Електронний журнал «Державне управління: удосконалення та розвиток» включено до переліку наукових фахових видань України з державного управління (Категорія «Б», Наказ Міністерства освіти і науки України № 1643 від 28.12.2019). Спеціальність – 281.

Державне управління: удосконалення та розвиток. 2025. № 5.

DOI: http://doi.org/10.32702/2307-2156.2025.5.24

УДК 004.9:351.72

Алієв Азер Аріф огли,

аспірант кафедри міжнародних відносин та політичного консалтингу,

ЗВО «Відкритий міжнародний університет розвитку людини «Україна»,

м. Київ, Україна

ORCID: https://orcid.org/0009-0009-2040-1323

ІНТЕГРАЦІЯ ЦИФРОВИХ ТЕХНОЛОГІЙ У МЕХАНІЗМИ ЗАБЕЗПЕЧЕННЯ НАЦІОНАЛЬНОЇ БЕЗПЕКИ ДЕРЖАВИ

Aliyev Azer,

Postgraduate student of the Department of International Relations and Political Consulting, Open International University of Human Development "Ukraine", Kyiv, Ukraine

INTEGRATION OF DIGITAL TECHNOLOGIES INTO THE MECHANISMS OF ENSURING NATIONAL SECURITY OF THE STATE

У статті розглядається комплекс теоретичних та прикладних аспектів інтеграції цифрових технологій у сучасну систему забезпечення національної безпеки держави. Цифровізація охоплює дедалі ширші сфери функціонування державних інституцій, зокрема оборону, правоохоронну діяльність, кібербезпеку, антикризове управління та інформаційну безпеку. Цей процес

супроводжується як появою нових можливостей, так і формуванням новітніх загроз, що вимагає переосмислення традиційних підходів до управління безпекою. У роботі здійснено аналіз ключових цифрових технологій, таких як штучний інтелект, великі дані (Big Data), блокчейн, Інтернет речей (IoT), хмарні обчислення, а також їх потенціал щодо посилення превентивного моніторингу загроз, оперативного реагування та прогнозування кризових ситуацій. Адже, вивчення інтеграції цифрових технологій у механізми забезпечення національної безпеки є надзвичайно актуальним у контексті зростаючих кіберзагроз, інформаційних війн та трансформації глобального безпекового середовища. Ефективне використання цифрових інструментів дозволяє державі оперативно реагувати на виклики, зміцнювати стратегічну стійкість та підвищувати рівень захищеності критично важливих інфраструктур.

Значну увагу приділено проблемам кібербезпеки та захисту критичної інформаційної інфраструктури, що становить основу цифрового середовища держави. Автором підкреслено необхідність формування інтегрованої цифрової стратегії національної безпеки, що поєднує технологічні, правові, організаційні та кадрові ресурси. Запропоновано концептуальний підхід до створення адаптивної системи цифрової безпеки, що здатна динамічно реагувати на зміни у спектрі загроз. Результати дослідження можуть бути використані як основа для розробки державних стратегій цифрової трансформації та модернізації безпекових структур у контексті сучасних глобальних викликів.

The article examines a set of theoretical and applied aspects of the integration of digital technologies into the modern system of ensuring the national security of the state. Digitalization is covering more and more areas of functioning of state institutions, including defense, law enforcement, cybersecurity, crisis management and information security. This process is accompanied by both the emergence of new opportunities and the formation of new threats, which requires a rethinking of

traditional approaches to security management. The paper analyzes key digital technologies, such as artificial intelligence, big data, blockchain, Internet of Things (IoT), cloud computing, and their potential to enhance preventive threat monitoring, rapid response and crisis forecasting. After all, the study of the integration of digital technologies into national security mechanisms is extremely relevant in the context of growing cyber threats, information wars and the transformation of the global security environment. Effective use of digital tools allows the state to respond quickly to challenges, strengthen strategic resilience and increase the level of security of critical infrastructures. In the current context of rapid digitalization of society and increasing threats in cyberspace, the integration of digital technologies into the national security system is gaining strategic importance. The implementation of intelligent monitoring systems, cybersecurity measures, big data analytics, and artificial intelligence is significantly transforming traditional approaches to the detection, prevention, and neutralization of threats to state security.

Considerable attention is paid to the problems of cybersecurity and protection of critical information infrastructure, which is the basis of the digital environment of the State. The author emphasizes the need to form an integrated digital national security strategy that combines technological, legal, organizational and human resources. The author proposes a conceptual approach to creating an adaptive digital security system capable of dynamically responding to changes in the spectrum of threats. The results of the study can be used as a basis for the development of state strategies for digital transformation and modernization of security structures in the context of current global challenges.

Ключові слова: цифрові технології, механізм, національна безпека, держава, інтеграція.

Keywords: digital technologies, mechanism, national security, state, integration.

