Філософія

УДК 316.4:004.8

DOI https://doi.org/10.5281/zenodo.18959852

Трансформація парадигми безпекового мислення в епоху алгоритмічного управління соціумом

Весеньов Євген Володимирович,
аспірант кафедри філософських, політичних і психологічних студій,
Черкаський державний технологічний університет, м. Черкаси, Україна,
https://orcid.org/0009-0002-6304-2868

Прийнято: 19.02.2026 | Опубліковано: 28.02.2026

Анотація: *Цифровізація суспільних процесів зумовлює глибинні зміни в способах конструювання безпеки та механізмах соціального регулювання. Інтеграція великих масивів даних, систем штучного інтелекту (далі – ШІ) та предиктивної аналітики трансформує традиційні уявлення про загрозу, контроль і відповідальність. У цих умовах безпекове мислення набуває нових ознак, пов'язаних із переходом від реактивного реагування до випереджального управління поведінковими моделями. Відповідно, це потребує концептуального переосмислення парадигмальних засад організації безпеки.*

Мета *статті полягає в теоретичному обґрунтуванні трансформації безпекового мислення під впливом алгоритмічного управління соціумом та моделюванні нової архітектури взаємодії між безпекою, свободою і контролем.*

Методи *роботи охоплюють системний аналіз, структурно-функціональний підхід, порівняльну реконструкцію еволюції безпекових парадигм, а також моделювання процесів алгоритмічного управління на основі концептуалізації цифрового нагляду та предиктивної аналітики.*

Результати *дослідження засвідчили, що відбувається зміщення суб'єктності безпеки від інституційних суб'єктів до алгоритмічних систем, які виконують функції збору, аналізу та прогнозування поведінкових ризиків. Встановлено, що об'єктом регулювання дедалі більше стають не події, а ймовірні траєкторії поведінки індивідів та груп. Запропоновано порівняльну таблицю еволюції безпекової парадигми, структурну схему алгоритмічного управління соціумом і матрицю трансформації балансу між безпекою, свободою та контролем. Доведено, що нова конфігурація управління характеризується превентивністю, циклічністю та інтеграцією цифрових інструментів у процес ухвалення рішень.*

Висновки. *Трансформація безпекового мислення має системний характер і пов'язана зі зміною онтології загрози, суб'єктності управління та нормативних меж втручання в соціальні процеси. Алгоритмічні механізми формують новий тип регулятивної раціональності, у межах якої безпека набуває прогностичного виміру. Отримані результати створюють підґрунтя для подальших досліджень нормативного забезпечення алгоритмічних систем і розроблення принципів їх відповідального застосування.*

Ключові слова: *цифровий нагляд, предиктивна аналітика, штучний інтелект, поведінкове профілювання, соціальне регулювання, регулятивна раціональність, цифрова влада.*

 ISSN: 3083-5712

Transformation of the security thinking paradigm in the era of algorithmic governance of society

Yevhen Vesenov,
Postgraduate Student of the Department of Philosophical, Political and Psychological Studies, Cherkasy State Technological University, Cherkasy, Ukraine, https://orcid.org/0009-0002-6304-2868

Abstract. *The digitalization of social processes entails profound changes in the ways security is constructed and in the mechanisms of social regulation. The integration of large-scale data sets, artificial intelligence systems, and predictive analytics transforms traditional understandings of threat, control, and responsibility. Under these conditions, security thinking acquires new features associated with the shift from reactive response to anticipatory management of behavioral models. This, in turn, necessitates a conceptual rethinking of the paradigmatic foundations of security organization.*

The objective *of the study is to provide a theoretical substantiation of the transformation of security thinking under the influence of algorithmic governance of society and to model a new architecture of interaction between security, freedom, and control.*

Methods*. The research methodology includes systemic analysis, a structural-functional approach, comparative reconstruction of the evolution of security paradigms, and modeling of algorithmic governance processes based on the conceptualization of digital surveillance and predictive analytics.*

Results. *The findings demonstrate a shift in the subjectivity of security from institutional actors to algorithmic systems that perform the functions of collecting, analyzing, and forecasting behavioral risks. It has been established that the object of regulation increasingly shifts from actual events to probable trajectories of*

individual and group behavior. The study proposes a comparative table of the evolution of security paradigms, a structural model of algorithmic governance of society, and a matrix of transformation of the balance between security, freedom, and control. It is argued that the emerging configuration of governance is characterized by preventiveness, cyclicality, and the integration of digital tools into decision-making processes.

