

В. В. Димитрієв

здобувач наукового ступеня кандидата наук

СТРАТЕГІЧНІ НАПРЯМИ РОЗВИТКУ ІНФОРМАЦІЙНОЇ ПОЛІТИКИ УКРАЇНИ В КОНТЕКСТІ ГЛОБАЛЬНИХ ВИКЛИКІВ

У статті досліджено стратегічні напрями розвитку інформаційної політики України в умовах сучасних глобальних викликів, таких як діджиталізація, кібербезпека, інформаційні атаки, дезінформація та гібридні загрози. Розвиток інформаційної політики розглядається як один із ключових чинників, що визначає здатність країни забезпечувати національну безпеку, стійкість суспільства до інформаційного впливу та конкурентоспроможність в умовах глобального інформаційного середовища. Проаналізовано поточний стан інформаційного простору України, що вимагає посилення кібербезпеки та захисту критичної інфраструктури, протидії дезінформації та фейковим новинам, а також активної цифровізації економіки. Стаття виділяє основні глобальні загрози, з якими стикається Україна, такі як кібератаки та інформаційні маніпуляції, що використовуються в рамках гібридної війни. Запропоновано чотири основні стратегічні напрями розвитку інформаційної політики України: посилення кібербезпеки та захисту критичних інформаційних систем, боротьба з фейковими новинами, підтримка цифрової трансформації економіки та суспільства, а також розширення міжнародної співпраці та інтеграція у глобальні інформаційні мережі. Увагу приділено значенню міжнародного співробітництва з метою обміну досвідом, технологіями та спільного реагування на новітні інформаційні загрози. Зазначені стратегічні напрями розвитку інформаційної політики не лише сприятимуть підвищенню національної безпеки, але й створюватимуть умови для активного залучення України до глобальних інформаційних процесів, сприяючи її інтеграції у світову цифрову економіку. Це, у свою чергу, дозволить Україні посилити свою позицію на міжнародній арені та зменшити залежність від зовнішніх інформаційних впливів. Особлива увага у статті приділена питанням кібербезпеки, яка в сучасних умовах є ключовим компонентом національної безпеки. Кіберпростір стає полем для проведення військових дій нового покоління, що вимагає розробки ефективних механізмів захисту та стратегії швидкого реагування на кіберзагрози. Досвід останніх років показує, що Україна перебуває на передовій кіберконфліктів, і розробка національної кіберстратегії є надзвичайно важливою для мінімізації ризиків у цій сфері. Зроблено висновок, що реалізація цих стратегічних напрямів є необхідною умовою для ефективною протидії сучасним викликам, забезпечення інформаційної безпеки та побудови конкурентоспроможної інформаційної екосистеми в Україні. Розвиток інновацій та діджиталізації розглядається як ключовий чинник для забезпечення сталого економічного розвитку та соціальної стабільності держави.

Ключові слова: інформаційна політика, кібербезпека, фейкові новини, гібридні загрози, діджиталізація, Україна.

Постановка проблеми. Інформаційна політика сьогодні є важливим елементом державного управління, яка впливає на безпеку, економіку, соціальний розвиток та міжнародні відносини країн у всьому світі. Роль інформації у сучасному суспільстві набуває все більшої ваги, а інформаційні технології та засоби комунікації стали невід'ємною частиною не лише повсякденного життя людей, але й інструментом геополітичного впливу. У зв'язку з цим, розробка ефективною інформаційної політики є стратегічно важливою для забезпечення стій-

кості держави перед зовнішніми та внутрішніми загрозами, а також для просування національних інтересів на міжнародній арені. Україна, як країна, яка знаходиться у стані гібридної війни з моменту анексії Криму та початку військових дій на Сході в 2014 році, відчуває особливу необхідність у зміцненні інформаційного простору та захисту від інформаційних атак. Ця війна, яка ведеться не тільки на військових полях, але й у кіберпросторі та медіасередовищі, змусила уряд країни переглянути підходи до інформаційної політики та значно посилити заходи без-

