

ІНФОРМАЦІЙНА БЕЗПЕКА ТА ЗАХИСТ ІНФОРМАЦІЇ В УМОВАХ СУЧАСНИХ ВИКЛИКІВ УКРАЇНИ

Бондар Богдан Юрійович, студент IV курсу (групи ІБ-41) спеціальності 029 Інформаційна, бібліотечна та архівна справа Університету Григорія Сковороди в Переяславі.

Науковий керівник: Плужник О.В., доктор філософії, доцент, доцент кафедри соціальних комунікацій, документознавства та інформаційної діяльності Університету Григорія Сковороди в Переяславі.

У статті розглядаються актуальні проблеми інформаційної безпеки України в умовах триваючого військового конфлікту та зростаючих зовнішніх загроз. Підкреслюється важливість створення ефективних механізмів захисту інформації на всіх рівнях, враховуючи швидкий розвиток цифрових технологій та нові виклики, пов'язані з кіберзлочинністю і дезінформацією. Аналізуються існуючі технологічні, правові та організаційні заходи, що реалізуються для захисту інформаційного простору держави, а також пропонується комплексний підхід до вирішення проблем, який включає співпрацю держави, бізнесу та суспільства.

Ключові слова: інформаційна безпека, інформація, інформаційні технології, кіберзагрози, суспільство.

Триваючий конфлікт в Україні та зовнішні загрози роблять захист даних пріоритетним завданням для держави і суспільства. У контексті військових дій інформаційна безпека стає ключовим елементом національної безпеки. Це підкреслює необхідність створення ефективних механізмів захисту інформації на всіх рівнях – від державних органів до приватних компаній. Швидкий розвиток цифрових технологій у свою чергу також створює нові виклики для безпеки інформації, особливо в умовах зростання використання електронних сервісів та дистанційної роботи. З одного боку, технології спрощують доступ до ресурсів і послуг, з іншого – збільшують уразливість систем. Економічні труднощі, спричинені конфліктом та нестабільною ситуацією, підвищують ризики шахрайства і кібератак, оскільки зловмисники намагаються скористатися вразливостями в системах безпеки. Загалом, цілісна система інформаційної безпеки є критично важливою для збереження конфіденційності, цілісності та доступності даних у сучасному світі, що невпинно змінюється.

Мета статті детально розглянути основні виклики, з якими стикається Україна в інформаційній сфері, особливо в умовах посилення зовнішнього впливу та кіберзагроз; дослідити існуючі технологічні, правові та організаційні заходи, які реалізуються для захисту інформаційного простору держави.

В умовах зростаючих кіберзагроз і посилення інформаційного тиску на Україну численні наукові та практичні роботи присвячені вирішенню проблем інформаційної безпеки.

Горулько В.В. досліджує інформаційну політику держави як ключову складову національної безпеки, акцентуючи на важливості захисту інформаційних інтересів особи, суспільства та держави в умовах сучасних загроз. Автор аналізує ризики, пов'язані з кібертероризмом, агресивною пропагандою та іншими дестабілізуючими впливами. У статті наголошується на потребі регулювання інформаційної діяльності відповідно до реалій сучасного світу та міжнародних стандартів, щоб ефективно захистити національні інтереси України (Горулько, 2022).

Подорожна Т.С. досліджує забезпечення інформаційної безпеки України в умовах загроз з боку російської федерації. Авторка акцентує на важливості стійкості інститутів публічної влади та дотриманні прав людини, які залежать від інформаційної безпеки. Обговорюються принципи конфіденційності та правові засади захисту приватного життя. Наголошується на необхідності розширення повноважень органів влади в доступі до особистої інформації з дотриманням принципу пропорційності (Подорожна, 2023).

Пугачов О.І. досліджує інформаційну безпеку України в умовах військового конфлікту та глобалізації, акцентуючи на викликах, таких як дезінформація та кіберзлочинність. Автор підкреслює важливість виявлення проблем захисту інформаційного простору та розробки ефективних заходів для протидії загрозам. Метою його дослідження є аналіз стану інформаційної безпеки, використовуючи різні методи. Автор наголошує на необхідності координації зусиль держави, громадянського суспільства та міжнародних партнерів для захисту національних інтересів в умовах глобалізації та гібридної війни (Пугачов, 2024).

