DOI https://doi.org/10.30525/978-9934-26-223-4-106

ОСНОВИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЕРЖАВИ В УМОВАХ ВІЙНИ

Гбур З. В.

Постановка проблеми. В кінці XX століття інформація для кожної країни стає стратегічно важливим ресурсом, від ефективного використання якого залежить безпека держави й перспективи формування демократичного суспільства.

На тлі переходу суспільства від індустріального до інформаційного підвищується значимість вмінь орієнтуватися в постійно зростаючому потоці інформації, ефективно з нею працюючи. Можливості глобальної мережі, що активно використовуються в усіх сферах суспільного життя, ґрунтуються на інформаційних ресурсах, які представляють собою сукупність даних, які організовані в інформаційних системах для отримання достовірних даних в різних галузях знань та практичній діяльності. Однак, одночасно зі зростанням ролі інформації підвищується й важливість її захисту, яка забезпечується шляхом застосування інструментів інформаційної безпеки, зокрема, особливої актуальності дане питання набирає в умовах війни.

З розвитком та впровадженням інформаційних технологій трансформуються звичні критерії оцінки військової потужності та політичних можливостей держав світу. Видозмінюються традиційні форми силового протиборства. На перший план виходять військові дії (різні за формами та способами застосування військ), основні цілі яких досягаються за рахунок технологічних та головним чином інформаційних переваг.

Інформаційна експансія активно використовується провідними державами світу для реалізації своїх геополітичних інтересів, а оскільки геополітичні інтереси різних країн все більш жорстко стикаються на світовій арені, інформаційна боротьба в світовому просторі перетворюється в інформаційну війну.

Метою інформаційної війни є досягнення інформаційного домінування. Причиною інформаційних війн є ті ж самі принципи, що й в випадку звичайних війн. В ході інформаційної війни застосовуються активні методи трансформації інформаційного простору. Одні країни намагаються нав'язати іншим бажані типи поведінки. Інформаційні війни спрямовані на зміну поглядів, світогляду населення, підрив суспільної системи противника.

Особливого значення та актуальності в спектрі суспільних відносин набувають проблеми забезпечення інформаційної безпеки, оцінка та аналіз інформаційних загроз в контексті війни та практичне застосування інформаційного опору з метою захисту територіальної цілісності України та її суверенітету, що становить концептуальні основи діяльності суспільства.

Аналіз останніх досліджень і публікацій. Дослідженню теоретико-методологічних основ інформаційної безпеки держави присвячено наукові роботи відомих вітчизняних науковців. Серед сучасних вітчизняних дослідників хотілося б відзначити праці: О. Адамчука, Г. Атаманова, О. Бандурки, О. Барановського, А. Берко, О. Глазової, В. Гурковського, В. Домарьова, Б. Кормича, В. Ліпкана, Н. Нижник, О. Олексюка, В. Пилипчука, М. Швеця тощо. На даний час Україна перебуває в стані війни, в тому числі й інформаційної війни, все динамічнішими стають її зовнішні та внутрішні загрози, які спрямовані на зруйнування національного суверенітету та територіальної цілісності України. Отже, в умовах війни дана проблематика наукових досліджень є актуальною та своєчасною.

Метою є дослідження теоретичних аспектів інформаційної безпеки України як важливої складової національної безпеки держави в умовах війни.

Виклад основного матеріалу. В XXI столітті, яке можна назвати «інформаційним», індустріальний етап суспільного розвитку змінюється на інформатизацію, що забезпечує суспільству найбільш ефективний та динамічний розвиток на основі максимально повного використання наявних інформаційних ресурсів. Інформація стає стратегічним ресурсом суспільства та його рушійною продуктивною силою, оскільки матеріальні ресурси поступово втрачають своє значення, а на зміну їм надходять неухильно зростаючі інформаційні ресурси.