Постановка проблеми у загальному вигляді та її зв'язок із важливими науковими чи практичними завданнями. У сучасних умовах глобалізації та стрімкого розвитку інформаційно-комунікаційних технологій цифрова трансформація охоплює всі сфери суспільного життя, зокрема сферу національної безпеки. З одного боку, цифрові технології відкривають нові можливості для ефективнішого управління безпековими процесами, прогнозування загроз, швидкого реагування та координації між державними органами. З іншого боку, цифровізація створює нові вразливості, пов'язані з кіберзагрозами, витоком конфіденційної інформації та зростанням залежності від цифрової інфраструктури. На цьому тлі виникає нагальна потреба в науковому обґрунтуванні підходів до інтеграції цифрових технологій у систему національної безпеки, що дозволить підвищити її ефективність та адаптивність до нових викликів. Проблема полягає у недостатньому теоретичному та практичному опрацюванні механізмів такої інтеграції, а також у відсутності системного бачення ризиків і переваг цифровізації для безпекового сектора.

Аналіз останніх досліджень і публікацій. Питання щодо інтеграції цифрових технологій у механізми забезпечення національної безпеки держави досліджують як відчизняні так і зарубіжні дослідники, варто розглянути основні думки.

На думку Іванова О. М. [1] цифрова трансформація суспільних процесів позитивно впливає на розбудову взаємодії між владою та громадянами, водночас окреслюючи основні напрями діяльності та ключові тренди цифровізації у сфері GovTech.

Петров І. С. [2] підкреслює, що кібератаки на об'єкти критичної інфраструктури можуть мати руйнівні наслідки для національної безпеки, економіки та суспільства, що зумовлює необхідність ефективного правового регулювання у цій сфері.

В свою чергу, Сидоренко Л. П. [3] вказує, що інтеграція України в цифровий глобальний простір сприятиме прискоренню економічного

відновлення та зміцненню позицій на міжнародній арені, одночасно зберігаючи національні інтереси та посилюючи конкурентоспроможність економіки.

Мельник Ю. В. [4] зазначає, що інтеграція цифрових технологій, таких як блокчейн, є ключовою для підвищення прозорості та ефективності державної підтримки, що сприяє зміцненню національної безпеки в умовах зростання глобальних загроз.

David S. Alberts [5] у своїх працях для NATO CCDCOE та DoD Command & Control Research Program стверджує, що адаптивність, інформаційна перевага та мережево-центрична взаємодія — ключові умови для цифрового переосмислення національної оборони в умовах гібридних загроз.

На думку, Luciano Floridi [6] цифрова безпека не може існувати без етичних рамок — зокрема, захисту цифрових прав людини, приватності та інформаційної автономії (2020).

Klaus Schwab [7] вказує, що держави, які не інтегрують цифрові технології у свої безпекові системи, залишаються вразливими до нових типів загроз, включаючи кібертероризм та інформаційні війни.

Richard A. Clarke [8] наголошує на важливості створення багаторівневої системи кібероборони, що включає не лише технології, а й міжвідомчу координацію, співпрацю з приватним сектором і підготовку громадянського суспільства.

Myriam Dunn Cavelty [9] вважає, що цифрові технології змінюють саму природу національного суверенітету, переносячи акцент із територіального на інформаційний контроль.

На нашу думку, і в українських, і в зарубіжних дослідженнях простежується консенсус щодо ключової ролі цифрових технологій у забезпеченні національної безпеки. Водночас зарубіжна наука акцентує увагу на етичних та інституційних аспектах, тоді як українські дослідники зосереджені на практичному захисті інфраструктури в умовах реальної війни.

Формулювання цілей статті (постановка завдання). Метою дослідження є формування теоретико-методологічних засад та визначення прикладних підходів до інтеграції цифрових технологій у механізми забезпечення національної безпеки держави з метою підвищення ефективності реагування на сучасні загрози та зміцнення системи національної безпеки в умовах цифрової трансформації.

Виклад основного матеріалу дослідження. У сучасному світі, що характеризується стрімким розвитком інформаційно-комунікаційних технологій, питання національної безпеки набуває нових вимірів. Традиційні підходи до захисту державного суверенітету, територіальної цілісності та громадської безпеки поступово доповнюються цифровими механізмами, які стають ключовими інструментами у виявленні, попередженні та нейтралізації загроз. Інтеграція цифрових технологій у систему національної безпеки відкриває нові можливості для ефективного управління ризиками, посилення кібербезпеки та забезпечення стійкості до гібридних впливів, що робить цю тему надзвичайно актуальною для наукового осмислення й практичного впровадження.

Крім того, у контексті глобалізації та стрімкої цифровізації усіх сфер суспільного життя, забезпечення національної безпеки набуває нових пріоритетів і форм. Зростання кількості кіберзагроз, інформаційних атак та використання цифрових каналів для гібридного впливу вимагає принципово нового підходу до побудови безпекових механізмів. Інтеграція цифрових технологій у систему національної безпеки стає ключовим чинником стратегічної стійкості держави [1].

Цифрова трансформація розглядається як невід’ємна частина модернізації безпекових інститутів держави. Теоретичне підґрунтя інтеграції цифрових технологій формують концепції цифрового суверенітету, інформаційної переваги та системного аналізу загроз.