Conclusions. *The transformation of security thinking is systemic in nature and is associated with changes in the ontology of threat, the subjectivity of governance, and the normative boundaries of intervention in social processes. Algorithmic mechanisms form a new type of regulatory rationality within which security acquires a predictive dimension. The results provide a conceptual foundation for further research on the normative regulation of algorithmic systems and the development of principles for their responsible application.*

Keywords: *digital surveillance, predictive analytics, artificial intelligence, behavioral profiling, social regulation, regulatory rationality, digital power.*

Постановка проблеми. Інтенсивний розвиток цифрових технологій змінює логіку функціонування державних і наддержавних систем управління. Безпека більше не обмежується захистом території або інституційного порядку. Вона дедалі частіше конструюється через механізми збору, аналізу та прогнозування даних, що дають змогу передбачати поведінкові ризики та здійснювати превентивний вплив на соціальні процеси.

У цих умовах виникає проблема концептуального осмислення змін, які відбуваються у сфері безпекового мислення. Традиційні підходи, що ґрунтуються на реактивній логіці та ієрархічній моделі влади, є недостатніми для пояснення нових форм контролю, де алгоритмічні системи виконують функції аналізу й ухвалення управлінських рішень.

 ISSN: 3083-5712

Зв’язок вказаної проблеми з важливими науковими та практичними завданнями полягає в необхідності розроблення нових теоретичних моделей функціонування безпеки в цифровому середовищі, визначення меж допустимого алгоритмічного втручання в соціальні процеси, формування регуляторних механізмів, здатних забезпечити баланс між захистом суспільства та збереженням прав і свобод людини.

Отже, проблема трансформації безпекового мислення має міждисциплінарний характер і безпосередньо пов’язана із сучасними викликами цифрового управління.

Аналіз останніх досліджень і публікацій. Проведений аналіз наукових джерел засвідчує міждисциплінарний характер дослідження трансформації безпекового мислення в умовах алгоритмічного управління соціумом. Опрацьовані роботи охоплюють проблематику кібербезпеки, цифровізації державного управління, культурно-ціннісних трансформацій, психологічних механізмів інформаційного впливу та регуляторних аспектів застосування ШІ. Сукупно вони формують теоретико-методологічне підґрунтя для осмислення зміни логіки безпеки в цифрову епоху.

Модель безпеки та контролю доступу до даних у хмарних сервісах на основі механізму керування ідентифікацією та доступом (Identity and Access Management, далі – IAM), що дає змогу конкретизувати інструментальний рівень алгоритмічного управління доступом до інформаційних ресурсів, розробляють А. Партика та Я. Захарова. Вони пропонують концепцію, яка демонструє перехід від статичних моделей захисту до динамічного управління ідентичностями, що безпосередньо пов’язано зі зміною суб’єктності безпеки [1]. Сучасні кіберзагрози критичної інфраструктури України та світу аналізують А. Ільєнко, В. Телющенко та О. Дубчак, акцентуючи на зростанні складності атак і гібридному характері ризиків. Водночас їхнє дослідження

ISSN: 3083-5712

підкреслює необхідність переходу до превентивних та прогностичних моделей забезпечення стійкості [2].

У своїй статті А. Бойко окреслює мову як інструмент трансляції цінностей та формування культурної ідентичності [3]. У напрямі нашої проблематики це допомагає інтерпретувати безпекове мислення як ціннісно зумовлену категорію, що визначається через дискурсивні практики. Автори А. І. Бойко та А. О. Бойко вивчають систему цінностей як фундамент культурної ідентичності сучасного суспільства, що дає змогу розглядати алгоритмічне управління не лише як технологічний, а і як культурно-нормативний феномен [4].

Метод оцінювання рівня підвищення кіберзахисту критичної інфраструктури держави пропонують О. Корченко, Є. Іванченко, О. Бакалинський, Д. Мялковський та Д. Зубков [5]. Це напрацювання важливе для формування критеріїв вимірювання ефективності алгоритмічних рішень у сфері безпеки. Застосування ШІ для характеристики стану кібербезпеки критичної інфраструктури обґрунтовують Г. Гайдур, С. Гахов та О. Скибун [6]. Дослідження демонструє зміщення центру ухвалення рішень у бік алгоритмічних систем аналізу ризиків.

Науковці В. Балацька, В. Побережник та І. Опірський розглядають використання блокчейн-технологій та NFT для розмежування доступу до державних реєстрів, що актуалізує проблему децентралізації контролю та трансформації механізмів довіри [7]. Підходи до гарантування інформаційної безпеки в кіберпросторі систематизують В. Хорошко, М. Шелест, Ю. Ткач та І. Дюба, підкреслюючи необхідність інтеграції технічних та організаційних механізмів захисту [8]. Ретроспективний аналіз цифровізації в системі національної безпеки здійснює Т. Яровой, акцентуючи на ролі публічного управління [9]. Відповідно, це дає змогу простежити еволюцію управлінських моделей від адміністративних до цифрових.