Швидкий розвиток інформаційно-комунікаційних технологій призвів до суттєвих трансформацій життя суспільства та змін наукових картин світу. Важливим економічним ресурсом визнається саме інформація. Успішному вирішенню соціально-економічних та політичних проблем сприятиме ефективна організація інформаційних процесів, що суттєво збільшить рентабельність багатьох видів діяльності.

Починаючи з XX століття поняття «інформація» розпочало своє застосування в наукових галузях та отримало значну кількість тлумачень, зокрема, інформація безпосередньо пов'язана з функцією управління та є невід'ємною властивістю кожного матеріального суб'єкта.

Як зазначає науковець О. С. Бодрук, інформація як фізична субстанція представляє собою міру неоднорідності розподілу матерії та енергії в просторі

та в часі, міру змін, якими супроводжуються всі процеси, що протікають в світі[1].

Згідно із Законом України «Про інформацію», інформація – будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді[2].

Науково-технічна інформація – будь-які відомості та/або дані про вітчизняні та зарубіжні досягнення науки, техніки і виробництва, одержані в ході науково-дослідної, дослідно-конструкторської, проектно-технологічної, виробничої та громадської діяльності, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді[3,4].

На даний час світ опинився перед новими викликами у галузі забезпечення інформаційної безпеки, яка в умовах глобалізації та інтеграції є ключовим чинником забезпечення спроможності країни долати кризові явища зовнішньої агресії. Особливо гостро ця проблема привертає увагу до тих процесів, що відбуваються в Україні в умовах війни та окупації частини української території. Тільки своєчасне виконання заходів з управління інформаційною безпекою з боку держави допоможуть здолати загрози політичному та соціально-економічному життю України.

Держави з розвинутим інформаційним середовищем використовують своє домінуюче становище в інформаційному просторі для досягнення економічних та військово-політичних цілей. Традиційні засоби війни достатньо витратні, тоді як інформаційні засоби впливу є прекрасною альтернативою. Спектр впливу достатньо широкий: від дискредитації роботи державних органів до нанесення ударів по критично важливій інфраструктурі. Проведення такого комплексу дій призводить до втрати управління в державі, економічного спаду, створюються умови для виникнення громадянських конфліктів.

В липні 2016 р. в Варшаві на черговій сесії НАТО кіберпростір віднесено до переліку сфер ведення військових дій. На сесії були прийняті «Зобов'язання щодо забезпечення кібероборони», що передбачають фінансування профільних програм, розвиток взаємодії між національними структурами, активізацію обміну даними про кіберзагрози, підвищення кваліфікації працівників національних структур в сфері кібербезпеки, відпрацювання питань кібероборони в процесі заходів оперативної та бойової підготовки[5].

Інформаційна безпека може розглядатися як стан захищеності даних, при якому забезпечується їх конфіденційність, доступність, цілісність, а також комплекс заходів, пов'язаних з досягненням даного стану. Такий підхід має технологічний характер.

На даний час існує три основні підходи до визначення сутності поняття «інформаційна безпека» (рис. 1).[6]

Рис. 1. Підходи до трактування поняття «інформаційна безпека»

Джерело[6]

Конституцією України в ст. 17 зазначено, що захист суверенітету та територіальної цілісності України, забезпечення її економічної та інформаційної безпеки є найважливішими функціями держави, справою всього Українського народу[7].

Зміст інформаційної безпеки розкривається в Доктрині інформаційної безпеки України від 25 лютого 2017 р.[8], зокрема, як невід'ємна складова кожної зі сфер національної безпеки і як важлива самостійна сфера забезпечення національної безпеки.

На думку В. В. Шемчука, правовідносини, що виникають під час здійснення превентивних і захисних заходів в інформаційному середовищі людини, суспільства та держави складають сутність поняття «інформаційна безпека»[9].

Вчений В. С. Цимбалюк вважає, що інформаційна безпека України це стан захищеності її наці-

[1] Бодрук О. С. Структури воєнної безпеки: національний та міжнародний аспекти: Монографія. Київ : НІПМБ, 2001. 300 с.

