Проте в усіх цих випадках надзвичайно важливо дотримуватися етичних стандартів та захищати особисті дані. Забезпечення конфіденційності та приватності даних важливо не лише з етичних міркувань, але й для запобігання можливим репресіям і діям, які порушують права людини. Загалом, використання інструментів OSINT в умовах воєнного конфлікту може виявитися вирішальним чинником для прийняття правильних військових стратегічних та тактичних рішень. Швидке отримання, аналіз та використання критично важливої інформації може забезпечити ефективну відповідь на виклики воєнного конфлікту.

Список використаних джерел:

1. Розвідка на основі відкритих джерел. Інформаційний Інтернет-ресурс Вікіпедія. URL: https://uk.wikipedia.org/wiki/Розвідка_на_основі_відкритих_джерел (дата звернення: 17.04.2024).

2. Що таке OSINT і як він допоміг викрити вбивства у Бучі. Explainer - пояснюємо новини. Інформаційний Інтернет-ресурс URL: https://explainer.ua/shho-take-osint-i-yak-vin-dopomig-vikriti-vbivstva-u-buchi/ (дата звернення: 17.04.2024).

Грянко Анна Георгіївна
студентка 102 БПМС навчальної групи ННІ № 1 НАВС

Науковий керівник:
Яровий Кирило Васильович
кандидат юридичних наук, старший викладач кафедри інформаційних технологій та кібербезпеки ННІ № 1 НАВС, капітан поліції

АНАЛІЗ ПРОБЛЕМ ІНФОРМАЦІЙНОГО ЗАБЕЗПЕЧЕННЯ У ХОДІ ВОЄННОГО ЧАСУ

Інформаційне забезпечення відіграє вирішальну роль під час ведення бойових дій. Своєчасний доступ до достовірної та актуальної інформації є критично важливим для прийняття правильних рішень і досягнення перемоги. Однак у ході війни виникають численні проблеми, пов’язані з інформаційним забезпеченням, які можуть серйозно вплинути на хід бойових дій.

Під інформаційним забезпеченням розуміється комплекс заходів щодо збору, обробки, зберігання, поширення та захисту інформації, необхідної для планування, підготовки та ведення військових операцій. Воно охоплює різноманітні аспекти, починаючи від технічного та програмного забезпечення систем зв’язку та інформаційних мереж і завершуючи підготовкою

висококваліфікованого персоналу, здатного ефективно працювати з величезними масивами даних. Незважаючи на те, що зазначену проблематику вивчали В. Богуш, О. Юдін, Я. Варивода, І. Воробйова, Б. Грушин, Д. Думанський та інші. Проте, порушене питання залишається актуальним.

У сучасних реаліях, коли війни все частіше ведуться не лише на фізичному, а й на інформаційному та кіберпросторі, забезпечення надійного інформаційного супроводу військових дій стає одним із визначальних чинників успіху [1, с. 69]. Проте, на цьому шляху постають численні проблеми та виклики, які необхідно вчасно виявляти та знаходити шляхи їх розв'язання.

Аналізуючи наукові статті та праці науковців виокремлюють такі проблеми:

1. Забезпечення безпеки інформації. Одна з найбільших проблем інформаційного забезпечення під час війни – це забезпечення безпеки інформації. Витік конфіденційних даних може поставити під загрозу безпеку військових операцій, життя солдатів та цивільного населення. Зловмисник може використовувати зазначену інформацію для планування контратак, саботажу чи дезінформації [2, с. 39].

2. Управління великими обсягами інформації. Під час війни генерується величезна кількість інформації з різноманітних джерел, таких як розвідувальні дані, поля бою, цивільні та інші джерела. Управління цими великими масивами даних, їх збір, обробка, аналіз та розповсюдження є складним завданням, особливо в умовах обмеженого часу та ресурсів.