Концепцію адаптивного управління інформаційною безпекою в хмарно орієнтованих системах, що актуалізує потребу в гнучких алгоритмічних механізмів реагування, розробляють С. Рзаєва, П. Складанний, Ю. Костюк, В. Абрамов та В. Кравченко [10].

Оновлений стандарт ISO/IEC 27002:2022 аналізують Н. Кухарська, С. Семенюк та О. Полотай, демонструючи інституціоналізацію нових вимог до управління інформаційними ризиками [11]. Науковці С. Базарний, Н. Микитюк та О. Терновий досліджують психологічний вплив ботів у соціальних мережах, що розкриває поведінковий вимір алгоритмічного впливу та підтверджує зміну об'єкта безпеки з подій на поведінкові патерни [12].

Дослідники А. Бойко (A. Boyko), І. Наглюков (I. Nahliukov), М. Балух (M. Balukh), Г. Зінченко (H. Zinchenko) та Л. Костенюк (L. Kosteniuk) підкреслюють роль освітніх програм у формуванні культури безпеки, що дає змогу розглядати безпекове мислення як соціально сконструйований процес [13]. Феномен surveillance capitalism і системні цифрові ризики концептуалізує Д. Керран (D. Curran), наголошуючи на взаємопов'язаності даних та зростанні системної вразливості в умовах алгоритмічного управління. [14] Учені Дж. Саура (J. Saura), Д. Рібейро-Соріано (D. Ribeiro-Soriano) та Д. Паласіос-Маркіс (D. Palacios-Marqués) аналізують проблеми приватності під час впровадження ШІ в державному управлінні, що актуалізує нормативний вимір трансформації безпеки [15]. У культурологічному дослідженні урбаністичного простору Д. Боклах порушує питання символічних конструкцій соціального середовища, що дає змогу розглядати алгоритмічне управління як форму реконфігурації соціального простору [16]. Воєнізацію освітнього процесу як інструмент ідеологічного впливу аналізує П. Лисянський, демонструючи зв'язок між освітньою політикою, становленням світогляду та безпековими стратегіями держави [17].

 ISSN: 3083-5712

Отже, систематизація наукових праць дає змогу виокремити кілька напрямів дослідження, а саме: технологічно-інструментальний (кіберзахист, ШІ, блокчейн, ІАМ), управлінський (цифровізація публічного управління, стандарти безпеки), поведінково-психологічний (вплив ботів, формування культури безпеки), нормативно-ціннісний (приватність, культурна ідентичність, освітній вплив). Водночас, попризначну кількість досліджень, немає цілісної концептуальної моделі, яка б інтегрувала технологічний, поведінковий та нормативний виміри в єдину парадигмальну рамку. Саме ця прогалина зумовлює необхідність подальшого теоретичного осмислення трансформації безпекового мислення в умовах алгоритмічного управління соціумом.

Виділення невирішених раніше частин загальної проблеми. Попри наявність значного масиву досліджень у сфері цифрового нагляду, штучного інтелекту та управлінських інновацій, залишаються аспекти, що не отримали належного концептуального узагальнення. Зокрема, недостатньо вивченим є питання зміни суб'єктності безпеки. У більшості праць алгоритмічні системи розглядають як інструменти, проте не аналізують їх роль як активних учасників управлінського процесу, що впливають на формування рішень. Також немає системної реконструкції еволюції безпекової парадигми з урахуванням переходу від подієвої до поведінкової логіки регулювання. Праці зосереджуються на технологічних моментах, залишаючи поза увагою зміни онтології загрози. Водночас не до кінця опрацьованим є питання нормативного балансу між безпекою, свободою та контролем в умовах алгоритмічного управління. Причиною цього є швидкість технологічних змін та відставання правових механізмів від практик цифрового впровадження.

Вирішення зазначених аспектів є необхідним для формування цілісної теоретичної моделі трансформації безпекового мислення. У межах статті передбачено аргументувати зміну архітектури управління, змоделювати

 ISSN: 3083-5712

механізм алгоритмічного впливу та виявити ризикові зони нової регулятивної конфігурації.

