А. Валюх
(ГО «Наука, інновації та розвиток»)

ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЕРЖАВИ В УМОВАХ ВІЙНИ: ОСНОВНІ ІНСТРУМЕНТИ ТА МІЖНАРОДНИЙ ДОСВІД

Інформаційна безпека є критично важливим елементом національної безпеки України, особливо сьогодні, в умовах війни. В сучасних війнах інформація стає такою ж важливою зброєю, як і традиційні види озброєння. Успішне забезпечення інформаційної безпеки держави потребує комплексного підходу, що включає правові, технічні, економічні й організаційні заходи. Збереження секретності даних під час війни є критично важливим для національної безпеки, оскільки інформація може визначати хід бойових дій, стратегічні рішення та моральний дух як військових, так і цивільного населення. Витік секретних даних може призвести до серйозних наслідків, включаючи втрату військових позицій, знищення критичної інфраструктури та загрозу життю військовослужбовців і мирних жителів (Rid, T., 2020).

Сучасні війни ведуть не лише на полі бою, а й у кіберпросторі. Ворог використовує методи кібератак, шпигунства та дезінформації задля отримання стратегічної переваги. Тому держава повинна застосовувати передові технології шифрування, захищені комунікаційні канали та системи контролю доступу до конфіденційної інформації (Якимчук А., Валюх А., Пахаренко О, 2020; Yakymchuk A.,Valyukh A. et al., 2020). Окрім технічних заходів, важливу роль відіграє підготовка персоналу, який працює з чутливими даними. Недбале поводження з інформацією або її витік через соціальну інженерію можуть мати катастрофічні наслідки (Цимбалюк В. В., 2020). Захист секретних даних забезпечує ефективність військових операцій, мінімізує ризики та сприяє стратегічній стабільності держави. Саме тому в умовах війни контроль за інформацією стає ключовим елементом загальної безпеки.

У даному дослідженні узагальнено основні інструменти забезпечення інформаційної безпеки, які варто застосувати в Україні. Серед них як найважливіші пропонується виділити такі:

1.*Законодавче регулювання.* Прийняття та вдосконалення законодавчих актів щодо протидії інформаційним загрозам. Тут важливим аспектом залишається запровадження санкцій за поширення дезінформації та колабораціонізм в інформаційній сфері.

2.*Кібербезпека.* Захист критичної інформаційної інфраструктури від кібератак, використання системи моніторингу та виявлення кіберзагроз, співпраця з міжнародними партнерами у сфері кібербезпеки.

3.*Протидія дезінформації.* Створення центрів стратегічних комунікацій для оперативного реагування на інформаційні атаки, використання фактчекінгових платформ для виявлення й спростування фейкових новин.

4.*Розвиток національних медіа.* Підтримка незалежних національних ЗМІ та створення державних платформ задля поширення достовірної інформації, посилення державного мовлення та інформаційного впливу за кордоном.

5.*Освітні й інформаційні кампанії.* Підвищення медіаграмотності населення, проведення навчальних програм щодо інформаційної безпеки для державних службовців та військових.

У даному дослідженні узагальнено міжнародний досвід у сфері дотримання військової безпеки та проаналізовано основі її інструменти (таб. 1).

Таблиця 1.

Інструменти забезпечення військової безпеки

Держава	Основні інструменти інформаційної безпеки	Електронне врядування	Захист секретних даних
США	Агентство CISA, закони проти дезінформації, кібербезпека	Програми цифрової безпеки та кіберзахист урядових установ	Класифіковані урядові мережі, система Secure Compartmented Information Facility (SCIF)
ЄС	EUvsDisinfo, Європейський акт про цифрові послуги	Платформи відкритих даних, регулювання соцмереж	Загальноєвропейські стандарти шифрування, GDPR
Естонія	Кібербезпека, Центр передового досвіду НАТО	Електронний уряд (e-Estonia), ID-карти, онлайн-голосування	X-Road для захищеного обміну даними, резервні сервери в інших країнах
Ізраїль	Кібердиректорат, штучний інтелект у боротьбі з дезінформацією	Розвинена система електронного управління та кіберзахисту	Використання технологій ізраїльських кіберкомпаній, багаторівневі захисні протоколи
Україна	Кіберполіція, Центр протидії дезінформації, стратегічні комунікації ЗСУ	Дія, електронні сервіси держуправління	Кіберзахист військових мереж, співпраця з НАТО у сфері інформаційної безпеки