3. Забезпечення достовірності та актуальності інформації. У ході війни інформація може бути спотворена, неповною або застарілою. Дезінформація та пропаганда можуть бути використані противником для введення в оману та дезорієнтації. Забезпечення достовірності та актуальності інформації є критично важливим для прийняття правильних рішень [3, с. 32].

4. Інтеграція різнорідних систем. Сучасні збройні сили використовують різноманітні системи та платформи для збору, обробки та передачі інформації. Інтеграція цих різнорідних систем для забезпечення ефективного обміну інформацією та співпраці є складним завданням.

5. Забезпечення безперервності зв'язку. Під час бойових дій комунікаційні лінії та інфраструктура можуть бути пошкоджені або виведені з ладу. Забезпечення безперервності зв'язку та передачі інформації в таких умовах є критично важливим для координації дій та прийняття рішень [4, с. 167].

Підсумовуючи, слід зазначити, що сучасні війни висувають надзвичайно високі вимоги до систем інформаційного забезпечення та підкреслюють їхню критичну важливість для успішного ведення військових операцій. Серед ключових проблем, що постають на цьому шляху, можна виділити загрози інформаційній безпеці та кібербезпеці, складність управління величезними потоками даних, технічну застарілість наявних систем та недостатню кваліфікацію персоналу.

Для вирішення зазначених проблем необхідно вжити комплекс заходів.

По-перше, потрібно удосконалити законодавче регулювання у сфері інформаційного забезпечення та привести нормативно-правову базу у відповідність із сучасними вимогами. *По-друге*, життєво необхідною є масштабна модернізація технологічної інфраструктури, впровадження новітнього обладнання та програмного забезпечення. *По-третє*, має бути створена єдина універсальна інформаційна система управління ресурсами, яка б об'єднувала всі задіяні у військових діях сили та засоби.

Нарешті, надзвичайно важливим є підвищення кваліфікації персоналу, задіяного в інформаційному супроводженні військових операцій, розширення можливостей для фахового навчання, обміну досвідом та залучення провідних експертів цієї галузі. Лише за умови комплексного підходу до вирішення існуючих проблем можна сподіватися на побудову надійної та дієвої системи інформаційного забезпечення військових дій.

Забезпечення доступу до надійної та актуальної інформації для правоохоронних органів, співпраця між ними на національному та міжнародному рівнях, а також використання передових технологій інформаційної безпеки є важливими складовими ефективної системи правоохоронного заходу. Розвиток інформаційних технологій та постійне удосконалення процесів обробки та аналізу даних мають визначальне значення для підвищення ефективності правоохоронної діяльності та забезпечення гармонійного розвитку суспільства [5, с. 106].

Варто розуміти, що виклики у сфері інформаційного супроводження війн будуть постійно зростати у міру розвитку новітніх технологій та еволюції стратегій ведення конфліктів. Тому потрібно не лише швидко реагувати на поточні проблеми, а й розробляти довгострокові перспективні рішення для забезпечення стабільної переваги у цій критично важливій сфері.

Список використаних джерел:

1. Дубов Д. В. Кіберпростір як новий вимір геополітичного суперництва : монографія / Д. В. Дубов. – К.: НІСД, 2014. – 328 с.

2. Адміністративно-правове забезпечення інформаційної гігієни під час воєнного стану в Україні / Євген Володимирович Курінний // Науковий вісник Дніпропетровського державного університету внутрішніх справ. – 2023. – № 1 (122). – С. 38-43.

3. Дезінформація як загроза національній безпеці Європейського Союзу: проблеми та підходи / Оксана Звоздецька // Історико-політичні проблеми сучасного світу. – 2021. – Т. 43.– С. 30-39.

4. Інформаційна безпека людини: теорія і практика: монографія. – Київ: ТОВ «Видавничий дім «АртЕк», 2018 – 446 с.

5. Кудінов В. А., Яровий К. В. Інформаційне забезпечення правоохоронної діяльності: навч.-практ. посіб. Київ: Нац. акад. внутр. справ, 2024. 120 с.