Формулювання цілей статті (постановка завдання). Метою статті є теоретичне осмислення трансформації безпекового мислення в умовах алгоритмічного управління соціумом та обґрунтування нової моделі взаємодії між безпекою, свободою і контролем. Для досягнення дослідницької мети поставлено такі завдання:

1) здійснити порівняльну реконструкцію еволюції безпекової парадигми та обґрунтувати перехід від реактивної до прогностичної логіки управління;

2) розробити структурну модель алгоритмічного управління соціумом та визначити зміну суб'єктності в процесі ухвалення управлінських рішень;

3) сформувати матрицю трансформації балансу між безпекою, свободою й контролем та окреслити основні ризики нової регулятивної конфігурації.

Виклад основного матеріалу дослідження. Сучасний розвиток соціуму засвідчує, що безпека перестає бути виключно сферою реагування на вже наявні загрози та дедалі більше інтегрується в процеси цифрового моделювання й управління поведінковими процесами. Алгоритмізація публічного управління, впровадження систем штучного інтелекту та інтенсивне використання великих масивів даних трансформують саму онтологію безпеки – від захисту території до контролю динаміки інформаційних і когнітивних потоків. Дослідження новітніх кіберзагроз критичної інфраструктури демонструють, що безпекові ризики набувають системного та мережевого характеру, виходячи за межі традиційної військово-політичної логіки [2, с. 150]. Водночас поширення цифрового нагляду та феномену системних цифрових ризиків актуалізують проблему структурної

 ISSN: 3083-5712

вразливості соціальних систем в умовах тотальної взаємопов'язаності [14]. У сфері державного управління застосування алгоритмічних рішень на основі поведінкових даних породжує нові виклики щодо балансу між ефективністю управління та гарантіями прав і свобод громадян [15]. Отже, трансформація парадигми безпекового мислення відображає глибинний зсув від реактивного контролю до предиктивного управління соціальною динамікою, що потребує системної реконструкції її концептуальних засад.

Проведений аналіз наукової літератури показав, що парадигма безпекового мислення історично формувалася в межах інституційно-державницького підходу, де безпеку трактували як функцію суверенної влади та механізм підтримання політичної стабільності. У класичному вимірі вона була пов'язана з територіальністю, монополією держави на легітимне насильство та інституційним контролем над ресурсами. Водночас процеси цифровізації публічного управління й стрімке впровадження інтелектуальних інформаційних систем зумовили якісні зміни в структурі загроз і способах їх нейтралізації, що засвідчили сучасні дослідження кіберзахисту та цифрової трансформації сектору безпеки [9, с. 175]. При цьому розвиток методів оцінювання стану кіберзахисту об'єктів критичної інфраструктури демонструє перехід від фрагментарного реагування до системного моніторингу й аналітики ризиків [5, с. 3]. У цих умовах доцільною постає порівняльна реконструкція компонентів трансформації безпекової парадигми, що дає змогу простежити еволюцію від реактивної моделі реагування до превентивно-прогностичної моделі управління поведінковими процесами (табл. 1). Саме така реконструкція уможливлює концептуалізацію алгоритмічної безпеки як нової форми організації влади в цифровому соціумі.

Таблиця 1

Трансформація парадигми безпекового мислення

Критерій	Класична парадигма	Цифрова парадигма	Алгоритмічна парадигма
Суб'єкт безпеки	Держава	Держава та корпорації	Алгоритмічні системи
Об'єкт безпеки	Територія, суверенітет	Інформаційний простір	Поведінкові патерни
Тип загроз	Фізичні, військові	Кіберзагрози	Поведінкова нестабільність
Механізм реагування	Постфактум контроль	Моніторинг у реальному часі	Предиктивне управління
Інструменти	Силові структури	Big Data, цифровий нагляд	Штучний інтелект, предиктивна аналітика
Логіка дії	Реактивна	Оперативна	Прогностична

Джерело: сформовано автором на основі [1, с. 12; 2, с. 151; 6, с. 32]

Порівняльна таблиця 1 засвідчує, що трансформація парадигми безпеки відбувається не лише на рівні інструментального оновлення технологій, а передусім на рівні зміни логіки владарювання та типу раціональності управління. Якщо класична парадигма ґрунтувалася на територіально-інституційній суб'єктності держави, а цифрова – на розширенні простору моніторингу через інформаційні мережі, то алгоритмічна парадигма переносить центр ваги на обробку поведінкових даних та предиктивне моделювання соціальної динаміки.

Отже, простежується зміна самого об'єкта безпеки, тобто замість фізичного простору чи інформаційної інфраструктури головним стає управління поведінковими траєкторіями індивідів і груп. Відповідно це означає перехід від контролю події до управління ймовірністю події, що

формує нову архітектуру влади – розподілену, алгоритмічно опосередковану та засновану на аналітиці великих даних. Для цього дослідження така модель створює теоретичну основу для подальшого осмислення алгоритмічного управління соціумом як феномену, що трансформує не лише безпекові практики, а й саму природу соціального порядку.

