ОСОБЛИВОСТІ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЕРЖАВИ В УМОВАХ ЗБРОЙНОЇ АГРЕСІЇ

Світличний В. [1], Матвійчук А.[1]

[1]*Харківський національний університет внутрішніх справ, e-mail: vit.svet@ukr.net*

Вступ

В умовах сучасної війни інформаційна безпека набуває такого ж критичного значення, як оборона територій чи забезпечення матеріально-технічної спроможності армії. Інформаційна сфера стала самостійним полем бою, де вирішуються питання морального духу населення, міжнародної підтримки, ефективності управління та спроможності держави протидіяти ворожим впливам. У випадку України, яка з 2014 року перебуває в стані гібридної війни, а з 2022 року – у стані повномасштабної збройної агресії з боку Російської Федерації, питання забезпечення інформаційної безпеки постало з особливою гостротою.

Викладення основного матеріалу

Сутність інформаційної безпеки держави в умовах війни полягає в захисті критичної інформаційної інфраструктури, протидії дезінформації, збереженні стійкої комунікації між органами влади, військовими та суспільством, а також у захисті інформаційних прав громадян. В умовах воєнного стану інформаційний простір зазнає потужного тиску – як з боку ворожих інформаційно-психологічних операцій (ІПсО), так і в результаті кібератак на державні ресурси, мережі енергетики, транспорту, банківської системи.

Однією з ключових особливостей забезпечення інформаційної безпеки в умовах збройної агресії є необхідність швидкого реагування на зміну обстановки. Інформаційні загрози часто є динамічними, комплексними

та непередбачуваними. Це вимагає від державних органів створення гнучких систем моніторингу, виявлення загроз, оперативного аналізу інформаційного середовища та координації дій між усіма безпековими структурами.

Надзвичайно важливу роль відіграє інформаційна протидія ворогу. Росія системно використовує пропаганду, фейки, маніпуляції, підроблені документи та змонтовані відео для дестабілізації ситуації, сіяння паніки та розколу в українському суспільстві. У відповідь Україна реалізує заходи із забезпечення прозорості, оперативної публічної комунікації, перевірки фактів (fact-checking) та централізації офіційної інформації. Створення та робота таких ресурсів, як «Єдиний портал правди», Офіс стратегічних комунікацій, кіберполіції та спецпідрозділів СБУ, дозволяє значно ефективніше протидіяти інформаційним атакам.

Ще однією важливою особливістю є підвищена вразливість критичної інфраструктури до кіберзагроз. Ураження серверів органів влади, систем зв'язку, реєстрів, банківської інфраструктури – усе це може призвести до паралічу управління державою. Тому основними завданнями в цій сфері є забезпечення безперервності роботи інформаційних систем, впровадження засобів шифрування та резервного копіювання, розподіл інфраструктури на незалежні вузли, а також – створення надійних механізмів обміну інформацією між військовими, урядом та міжнародними партнерами.

Окремим напрямом є розбудова цифрової стійкості громадян. В умовах масових дезінформаційних кампаній важливо, щоб населення було здатне критично мислити, перевіряти джерела інформації, розпізнавати маніпуляції. Звідси випливає потреба в національній стратегії медіаграмотності, регулярних просвітницьких кампаніях, співпраці з журналістами та лідерами громадської думки.

Інформаційна безпека в умовах збройної агресії – це не лише технічне завдання. Це стратегічна складова національної безпеки, яка впливає на хід війни не менше, ніж успішні дії на фронті. Інформація може бути зброєю, а може бути щитом. Тому завдання держави – навчитися

ефективно нею володіти, захищати й управляти в інтересах національного суверенітету, громадянського миру та перемоги.

Важливою складовою забезпечення інформаційної безпеки держави є налагодження ефективної міжвідомчої взаємодії. В умовах воєнного стану особливої актуальності набуває координація дій між Службою безпеки України, Держспецзв'язку, Міністерством оборони, Міністерством цифрової трансформації, Національним центром оперативно-технічного управління мережами телекомунікацій та іншими структурами. Їх спільні зусилля спрямовані не лише на відбиття зовнішніх атак, але й на формування проактивної інформаційної політики, яка зміцнює єдність суспільства і довіру до державних інституцій [1].

Варто також зазначити, що війна створила унікальні умови для розвитку кіберволонтерського руху. Тисячі IT-спеціалістів об'єдналися в спільноти, які виконують завдання зі зламу ворожих ресурсів, виявлення агентурних мереж, захисту українських сайтів та баз даних, а також інформаційної протидії пропаганді на міжнародному рівні. Такий феномен самоорганізації є новим елементом інформаційної безпеки, що доповнює класичні державні підходи.

У межах міжнародної співпраці важливе значення має обмін даними та координація з партнерами з НАТО, ЄС, країн-союзників, а також із глобальними цифровими гігантами, такими як Google, Meta, Amazon Web Services. Ці партнери допомагають відбивати масштабні DDoS-атаки, відновлювати цифрову інфраструктуру, блокувати шкідливий контент і дезінформацію. Крім того, міжнародні платформи сприяють глобальному поширенню правдивої інформації про війну в Україні, що має велике значення для зміцнення підтримки з боку світової спільноти [2].

Однак, попри успіхи, залишаються проблемні питання, які потребують системного вирішення. Серед них – фрагментарність нормативно-правового забезпечення у сфері інформаційної безпеки, недостатній рівень цифрової безпеки в регіональних органах влади, слабкий рівень

медіаграмотності окремих груп населення, а також нестача висококваліфікованих фахівців у сфері кіберзахисту. Вирішення цих проблем потребує як інституційного реформування, так і довгострокових інвестицій в освіту, дослідження та цифрову інфраструктуру.

Висновки

У підсумку, можна стверджувати, що забезпечення інформаційної безпеки в умовах збройної агресії – це необхідна умова збереження державності, стабільності та перемоги у війні. Це багатовимірний процес, що включає технічні, правові, організаційні, психологічні та освітні компоненти. Український досвід опору інформаційним і кіберзагрозам в умовах війни вже сьогодні формує нові підходи до національної безпеки, які матимуть значення не лише для України, а й для всього демократичного світу.

Список використаних джерел

1. Нові правила: інформаційна безпека під час війни. Одеська національна наукова бібліотека. Офіційний веб-сайт. URL: https://odnb.odessa.ua/view_post.php? id=4286 (дата звернення: 11.05.2025).

2. Як протидіяти кіберзагрозам та захистити системи від ворожих кібератак – важливі рекомендації та допомога CERT-UA. Урядовий портал Єдиний веб-портал органів виконавчої влади України. URL: https://www.kmu.gov.ua/news/yak-protydiiaty-kiberzahrozam-ta-zakhystyty-systemy-vid-vorozhykh-kiberatak-vazhlyvi-rekomendatsii-ta-dopomoha-cert-ua (дата звернення: 11.05.2025).