Зокрема, кібербезпека визначається як складова національного суверенітету в новій сфері — кіберпросторі. Інформаційна безпека, у свою

чергу, розглядається крізь призму протидії деструктивним впливам, маніпуляціям, дезінформації та інформаційно-психологічним операціям, які можуть мати стратегічні наслідки для функціонування держави [2].

Аналіз загроз у цифровому середовищі здійснюється з позицій системного підходу: вивчаються типи ризиків, їх джерела та механізми взаємодії з іншими складовими національної безпеки — політичною, економічною, воєнною та соціальною.

Доцільно зазначити, що аналіз загроз у цифровому середовищі здійснюється з позицій системного підходу, що передбачає комплексне врахування взаємозв'язків між різними видами ризиків, джерелами їх походження та впливом на ключові елементи національної безпеки. Такий підхід дозволяє не лише ідентифікувати конкретні загрози, але й оцінити їхню здатність провокувати каскадні наслідки в суміжних сферах.

Зокрема, політичні ризики можуть виникати внаслідок кібератак на державні інститути, що дестабілізує систему управління, підриває довіру громадян до влади та створює умови для зовнішнього впливу на внутрішньополітичні процеси. Економічна безпека потерпає від цифрових атак на фінансові установи, логістичні ланцюги, енергетичну інфраструктуру, що може викликати системні збої в економіці держави [3].

У воєнній сфері, цифрові технології відкривають нові театри бойових дій — зокрема, у кіберпросторі, де проводяться інформаційно-психологічні операції, електронні диверсії, втручання в системи зв'язку та управління військами. Це змінює саму концепцію війни, в якій домінують асиметричні та гібридні засоби впливу.

Соціальна безпека піддається ризикам унаслідок маніпуляцій у медіапросторі, розповсюдження дезінформації, втручання у суспільну свідомість через алгоритми соціальних мереж. Це здатне спричинити масові психологічні ефекти, деструкцію національної ідентичності та соціальну напругу.

Таким чином, цифрове середовище стає мультивекторним простором загроз, у якому порушення однієї компоненти може спричинити ланцюгову реакцію, що впливає на всю систему національної безпеки. Саме тому системний підхід дозволяє не лише фіксувати загрози, а й прогнозувати їх розвиток, моделювати сценарії та розробляти комплексні механізми реагування, інтегруючи ресурси з різних секторів — державного, громадського та приватного.

На прикладному рівні цифрові технології реалізуються через інноваційні інструменти:

1) Штучний інтелект (ШІ) використовується для обробки та аналізу великих масивів даних (Big Data), автоматизованого виявлення загроз, прогнозування кризових ситуацій.

2) Цифрові платформи управління безпекою забезпечують координацію між різними державними структурами, включаючи ситуаційні та аналітичні центри, що дозволяє оперативно реагувати на динамічні виклики.

3) Системи моніторингу критичної інфраструктури з використанням сенсорів, IoT-рішень та технологій захисту в реальному часі посилюють безпеку вразливих об'єктів державного значення.

4) Мобільні додатки та сервіси раннього оповіщення, як-от «єППО» або платформи сповіщення про небезпеку, забезпечують зворотний зв’язок з громадськістю та сприяють підвищенню рівня громадянської безпеки.

5) Партнерство з приватним сектором та міжнародними організаціями дає змогу впроваджувати інноваційні технології, залучати експертизу та синхронізувати національні підходи з глобальними стандартами [4].

Важливо відмітити, що інтеграція цифрових технологій у механізми забезпечення національної безпеки є важливою передумовою підвищення спроможності держави до ефективного реагування на сучасні загрози. Поєднання теоретичних засад цифрової трансформації з практичними інструментами зміцнює інформаційний, кібернетичний і стратегічний потенціал держави. Подальші дослідження у цій сфері мають бути спрямовані

на формування комплексної цифрової безпекової політики, інтеграцію технологій в управлінські процеси та розвиток міжсекторальної взаємодії.

Цифровізація охоплює дедалі ширші сфери функціонування державних інституцій, включаючи критично важливі напрями, такі як оборона, правоохоронна діяльність, кібербезпека, антикризове управління та інформаційна безпека. Це зумовлено прагненням до підвищення ефективності державного управління, оперативності прийняття рішень, прозорості процесів та оптимального використання ресурсів. Водночас цифрова трансформація відкриває нові горизонти у сфері безпеки, надаючи державним органам доступ до сучасних аналітичних інструментів, систем штучного інтелекту, хмарних платформ, технологій блокчейн і великих даних.

Проте разом із відкриттям нових можливостей цифровізація створює середовище підвищеної вразливості, у якому виникають складні та динамічні загрози. Зокрема, широке впровадження цифрових сервісів супроводжується зростанням ризику кібератак, витоку конфіденційної інформації, маніпулювання громадською думкою через алгоритми соціальних мереж, використанням дронів і автономних систем у терористичних цілях. Крім того, цифрові платформи можуть стати інструментом зовнішнього втручання у політичні процеси, зокрема шляхом атак на виборчу інфраструктуру, інформаційний простір чи системи державного управління [5].

