки вони є одним з ключових засобів спілкування. Крім того, у середовищі користувачів мережі постійно підтримують зв'язок близько 60 % осіб, які перебувають у категорії «Друзі»; основним критерієм додавання осіб у категорію «Друзі» є близькі дружні стосунки та в більшості випадків інформація, що розміщена на персональній сторінці, відповідає дійсності. Добування відомостей шляхом аналізу соціальних медіа ще називають SOCMINT.

Наразі виділяють сім основних різновидів соціальних медіа, до яких належать: соціальні мережі, блоги, форуми, сайти відгуків, сервери фото- і відеохостингу, віртуальні служби знайомств і геосоціальні мережі.

Далі більш детально розглянемо кожен із них:

1) соціальна мережа – онлайн-сервіс, призначений для побудови, відображення та організації соціальних взаємовідносин, що забезпечує надання широкого спектра можливостей для обміну інформацією, можливість користувача надати інформацію про самого себе (створити свій профіль), побудувати зв'язки, знайти друзів за інтересами, підключити родичів, колег, однокласників тощо;

2) блог – веб-сайт, основним змістом якого є періодичні записи користувачів (текст, зображення або мультимедіа). Для блогів характерні недовгі записи тимчасової значущості, блоги зазвичай публічні й передбачають сторонніх читачів, які можуть вступити в публічне обговорення з автором (у коментарі до блогозапису або свого блогу);

3) веб-форуми – веб-додатки, призначені для організації спілкування відвідувачів деяких інтернет-ресурсів (веб-сайтів або порталів). На ресурсах веб-форуму користувачі пропонують цікаві для них теми, які потім обговорюються іншими користувачами шляхом розміщення повідомлень (posting) всередині цих тем;

4) веб-сайти відгуків створюються з метою підвищення ефективності та якості наданих послуг і товарів. Користувачі, які відвідують веб-сайти відгуків, залишають там свої повідомлення, беруть участь в анкетуванні, формують думки про ту чи іншу послугу або товар;

5) фотохостинг – це веб-сайт, який дає змогу публікувати будь-які зображення (найчастіше – цифрові фотографії) в мережі Інтернет. Основною перевагою фотохостингу є зручність демонстрації розміщених фотографій. Відеохостинг набирає популярності у зв'язку з розвитком широкосмугового доступу в інтернет;

6) віртуальна служба знайомств являє собою інтернет-сервіс, який надає послуги віртуального знайомства користувачів з метою спілкування, створення родини, відносин та ін. Під час використання віртуальної служби знайомств користувач створює анкету, в якій зазначає свій псевдонім та інші параметри (стать, вік, мету знайомства, інтереси, фотографії). Після реєстрації користувач може спілкуватися з іншими користувачами, отримувати повідомлення і відповідати на них;

7) геосоціальні мережі – це різновид соціальних мереж, в яких користувачі залишають дані про своє місцезнаходження, що дає змогу об'єднувати і координувати їх дії на підставі інформації про те, які люди присутні в тих чи інших місцях, які події там відбуваються.

До найпоширеніших соціальних мереж, які можуть бути цікавими для добування персональних відомостей, можна віднести: Facebook; Twitter; Instagram; Google+; LinkedIn; Badoo; Livejournal; «ВКонтакте», «Одноклассники», а також відеохостинг YouTube та медійний застосунок ТікТок.

Загальновідомим прикладом використання OSINT не державними установами, а, наприклад, волонтерською спільнотою, є проєкти «Інформнапалм», «Миротворець» та «Bellingcat».

Для здійснення SOCMINT необхідно дотримуватися загальних підходів, а саме:

– володіти навичками роботи із програмним забезпеченням збирання та аналізу постів у Facebook, Twitter та зарубіжних регіональних соціальних мережах;

– вільно володіти мовою досліджуваних соціальних мереж;

– зосереджуватися на постах, викладених у заданий період часу із заданого географічного району;

– виявляти зв'язки автора конкретного допису з іншими користувачами соціальної мережі, а також встановлювати фізичне місцезнаходження його контактів.