пеки в цьому напрямку. Сучасні інформаційні загрози, такі як кібератаки, дезінформація, пропаганда та фейкові новини, стали новим типом зброї, яка використовується для дестабілізації суспільства, послаблення економіки та підризу довіри до державних інституцій. Таким чином, розвиток інформаційної політики України в контексті глобальних викликів вимагає системного підходу, який об'єднує як захист національного інформаційного простору, так і розвиток цифрових технологій та міжнародного співробітництва. Україна має можливість не лише захистити свої інтереси на інформаційному фронті, але й стати активним учасником глобального цифрового розвитку, створюючи умови для сталого економічного зростання та соціальної стабільності. Це робить актуальною задачу визначення стратегічних напрямів розвитку інформаційної політики, які враховували б сучасні реалії та перспективи, а також можливості й загрози, що виникають у новій інформаційній епосі.

Аналіз останніх досліджень і публікацій.

Огляд наукових публікацій, присвячених питанням інформаційної безпеки України, показує різноманіття проблем і рішень, запропонованих дослідниками для їх подолання. Однією з найбільш значущих робіт у цій сфері є дослідження Ігоря Козловського та Сергія Грищенка (2020), яке зосереджене на аналізі кібератак на критичну інфраструктуру України. У дослідженнях Юрія Радченка (2018) розглядається рівень захисту державних інформаційних систем від кібератак із використанням новітніх технологій, зокрема штучного інтелекту та машинного навчання. Олександр Литвиненко (2019) у своїх роботах вивчає вплив дезінформації та фейкових новин на українське суспільство в умовах конфлікту з Росією. Катерина Крук (2020) детально досліджує механізми розповсюдження пропаганди в українському інформаційному просторі, наголошуючи на проблемах дезінформації. Михайло Гончар (2018) аналізує важливість співпраці з НАТО та Європейським Союзом у розвитку системи кібербезпеки України. У свою чергу, Юлія Василенко (2019) зосереджується на інституційній структурі інформаційної безпеки України, підкреслюючи, що відсутність єдиного координаційного центру ускладнює управління реагуванням на нові загрози. Загалом, огляд наукових праць підтверджує значний інтерес дослідників до проблематики інформаційної безпеки України та широкий спектр підходів до її вирішення.

Метою статті є визначення стратегічних напрямів розвитку інформаційної політики України в умовах сучасних глобальних викликів, таких як кібербезпека, дезінформація, гібридні загрози та діджиталізація суспільства.

Виклад основного матеріалу. На сьогоднішній день інформаційна політика України є важливим елементом державного управління, спрямованим на захист національних інтересів у сфері інформаційних технологій та комунікацій. Ситуація в інформаційному просторі країни характеризується складними викликами, що зумовлені як внутрішніми факторами, так і зовнішніми загрозами. У сучасних умовах Україна змушена протистояти інтенсивним інформаційним атакам, що використовуються іншими державами як засіб ведення гібридної війни, спрямованої на дестабілізацію політичної, економічної та соціальної ситуації в країні.

Основою державної інформаційної політики є низка законодавчих актів та стратегій, прийнятих на державному рівні. Зокрема, одним із ключових документів є Національна стратегія інформаційної безпеки, яка визначає основні напрями розвитку інформаційного простору, завдання щодо захисту критичної інфраструктури, протидії дезінформації та підвищення рівня кібербезпеки. Прийняття цієї стратегії стало відповіддю на численні кібернетичні атаки на державні установи та інфраструктурні об'єкти, які мали місце в останні роки, зокрема, атаки на енергетичний сектор у 2015 році та масова кібератака за допомогою вірусу Petya в 2017 році [1].

Важливим аспектом інформаційної політики України є боротьба з дезінформацією та фейковими новинами. З початком військового конфлікту на Донбасі та анексією Криму в 2014 році, країна зіткнулася з масштабними інформаційними кампаніями, спрямованими на маніпуляцію громадською думкою, підризу довіри до державних інституцій та формування негативного іміджу України на міжнародній арені. Для боротьби з цими явищами було створено низку ініціатив, таких як підвищення медіаграмотності населення, розвиток національних інформаційних ресурсів та співпраця з міжнародними партнерами для протидії дезінформації.

