УДК 351.86
DOI https://doi.org/10.32782/1813-3401.2024.1.27

С. О. Лисенко
доктор юридичних наук, професор,
директор Інституту безпеки
ПрАТ «Вищий навчальний заклад «Міжрегіональна Академія управління персоналом»
ORCID ID: 0000-0002-7050-5536

ПРИНЦИПИ ДЕРЖАВНОГО УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ ТА ЇХНЯ ХАРАКТЕРИСТИКА

Статтю присвячено дослідженню принципів державного управління інформаційною безпекою та їхня роль у суспільстві та державі. Під час проведення дослідження було виконано аналіз сучасних стратегій та методів забезпечення інформаційної безпеки на державному рівні, що включає в себе як стратегічне, так і тактичне планування. Вивчення цих підходів дозволило отримати глибше розуміння та оцінку ефективності заходів, спрямованих на збереження та захист інформаційних ресурсів держави.

Великої уваги заслуговує підхід управління інформаційною безпекою держави, тому варто спочатку визначити певні принципи державного управління інформаційною безпекою суспільстві та державі, які становлять фундаментальну основу для розробки ефективних стратегій та тактик у цій сфері. Такий підхід дозволяє розуміти важливість управління інформаційною безпекою як ключового елементу національної безпеки та стабільності, а також сприяє визначенню пріоритетних напрямків діяльності для забезпечення захисту інформаційних ресурсів та мінімізації загроз їхньому недоторканню.

Основна увага прикута до принципів управління державною інформаційною безпекою оскільки вона є основою, яку встановлюють ключові правила організації та проведення управлінських заходів у сфері захисту інформації. Вони визначаються законодавством або узагальнюють існуючі юридичні норми країни. Ці принципи сприяють забезпеченню відповідного рівня інформаційної безпеки, що є важливим фактором для ефективного функціонування суспільства, зміцнення національної безпеки та захисту національних інтересів у світі, а також забезпеченню недоторканості та приватності особистої інформації громадян, що є фундаментальним для збереження демократичних цінностей та правової держави.

У статті розглянуто основні категорії принципів державного управління та їхні особливості, включаючи соціально-політичні, організаційні та функціональні аспекти. Також будуть визначені додаткові принципи розвитку управління в галузі інформаційної безпеки, зокрема у контексті впровадження штучного інтелекту, яке відбувається не лише в Україні, а й у всьому світі.

Ключові слова: *державне управління, штучний інтелект, інформаційна безпека, правове забезпечення, OSINT, принципи державного управління, управління інформацією.*

Обґрунтування актуальності обраної теми. Інформаційна безпека стає все більш важливою у контексті зростання кіберзагроз та технологічного розвитку. Зростання кількості кібератак та інформаційних вторгнень свідчить також про необхідність ефективного управління інформаційною безпекою. Вразливість держав перед кіберзагрозами може помітно впливати на економіку, політичну стабільність та національну безпеку. В свою чергу швидкий технологічний розвиток (зокрема - в галузі штучного інтелекту, обробки великих даних та Інтернету речей), ставить перед урядами нові виклики щодо забезпечення безпеки інформаційних систем та даних громадян. Інформаційна безпека є ключовою у вирішенні питань приватності та захисту особистої інформації громадян. Високий рівень інформаційної безпеки дозволяє зберігати довіру громадян до уряду та захищати їхні права на конфіденційність.

Актуальність теми визначається не лише тим, що сучасний світ стає все більш цифровим і залежним від інформаційних технологій, але й тим, що це створює нові виклики та загрози. Зростання кількості кібератак, витоків даних, маніпуляцій з інформацією, а також вплив штуч-

ного інтелекту та автоматизованих систем на суспільство, вимагає розробки та впровадження ефективних стратегій та принципів управління інформаційною безпекою. Ці принципи повинні враховувати не лише технічні аспекти, але й правові, етичні та соціальні аспекти, щоб забезпечити високий рівень захисту інформації та приватності громадян, а також зберегти довіру до цифрових технологій та державних установ.

Метою статті є систематизація та аналіз принципів державного управління інформаційною безпекою, з метою надання чіткого уявлення про їхню сутність та значення в сучасному світі.

Виклад основного матеріалу. Аналіз основних категорій принципів державного управління та їх характеристики, дає підстави вважати, що соціально-політичні, організаційні та функціональні принципи залишаються основними групами принципів, відповідно до теоретичної класифікації в даній галузі.