Моніторинг соціальних медіа є роботою з великими об'ємами інформації, тому для полегшення застосовують різні допоміжні сервіси. Є низка доступних сервісів для ефективного моніторингу соціальних медіа, серед яких найбільше використовують такі:

1. Seesmic – безкоштовний сервіс моніторингу соціальних медіа. Підтримує моніторинг таких ресурсів, як: Twitter, Facebook, LinkedIn, Chatter, GoogleBuzz, Ping.fm. Наявні додатки як для веб, так і для персонального комп'ютера, iPhone, Android, Windows Mobile.

2. Socialmention – платформа безкоштовного пошуку та аналізу інформації в соціальних мережах. Система веде пошук згадок в обраних мережах або в усіх мережах відразу. Надає аналіз частоти згадувань, пов'язані ключові слова, популярні джерела та багато іншого. Охоплення системи – більш 100 соціальних медіа, включно із соціальними мережами, соціальними закладками, блогами, форумами тощо.

3. Hootsuite – багатофункціональний сервіс для роботи з соціальними медіа. Система Hootsuite дає змогу працювати з обліковими записами Twitter, Facebook, LinkedIn, MySpace і Foursquare, з блогами на WordPress. Сервіс Hootsuite є сертифікованим партнером Twitter. Забезпечує відправлення повідомлень за розкладом, можливість відстежувати їх за ключовими словами і згадками. Система Hootsuite також надає повноцінну інтеграцію з Facebook. Система Hootsuite умовно-платна. Доступна на мобільних платформах: iPhone, Android. Усі мобільні програми безкоштовні.

4. Socialbakers – сервіс збору статистики про роботу соціальних мереж. Система Socialbakers відома своїми рейтингами брендів на Facebook у різних категоріях. Крім Facebook, сервіс Socialbakers надає можливість безкоштовного моніторингу інформації в таких мережах, як Twitter, Google+, LinkedIn.

5. SocialSeek – простий у використанні безкоштовний сервіс моніторингу кількох соціальних медіа в режимі реального часу. Забезпечує пошук у новинах, блогах, Twitter, Facebook, Youtube.

6. Socialpointer – простий сервіс моніторингу в соціальних мережах, новинах, блогах.

7. PeerIndex – безкоштовний сервіс аналізу соціальних медіа Twitter, Facebook, LinkedIn. Визначає розміри «соціального капіталу» або впливовості компанії, професіонала, публікації та ін.

8. PostRank – сервіс компанії Google, що дає змогу в режимі реального часу аналізувати інформацію за темами, тенденціями, подіями, що мають відношення до особи чи бізнесу.

9. Topsy – безкоштовний сервіс пошуку в режимі реального часу з соціальних медіа.

10. HowsSciable (howsociable.com) – безкоштовний інструмент моніторингу брендів і ключових слів у 32 соціальних мережах.

11. Twitalyzer – аналітична програма-клієнт для Twitter, яка дає змогу відстежувати кількість переходів, аналізувати позитивні й негативні коментарі, сегментувати аудиторію. Програма інтегрована з системою GoogleAnalytics, виводить інтерактивні діаграми та має графічні інструменти.

12. WildFire – багатофункціональний онлайн-сервіс для комерційного медіамаркетингу в соціальних мережах, містить інструмент WildFire Messages, призначений для створення, моніторингу та управління повідомленнями. Створює можливість налаштувати відкладене відправлення повідомлень у соціальні мережі за розкладом.

13. Kurrently – безкоштовна пошукова система за соціальними мережами Twitter та Facebook, яка дає можливість відстежувати і поширювати цільову інформацію з соціальних мереж.

14. Trackur – комерційний онлайн-інструмент моніторингу та аналізу соціальних медіа. Дає змогу відслідковувати репутацію брендів за новинними веб-сайтами, блогами, форумами, соціальними мережами Twitter, Google+ та Facebook.

15. Semantic Force – сервіс, що забезпечує моніторинг неструктурованих джерел-коментарів у мережевих ЗМІ та інтернет-магазинах. Сервіс видає понад 20 видів аналітичних звітів.

Сервіс Semantic Force інтегрований із зовнішніми системами: Klout, Copiny, Google Analytics.

16. Tweet Deck – безкоштовний кросплатформений додаток для управління і відстеження повідомлень у соціальних мережах Twitter, Facebook, MySpace, LinkedIn. Підтримує багатоканальний інтерфейс, фільтри, у тому числі за ключовими словами.