Інформаційна безпека та захист інформації є критично важливими аспектами в сучасній Україні, особливо в умовах швидкого розвитку технологій і зростання кіберзагроз. У глобалізованому світі, де дані стали основним ресурсом, забезпечення їхньої конфіденційності, цілісності та доступності стає надзвичайно актуальним. Україні, як державі, що переживає численні виклики на політичному та економічному рівні, необхідно впроваджувати сучасні рішення для протидії кіберзлочинності та захисту національних інтересів. Варто акцентувати увагу на важливості створення комплексної системи інформаційної безпеки, що включає не лише технологічні, а й правові та організаційні аспекти. Справжня безпека інформації передбачає активну співпрацю державних установ, бізнесу та суспільства, що є ключовим фактором для стійкого розвитку країни в умовах сучасних викликів.

Одним із яких є триваючий військовий конфлікт, який загострює проблеми підтримання стабільного інформаційного середовища. Агресивна політика російської федерації не лише загрожує суверенітету України, а й є каталізатором систематичного поширення негативної пропаганди, спрямованої на підриив суспільної довіри та єдності. Цей потік упередженої інформації ускладнює інформаційний простір, оскільки неконтрольованим потоком інформації можуть легко маніпулювати інші організації для просування дезінформаційних кампаній, що ще більше дестабілізує національний наратив і суспільне сприйняття (Вимоги

до захисту інформації в інформаційних системах у воєнний час: роз'яснення Держспецзв'язку, 2024).

Зважаючи на триваючу загрозу нових атак з боку Росії, з-поміж українських чиновників спостерігається підвищене усвідомлення вразливості їхніх інформаційних систем, що наголошує на необхідності підвищеної пильності та готовності у сфері кібербезпеки. Ця нагальність була ще більше посилена відповідями членів НАТО, чиє безпосереднє прийняття рішень і стратегічна підтримка перед обличчям російської агресії мають прямий вплив на стратегії інформаційної безпеки України. Спільні зусилля між союзниками по НАТО не тільки зміцнюють обороноздатність України, але й забезпечують важливі механізми обміну розвідувальними даними, які покращують обізнаність про ситуацію та здатність реагувати на потенційні кіберзагрози які створюють пряму загрозу цілісності та надійності інформаційних систем України (Романюк, & Паливода, 2024). Невисокий рівень розвитку інформаційної інфраструктури в Україні ще більше посилює ці вразливості, ускладнюючи конкуренцію з іноземними інформаційними програмами, які часто домінують у медіа ландшафті (Вимоги до захисту інформації в інформаційних системах у воєнний час: роз'яснення Держспецзв'язку, 2024).

У цьому контексті Україна має продовжувати вдосконалювати свій підхід до інформаційної безпеки шляхом інтеграції уроків, отриманих як із внутрішнього досвіду, так і з передового міжнародного досвіду, забезпечуючи, щоб її захист був достатньо надійним, щоб протистояти складнощам сучасної інформаційної війни.

Серед найактуальніших загроз національній інформаційній безпеці Подорожна Т.С. виділяє: протиправний вплив на національні інформаційні ресурси, інформаційно-телекомунікаційні системи та інформаційну інфраструктуру, а також на критично важливі інформаційні структури; використання засобів та методів для поширення недостовірної (фейкової) інформації з метою дезінформації, в тому числі шляхом психологічного впливу на людей для їх дезорганізації та придушення волі; несанкціоноване втручання в національний інформаційний простір. У зв'язку з цим, трансформація інформаційного простору в умовах геополітичних змін та загострення соціально-економічних і міжнародних протиріч визначає новий вектор розвитку правового регулювання інформаційної безпеки в Україні з урахуванням міжнародних стандартів у цій сфері (Подорожна, 2023).

Зважаючи на ці виклики, державним органам і не державним інституціям вкрай необхідно визначити пріоритети розвитку ефективної системи інформаційної безпеки, яка не лише протидіє цим загрозам, а й захищає інформаційний суверенітет України. Крім того, зростаюча складність та динаміка кіберзагроз підкреслюють необхідність постійного оновлення стратегій захисту інформаційного простору. Недавні події значно змінили ландшафт інформаційної безпеки в Україні, вимагаючи активного та адаптивного підходу до захисту її цифрової інфраструктури (Пугачов, 2024), (Вимоги до захисту інформації в інформаційних системах у воєнний час: роз'яснення Держспецзв'язку, 2024).