[2] Про інформацію Закон України № 2657-XII від 02.10.1992. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text.

[3] Бусел В. Т. Великий тлумачний словник сучасної української мови.Київ : ВТФ «Перун», 2007. 1736 с.

[4] Там само.

[5] Цимбалюк В. С. Правове регулювання інформаційної безпеки в Україні: проблеми теорії та практики. *Адміністративне право і процес*. 2014. № 2 (8). С.22–30.

[6] Бодрук О. С. Структури воєнної безпеки: національний та міжнародний аспекти: Монографія. Київ : НІПМБ, 2001. 300 с.

[7] Конституція України Прийнята Верховною Радою України 28.06.1996. URL: http://zakon3.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80/ ed19960628.

[8] Про Доктрину інформаційної безпеки України Указ Президента України від 25.02.2017 № 47/2017. URL: https://www.president.gov.ua/documents/472017-21374.

[9] Ніщименко О. А. Інформаційна безпека України на сучасному етапі розвитку держави і суспільства. *Наше право*. 2016. № 1. С. 17–23.

ональних інтересів в інформаційній сфері, який визначається поєднанням збалансованих інтересів особи, суспільства та держави[10].

Заслуговує на увагу думка науковця Л. О. Кочубей, яка вважає, що інформаційна безпека характеризує стан захищеності життєво важливих інтересів, інформаційну озброєність держави, суспільства, особистості, за якої жодні інформаційні впливи на них неспроможні викликати деструктивні думки і дії, що призводять до негативних відхилень на шляху стійкого прогресивного розвитку названих суб'єктів[11].

Отже, під інформаційною безпекою потрібно розуміти стан захищеності держави від протиправної інформації, яка чинить перешкоди сталому розвитку держави.

Забезпечення інформаційної безпеки ґрунтується на наступних принципах:

1. Принцип системності. Відповідно до якого, захисні заходи повинні бути спрямовані на ліквідацію інформаційних атак з боку зовнішніх та внутрішніх джерел, а також враховувати засоби захисту та канали закритого доступу. Засоби захисту повинні використовуватись адекватно можливим видам загроз та функціонувати у вигляді комплексного захисту, технічно доповнюючи один одного.

2. Принцип міцності. Встановлює, що правила забезпечення інформаційної безпеки повинні охоплювати всі зони безпеки, мати рівну надійність захисту та дозволяти визначати можливі загрози.

3. Принцип багаторівневого захисту. Орієнтований на створення меж захисту інформаційної системи, що складаються з послідовно розташованих зон безпеки, ключова з яких знаходиться всередині всієї системи.

4. Принцип безперервності. Відповідно до якого, функціонування системи інформаційної безпеки повинно бути безперервним.

5. Принцип розсудливості. Визначається в розумності застосування захисних заходів з потрібним ступенем безпеки. В основі даного принципу знаходиться доцільність високих матеріальних витрат та раціональність їх подальшого використання[12].

На початку XXI ст. Україна стала об'єктом гібридної війни зі сторони Росії, основою якої є потужна інформаційно-пропагандистська складова. 24 лютого 2022 року Верховною радою України було введено воєнний стан через пряме повномасштабне вторгнення Росії на територію України. Президентом України було підписано Указ «Щодо реалізації єдиної інформаційної політики в умовах воєнного стану»[13].

В даний час Україні слід побачити у війні не лише негативне. Я. Грицак зазначає, що війна це також шанс для побудови нової України – проведення радикальних реформ заради модернізації держави у всіх сферах. Під цим кутом зору війна може відкрити нові перспективи «перезавантаження», стати потужним модернізаційним чинником[14].

Останніми роками Україна зробила важливі кроки щодо регулювання інформаційної безпеки на нормативно-правовому рівні. Зокрема, 28 грудня 2021 року було затверджено Стратегію інформаційної безпеки, головною метою прийняття якої є посилення спроможностей щодо забезпечення інформаційної безпеки держави, її інформаційного простору, підтримки інформаційними засобами та заходами соціальної та політичної стабільності, оборони держави, захисту державного суверенітету, територіальної цілісності України, демократичного конституційного ладу, забезпечення прав та свобод кожного громадянина[15].