Крім того, для аналізу та верифікації інформації (даних) в інтересах OSINT використовують програмні засоби (сервіси) за напрямами:

– верифікація (перевірка на достовірність) фото і відео;

– візуалізація (інфографіка);

– автоматизований аналіз текстових даних;

– встановлення автора (першоджерела) зображення (відео);

– підтвердження місця, дати і приблизного часу, коли зображення (відео) було отримано або зафіксовано;

– підтвердження, що зображення (відео) є саме тим, що позначено (запропоновано) до розгляду.

У залежності від завдання щодо обробки інформації (даних), зокрема їх аналізу та верифікації в інтересах розвідувального забезпечення ведення операцій сил оборони, рекомендується використовувати такі наявні програмні засоби та інтернет-сервіси для виконання завдань:

1) верифікації (перевірка на достовірність) фото і відео – програмні сервіси Exif Viewer, FotoForensics, ImgOps, TinEye, YouTube data viewer;

2) верифікації деякої текстової інформації – програмні сервіси Trooclick, Snopes, FactCheck.org, Detecting Fake News;

3) візуалізації – програмні сервіси Google Data Studio, Power BI, Tableau, ChartBlocks, Plotly, Infogram; інфографіки – програмні сервіси Canva, Piktochart, Snappa, Easel.ly, Draw.io;

4) автоматизованого аналізу текстових даних – програмні сервіси GATE, KNIME, RapidMiner.

Підсумовуючи викладене, варто наголосити, що добування розвідувальних відомостей від місцевого населення та з відкритих джерел інформації є невід'ємною складовою розвідувальної діяльності. Ці процеси допомагають розвідувальним підрозділам мати повне уявлення про обстановку, забезпечують оперативність та точність розвідувальних відомостей, що, зі свого боку, сприяє успішному виконанню завдань із забезпечення національної безпеки формуваннями НГУ.

Висновки

Досвід організації та здійснення заходів особової розвідки в інтересах розвідувального забезпечення операцій угруповання військ сил оборони держави з відбиття агресії російської федерації дає підстави сформувати висновки про те, що розвідка за відкритими джерелами, зокрема дії населення щодо документування та поширення інформації про дії противника, суттєво сприяють підвищенню спроможностей розвідувального забезпечення операцій сил оборони у воєнний період.

Водночас основними умовами ефективного використання отриманої розвідувальної інформації в органах управління Національної гвардії України є:

– створення систем аналізу інформації та єдиного центру її обробки;

– скорочення часу проходження інформації від першоджерела до центру обробки;

– забезпечення належної якості первинної обробки інформації (фото-, відеофіксація тощо);

– спроможність органів управління приймати, обробляти та використовувати зазначену інформацію.

Подальший розвиток спроможностей особової розвідки в Національній гвардії України можливий такими шляхами:

– створення програмного забезпечення із захищеними каналами передачі даних, які доступні для використання на поширених абонентських телекомунікаційних пристроях (терміналах) на базі Android, IOs, Windows, із вбудованою функцією швидкого видалення цього програмного забезпечення та слідів передачі даних;

– розгортання резервних мереж передачі даних, наприклад, Starlink, на випадок знищення (подавлення) основних телекомунікаційних мереж;

– впровадження систем інтелектуального розпізнавання даних у роботу центрів збору та обробки інформації: фото-, відео- зокрема, розпізнавання облич, техніки, місцевих орієнтирів, форм документів тощо.

Напрямком подальшого дослідження є визначення та обґрунтування організаційно-штатної структури, завдань і функцій підрозділів особової розвідки формувань Національної гвардії України для проведення розвідувальних дій у сучасних умовах.

Перелік джерел посилання

1. Кожушко О. С. Розвідка відкритих джерел інформації (OSINT) у розвідувальній практиці США. *Науковий вісник Інституту міжнародних відносин Національного авіаційного університету*. Київ. 2011. № 4 (2). С. 68–74.

2. Бурба В. В. Організаційно-правові засади використання розвідки з відкритих джерел інформації (OSINT) в діяльності розвідувальних служб європейських країн. *Навчально-науковий інститут перепідготовки та підвищення кваліфікації кадрів Служби безпеки України.* Київ. 2019. № 11. Ч. 1. С. 11–19.

3. Муравська Ю. Парадигма розвитку військової розвідки в Україні. *Західноукраїнський національний університет*. Тернопіль. 2022. № 4. С. 102–106.