У таких умовах виникає необхідність переосмислення традиційних моделей управління безпекою, які були орієнтовані переважно на фізичний захист території та інституцій. Сучасна парадигма безпеки вимагає інтеграції цифрових технологій у всі рівні ухвалення рішень, розбудови кіберрезистентних структур, формування ефективної цифрової культури в держслужбі, а також розробки гнучких, адаптивних механізмів реагування на нові типи загроз. Це також означає потребу у постійній міжвідомчій координації, участі приватного сектору та міжнародному співробітництві, адже цифрові загрози не мають кордонів і часто мають транснаціональний характер.

Отже, цифровізація є не лише технологічним, але й стратегічним викликом, який вимагає системного бачення, оновлення нормативно-правової бази та зміни підходів до формування політики національної безпеки в умовах цифрової епохи.

Доцільно здійснити, аналіз ключових цифрових технологій у контексті національної безпеки [6]:

1) Штучний інтелект (ШІ / AI)

Штучний інтелект є одним із найбільш перспективних інструментів у сфері національної безпеки. Завдяки алгоритмам машинного навчання та обробки природної мови, ШІ дозволяє:

- здійснювати автоматизовану обробку великих обсягів інформації з відкритих джерел;
- виявляти загрози в режимі реального часу (наприклад, кібератаки або спроби втручання у вибори);
- застосовуватись для розвідки та контррозвідки, прогнозування кризових ситуацій, координації оборонних операцій;
- формувати рекомендаційні системи для антикризового управління та стратегічного планування.

Проте, ШІ несе ризики, пов’язані з автономністю прийняття рішень, етичними викликами та потенційним використанням у злочинних цілях.

2) Великі дані (Big Data)

Big Data охоплюють масиви неструктурованої інформації (соціальні мережі, відеоспостереження, дані з датчиків), які аналізуються для виявлення аномалій, тенденцій та загроз. Основні переваги:

- раннє попередження про ризики (терористичні загрози, епідемії, деструктивні кампанії в інформаційному просторі);
- аналіз поведінкових моделей населення, що дозволяє виявляти потенційно небезпечну активність;
- інтеграція даних з різних систем (державні реєстри, безпекові платформи, моніторингові центри).

3) Блокчейн (Blockchain)

Блокчейн як технологія розподіленого реєстру забезпечує високий рівень прозорості, незмінності та надійності збереження інформації. Застосування у сфері нацбезпеки:

- захист державних реєстрів та баз даних від несанкціонованих змін;
- ідентифікація користувачів та безпечне управління доступом до критичних інформаційних систем;
- запобігання підробці документів, зокрема в оборонному секторі;
- забезпечення довіри до виборчих процесів через прозорість електронного голосування.

4) Інтернет речей (IoT)

IoT передбачає з'єднання в мережу великої кількості пристроїв (камер, сенсорів, дронів, трекерів), які передають дані в реальному часі. У сфері безпеки це дозволяє:

- моніторити об'єкти критичної інфраструктури (енергетика, транспорт, водопостачання);
- здійснювати розвідку та спостереження з використанням автономних систем;
- впроваджувати розумне місто з інтегрованою системою відеоаналітики, сигналізації та реагування;
- підвищити ситуаційну обізнаність оперативних підрозділів.

Проблеми включають кібервразливість пристроїв, відсутність єдиних стандартів захисту та можливість зловживань.

5) Хмарні обчислення (Cloud Computing)

Хмарні технології надають масштабовану інфраструктуру для зберігання та обробки даних з високим рівнем доступності. Переваги:

- централізоване управління безпековими даними з можливістю швидкого доступу та обробки;
- підтримка аналітичних платформ та ситуаційних центрів;

- можливість резервного копіювання і відновлення даних після атак або технічних збоїв;

- гнучке масштабування в умовах криз [7].

Разом з тим, існує загроза централізації уразливостей, якщо не забезпечено надійного захисту доступу та відповідності нормативам.

Таким чином, ці технології мають величезний потенціал для модернізації системи національної безпеки, але потребують виваженого підходу до впровадження, з урахуванням кіберризиків, етичних аспектів та нормативного забезпечення.

Інтеграція сучасних цифрових технологій у механізми забезпечення національної безпеки держави відкриває принципово нові можливості для переходу від реактивної до превентивної моделі безпекової політики. На відміну від традиційних підходів, орієнтованих на реагування після настання загроз, цифрові інструменти дозволяють здійснювати безперервний моніторинг, аналіз і прогнозування потенційно небезпечних процесів у реальному часі.

Застосування штучного інтелекту та великих даних забезпечує автоматичну ідентифікацію аномалій та виявлення патернів поведінки, що можуть сигналізувати про наближення кризових ситуацій (зокрема, ескалацію конфліктів, терористичну активність, соціальну нестабільність). Алгоритми прогнозної аналітики дозволяють моделювати розвиток сценаріїв загроз із врахуванням великої кількості змінних та динамічних факторів, включаючи поведінкові, економічні, інформаційні та екологічні.