Подальше вивчення алгоритмічної парадигми безпеки потребує переходу від загальнотеоретичного аналізу до виявлення її внутрішньої структурної логіки. Якщо алгоритмічна раціональність стає визначальною для сучасного управління, то виникає питання щодо архітектури взаємодії даних, аналітичних інструментів і управлінських рішень. Наявні дослідження впровадження штучного інтелекту в системи кіберзахисту та оцінювання стану критичної інфраструктури демонструють, що рішення дедалі частіше ухвалюються на основі автоматизованої обробки поведінкових і технічних показників [6, с. 31]. Водночас використання поведінкових даних у державних алгоритмічних системах актуалізує питання прозорості, відповідальності та ризиків концентрації цифрової влади.

У такій конфігурації алгоритмічне управління постає не як окремий технологічний інструмент, а як цілісна багаторівнева система, де збір даних, їх аналітична інтерпретація та імплементація управлінських рішень утворюють замкнений контур впливу на соціальну динаміку [10]. Саме тому наступним логічним кроком є побудова структурної моделі алгоритмічного управління соціумом, яка дасть змогу візуалізувати механізм трансформації даних у владні практики.

Алгоритмічне управління соціумом виникає як результат інституційної інтеграції цифрових платформ, аналітики великих даних та систем штучного інтелекту в механізми публічного й корпоративного врядування. Відповідно його функціонування спирається на безперервний збір, агрегацію та інтерпретацію масивів даних, що відображають як технічні параметри

функціонування інфраструктур, так і поведінкові характеристики індивідів та груп. Сучасні дослідження у сфері оцінювання кіберзахисту та застосування штучного інтелекту в управлінні критичною інфраструктурою засвідчують перехід до моделей, у яких аналітичні модулі стають основною ланкою ухвалення рішень [8, с. 77]. Водночас аналіз системних цифрових ризиків показує, що зростання взаємопов'язаності даних формує нову конфігурацію влади, де прогнозування імовірної поведінки стає стратегічним ресурсом управління [14].

Отже, алгоритмічне управління доцільно розглядати як структурно організований процес, у межах якого дані трансформуються в управлінські впливи через послідовність аналітичних операцій. Для його концептуальної впорядкованості пропонуємо структурну модель, що відображає логіку перетворення інформаційних потоків на механізми соціальної регуляції (рис. 1).