4. Минько О. В., Іохов О. Ю., Оленченко В. Т., Власов К. В. Використання технологій OSINT для отримання розвідувальної інформації. *Полтавський національно-технічний університет імені Юрія Кондратюка*. Полтава. 2016. Вип. 4. С. 81–84.

5. Лисенко С. В., Ковтонюк Д. О., Афанасьєв В. В., Кузнецов В. В. Проблемні питання виконання завдань розвідки частинами та підрозділами Національної гвардії України в антитерористичній операції. *Національна академія Національної гвардії України*. Харків. 2015. № 1 (52). С. 53–57.

6. Військовий стандарт 01.101.006. Воєнна розвідка. Військова розвідка. Терміни та визначення. Міністерство оборони України. Київ. 2020.

7. Бомбардування торгового центру «Retroville» у Києві. Електронна енциклопедія Wikipedia. URL : http://surl.li/fsayl (дата звернення: 12.06.2023).

8. Розвідка на основі відкритих джерел. Електронна енциклопедія Wikipedia. URL: http://surl.li/erhcx (дата звернення: 12.06.2023).

Стаття надійшла до редакції 09.07.2023 р.

UDC 355.4

V. Butuzov, D. Kovtoniuk, I. Luhovskyi

SPECIFIC FEATURES OF ORGANIZATION AND CONDUCTING OF PERSONAL INTELLIGENCE BY INTELLIGENCE UNITS OF THE NATIONAL GUARD OF UKRAINE DURING PARTICIPATION IN COUNTERING ARMED AGGRESSION

The article examines the peculiarities of organization and conduct of personal intelligence by the defense forces of Ukraine based on the analysis of experience in performing reconnaissance tasks during the repulsion of full-scale armed aggression by the russian federation. It clarifies the list of main tasks of personal intelligence in modern conditions and discusses the problematic issues related to the collection of intelligence information from the local population. It describes general approaches to obtaining information through the analysis of social media and monitoring services used for this purpose. Furthermore, it outlines the ways to further develop the capabilities of personal intelligence within the National Guard of Ukraine.

Personal intelligence, in this article, refers to a complex of measures and actions carried out by designated units using methods of acquiring information from human resources (sources) in order to provide intelligence information to military command (staff) for the purpose of preparing and conducting combat (special) operations by military units (subunits) of the defense forces of Ukraine. It provides detailed information that helps confirm or refute intelligence information, enables obtaining answers to specific questions, and increases the reliability of information used by defense management authorities for decision-making.

Conducting personal intelligence through obtaining information from the local population is one of the effective methods of collecting intelligence information in dynamic combat situations. This approach involves interacting with individuals residing in territories occupied by the enemy or having access to valuable information concerning enemy actions, population attitudes, significant events, and other intelligence-relevant aspects.

In addition to obtaining information from the local population, gathering intelligence from open sources is a particular tool that helps collect valuable data for the effective execution of reconnaissance tasks by intelligence units within the National Guard of Ukraine formations.

The acquisition of intelligence information from the local population and open sources is an integral component of reconnaissance activities. These processes assist reconnaissance units in having a comprehensive understanding of the situation, ensuring the timeliness and accuracy of intelligence information, thereby contributing to the successful accomplishment of tasks and ensuring national security by the National Guard of Ukraine formations.

The experience of organizing and conducting personal intelligence activities to provide reconnaissance support for operations of the defense forces in countering the aggression of the russian federation allows drawing conclusions that intelligence from open sources, including the actions of the population regarding documenting and disseminating information about enemy activities, significantly contributes to enhancing the capabilities of reconnaissance support for defense operations in repelling armed aggression.

Keywords: *armed aggression, intelligence information, personal intelligence, intelligence support of operations, network reconnaissance.*

Бутузов Віталій Юрійович – ад'юнкт Національної академії Національної гвардії України
https://orcid.org/0000-0002-6909-424X

Ковтонюк Денис Олегович – кандидат військових наук, начальник відділу розвідки штабу Північного Київського територіального управління Національної гвардії України
https://orcid.org/0000-0002-1884-5744

Луговський Ігор Станіславович – кандидат військових наук, доцент, доцент кафедри оперативного та логістичного забезпечення Національної академії Національної гвардії України
https://orcid.org/0000-0001-5052-322X