Україна активно розробляє спеціальні правові принципи захисту недоторканності приватного життя, наголошуючи на необхідності конфіденційності, цілісності та доступності інформаційних систем. Ці законодавчі рамки спрямовані не тільки на захист персональних даних, а й на встановлення додаткових механізмів для захисту практик збору та обробки даних. Однак нещодавня ескалація загроз національній безпеці спонукала уряд розширити повноваження, дозволивши доступ до особистої інформації та її обробку з менш суворими обмеженнями, що викликає занепокоєння щодо балансу між безпекою та правами на конфіденційність. У цьому контексті критичним стає принцип пропорційності, оскільки обмеження прав людини мають бути виправдані в ім'я національної та інформаційної безпеки. Крім того, стабільність інститутів публічної влади має вирішальне значення для дотримання прав людини, але нинішня ситуація кидає виклик самим основам правопорядку (Пугачов, 2024).

Неадекватність захисту національного інформаційного простору від зовнішньої пропаганди та психологічної війни підкреслює нагальну потребу державних органів та недержавних інституцій у пріоритеті створення ефективної системи захисту інформації. Оскільки Україна справляється з цими складнощами, увага повинна також поширюватися на аналіз іноземного досвіду протидії негативній пропаганді, що може дати розуміння того, як підвищити стійкість її інформаційної інфраструктури та забезпечити надійний захист від маніпулятивного впливу (Романюк, & Паливода, 2024). Вивчення міжнародних практик у поєднанні з удосконаленням національного законодавства дозволить створити ефективну систему протидії дезінформації. Правова база, встановлена різними законами, такими як «Про інформацію» та «Про національну безпеку України», створює основу стратегії інформаційної безпеки країни, забезпечуючи дотримання як державними, так і приватними структурами необхідних протоколів.

Крім того, такі ініціативи, як «Національна програма інформатизації» та «Стратегія інформаційної безпеки», затверджені Указами Президента, ілюструють структурований підхід до впровадження ефективних заходів безпеки по всій країні. Однак, незважаючи на цю основу, залишаються значні прогалини; наприклад, помітною є відсутність законодавчого забезпечення створення національних інформаційних ресурсів та міжнародних інформаційних обмінів, що перешкоджає можливості країни модернізувати свою інформаційну політику у відповідності до міжнародних стандартів. Відсутність регулювання щодо статусу конфіденційної інформації, включаючи різні види таємниці, такі як банківська та медична, підкреслює недоліки в поточній законодавчій базі, які необхідно усунути для ефективного захисту конфіденційних даних. Ці недоліки вказують на нагальну потребу в комплексній державній політиці, яка не тільки покращить поточний стан інформаційної безпеки, але й зміцнить міжнародну репутацію України та стійкість проти тактики гібридної війни, де маніпулювання інформацією становить значну загрозу (Горулько, 2022). Таким чином, розробка та вдосконалення цих політик є важливими для створення

надійного середовища інформаційної безпеки, яке може протистояти виникаючим викликам і захищати національні інтереси.

Отже Інформаційна безпека та захист інформації в сучасній Україні є критично важливими аспектами національної безпеки. З огляду на постійні загрози з боку Росії та інших зовнішніх факторів, забезпечення цілісності та захищеності інформаційних систем держави стає пріоритетом. Це вимагає комплексного підходу, що поєднує технологічні, правові та організаційні заходи, а також підвищення рівня обізнаності й професійної підготовки у сфері кібербезпеки. Тільки активні та гнучкі стратегії здатні ефективно реагувати на сучасні різнопланові виклики в інформаційному середовищі України.

Аналіз критичної важливості забезпечення інформаційної безпеки України в умовах сучасних загроз підкреслює необхідність комплексного підходу, який поєднує технологічні, правові та організаційні заходи для ефективної протидії як зовнішнім, так і внутрішнім викликам. Серед основних перспектив виділяється підвищення рівня кібербезпеки. Враховуючи динамічні кіберзагрози, важливо активно вдосконалювати кіберзахист державних та приватних інформаційних систем, посилюючи технічні рішення та готуючи фахівців у галузі кібербезпеки.