Соціально-політичні принципи державного управління інформаційною безпекою охоплюють найзагальніші правила та положення, які впливають на всю систему державного управління вцілому. Вони корелюються із головними законами країни та відповідають принципам міжнародного права [1].

Принцип демократизму у державному управління ґрунтується на конституційних засадах. Так, відповідно до статті 1 Конституції України, держава є суверенною, незалежною, демократичною, соціальною та правовою. У контексті ж інформаційної безпеки, демократизм означає залучення громадян до процесу прийняття рішень, що стосуються захисту інформації та забезпечення їхнього права на доступ до інформації.

Наступний принцип державного управління стосується участі населення в управлінні державою, задекларований у статті 5 Конституції України та зазначає, що народ є єдиним джерелом влади. Участь громадян у державному управлінні забезпечується через референдуми, делегування влади відповідним органам, службу у державних органах, об'єднання у політичні партії та звернення до органів влади з пропозиціями та рекомендаціями.

Законність також є одним з основоположних принципів державного управління. Статті 6 і 19 Конституції України визначають, що всі органи влади здійснюють свої повноваження у встановлених межах та відповідно до законів України. Це стосується і сфери інформаційної безпеки, де важливим є дотримання правових норм у всіх аспектах діяльності.

Гласність, як принцип державного управління, забезпечує прозорість у діяльності державних органів, дозволяючи громадянам бачити процеси прийняття рішень у сфері інформаційної безпеки та захисту особистих даних. Це, серед іншого, підвищує довіру населення до державних інституцій. Вони ж управляються відповідними органами та мають певний громадський контроль від населення у вигляді відкритості, підзвітності та проінформованості. З іншого боку, саме гласність забезпечує високий ступінь ефективності OSINT-технологій та самої процедури.

Такий принцип державного управління, як об'єктивність, передбачає врахування реальних можливостей держави щодо реалізації управлінських рішень [2]. Це стосується матеріальних, технічних та інтелектуальних ресурсів, які використовуються для забезпечення інформаційної безпеки суспільства .

Організаційні принципи державного управління стосуються структурної побудови та функціонування державних органів, що займаються організацією інформаційної безпеки в Україні [3].

При цьому, галузевий принцип державного управління інформаційною безпекою відповідає за однорідні за характером функціонування об'єкти адміністративної діяльності. Вони закріплюються за відповідним органом управління, що забезпечує спеціалізований підхід до інформаційної безпеки.

Натомість, територіальний принцип державного управління передбачає управління інформаційною безпекою на визначених територіях, що дозволяє враховувати специфіку регіонів, населення та їхні потреби у захисті інформації. Це також стосується і боротьби із інформаційно-психологічними операціями агресорів під час оголошеної та неоголошеної війни [4].

Останні, функціональні принципи державного управління інформаційною безпекою, відповідають за функціонування системи безпеки. Функціональні принципи визначають зміст діяльності управлінських структур у сфері інформаційної безпеки певні напрямки діяльності, зокрема - нормативність, єдиноначальність і колегіальність [5].

Нормативність діяльності та принцип нормативності державного управління передбачає, що діяльність державних органів регулюється нормативними актами, які визначають правила та процедури у сфері інформаційної безпеки.

Єдиноначальність і колегіальність, як принципи державного управління інформаційною безпекою України, забезпечують ефективність управління, завдяки чіткій ієрархії та можливості колективного ухвалення рішень.

Принцип відповідальності за прийняті рішення, в межах державного управління інформаційною безпекою, підкреслює необхідність відповідальності державних службовців за свої дії у відповідній сфері [6]. Серед іншого, зазначений принцип сприяє підвищенню якості управління та гарантує зворотній зв'язок між владою та населенням.

Попри визначення загальних принципів державного управління інформаційною безпекою, сучасність ставить перед державою нові завдання. Швидке просування штучного інтелекту (ШІ) ставить перед урядами країн нові виклики щодо забезпечення інформаційної безпеки. Останні дослідження, проведені за замовленням Міністерства закордонних справ США, виявили ряд ризиків та небезпек, пов'язаних із розвитком інформаційних систем, що визначає перелік перших наступних кроків в державному управлінні [7].