Ефективність сучасної зброї все більше визначається не стільки вогневою потужністю, скільки ступенем інформаційної забезпеченості. В змісті військових дій зросла значимість інформаційно-технічного протиборства. Переваги в ступені інформованості – неодмінна умова перемоги в повітряному, морському та сухопутному бою. Про це свідчить досвід озброєних конфліктів та локальних війн сучасності.

Ключовими заходами щодо забезпечення ефективної діяльності у сфері державного управління інформаційною безпекою є:

• розробка показників оцінки ефективності систем захисту інформаційної безпеки держави;моніторинг та ідентифікація появи дестабілізуючих факторів та загроз;

• організація проведення фундаментальних та прикладних наукових досліджень в галузі забезпечення інформаційної безпеки;

• розробка відповідної нормативно-правової бази;

• протистояння загрозі інформаційної війни[16].

Інформаційна безпека є важливою функцією держави, повинна передбачати, насамперед, формування відповідними державними органами політики організаційно-правових механізмів в галузі інфор-

[10] Ніщименко О. А. Інформаційна безпека України на сучасному етапі розвитку держави і суспільства. Наше право. 2016. № 1. С. 17–23.

[11] Кочубей Л.О. Інформаційна безпека держави: інструменти захисту українського інформаційного поля (на прикладі особливостей інформаційно-комунікаційних технологій у сучасному Донбасі). *Наукові записки Інституту політичних і етнонаціональних досліджень імені І. Ф. Кураса*. 2015. Вип. 3. С. 220–237.

[12] Гончаренко О., Джангужин Р., Лисицин Е. Громадянський контроль і система національної безпеки. *Національна безпека України*. 2003. № 1. С. 39–46.

[13] President of Ukraine (2022), URL: https://www.president.gov.ua/documents/6852021-41069n(Accessed 3 April 2022).

[14] Магда Є. В. Гібридна війна: вижити і перемогти. Х. : Віват, 2015. 304 с.

[15] President of Ukraine (2022), URL: https://www.president.gov.ua/documents/6852021-41069n(Accessed 3 April 2022).

[16] Кравець Є. А. Інформаційна безпека держави. Київ : Укр. енцикл., 1992. 1235 с.

