У чинному законодавстві України наявні проблеми із визначенням співвідношення й розмежуванням оперативно-розшукової, розвідувальної та контррозвідувальної діяльності. Так, функція забезпечення національної безпеки від зовнішніх загроз покладається на розвідувальні органи, що визначено Законом України «Про розвідувальні органи України». Коли мова йде про легендоване введення оперативного працівника у злочинну організацію, то такі заходи є розвідувальними по суті й за призначенням, але проводяться в рамках оперативно-розшукової діяльності. Ба більше, існує точка зору, що сучасний кримінальний аналіз (КА), використовуючи і методи розвідки, фактично перетворюється в останню, адже практична модель кримінальної розвідки (КРР) включає пошук інформації, її узагальнення й аналіз, використання одержаних даних для пошуку нової інформації та її перевірки, подальший аналіз тощо.

Крім того, розбіжності у тлумаченні змісту КРР існують у вітчизняній науці. Кримінальна розвідка, наприклад, розглядається як одна із функцій оперативно-розшукової діяльності та реалізується шляхом використання системи розвідувальних, пошукових, інформаційно-аналітичних заходів, у т.ч. із застосуванням оперативних та оперативно-технічних засобів, спрямованих на своєчасне виявлення та нейтралізацію реальних і потенційних кримінальних загроз суспільній безпеці. З іншої точки зору, КРР трактується як різновид розвідувальної діяльності, форма прихованого розслідування, комплекс гласних і негласних, оперативно-розшукових, інформаційно-аналітичних заходів. Узгодження в концептуальному, нормативному й практичному вимірах співіснування ОРД та новітніх модельних форм правоохоронної діяльності важливе для широкої сфери правоохоронних та спеціальних органів (служб) України. З цього випливає необхідність понятійного й нормативного визначення ієрархії (співвідношення): ОРД як такої та кримінальної розвідки; правоохоронної та розвідувальної діяльності; КРР та оперативного обслуговування; кримінального аналізу та інших видів розвідувального й інформаційного забезпечення правоохоронної діяльності, де кримінальний аналіз виступає більш широкою сферою і поглинає кримінальну розвідку як таку.

***Датчук Денис,***
*ад'юнкт докторантури та ад'юнктури,*
*Національна академія Національної гвардії України*

***Луговський Ігор,***
*кандидат військових наук, доцент,*
*Національна академія Національної гвардії України*

## РЕЗУЛЬТАТ РАНЖИРУВАННЯ ФАКТОРІВ, ЩО ВПЛИВАЮТЬ НА РОЗВІДУВАЛЬНЕ ЗАБЕЗПЕЧЕННЯ ФОРМУВАНЬ НАЦІОНАЛЬНОЇ ГВАРДІЇ УКРАЇНИ В СУЧАСНИХ УМОВАХ

В умовах збройної агресії російської федерації проти України значно зросла роль та значення розвідувального забезпечення у діяльності формувань Національної гвардії (далі – НГ) України. Розвідувальне забезпечення (далі – РЗ)

в умовах воєнного стану стало ключовим елементом у системі управління та прийняття рішень, оскільки саме своєчасне, достовірне та повне розвідувальне забезпечення дозволяє ефективно здійснювати планування та реалізацію службово-бойових завдань.

Аналіз сучасного стану РЗ показав, що формування НГ України потребують адаптивної, гнучкої та технологічно підготовленої системи збору, обробки та передачі розвідувальної інформації. Основними чинниками, що обумовлюють необхідність удосконалення цієї системи, є високий динамізм бойових дій, широке застосування противником засобів РЕР і РЕБ, кіберзагроз, а також багаторівнева міжвідомча взаємодія з іншими компонентами сектору безпеки і оборони України.

Метою проведеного дослідження стало системне виявлення та ранжування факторів, які впливають на РЗ формувань НГ України. Для цього було визначено 30 факторів, згрупованих у три рівні: макрофактори (зовнішнє середовище), мезофактори (взаємодія підрозділів і органів управління), мікрофактори (внутрішня організація та ресурси).

У ході дослідження було застосовано метод експертного оцінювання з подальшим апріорним ранжуванням (далі – МАР). Коефіцієнт конкордації Кендалла, розрахований у програмному середовищі Excel, дозволив оцінити рівень узгодженості думок експертів та достовірність отриманих результатів. За результатами експертного оцінювання виділено 20 найбільш значущих факторів та з використанням МАР визначено їх місце серед найбільшвпливових факторів. До найважливіших було віднесено: рівень технологічного розвитку, доступність цифрових технологій та платформ, наявність резерву фахівців і засобів, а також часові ресурси на підготовку до розвідки.

Натомість менш значущими було визначено: організаційно-штатну структуру органів розвідки, чинну нормативно-правову базу та ступінь формалізації потреб споживачів розвідувальної інформації. Це вказує на те, що сучасне РЗ потребує не лише вдосконалення структури, а й інноваційного підходу до технологій збору та аналітики даних.

Особливої уваги заслуговує пропозиція щодо впровадження елементів штучного інтелекту (далі – ШІ) у РЗ. Застосування інтелектуальних систем уможливлює автоматичне виявлення загроз, формування прогнозів розвитку ситуації, оперативну обробку великих обсягів інформації в реальному часі. Пропонується визначення ШІ у системі РЗ – це комплекс інтелектуальних цифрових технологій, здатних автоматично обробляти великі масиви інформації, виявляти загрози, прогнозувати розвиток оперативної обстановки та приймати рішення з мінімальним впливом людського чинника. Такі системи працюють безперервно, здатні до самоосвіти та удосконалення під час виконання завдань, що забезпечує високу адаптивність до змін у бойовому середовищі.

В умовах гібридної війни впровадження ШІ у розвідувальні підрозділи НГ України значно підвищує ефективність добування, оброблення та використання РІ. З позиції оперативного планування впровадження ШІ дозволить підвищити темпи прийняття рішень, зменшити вплив людського фактора та підвищити стійкість до інформаційного впливу з боку противника. Крім того, сучасні алгоритми машинного

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).