Протидія дезінформації та пропаганді також має ключове значення. Необхідно створити надійну систему моніторингу інформаційного простору для своєчасного виявлення дезінформаційних загроз, зокрема маніпулятивного впливу, що підриває громадську довіру до інституцій. Ефективний захист інформаційного суверенітету України залежить від міжнародного співробітництва. Обмін досвідом та впровадження міжнародних стандартів допоможуть Україні краще протидіяти кіберзагрозам та інформаційним атакам.

Розвиток правової бази є також важливим аспектом. Адаптація законодавства, що спрямоване на захист персональних даних і конфіденційної інформації, дозволить зміцнити державний контроль і забезпечити дотримання стандартів інформаційної безпеки. Отже, для ефективного забезпечення інформаційної безпеки Україні необхідний комплексний підхід, що включає технічні, правові та організаційні заходи. Співпраця з міжнародними партнерами та вдосконалення національного законодавства допоможуть протидіяти кіберзагрозам і дезінформації, зміцнюючи інформаційний суверенітет країни та її стійкість до сучасних викликів.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Вимоги до захисту інформації в інформаційних системах у воєнний час: роз'яснення Держспецзв'язку. 2024. URL: <https://telas.kiev.ua/hhaluzi/vimogi-do-zakhistu-informatsiji-v-informatsijnikh-sistemakh-u-voennij-chas-roz-yasnennya-derzhspetszv-yazku.html>.

2. Горулько В.В. Роль і місце інформаційної безпеки в загальній системі національної безпеки держави. *Вісник Харківського національного університету імені В.Н. Каразіна. Серія «Право»*. 2022. № 34. С. 103–108.

3. Подорожна Т.С. Забезпечення інформаційної безпеки України в умовах сучасних викликів та загроз з боку РФ. *Аналітично-порівняльне правознавство*. 2023. № 6. С. 491–497.

4. Пугачов О.І. Проблеми забезпечення інформаційної безпеки України в сучасних умовах. *Проблеми сучасних трансформацій. Серія: право, публічне управління та адміністрування*. 2024. № 12. URL: <https://doi.org/10.54929/2786-5746-2024-12-02-15>

5. Романюк Ю., Паливода В. Місце і роль України в процесі трансформації світопорядку. 2024. URL: <https://bintel.org.ua/analytics/misce-i-rol-ukrayini-v-procesi-transformaciyi-svitoporyadku/>

REFERENCE

1. Vymohy do zakhystu informatsii v informatsiinykh systemakh u voiennyi chas: roz'iasnennia Derzhspetsviazku. 2024. URL: <https://telas.kiev.ua/hhaluzi/vimogi-do-zakhystu-informatsiji-v-informatsijnikh-sistemakh-u-voennij-chas-roz-yasnennya-derzhspetszv-yazku.html>.

2. Horulko V.V. Rol i mistse informatsiinoi bezpeky v zahalnyi systemi natsionalnoi bezpeky derzhavy. *Visnyk Kharkivskoho natsionalnoho universytetu imeni V.N. Karazina. Seriiia «Pravo»*. 2022. № 34. С. 103–108.

3. Podorozhna T.S. Zabezpechennia informatsiinoi bezpeky Ukrainy v umovakh suchasnykh vyklykiv ta zahroz z boku RF. *Analitychno-porivnialne pravoznavstvo*. 2023. № 6. С. 491–497.

4. Puhachov O.I. Problemy zabezpechennia informatsiinoi bezpeky Ukrainy v suchasnykh umovakh. *Problemy suchasnykh transformatsii. Seriiia: pravo, publichne upravlinnia ta administruvannia*. 2024. № 12. URL: <https://doi.org/10.54929/2786-5746-2024-12-02-15>

5. Romaniuk Yu., Palyvoda V. Mistse i rol Ukrainy v protsesi transformatsii svitoporiadku. 2024. URL: <https://bintel.org.ua/analytics/misce-i-rol-ukrayini-v-procesi-transformaciyi-svitoporyadku/>