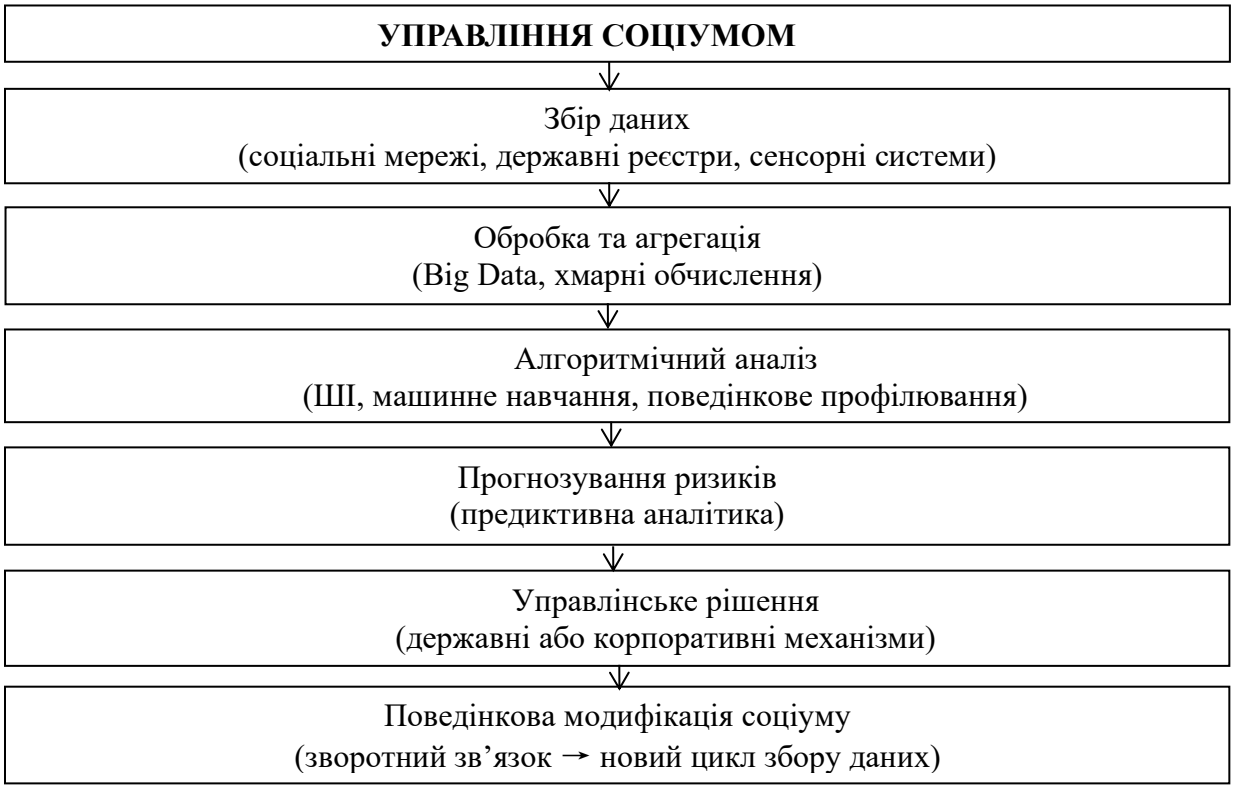

Рис. 1. Модель алгоритмічного управління соціумом

Джерело: сформовано автором на основі [5, с. 3; 9, с. 175; 11, с. 76]

Запропонована модель демонструє послідовний та самовідтворюваний характер алгоритмічного управління, у межах якого безпека перетворюється на процес безперервного збору, аналізу та передбачення. Кожен етап – від акумуляції даних до поведінкової модифікації – не є ізольованим, а формує замкнений контур зворотного зв'язку, що підсилює аналітичну спроможність системи в наступному етапі.

Принциповим є те, що центр ухвалення рішень поступово зміщується від людини-оператора до алгоритмічно опосередкованих систем, які здійснюють попередню селекцію ризиків і визначають пріоритетність управлінських реакцій. У такій конфігурації алгоритм є не лише інструментом реалізації політики безпеки, а й активним елементом становлення управлінської раціональності. Відповідно це дослідження створює підстави для обґрунтування розуміння трансформації суб'єктності безпеки, тобто вона набуває гібридного характеру, де людські та машинні компоненти співдіють у межах єдиної аналітичної екосистеми. Саме ця гібридизація управління є основною ознакою переходу до алгоритмічної парадигми безпекового мислення.

Отже, сформована модель алгоритмічного управління дала змогу окреслити внутрішню логіку функціонування нової безпекової раціональності та показати, як дані трансформуються в управлінські впливи. Водночас сама наявність такого послідовного механізму неминуче актуалізує питання його нормативних і ціннісних меж. Якщо алгоритм стає співучасником ухвалення рішень, то змінюється не лише інструментарій безпеки, а й баланс між захистом, свободою та контролем. Вивчення системних цифрових ризиків та впровадження алгоритмічних рішень у державному секторі засвідчують, що ефективність прогнозування прямо корелює зі зростанням обсягу втручання в приватну й соціальну сфери [7, с. 99]. У цьому розумінні виникає потреба не

 ISSN: 3083-5712

лише технічного, а й аксіологічного аналізу наслідків алгоритмічного управління. Саме тому логічним продовженням дослідження є матричне моделювання трансформації балансу «безпека – свобода – контроль» як головного індикатора зміни парадигми.

Алгоритмічне управління радикалізує класичну дилему співвідношення безпеки та свободи, оскільки до неї додається третій вимір – цифрово-алгоритмічний контроль, що функціонує в режимі постійного моніторингу та предиктивної аналітики. На відміну від традиційних форм нагляду, алгоритмічні системи здійснюють неперервну обробку поведінкових даних, створюючи умови для превентивного втручання ще до настання події. Сучасні дослідження впровадження штучного інтелекту в управлінні інформаційною безпекою та критичною інфраструктурою демонструють, що такі системи підвищують ефективність реагування, але водночас розширюють межі цифрового спостереження [6, с. 33]. Паралельно аналіз проблем приватності в умовах використання поведінкових даних у державних алгоритмічних системах акцентує на ризиках надмірної концентрації цифрової влади [15]. У зв'язку із цим доцільним є застосування матричного підходу, який дає змогу структуровано відобразити взаємозв'язок між рівнями впливу алгоритмічного управління та потенційними зонами нормативної напруги (табл. 2).