У сфері оперативного реагування хмарні обчислення та інтернет речей створюють технологічну основу для мобільних ситуаційних центрів, інтегрованих систем раннього сповіщення та координації дій між різними відомствами. Дані з сенсорів, дронів, відеоаналітики та кібермоніторингу дозволяють приймати рішення швидше, точніше та з урахуванням актуального контексту [8].

Крім того, блокчейн виступає інструментом прозорої верифікації інформації, фіксації подій і захисту цифрової ідентичності, що є критично важливим у контексті антикризового управління та кібербезпеки.

Узагальнюючи варто відмітити, що цифрові технології забезпечують створення багаторівневої, інтегрованої, адаптивної системи національної безпеки, здатної не лише ефективно реагувати на поточні загрози, але й прогнозувати ризики, локалізувати їх на ранніх етапах та мінімізувати наслідки криз шляхом проактивного управління.

Інтеграція сучасних цифрових технологій у механізми забезпечення національної безпеки держави відкриває принципово нові можливості для переходу від реактивної до превентивної моделі безпекової політики. На відміну від традиційних підходів, орієнтованих на реагування після настання загроз, цифрові інструменти дозволяють здійснювати безперервний моніторинг, аналіз і прогнозування потенційно небезпечних процесів у реальному часі [9].

Застосування штучного інтелекту та великих даних забезпечує автоматичну ідентифікацію аномалій та виявлення патернів поведінки, що можуть сигналізувати про наближення кризових ситуацій (зокрема, ескалацію конфліктів, терористичну активність, соціальну нестабільність). Алгоритми прогнозної аналітики дозволяють моделювати розвиток сценаріїв загроз із врахуванням великої кількості змінних та динамічних факторів.

У сфері оперативного реагування хмарні обчислення та інтернет речей створюють технологічну основу для мобільних ситуаційних центрів, інтегрованих систем раннього сповіщення та координації дій між різними відомствами. Дані з сенсорів, дронів, відеоаналітики та кібермоніторингу дозволяють приймати рішення швидше, точніше та з урахуванням актуального контексту.

Блокчейн виступає інструментом прозорої верифікації інформації, фіксації подій і захисту цифрової ідентичності, що є критично важливим у контексті антикризового управління та кібербезпеки.

З початком повномасштабного вторгнення РФ у 2022 році Україна продемонструвала високу адаптивність у використанні цифрових рішень для цілей оборони та безпеки. Серед ключових прикладів [10-13]:

1) Платформа "Дія" стала не лише цифровим державним сервісом, а й елементом інформаційної безпеки, завдяки можливості оперативного інформування громадян, проведення опитувань та забезпечення цифрової ідентифікації.

2) Система "Дельта" — ситуаційна платформа, яка акумулює дані з відкритих джерел, безпілотників, супутників і надає реальну картину бойових дій для координації дій ЗСУ та партнерських сил.

3) Використання ШІ для аналізу супутникових знімків і розпізнавання об'єктів (у співпраці з міжнародними компаніями та волонтерськими ІТ-спільнотами) суттєво прискорило виявлення переміщення ворожої техніки.

4) Кіберкоманда України на рівні держави та волонтерських структур здійснює активний моніторинг кіберпростору, запобігаючи атакам на критичну інфраструктуру, банки, урядові системи.

5) Сприяння хмарним платформам (Google Cloud, Amazon Web Services) дозволило захистити державні дані від фізичного знищення та організувати безперервний доступ до ключових інформаційних систем [14].

Як результат, ці приклади свідчать про успішну апробацію цифрових технологій у кризових умовах і підтверджують їх критичну роль у забезпеченні національної безпеки як у воєнний, так і в мирний час.

Особлива увага в сучасному дискурсі національної безпеки підкреслює необхідність формування інтегрованої цифрової стратегії, яка має поєднувати технологічні, правові, організаційні та кадрові ресурси в єдину, скоординовану систему протидії загрозам. Така стратегія не може обмежуватись лише впровадженням новітніх технологій — вона повинна передбачати системний підхід, де інновації підтримуються належним правовим регулюванням, стійкою інституційною структурою та високим рівнем цифрової компетентності персоналу.

З технологічного боку, мова йде про розвиток інфраструктури безпеки, використання інструментів штучного інтелекту, блокчейну, великих даних, IoT та хмарних сервісів. Проте, без правового супроводу, який встановлює чіткі межі обробки даних, кіберетики, захисту персональної інформації та цифрових прав, ефективність цих технологій може бути знівельована.

Організаційна складова включає створення міжвідомчих координаційних центрів, формування механізмів обміну даними між державними, приватними та міжнародними структурами, а також реалізацію прозорої системи управління ризиками [15].

Крім того, кадровий потенціал стає критичним чинником. Висококваліфіковані фахівці у сфері кібербезпеки, аналітики даних, IT-архітектори та цифрові юристи мають бути залучені до процесу формування і реалізації цифрової стратегії. Це вимагає системи підготовки, перепідготовки та мотивації відповідних кадрів, а також інтеграції цифрової грамотності у сферу державного управління загалом.

