

Антон РЯПОЛОВ

аспірант кафедри
теорії держави та права
Дніпровського державного
університету внутрішніх справ
(м. Дніпро, Україна)

<https://orcid.org/0009-0007-1693-507X>

ІНФОРМАЦІЙНА БЕЗПЕКА ЛЮДИНИ ТА ГРОМАДЯНИНА ЯК СКЛАДОВА НАЦІОНАЛЬНОЇ БЕЗПЕКИ ДЕРЖАВИ: ЗАГРОЗИ ТА ВИКЛИКИ

В умовах посилення зовнішніх загроз інформаційна безпека для України постає критично важливою частиною публічного управління. Національна концепція інформаційної безпеки значно розвинулася протягом останніх десятиліть, увібравши в себе заходи технічного захисту, соціально-правові та політичні аспекти. Безпека особистої інформації, як підгрупа інформаційної безпеки, стосується захисту прав особи в контексті кіберзагроз, дезінформації та несанкціонованого порушення даних. Тому цілком очевидним є розгляд та розв'язання актуальних питань інформаційної безпеки людини та громадянина як частини національної безпеки держави.

Російська агресія, інші дестабілізуючі фактори зовнішнього та внутрішнього характеру змушують державу постійно шукати способи підвищення інформаційної безпеки людини та громадянина як частини національної безпеки держави. Взаємопов'язаний характер сучасних інформаційних систем означає, що окремі вразливі місця можуть потенційно перерости в загрози національній безпеці [1, с. 75]. Забезпечення цілісності, конфіденційності та доступності персональних даних має важливе значення для збереження суспільної довіри та стабільності держави. Враховуючи все більшу залежність держав від цифрових технологій, порушення безпеки особистої інформації можуть призвести до дестабілізації на національному рівні.

Структура інформаційної безпеки побудована на трьох основних стовпах: конфіденційність, цілісність і доступність. Безпека особистої інформації зосереджена насамперед на захисті конфіденційності, водночас гарантуючи, що права доступу збалансовані відповідно до принципів прозорості та підзвітності в діяльності державних органів. Так, Солмс і В. Нікерк зауважують на тому, що безпека індивідуальних даних формує фундаментальний рівень інформаційної стійкості держави [2, с. 99]. Особиста інформація є важливим активом для людей, і будь-які недоліки в її захисті безпосередньо впливають на суспільний добробут і довіру до державних установ.

У сучасному цифровому світі межі між особистою та національною безпекою стають дедалі більш розмитими, формуючи певний зв'язок між безпекою особистої інформації та національною безпекою. З одного боку, надійна система захисту особистої інформації підвищує стійкість держави, зменшуючи такі ризики, як кібершпигунство, викрадення особистих даних і масштабні витоки даних. З іншого боку, проблеми у захисті індивідуальних даних можуть підірвати національну безпеку, про що свідчать випадки з російським гібридним впливом, коли витік персональних даних використовується як зброя для політичної дестабілізації.

Концепція безпеки особистої інформації охоплює кілька вимірів, зокрема конфіденційність даних, цифрові права та обізнаність щодо кібербезпеки. Роль особи в національній безпеці еволюціонувала від пасивного суб'єкта до активного учасника екосистеми інформаційної безпеки [3, с. 132]. Ця зміна парадигми вимагає всебічного вивчення того, як механізми захисту особистої безпеки впливають на результати національної безпеки. Нові загрози, такі, наприклад, як кібератаки на основі штучного інтелекту, вимагають постійних інновацій у заходах кібербезпеки.

Водночас у правовій державі ці аспекти підлягають належному нормативно-правовому регулюванню. Україна зробила значний крок у цьому напрямі завдяки прийняттю Закону України «Про основні засади забезпечення кібербезпеки України» та затвердженню Стратегії кібербезпеки України. Зокрема, у вказаній стратегії наголошується на захисті критичної інформаційної інфраструктури та персональних даних [4, с. 10]. Дійсно, технологічний прогрес створив як можливості, так і проблеми для безпеки особистої

інформації. Шифрування, безпечні методи автентифікації та системи виявлення вторгнень є важливими інструментами для запобігання несанкціонованому доступу до конфіденційних даних.