Проте, попри активну роботу у цьому напрямку, Україна все ще залишається вразливою до зовнішніх інформаційних впливів. Значна частина інформаційного простору залишається під контролем олігархічних медіагруп, що часто використовують свої ресурси для просу-

вання політичних або економічних інтересів, що може створювати викривлену картину реальності. Водночас, соціальні мережі, які стали головним джерелом новин для багатьох українців, є активним полем для розповсюдження фейкових новин і маніпуляцій.

Додатковим викликом для інформаційної політики України є швидка діджиталізація суспільства. Інтернет і цифрові технології сьогодні проникають в усі сфери життя, змінюючи способи спілкування, ведення бізнесу, надання державних послуг і взаємодії громадян з державними органами. Хоча діджиталізація відкриває значні можливості для розвитку економіки та підвищення якості життя, вона також підвищує ризики інформаційної вразливості та створює нові загрози у сфері кібербезпеки. У цьому контексті, держава повинна розробити та впровадити комплексні заходи щодо захисту даних, конфіденційності та приватності громадян.

Інформаційна політика України також активно розвивається у напрямку міжнародного співробітництва. Уряд України активно працює над інтеграцією у глобальні інформаційні структури, такі як співпраця з Європейським Союзом у сфері кібербезпеки та інформаційних технологій, участь у програмах НАТО, спрямованих на протидію гібридним загрозам. Це дозволяє Україні не лише захищати свій інформаційний простір, а й вивчати найкращі світові практики та запозичувати досвід інших держав у боротьбі з новітніми викликами [2].

Попри всі досягнення та зусилля, у інформаційній політиці України залишаються значні прогалини. Недостатня координація між різними державними відомствами, обмежене фінансування кібербезпеки та недостатній рівень цифрової грамотності населення є основними проблемами, які потребують негайного вирішення. Водночас, не менш важливо забезпечити подальшу демократизацію медіасфери, зниження впливу політичних і бізнесових інтересів на редакційну політику медіа та розвиток незалежних інформаційних платформ.

Загалом, поточний стан інформаційної політики України можна охарактеризувати як фазу активного реформування та адаптації до нових глобальних викликів. Попри значні досягнення у створенні нормативної бази та посиленні кібербезпеки, перед країною стоять численні виклики, пов'язані з необхідністю побудови стійкої інформаційної інфраструктури, захисту від

зовнішніх інформаційних загроз і забезпечення розвитку цифрових технологій.

Глобальні виклики для інформаційної політики України охоплюють широкий спектр питань, що включають кібербезпеку, дезінформацію, гібридні загрози, швидку діджиталізацію суспільства та технологічну нерівність. У сучасних умовах, коли інформаційний простір стає головним полем для геополітичних протистоянь та маніпуляцій, ці виклики значно впливають на здатність України ефективно захищати свої національні інтереси та забезпечувати стабільність держави [3-4].

1. Кібербезпека. Одним з найбільших викликів для інформаційної політики є кібербезпека. Сучасні кібератаки стають все більш складними та руйнівними, використовуючи новітні технології, такі як штучний інтелект і машинне навчання, для розробки шкідливих програм та здійснення атак на критичну інфраструктуру. Україна неодноразово ставала об'єктом масштабних кібератак, таких як атака на енергетичну систему у 2015 році та вірус-шифрувальник Petya у 2017 році, які паралізували діяльність як державних, так і приватних організацій.

Ці атаки виявили вразливість національної критичної інфраструктури, включаючи системи енергопостачання, транспортні мережі та банківський сектор, до деструктивних дій з боку кіберагресорів. Захист від таких загроз вимагає комплексного підходу, включаючи модернізацію кібернетичних систем, посилення заходів безпеки, проведення навчань з реагування на інциденти та посилення співпраці з міжнародними партнерами у сфері кібербезпеки.

2. Фейкові новини та дезінформація. Фейкові новини та дезінформація стали одним із найпотужніших інструментів ведення інформаційної війни, спрямованої на вплив на громадську думку, політичні процеси та соціальну стабільність. Вони активно використовуються для маніпуляції суспільством, створення недовіри до державних інституцій, розпалювання соціальних конфліктів та втручання у виборчі процеси. У випадку України такі інформаційні атаки часто організуються ззовні з метою послаблення внутрішньої єдності та дискредитації її на міжнародній арені [5].