Таблиця 2

Матриця трансформації балансу в умовах алгоритмічного управління

Рівень впливу	Посилення безпеки	Обмеження свободи	Зона ризику
Індивідуальний	Превентивний захист	Втрата приватності	Алгоритмічна дискримінація
Соціальний	Прогнозування конфліктів	Поведінкова стандартизація	Маніпуляція свідомістю
Державний	Оперативне реагування	Надмірний нагляд	Концентрація цифрової влади

Джерело: сформовано автором на основі [1, с. 12; 8, с. 77; 12, с. 67; 15]

Запропонована матриця в межах алгоритмічної парадигми фіксує системну напругу між трьома взаємопов'язаними вимірами – безпекою, свободою та контролем. Вона демонструє, що кожне посилення безпеки на індивідуальному, соціальному чи державному рівнях супроводжується відповідним ризиком звуження автономії та зростанням інтенсивності цифрового нагляду. Отже, алгоритмічне управління не є нейтральним технологічним засобом, а структуроутворювальним чинником нової конфігурації владних відносин.

Особливо принциповим є те, що зона ризику формується не на периферії системи, а в самій її логіці: предиктивність потребує масиву даних, масив даних – нагляду, а нагляд трансформує соціальну поведінку. У результаті безпека набуває характеру постійного передбачення, а свобода – умовного статусу, залежного від алгоритмічної інтерпретації поведінки. Для дослідження це означає необхідність переосмислення нормативної архітектури безпеки: мова йде не лише про вдосконалення регуляторних механізмів, а про створення нової етики алгоритмічного врядування, де технологічна ефективність має бути збалансована принципами прозорості, підзвітності та збереження людської суб'єктності. Отже, наведене вище не лише репрезентує результати порівняльного та структурного аналізу трансформації безпекового мислення, а й обґрунтовує концептуальний перехід до алгоритмічної моделі соціального управління як основного виклику сучасної теорії безпеки.

Висновки. Проведене дослідження дало підстави стверджувати, що трансформація парадигми безпекового мислення має не фрагментарний, а системний характер і зумовлена глибинною інтеграцією алгоритмічних механізмів у процеси соціального управління. У процесі порівняльного аналізу встановлено, що відбувається зміна самої раціональності безпеки, тобто від реактивного реагування на події до превентивно-прогностичного управління

 ISSN: 3083-5712

поведінковими траєкторіями. Безпека в алгоритмічну епоху постає як процес безперервного аналізу даних, моделювання ризиків і коригування соціальної динаміки.

Розроблена структурна модель алгоритмічного управління дала змогу концептуалізувати внутрішню архітектуру цього процесу та обґрунтувати зміщення суб'єктності від виключно інституційно-державного центру до гібридної конфігурації, де алгоритмічні системи є співучасниками ухвалення рішень. Водночас матриця трансформації балансу «безпека – свобода – контроль» продемонструвала, що зростання ефективності прогнозування супроводжується формуванням нових зон нормативної напруги – від алгоритмічної дискримінації до концентрації цифрової влади та стандартизації поведінки.

Доведено, що алгоритмічне управління є основним чинником переосмислення сучасної безпекової парадигми, а запропонована концептуальна модель допомагає інтегрувати технологічний, управлінський та аксіологічний виміри в єдину аналітичну рамку. Наукова новизна полягає в поєднанні порівняльного, структурного та матричного підходів для комплексного опису трансформації безпекового мислення під час цифрової трансформації.

Перспективними напрямами подальших наукових досліджень є розроблення моделей підзвітності алгоритмічних систем у сфері публічного управління та безпеки з урахуванням принципів прозорості й аудиту рішень; формування етичних стандартів алгоритмічного врядування, що забезпечують баланс між ефективністю прогнозування та збереженням людської суб'єктності; емпіричне вивчення впливу алгоритмічних систем на поведінкові патерни соціуму, зокрема в умовах кризових і воєнних викликів. Отже, проблема трансформації безпекового мислення в епоху алгоритмічного управління не вичерпується технічним виміром, а потребує подальшого

ISSN: 3083-5712

міждисциплінарного осмислення, де поєднуються безпекознавство, теорія управління, цифрова етика та правові компоненти.