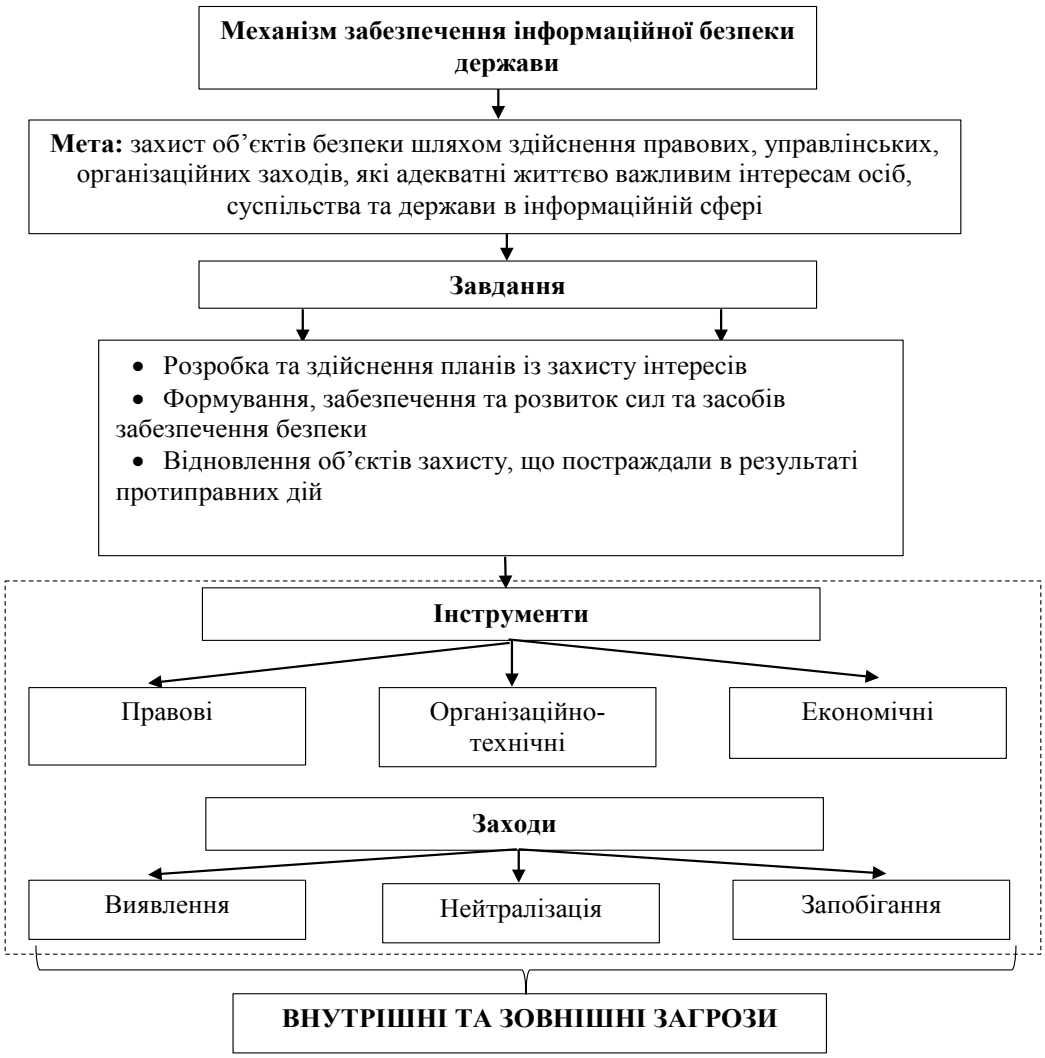

Рис. 2. Механізм забезпечення інформаційної безпеки держави

Джерело: складено автором

маційної безпеки. Важлива роль в даному напрямі належить державним органам, які відповідно до наданих повноважень в сферах своєї відповідальності повинні здійснювати організаційне, нормативно-правове, матеріально-технічне та фінансове забезпечення реалізації державної політики інформаційної безпеки[17].

З метою ефективного, планомірного та контрольованого забезпечення цілісної військової безпеки необхідно функціонування за єдиним сценарієм системи військової безпеки, що виражається в ефективній діяльності трьох компонентів: управлінського, силового та забезпечувального. Система забезпечення безпеки повинна не тільки реагувати на загрози та виклики, але й володіти передбаченням можливих загроз.

Основним чинником вимог до системи забезпечення військової безпеки є поєднання централізованого та децентралізованого управління засобами забезпечення інформаційної безпеки.

Механізм забезпечення інформаційної безпеки є невід'ємною складовою в процесі реалізації національної безпеки (рис. 2).

Серед ключових напрямів, які має виконувати механізм забезпечення інформаційної безпеки варто відзначити наступні:

• виявлення внутрішніх та зовнішніх загроз інформаційній безпеці держави;

• визначення індикаторів інформаційної безпеки та їх порівняння нормативними показниками;

• формування та реалізація системи моніторингу, яка включає: спостереження, збір, обробку, збереження та аналіз інформації щодо стану інформаційної безпеки держави;

• розробка заходів, спрямованих на забезпечення стабільності інформаційної безпеки держави[18].

[17] Шипілова Л. М. Порівняльний аналіз ключових понять і категорій основ національної безпеки України: автореф. дис. … к. політ. н.: 21.01.01. Київ, 2007. 20 с.