Серед іншого, на думку дослідників, назріла необхідність створити спеціальне агентство, яке буде визначати максимально допустимий рівень обчислювальної потужності для навчання моделей ШІ та видавати дозволи компаніям на застосування цього рівня. Пропонується також законодавчо заборонити публічне розкриття особливостей функціонування потужних моделей ШІ, щоб уникнути зловживань та забезпечити контроль над технологіями. Відтак, необхідно посилити контроль за виробництвом та експортом чіпів для ШІ. Контроль над виробництвом і експортом апаратних компонентів для ШІ допоможе обмежити доступ до критичних технологій та оптимізує державне управління цією галуззю. Для цього варто спрямувати державні кошти на дослідження у сфері безпеки ШІ, що сприятиме розвитку безпечних технологій та мінімізації ризиків державного управління інформаційною безпекою.

Дослідники, які розробили звіт для замовлення Міністерства закордонних справ США стосовно впливу ШІ на близьке майбутнє, вважають, що державне обмеження тренувальних потужностей систем штучного інтелекту може зупинити змагання між лабораторіями та уповільнити виробництво більш потужних чіпів та обладнання. Згодом, майбутнє агентство з питань штучного інтелекту може підняти верхню межу обчислювальної потужності для тренування штучного інтелекту, якщо побачить докази того, що провідні моделі справді безпечні, або ж, навпаки, опустити межу, якщо є підтвердження небезпеки [8].

Проте, опрацювавши зазначений звіт, американський журнал TIME виявив дві категорії ризиків штучного інтелекту, які створюють загрозу державному управлінню інформаційною безпекою та на яких зосереджуються дослідники. Ризик вепонізації: «Такі системи можуть використовуватися для розробки і навіть запуску катастрофічних біологічних, хімічних або цифрових атак, або уможливити безпрецедентне застосування групи роботизованих пристроїв в якості зброї». Другим є ризик втрати контролю: «Існують причини припускати, що системи штучного інтелекту можуть стати неконтрольованими, якщо їх розвивати за допомогою сучасних технік, і почати поводитися вороже до людей за умовчанням» [9]. Обидві категорії ризиків посилює динаміка змагання в індустрії штучного інтелекту.

Ймовірність того, що перша компанія-розробник загального штучного інтелекту отримає всі супутні економічні переваги, змушує лабораторії ставити у пріоритет швидкість, а не безпеку. В такому разі гостро постає питання чіткого регулювання діяльності компаній розробників штучного інтелекту, що лягає відповідальністю на систему державного управління інформаційною безпекою [9].

У жовтні 2019 року Україна, що є членом Спеціального комітету зі штучного інтелекту при Раді Європи, приєдналася до Рекомендацій Організації економічного співробітництва і розвитку щодо штучного інтелекту (OECD/LEGAL/0449). Одним з основних завдань у галузі кібербезпеки, під час впровадження державної політики щодо розвитку штучного інтелекту, є захист комунікаційних, інформаційних та технологічних систем, а також інформаційних технологій. Особлива ж увага зосереджується на системах, які використовуються операторами ключових послуг, включаючи об’єкти критичної інфраструктури, оскільки вони є важливими для безперервності функціонування держави, суспільства та безпеки громадян [10].

Основні тези Концепції включають наступні напрямки державного управління, відповідно до встановлених принципів.

Згідно до вимог функціональних принципів державного управління, задекларований

захист фундаментальних прав, демократії та верховенства права. Концепція спрямована на забезпечення захисту фундаментальних прав людей, демократії та верховенства права, а також на стійкість довкілля від впливу штучного інтелекту.

Відповідно до соціально-політичних принципів державного управління запроваджено стимулювання інновацій. Водночас документ має на меті формально затвердити Європу як лідера в галузі інновацій та використання штучного інтелекту.

Організаційні принципи державного управління інформаційною безпекою відображені у регулюванні нормативною базою гострих кутів розвитку штучного інтелекту. Серед іншого, заборонено певні додатки штучного інтелекту, які загрожують правам громадян. До них відносяться: системи біометричної категоризації на основі конфіденційних характеристик; нецільовий збір зображень особи з Інтернету або записів камер відеоспостереження для створення баз даних розпізнавання облич; розпізнавання емоцій на робочому місці та в школах, соціальна оцінка, прогнозна поліція; маніпуляції людською поведінкою чи використанням уразливих місць людей [11].