У сукупності, інтегрована цифрова стратегія національної безпеки виступає як основа для створення стійкої, адаптивної, проактивної безпекової системи, здатної не лише реагувати на сучасні виклики, а й запобігати їм на етапі їх зародження.

Доцільно, проаналізувати етапи формування інтегрованої цифрової стратегії національної безпеки (табл. 1).

Таблиця 1. Етапи формування інтегрованої цифрової стратегії національної безпеки

№	Назва етапу	Особливості реалізації етапів формування інтегрованої стратегії національної безпеки
1	Аналіз цифрових викликів і загроз	ідентифікація основних ризиків у кіберпросторі та технологічному середовищі; оцінка стану наявної безпекової інфраструктури; виявлення вразливостей у критичних секторах (енергетика, оборона, зв'язок, фінанси тощо).
2	Визначення стратегічних цілей та пріоритетів	формулювання бачення цифрової безпеки держави; встановлення короткострокових, середньострокових та довгострокових завдань; визначення ключових показників ефективності (KPI) безпекових дій.
3	Моделювання нормативно-правової бази	розробка або оновлення законодавства у сфері кібербезпеки, цифрової конфіденційності, захисту даних; гармонізація з міжнародними стандартами (NIST, ISO, GDPR тощо); запровадження механізмів відповідальності та аудиту цифрової безпеки.
4	Формування технологічної архітектури	вибір пріоритетних цифрових технологій (ШІ, Big Data, Blockchain, IoT, Cloud); створення національних платформ безпеки (ситуаційні центри, SOC-центри, CERT/CSIRT); інтеграція державних та приватних інформаційних ресурсів в єдину систему обміну даними.
5	Організаційне забезпечення та інституційна координація	визначення ключових органів, відповідальних за реалізацію стратегії; створення центрів цифрової безпеки в органах державної влади; впровадження міжвідомчої координації та публічно-приватного партнерства.
6	Кадрова підготовка та цифрова освіта	створення навчальних програм з кібербезпеки та цифрової аналітики; розвиток системи сертифікації фахівців; формування національного кадрового резерву у сфері цифрової безпеки.
7	Впровадження, моніторинг і корекція	пілотне впровадження стратегії в окремих секторах; постійний моніторинг ефективності реалізації заходів; гнучке оновлення стратегії відповідно до змін у загрозах та технологіях.

Джерело: сформовано автором на основі даних [15-18]

Дані етапи утворюють логічну й адаптивну рамку для довготривалого та стійкого впровадження цифрової трансформації в систему національної безпеки.

Разом з тим, кібербезпека та захист критичної інформаційної інфраструктури залишаються одним із ключових викликів для цифрового середовища сучасної держави. Серед основних проблем виокремлюється недостатній рівень технічного захисту систем, фрагментованість управління безпековими процесами та відсутність єдиної координаційної структури. Також спостерігається низький рівень кіберграмотності персоналу, обмеженість ресурсів для постійного моніторингу загроз і реагування на інциденти. Законодавчі прогалини та правова неврегульованість у сфері відповідальності за кіберінциденти додатково ускладнюють захист КІІ. Зростання складності кіберзагроз і нерівномірне впровадження міжнародних стандартів захисту також створюють значні ризики для стабільного функціонування критичних цифрових систем.

Враховуючи вище зазначене, можна запропонувати, концептуальний підхід до побудови адаптивної системи цифрової безпеки держави, наступним чином:

1. Принципи побудови системи:

Адаптивність — здатність до автоматичного або керованого оновлення політик безпеки залежно від змін зовнішніх і внутрішніх загроз.

Інтегрованість — об’єднання різних рівнів безпеки (технічного, організаційного, правового) в єдину систему реагування.

Проактивність — переорієнтація з реактивної моделі захисту на передбачення, запобігання та нейтралізацію загроз на ранніх етапах.

Гнучкість масштабування — здатність розширювати систему в разі нових викликів (включення нових об’єктів, технологій, органів управління).

Прозорість і контроль — чіткі правила відповідальності, моніторинг рішень та відкритість дій у правових межах.

2. Ключові структурні компоненти системи:

- Інтелектуальний аналітичний модуль (IAM) -використання штучного інтелекту, Big Data та машинного навчання для аналізу поведінкових патернів, загроз і ризиків; постійне навчання моделей на основі нових даних (Data Feedback Loop).

- Центр динамічного управління ризиками (CDUR) - інституція, що акумулює вхідну інформацію (з IT-систем, сенсорів, соціальних мереж, міжнародних партнерів); Приймає рішення щодо рівня загрози та ініціює протоколи реагування в реальному часі.

- Модуль реагування та локалізації інцидентів (MRLI) - автоматизоване застосування сценаріїв дій за заданими шаблонами (playbooks) на випадок різних типів атак; підключення до інфраструктури оперативного реагування: CERT, SOC, кіберпідрозділів СБУ/МВС.