Розвинені держави світу давно використовують інноваційні інструменти захисту даних. Наприклад, Ізраїль здійснював користання національного кібердиректорату для координації інформаційної безпеки. Тут було створено розвинену систему кіберрозвідки й оперативного реагування на загрози. Нині країна активно застосовує штучний інтелект для виявлення й нейтралізації дезінформації. У Ізраїлі добре налагоджена співпраця між військовими, урядом та приватним сектором у сфері інформаційної безпеки (Rid, T., 2020).

США мають багатий досвід у забезпеченні секретності військових даних, зокрема через ретельну систему класифікації інформації. Важливі військові дані, такі як стратегії, плани операцій, технології та розвідка, зазвичай поділяють на кілька рівнів секретності: «confidential» (конфіденційно), «secret» (таємно) і «top secret» (цілком таємно). Кожен рівень передбачає відповідні заходи з обмеження доступу, контролю та захисту інформації (Stengel, R., 2019). Інститут Національної Безпеки (NSA) та Міністерство оборони США активно використовують сучасні технології шифрування і кібербезпеки для захисту даних від кібернападів і несанкціонованого доступу. Важливу роль в цьому процесі відіграють навчання і сертифікація військових і співробітників розвідувальних служб з питань безпеки. Тут функціонує Агентство з кібербезпеки та безпеки інфраструктури (CISA).Законодавство щодо боротьби з дезінформацією та кібератаками досить ґрунтовне (Nye, J. S., 2011).

Досвід США включає й інтенсивну співпрацю з союзниками в рамках НАТО та інших міжнародних організацій для забезпечення безпеки спільної військової інформації. Однак існують і випадки витоків інформації, як, наприклад, скандал з Едвардом Сноуденом, який став важливим уроком щодо необхідності посилення контролю та аудитів безпеки військових даних.

У Європейському Союзі діють різноманітні програми боротьби з фейковими новинами, такі як EUvsDisinfo. Тут запроваджено Європейський акт про цифрові послуги для регулювання соціальних мереж (Stengel, R., 2019). У Естонії створено потужну кібербезпекову інфраструктуру, а також функціонує Центр передового досвіду НАТО з питань кібероборони (CCDCOE) (Rid, T., 2020).

Висновки. Забезпечення інформаційної безпеки держави в умовах війни є багатокомпонентним процесом, що потребує комплексного підходу. Використання ефективних інструментів, таких як законодавче регулювання, кібербезпека, боротьба з дезінформацією та міжнародна співпраця, дозволяє мінімізувати інформаційні загрози. Досвід таких країн, як Ізраїль, США, Естонія та держави ЄС, демонструє важливість поєднання правових, технічних та освітніх заходів у сфері інформаційної безпеки.

Список використаних джерел

1. Nye, J. S. (2011). The Future of Power. PublicAffairs. P. 45-78.
2. Rid, T. (2020). Active Measures: The Secret History of Disinformation and Political Warfare. Farrar, Straus and Giroux. P. 102-134.
3. Stengel, R. (2019). Information Wars: How We Lost the Global Battle Against Disinformation and What We Can Do About It. Grove Press. P. 56-89.
4. Цимбалюк В. В. (2020). Інформаційна безпека держави: теоретико-правові засади. Київ: Видавничий дім "Юридична думка". С. 23-47.
5. Національна стратегія кібербезпеки України (2021). С. 5-30.
6. Yakymchuk A.,Valyukh A. et al. (2020). Public Administration and Economic Aspects of Ukraine’s Nature Conservation in Comparison with Poland. In: Kantola J., Nazir S., Salminen V. (eds) Advances in Human Factors, Business Management and Leadership. AHFE 2020. Advances in Intelligent Systems and Computing, vol 1209. Springer, Cham. Online 978-3-030-50791-6. Scopus.
7. Якимчук А.Ю., Валюх А.М., Пахаренко О.В. Стратегія інформаційного забезпечення управління еколого-економічною безпекою України в умовах військово-політичної нестабільності. Монографія. Рівне: НУВГП, 2020. 154 с.