

УДК 351.74:004

Лазарів Владислав,

аспірант кафедри управління та бізнес адміністрування

Прикарпатського національного університету

імені Василя Стефаника,

м. Івано-Франківськ, Україна

<https://orcid.org/0009-0008-6812-6124>

vlazariv@n-ix.com

ПУБЛІЧНЕ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ: СУЧАСНІ ВИКЛИКИ ТА ПЕРСПЕКТИВИ РОЗВИТКУ

З початком антитерористичної операції в Донецькій та Луганській областях у 2014 році Україна опинилася у нових реаліях. Безпека країни безумовна мала нові виклики. В умовах чіткого визначення євроінтеграційного вектору, країна мала звільнитися від економічних, соціальних, політичних та суспільних перешкод до такої співпраці. В свою чергу, розуміння країни-агресора, що Україна виходить із зони політичного контролю, спричинило додаткові фінансові вливання у системи інформаційної підтримки агресії: проведення інформаційної політики через засоби масової інформації, збір персональної інформації громадян України, які мали відношення до військового, волонтерського та громадського руху, кібератаки на інформаційні сервіси, пошук розвідувальних даних про військові, інфраструктурні, громадські об'єкти тощо. У 2022 році після початку повномасштабної військової агресії російської федерації проти України з'явилося чітке розуміння, що інформаційна безпека держави стане основою майбутньої перемоги, а розвиток інформаційних технологій забезпечить інвестиційну привабливість та конкурентоспроможність країни на світових ринках, що дасть можливість швидко та у повному обсязі відновити зруйновані війною об'єкти [1].

Аналізуючи сучасні виклики інформаційного забезпечення, доцільно визначити роль органів публічного управління у процесах побудови архітектуру інформаційної безпеки, зокрема, визначено наступні запити до органів публічної влади [2-3]:

- формування механізмів забезпечення захисту даних, що мають статус військової таємниці, дані, військового характеру, розвідувальних даних тощо;

- розробка ефективних систем захисту персональних даних громадян, в тому числі з метою їх особистої безпеки;

- забезпечення захисту інформаційних баз та інформації центральних, регіональних та місцевих органів влади, Міністерств та відомств, інституцій публічного управління тощо;

- розробка програм захисту баз даних фінансових установ;

- виявлення та призупинення діяльності організацій, які фінансують інформаційні впливання, що загрожують безпеці держави;

- формування прозорих та відкритих інформаційних джерел, спрямованих на задоволення запитів населення, бізнесу на надання адміністративних послуг;

- формування мобільного та відкритого доступу до офіційної інформації органів публічної влади, завданнями яких є інформаційна підтримка та роз'яснення населенню інформації про прийняття управлінських рішень на національному, регіональному та місцевому рівнях;

- організація системи взаємодії з обміну інформацією між міжнародними партнерами України, спрямованої на забезпечення національної безпеки, прав та свобод людини і громадянина, розвиток громадянського суспільства, формування умов для залучення інвестицій, розвитку бізнесу, розвитку громадянського суспільства;

- представництво України та організація її співпраці із міжнародними партнерами у рамках роботи у міжнародних громадських організаціях, сприяння поширенню інформації про їх діяльність та залучення населення до участі у програмах розвитку, грантової підтримки тощо;

- формування процесів інформаційного супроводу освітніх процесів для школярів та студентів в умовах нових викликів;
- пошуку механізмів розвитку якісного дистанційного навчання;
- підвищення цифрової грамотності населення;
- забезпечення ефективних комунікацій у ієрархічній системі публічної влади, а також горизонтальної системи комунікації між різними гілками та рівнями влади, приватним сектором, громадськістю.

Отже, визначивши сучасні виклики та роль органів публічної влади у побудові ефективної інформаційної системи на національному, регіональному та місцевому рівнях, доцільно визначити тенденції розвитку інформаційної політики України.

Тенденціями розвитку інформаційного простору в Україні мають стати загальні євроінтеграційні процеси, зокрема, формування сприятливих умов для розвитку цифрових ринків, відкритість даних при їх максимальному захисті, зростання кількості адміністративних послуг на платформі «Дія», розвиток застосунків, спрямованих на реалізацію запитів населення, розвиток офіційних інформаційних джерел, як в форматі офіційних сайтів, так і через використання соціальних мереж, формування швидкого доступу до інформації із мінімальними витратами часу та необхідністю оформлення документів чи пред'явлення документів для підтвердження особи, ключів, підписів тощо.

Отже, процеси цифровізації та розвитку інформаційних систем будуть продовжувати розвиватися. Стійкі тенденції до розвитку інформаційних систем визначають нові вимоги до забезпечення безпеки інформації, що стає базовим пріоритетом публічного управління.

Список використаних джерел:

1. Офіційний сайт European Union Institute for Security Studies. Конференція Інституту досліджень безпеки Європейського Союзу (EUISS), присвячена ролі Європи в геополітичному ландшафті, порушеному війною росії проти України. Електронний ресурс. URL: <https://www.iss.europa.eu/>
2. Офіційний сайт Президента України. Указ президента України №56/2022 «Про рішення Ради національної безпеки і оборони України від 30 грудня 2021 року «Про Стратегію забезпечення державної безпеки». Електронний ресурс. URL: <https://www.president.gov.ua/documents/562022-41377>
3. Офіційний сайт видання Liga.net, Проект, Неофіційний текст від 09.06.2015 (не набрав чинності) «Концепція інформаційної безпеки України (неофіційний текст). Електронний ресурс. URL: <https://ips.ligazakon.net/document/NT1607>