- Правова оболонка та аудит цифрової відповідальності - інтеграція цифрової безпеки в адміністративно-правову систему держави; реєстр цифрових інцидентів, аудит рішень ШІ, механізми прозорості та оскарження.

- Кадрово-освітній кластер - система підготовки та сертифікації кадрів у сфері кібербезпеки; цифрова освітня платформа для держслужбовців, військових і цивільного населення.

3. Механізм адаптації до загроз - періодичне оновлення карт ризиків і сценаріїв реагування; автоматичне розширення джерел даних при появі нових векторів атак; моделювання альтернативних сценаріїв розвитку криз на базі цифрових двійників ("digital twins"); ротація стратегій захисту з урахуванням глобальних трендів (зміна нормативів, стандартів, протоколів).

Отже, створення самонавчальної, багаторівневої, адаптивної цифрової системи безпеки, яка мінімізує час реакції на інциденти, дозволяє прогнозувати ризики з високою точністю і забезпечує стійкість держави перед багатовекторними загрозами в умовах постійної цифрової трансформації.

Висновки. Таким чином, цифрові технології стають системоутворювальним чинником національної безпеки, що проникає у всі ключові сфери – оборону, кібербезпеку, кризове управління, аналітику ризиків

та інформаційний захист. Інтеграція таких технологій, як штучний інтелект, Big Data, IoT, блокчейн та хмарні обчислення, суттєво посилює здатність держави до превентивного моніторингу, прогнозування та оперативного реагування на загрози.

Система цифрової безпеки має бути адаптивною, проактивною і багаторівневою, із можливістю постійного оновлення моделей загроз і сценаріїв реагування. Її побудова вимагає комплексного підходу, що поєднує технологічні, правові, кадрові та організаційні компоненти. Адже, формування інтегрованої цифрової стратегії національної безпеки є критично необхідним для забезпечення стійкості держави перед новітніми викликами. Така стратегія повинна охоплювати етапи аналізу загроз, нормативно-правове регулювання, технологічне оснащення, кадрову підготовку та безперервний моніторинг.

Український досвід демонструє як вразливість, так і адаптивний потенціал у сфері цифрової безпеки — особливо в умовах збройної агресії. Посилення взаємодії між державними органами, приватним сектором та міжнародними партнерами стає основою формування сучасної цифрової оборони. Тому, для захисту критичної інформаційної інфраструктури необхідно подолати проблеми фрагментованості, технічної відсталості, дефіциту фахівців і нормативної невизначеності, а також запровадити сталу систему реагування на динамічні кіберзагрози.

Література

1. Іванов О. М. Цифрова трансформація системи національної безпеки: виклики та перспективи. *Інформаційне право України.* 2023. №1. С. 22–29.
2. Петров І. С. Кібербезпека як складова національної безпеки України. *Наукові праці НАДУ.* 2022. №4. С. 45–51.
3. Сидоренко Л. П. Інтеграція цифрових технологій в антикризове управління: український контекст. *Стратегічні пріоритети.* 2024. №2(59). С. 66–72.

4. Мельник Ю. В. Блокчейн-технології в державному управлінні: перспективи для України. *Держава і право.* 2023. №89. С. 110–115.

5. Alberts D. S. The future of command and control: The human and machine interface. NATO CCDCOE, 2020. URL: https://ccdcoe.org/uploads/2020/12/Cyber-Threats-and-NATO-2030_Horizon-Scanning-and-Analysis.pdf

6. Floridi L. The fight for digital sovereignty: what it is, and why it matters, especially for the EU. *Philosophy & Technology.* 2020. Vol. 33. P. 369–378.

7. Schwab K. The Fourth Industrial Revolution: what it means and how to respond. *World Economic Forum.* 2016. URL: https://www.weforum.org/stories/2016/01/the-fourth-industrial-revolution-what-it-means-and-how-to-respond.

8. Clarke R. A. Press Briefing by Richard Clarke, National Coordinator for Security, Infrastructure Protection and Counter-terrorism. *The American Presidency Project.* 2000. URL: https://www.presidency.ucsb.edu/documents/press-briefing-richard-clarke-national-coordinator-for-security-infrastructure-protection.

9. Dunn Cavelty M. Cyber-Security and Threat Politics: US Efforts to Secure the Information Age. London: Routledge, 2008. 192 p.

10. Ковальчук В. М. Цифровізація державного управління як фактор підвищення рівня інформаційної безпеки. *Економіка і управління інформаційними системами*. 2022. № 5. С. 76–84.

11. Шевченко Н. П. Інтеграція цифрових технологій у систему управління інформаційною безпекою: перспективи та виклики. *Сучасні проблеми державного управління.* 2023. № 1. С. 48–58.

12. Бондаренко І. Л. Інформаційна безпека в умовах цифрової трансформації публічного управління. *Державне управління в умовах цифровізації.* 2022. №8. С. 33–41.