Природа цифрових загроз, що розвивається, вимагає нового розуміння безпеки особистої інформації. Інформаційна безпека людини та громадянина як частина забезпечення національної безпеки держави, на думку Т. Подорожної, має включати такі основні форми, як:

- 1) інформаційно-технічна безпека;
- 2) інформаційно-ідеологічна безпека;
- 3) інформаційно-психологічна безпека та
- 4) інформаційно-правова безпека [5, с. 505].

Інформаційно-технічна безпека передбачає захист даних і допоміжної інфраструктури від навмисних і випадкових технологічних загроз. Інформаційно-ідеологічна безпека спрямована на захист людей як від навмисного, так і від випадкового інформаційного впливу, який може порушити етичні норми чи завдати шкоди суспільним цінностям. Інформаційно-психологічна безпека стосується захисту психічного здоров'я та обізнаності людей від несприятливого інформаційного впливу, що дозволяє їм зберігати раціональну соціальну поведінку та особистий розвиток навіть за складних обставин. Інформаційно-правова безпека гарантує реалізацію прав особи на пошук, отримання, виробництво та поширення інформації, а також захист приватної інформації від несанкціонованого доступу або розголошення.

Не можна не помітити соціально-політичний контекст інформаційної безпеки. Довіра суспільства до державних інституцій значною мірою залежить від сприйняття ефективності механізмів захисту персональних даних. Крім того, поширення кампаній з дезінформації та розповсюдження фейкових новин підкреслило важливість навчання громадян інформаційної гігієни та розвитку цифрової грамотності. Взаємодія між урядом, інститутами громадянського суспільства та приватним сектором має вирішальне значення для досягнення комплексної інформаційної безпеки.

Концепція персональної інформаційної безпеки набуває чіткості, пропонуючи цілісний підхід до протидії сучасним інформаційним викликам. Одним із визначальних компонентів у створенні безпечного інформаційного середовища є становлення електронної держави. Це вимагає надійної інтеграції міжнародної правової бази з національним законодавством для розв'язання критичних проблем, таких як транскордонна передача даних і етичне використання технологій. Системи електронного врядування мають бути розроблені так, щоб гарантувати захист прав людей і водночас підтримувати довіру до цифрових взаємодій [6]. Успіх електронної держави залежить від її здатності врівноважувати інновації з безпекою особистої інформації.

Таким чином, роль інформаційної безпеки людини та громадянина в забезпеченні національної безпеки багатогранна і незамінна. Захищаючи права особи на конфіденційність і персональні дані, держави не тільки підтримують демократичні цінності, але й зміцнюють свою стійкість до внутрішніх і зовнішніх загроз. Для України належне правове регулювання цієї сфери, впровадження передових технологій і залучення суспільства є важливими для досягнення стійкої інформаційної безпеки людини та громадянина як складової національної безпеки держави. Зовнішня агресія вимагає постійного вдосконалення та адаптації до нових викликів, а також якісного захисту інформаційних прав людини та громадянина.

1. Золотар О. О. Інформаційна безпека людини: теорія і практика : монографія. Київ : ТОВ «Видавничий дім «АртЕк», 2018. 446 с.
2. Solms R., Niekerk J. V. From information security to cyber security. *Computers & Security*. 2013. No. 38. P. 97–102.
3. Ткачук Т. Ю. Правове забезпечення інформаційної безпеки в умовах євроінтеграції України : монографія. Київ : НА СБУ, 2018. 440 с.
4. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України» : Указ Президента України від 26 серпня 2021 р. № 447/2021. URL : <https://zakon.rada.gov.ua/laws/show/447/2021#Text>.
5. Подорожна Т. С. Інформаційна безпека людини в системі національної безпеки: виклики та загрози. *Аналітично-порівняльне правознавство*. 2024. № 2. С. 500–506.
6. Nalyvaiko L. State System Guarantees: Theoretical and Legal Characteristics // *The issues of improving legal knowledge in the XXI century: the unity of theory and practice : collective monograph*. Lviv ; Toruń : Liha-Pres, 2019. P. 131–150.