[18] Гончаренко О., Джангужин Р., Лисицин Е. Громадянський контроль і система національної безпеки. *Національна безпека України*. 2003. № 1. С. 39–46.

Структурні елементи інформаційної безпеки на міжнародному та внутрідержавному рівні включають:

• захист відомостей, що містять державну або комерційну таємницю;

• захист серверів державних установ та систем життєзабезпечення;

• захист безпеки даних як набір апаратних та програмних засобів, що забезпечують збереження інформації від неавторизованого доступу;

• інформаційно-психологічний блок, який передбачає реалізацію систем заходів, спрямованих на захист від цілеспрямованого впливу на суб'єкт нападу, його психологічний стан або імідж на міжнародній арені.

В умовах війни, коли країна стала об'єктом агресії і підпадає під значну низку інформаційних загроз, їх ліквідація вимагає вжиття певних організаційно-правових заходів. Стратегічна ціль забезпечення інформаційної безпеки як складової національної безпеки обумовлена національними інтересами України у внутрішньополітичній сфері, до яких відноситься збереження конституційного устрою, підтримка національної злагоди та єдність правового простору.

Головними напрямами вдосконалення системи забезпечення інформаційної безпеки є наступні:

• стратегічне стримування та ліквідація військових конфліктів, що можуть виникнути в результаті застосування інформаційних технологій;

• вдосконалення системи забезпечення інформаційної безпеки Збройних Сил України, військових формувань, включаючи в себе сили та засоби інформаційної протидії;

• прогнозування, виявлення та оцінка інформаційних загроз, включаючи загрози Збройним Силам України в інформаційній сфері.

Під час воєнного стану інформаційна зброя є достатньо потужним засобом ведення війни, оскільки її технічна інноваційність, потужність та непомітність є дуже небезпечними. Тому, інформаційна безпека України має ґрунтуватися на скоординованих діях державних установ та структур громадянського суспільства. В умовах війни значно зростає значення інформаційної культури як фактору посилення протидії інформаційній зброї в громадян та забезпечення державного суверенітету країни.

Висновки

Одним з першочергових завдань держави є забезпечення захисту інформації, що в свою чергу є гарантією національної безпеки. В результаті цивілізаційного розвитку інформація стає повноцінним ресурсом. Забезпечення інформаційної безпеки на даний час є не менш важливим напрямом державної політики, чим підтримка економічної стійкості та високих соціальних стандартів.

Основними напрямами щодо реалізації та захисту національних інтересів на сучасному етапі розвитку України в інформаційній сфері є наступні:

• розробка та прийняття довгострокової програми із забезпечення виходу на рівень провідних країн світу в галузі створення систем інформатизації та управління, що ґрунтуються на новітніх інформаційних технологіях;

• забезпечення свободи отримання та розповсюдження інформації громадянами, іншими суб'єктами суспільних відносин в інтересах формування громадянського суспільства, демократичної правової держави, розвитку науки та культури;

• забезпечення надійного захисту інформаційного потенціалу України від неправомірного його використання; здійснення контролю за експортом з держави інтелектуальної продукції, а також інформаційних банків даних;

• організація ефективної системи підготовки та перепідготовки кадрів в галузі забезпечення інформаційної безпеки;

• розвиток взаємодії державних та комерційних систем інформаційного забезпечення з метою більш ефективного використання інформаційних ресурсів держави.

Інформація про автора:

Гбур Зоряна Володимирівна,

доктор наук з державного управління, професор,
професор кафедри управління охороною здоров'я та публічного адміністрування
Національний університет охорони здоров'я України імені П.Л. Шупика
9, вул. Дорогожицька, Київ, 04112, Україна

Information about the author:

Hbur Zoryana Volodymyrivna,

Doctor of Science in Public Administration, Professor,
Professor at the Department of Health Care Management and Public Administration
Shupyk National Healthcare University of Ukraine
9, str. Dorogozhytska, Kyiv, 04112, Ukraine