13. Герасимчук В. Ю. Публічне управління інформаційною безпекою: цифрові технології як інструмент розвитку. *Журнал з публічного адміністрування.* 2023. №7. С. 95–102.

14. Коваль Я. С. Механізм державного управління національною економікою в умовах цифрової трансформації. *Публічне адміністрування та національна безпека.* 2023. №10. DOI: https://doi.org/10.25313/2617-572X-2023-10-9396.

15. Морозенко І. О. Використання блокчейн-технологій для посилення інформаційної безпеки у публічному управлінні. *Цифрові трансформації у публічному управлінні.* 2022. № 6. С. 25–33.

16. Чорна І. В. Сучасні цифрові технології як інструменти забезпечення інформа-ційної безпеки в публічному управлінні. *Міжнародний журнал з інформаційної безпеки*. 2022. № 4. С. 11–18.

17. Дяченко Р. А. Публічне управління інформаційною безпекою: цифрові методи та інструменти. *Політика та інформаційні технології*. 2022. № 9. С. 60–69.

18. Кузнєцова О. М. Вплив цифрових технологій на розвиток механізмів публічного управління та інформаційної безпеки. Аналіз і розвиток публічної політики. 2023. №2. С. 22–30.

References

1. Ivanov, O.M. (2023), “Digital transformation of the national security system: challenges and prospects”, *Informatsiine pravo Ukrainy*, vol. 1, pp. 22–29.

2. Petrov, I.S. (2022), “Cybersecurity as a component of Ukraine's national security”, *Naukovi pratsi NADU,* vol.4, pp. 45–51.

3. Sydorenko, L.P. (2024), “Integration of digital technologies into crisis management: The Ukrainian context”, *Stratehichni priorytety,* vol. 2(59), pp. 66–72.

4. Melnyk, Yu.V. (2023), “Blockchain technologies in public administration: prospects for Ukraine”, *Derzhava i pravo*, no. 89, pp. 110–115.

5. Alberts, D. S. (2020), “The future of command and control: The human and machine interface”, NATO CCDCOE, https://ccdcoe.org/uploads/2020/12/Cyber-Threats-and-NATO-2030_Horizon-Scanning-and-Analysis.pdf (Accessed 12 May 2025).

6. Floridi, L. (2020), “The fight for digital sovereignty: What it is, and why it matters, especially for the EU”, *Philosophy & Technology*, vol. 33, pp. 369–378.

7. Schwab, K. (2016), “The Fourth Industrial Revolution: What it means and how to respond”, *World Economic Forum*, available at: https://www.weforum.org/stories/2016/01/the-fourth-industrial-revolution-what-it-means-and-how-to-respond (Accessed 2 May 2025).

8. Clarke, R. A. (2000), “Press briefing by Richard Clarke, National Coordinator for Security, Infrastructure Protection and Counter-terrorism”, *The American Presidency Project*, available at: https://www.presidency.ucsb.edu/documents/press-briefing-richard-clarke-national-coordinator-for-security-infrastructure-protection (Accessed 27 April 2025).

9. Dunn Cavelty, M. (2008), Cyber-security and threat politics: US efforts to secure the information age, Routledge, London, UK.

10. Kovalchuk, V. M. (2022), “Digitalization of public administration as a factor in increasing information security”, *Ekonomika i upravlinnia informatsiinymy systemamy*, vol. 5, pp. 76–84.

11. Shevchenko, N.P. (2023), “Integration of digital technologies into information security management: Prospects and challenges”, *Suchasni problemy derzhavnoho upravlinnia*, vol. 1, pp. 48–58.

12. Bondarenko, I.L. (2022), “[Information security under digital transformation of public administration”, *Derzhavne upravlinnia v umovakh tsyfrovizatsii*, vol. 8, pp. 33–41.

13. Herasymchuk, V.Yu. (2023), “Public administration of information security: Digital technologies as a development tool”, *Zhurnal z publichnoho administruvannia*, vol. 7, pp. 95–102.

14. Koval, Ya.S. (2023), “Mechanism of state governance of the national economy in the context of digital transformation”, *Publichne administruvannia ta natsionalna bezpeka*, vol. 10. DOI: https://doi.org/10.25313/2617-572X-2023-10-9396.

15. Morozhenko, I.O. (2022), “Using blockchain technologies to strengthen information security in public administration”, *Tsyfrovi transformatsii u publichnomu upravlinni*, vol. 6, pp. 25–33.

16. Chorna, I.V. (2022), “Modern digital technologies as tools to ensure information security in public administration”, *Mizhnarodnyi zhurnal z informatsiinoi bezpeky*, vol. 4, pp. 11–18.

17. Diachenko, R.A. (2022), “Public administration of information security: Digital methods and tools”, *Polityka ta informatsiini tekhnolohii*, vol. 9, pp. 60–69.

18. Kuznetsova, O.M. (2023), “Impact of digital technologies on the development of public administration and information security mechanisms”, *Analiz i rozvytok publichnoi polityky*, vol. 2, pp. 22–30.

Стаття надійшла до редакції 13.05.2025 р.