Список використаної літератури

1. Партика А. І., Захарова Я. А. Модель безпеки та контролю доступу до даних у хмарних сервісах на основі механізму Identity and Access management (IAM). *Безпека інформації.* 2024. № 30 (1). С. 12–20. DOI: https://doi.org/10.18372/2225-5036.30.18575

2. Ільєнко А., Телющенко В., Дубчак О. Сучасні кіберзагрози критичної інфраструктури України та світу. *Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка».* 2025. № 3 (27). С. 150–164. DOI: https://doi.org/10.28925/2663-4023.2023.27.719

3. Бойко А. Мова як засіб трансляції цінностей і формування культурної ідентичності в освіті. *Humanities studies.* 2025. № 22 (99). С. 9–17. DOI: https://doi.org/10.32782/hst-2025-22-99-01

4. Бойко А. І., Бойко А. О. Система цінностей як фундамент культурної ідентичності в сучасному суспільстві: огляд основних проблем. *Культурологічний альманах.* 2024. № 4. С. 166–177. DOI: https://doi.org/10.31392/cult.alm.2024.4.19

5. Корченко О., Іванченко Є., Бакалинський О., Мялковський Д., Зубков Д. Метод оцінювання рівня підвищення стану кіберзахисту об’єктів критичної інфраструктури держави. *Science-based technologies.* 2024. № 61 (1). С. 3–20. DOI: https://doi.org/10.18372/2310-5461.61.18509

6. Гайдур Г. І., Гахов С. О., Скибун О. Ж. Оцінка стану кібербезпеки критичної інфраструктури з використанням ШІ. *Сучасний захист інформації.* 2025. № 2. С. 31–41. DOI: https://doi.org/10.31673/2409-7292.2025.020831

7. Балацька В., Побережник В., Опірський І. Використання non-fungible tokens та блокчейн для розмежування доступу до державних

реєстрів. *Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка».* 2024. № 4 (24). С.99–114. DOI: https://doi.org/10.28925/2663-4023.2024.24.99114

8. Хорошко В., Шелест М., Ткач Ю., Дюба І. Забезпечення інформаційної безпеки в кіберпросторі. *Безпека інформації.* 2024. № 30 (1). С. 77–78. DOI: https://doi.org/10.18372/2225-5036.30.18607.

9. Яровой Т. С. Ретроспектива цифровізації в системі національної безпеки: роль публічного управління. *Вчені записки ТНУ імені В. І. Вернадського. Серія: Публічне управління та адміністрування.* 2025. Т. 36 (75). № 1. С. 175–180. DOI: https://doi.org/10.32782/TNU-2663-6468/2025.1/29

10. Рзаєва С. Л., Складанний П. М., Костюк Ю. В., Абрамов В. О., Кравченко В. Г. Адаптивне управління інформаційною безпекою в хмарно-орієнтованих інтелектуальних транспортних системах. *Безпека інформації.* 2025. № 31 (1). С. 23–26. DOI: https://doi.org/10.18372/2225-5036.31.20634

11. Кухарська Н. П., Семенюк С. А., Полотай О. І. Ключові аспекти оновленого стандарту ISO/IEC 27002:2022. *Сучасний захист інформації.* 2025. № 2 (62). С. 76–87. DOI: https://doi.org/10.31673/2409-7292.2025.023969

12. Базарний С., Микитюк Н., Терновий О. Психологічний вплив штучних електронних акаунтів (ботів) на агентів соціальних мереж в інтересах інформаційної операції. *Безпека інформації.* 2024. № 30 (1). С. 67–72. DOI: https://doi.org/10.18372/2225-5036.30.18605.

13. Boyko A., Nahliukov I., Balukh M., Zinchenko H., Kosteniuk L. The impact of educational programmes on building safety culture in modern society. *Revista Eduweb.* 2024. Vol. 18. № 3. P. 178–192. DOI: https://doi.org/10.46502/issn.1856-7576/2024.18.03.14

14. Curran D. Surveillance capitalism and systemic digital risk: the imperative to collect and connect and the risks of interconnectedness. *Big Data & Society*. 2023. Vol. 10. № 1. DOI: https://doi.org/10.1177/20539517231177621

15. Saura J. R., Ribeiro-Soriano D., Palacios-Marqués D. Assessing behavioral data science privacy issues in government artificial intelligence deployment. *Government Information Quarterly*. 2022. Vol. 39. № 4. DOI: https://doi.org/10.1016/j.giq.2022.101679

16. Боклах Д. Ю. Топос європейського міста в художній рецепції творів Т. Шевченка: поліфонізм побудови урбаністичного часопросторового континууму. *Spheres of culture*. 2019. № 18. URL: https://library.dspu.edu.ua/wp-content/uploads/2024/07/sphere_2019_v_18.pdf (дата звернення: 10.12.2025).

17. Лисянський П. Л. Воєнізація освітнього процесу в РФ: загрози та наслідки. *Регіональні студії: науковий збірник*. 2024. № 38. С. 26–32. DOI: https://doi.org/10.32782/2663-6170/2024.38.4