Взагалі ж, правила використання систем високого ризику в державному управління інформаційною безпекою мають певні особливості. Згідно з умовами організаційних принципів державного управління інформаційною безпекою, можна використовувати штучний інтелект з високим ризиком лише у певних сферах соціальної діяльності. Приклади сфер державного управління інформаційною безпекою використання штучного інтелекту з високим ризиком включають: критичну інфраструктуру; освіту та професійну підготовку; працевлаштування; основні приватні та державні послуги (наприклад, охорону здоров'я, банки); певні системи правоохоронних органів; управління міграцією та кордонами; правосуддя та демократичні процеси.

Окремо варто зазначити, що правоохоронні органи не можуть використовувати біометричні системи ідентифікації, проте є винятки в особливих ситуаціях. У тексті йдеться і про те, що біометрична ідентифікація в реальному часі може бути розгорнута лише за дотримання суворих заходів безпеки, використання обмежене за часом та географією та за спеціального попереднього судового чи адміністративного дозволу [11].

Такі види використання можуть включати, наприклад, цілеспрямований пошук зниклого або запобігання терористичному нападу. Державне регулювання щодо використання таких систем постфактум вважається випадком, з високим ризиком адміністрування, який потребує судового дозволу, пов'язаного із кримінальним злочином.

Держава встановлює вимоги щодо принципу прозорості у державному управлінні використанням штучного інтелекту. Загальнодоступні системи повинні відповідати європейському законодавству про авторське право, публікувати детальну інформацію про контент, що використовується для навчання. Вимагається маркування зображень, аудіо- або відеоконтенту, створеного штучним інтелектом, з метою уникнення збентеження користувачів [12].

В останніх дослідженнях було зазначено, що рекомендації, стосовно управління промисловістю штучного інтелекту, можуть виглядати надто суворими, особливо в контексті кримінального покарання за використання відкритих систем або високого рівня розвитку штучного інтелекту. Дослідники приводять приклад марності впровадження в Сполучених Штатах кримінального покарання за використання відкритого коду штучного інтелекту[13]. Оскільки американське законодавство обмежується певною юрисдикцією, і розробники можуть легко перейти туди, де закони США не діятимуть.

Крім того, якщо уявити, що штучний інтелект також може використовуватись і проти демократії та свободи слова, то постає питання необхідності розширення заходів державного управління інформаційною безпекою за для суспільної безпеки всієї країни. Наприклад, у росії штучний інтелект використовується у якості інструменту пропаганди проти України, що демонструє потенційну небезпеку неправомірного та аморального використання технологій. Тому й збільшується актуальність посилення заходів інформаційної безпеки та їх державного управління.

Висновки та перспективи подальших досліджень. Принципи державного управління інформаційною безпекою, є основою для побудови ефективної системи захисту інформації в державі. Вони сприяють створенню прозорого, відповідального та ефективного управлінського апарату, здатного забезпечити національну безпеку та захист прав громадян.

У контексті швидкого розвитку штучного інтелекту, необхідно адаптувати існуючі принципи та вживати додаткових заходів для забезпечен-

ня безпеки новітніх технологій. Дотримання цих принципів дозволить знизити ризики та небезпеки, пов'язані з використанням штучного інтелекту, та забезпечить сталий розвиток у сфері інформаційної безпеки.

Завдяки швидкому розвитку технологій, зокрема штучного інтелекту, уже визначені принципи державного управління інформаційною безпекою потребують постійного оновлення та адаптації. Нові законодавчі ініціативи, демонструють важливість балансу між інноваціями та безпекою, забезпеченням основних прав громадян та захистом суспільства від потенційних ризиків.

Список використаної літератури:

1. Кузьменко Б., Чайковська О. Захист інформації. Ч. 1: Організаційно-правові засоби забезпечення інформаційної безпеки. Київ : *Вид. відділ КНУКІМ*, 2009. 83 с.
2. Кунєв Ю. Д. Принципи побудови та вдосконалення організаційної структури органіввнутрішніхсправ України: загальнотеоретичні аспекти державного управління : автореф. дис. ..канд. юрид. наук. Харків, 2001. 20 с.
3. Бакуменко В. Д. Державне управління : основи теорыъ, ысторыя ы практика: Навчальний посібник/ В. Д. Бакуменко, П. І. Надолішній, М. М. Їжа, Г. І. Арабаджи // За. Заг. ред. Ю. В. Ковбасюка, В. П. Трощинського, Ю. П. Сурміна. К. І., Бакуменка В. Д. Одеса: *ОРІДУ НАДУ*, 2009. 394 с.
4. Жовнірчик Я.Ф. Розвиток територіальної організації місцевого самоврядування в Україні : автореф. дис. ... канд. наук з держ. упр. : 25.00.04; *Нац. акад. держ. упр. при Президентові України*. Київ : *НАДУ*, 2005. 20 с.
5. ДСТУ 3396.2-97 Захист інформації. Технічний захист інформації. Терміни та визначення. Затверджено наказом Держстандарту України від 11.04.97 р. № 200.
6. Ярема О. Г., Єсімов С. С.. Предмет правового забезпечення 210 інформаційної безпеки в інформаційному праві. *Науковий вісник Львівського державного університету внутрішніх справ*. 2016. № 2. С. 244-252.
7. Бойко Д. Регулювання ШІ в Україні: головні тенденції та виклики [Електронний ресурс] Д. Бойко, І. Городиський // Центр Дністрянського. 2023. URL: https://dc.org.ua/news/regulyuvannya-shi-v-ukrayini-golovni-tendenciyi-ta-vyklyky.
8. Xing, J.(2019). The Application of Artificial Intelligence in Computer Network Technology in Big Data Era. *4thInternational Workshop on Materials Engineering and Computer Sciences*, 211–215. URL: https://doi.org/10.25236/iwmecs.2019.044
9. Регулювання штучного інтелекту: досвід США - Центр демократії та верховенства права. *Центр демократії та верховенства права* -. URL: https://cedem.org.ua/analytics/shtuchnyi-intelekt-usa/
10. Про схвалення Концепції розвитку штучного інтелекту в Україні : розпорядження Кабінету МіністрівУкраїни від 02.12.2020 No 1556-р // *Кабінет Міністрів України: офіц. сайт* . URL: https://www.kmu.gov.ua/npas/proshvalennya-koncepciyi-rozvitku-shtuchnogo-intelektu-v-ukrayinis21220
11. Про схвалення Концепції розвитку штучного інтелекту в Україні. Розпорядження Кабінету Міністрів України від 2 грудня 2020 р. № 1556-р. *Офіційний вебпортал парламенту України*. URL: https://zakon.rada.gov.ua/laws/show/1556-2020-р#Text
12. Економічна правда. У ЄС пропонують маркувати контент, створений штучним інтелектом. *Економічна правда*. URL: https://www.epravda.com.ua/news/2023/06/5/700828/
13. Can you trust ChatGPT's package recommendations? (2023). *Vulcan Cyber*. URL : https://vulcan.io/blog/ai-hallucinations-package-risk

Lysenko O. S. Principles of state management of information security and their characteristics

The article is devoted to the study of the principles of public administration of information security and their role in society and the state. In the course of the study, the author analyzed modern strategies and methods of ensuring information security at the state level, including both strategic and tactical planning. The study of these approaches allowed us to gain a deeper understanding and assessment of the effectiveness of measures aimed at preserving and protecting the state's information resources.

The approach of managing the information security of the state deserves much attention, so it is worthwhile to first define certain principles of state management of information security of society and the state, which form the fundamental basis for developing effective strategies and tactics in this area. Such an approach allows us to understand the importance of information security management as a key element of national security and stability, and also helps to identify priority areas of activity to ensure the protection of information resources and minimize threats to their inviolability.

The main focus is on the principles of state information security management, as it is the basis for establishing the key rules for organizing and conducting management activities in the field of information security. They are defined by legislation or summarize the existing legal norms of the country. These principles contribute to ensuring an appropriate level of information security, which is an important factor for the effective functioning of society, strengthening national security and protecting national interests in the world, as well as ensuring the inviolability and privacy of personal information of citizens, which is fundamental to preserving democratic values and the rule of law.

The article examines the main categories of public administration principles and their features, including socio-political, organizational and functional aspects. Additional principles for the development of governance in the field of information security will also be identified, in particular in the context of the introduction of artificial intelligence, which is taking place not only in Ukraine but also around the world.

Key words: *public administration, artificial intelligence, information security, legal support, OSINT, principles of public administration, information management.*