Дезінформаційні кампанії включають поширення спотвореної інформації через соціальні мережі, онлайн-медіа та інші цифрові платформи, що дозволяє швидко охопити широке коло користувачів. Боротьба з цими явищами вима-

гає застосування інноваційних технологій для виявлення та блокування фейкових новин, а також підвищення рівня медіаграмотності населення, щоб люди могли самостійно оцінювати достовірність отриманої інформації.

3. Гібридні загрози та інформаційні війни. Гібридні загрози поєднують у собі традиційні військові методи та нетрадиційні засоби впливу, такі як інформаційні атаки, пропаганда, економічний тиск та дипломатичні маніпуляції. Гібридна війна, яку веде Росія проти України, включає активне використання дезінформаційних кампаній для створення хаосу, підриву довіри до державних органів і створення розколу в українському суспільстві.

Україна, як держава, яка стикається з гібридними загрозами, потребує чіткої стратегії для нейтралізації цих ризиків. Це включає посилення координації між різними державними відомствами, підготовку до реагування на нові форми атак та побудову стійкої системи комунікацій, яка буде менш вразливою до зовнішнього впливу.

4. Діджиталізація суспільства. Швидка діджиталізація суспільства є як великою можливістю, так і значним викликом для інформаційної політики України. З одного боку, впровадження цифрових технологій і електронного урядування сприяє підвищенню ефективності державного управління, прозорості адміністративних процесів і зниженню рівня корупції. З іншого боку, збільшення кількості користувачів цифровими послугами підвищує ризики інформаційних вразливостей та кібератак, а також збільшує загрозу з боку дезінформаційних кампаній.

Цифрова трансформація потребує побудови надійної кібернетичної інфраструктури та розробки політик, що регулюють використання нових технологій з дотриманням етичних норм та захисту конфіденційності даних. Важливою складовою також є підготовка населення до безпечного користування цифровими технологіями через програми підвищення цифрової грамотності [6].

5. Технологічна нерівність та доступ до інформації. Одним із глобальних викликів для України є питання технологічної нерівності, яка виникає внаслідок нерівного доступу до цифрових ресурсів та інформації між різними регіонами країни. Низький рівень доступу до високошвидкісного Інтернету в сільських та віддалених районах, а також недостатнє технічне забезпечення шкодять можливостям громадян

брати активну участь у цифровій економіці та користуватись електронними державними послугами.

Подолання технологічної нерівності є важливим завданням інформаційної політики України, адже лише забезпечення рівного доступу до сучасних інформаційних технологій дозволить максимально ефективно інтегрувати всі частини суспільства у процес цифрової трансформації та сприяти економічному розвитку на всіх рівнях. Глобальні виклики, що постають перед інформаційною політикою України, вимагають комплексного підходу, злагоджених дій на національному та міжнародному рівнях, а також впровадження сучасних технологій для забезпечення інформаційної безпеки. Для успішного протистояння цим викликам необхідно посилити державне регулювання у сфері кібербезпеки, розробити механізми для ефективної боротьби з дезінформацією, а також активно працювати над розвитком цифрової інфраструктури та зниженням технологічної нерівності. Тільки так Україна зможе стати стійкою до зовнішніх інформаційних атак і успішно інтегруватись у глобальне інформаційне суспільство.

Стратегічні напрями розвитку інформаційної політики України визначаються необхідністю забезпечення національної безпеки, соціальної стабільності, економічного розвитку та інтеграції в глобальне інформаційне суспільство. Сучасні глобальні виклики, такі як кіберзагрози, інформаційні війни, дезінформація та швидка цифрова трансформація, вимагають від України створення комплексної стратегії для захисту свого інформаційного простору і розвитку цифрових технологій. Нижче розглянуто ключові напрями, які мають стати основою для ефективної інформаційної політики держави [6-7].

1. Розвиток кібербезпеки та захисту критичної інфраструктури. Кібербезпека є найважливішим пріоритетом у стратегічному плануванні інформаційної політики України, оскільки країна неодноразово зазнавала масштабних кібератак з боку агресорів. Для ефективного захисту критичної інфраструктури, яка включає енергетичні системи, транспорт, фінансовий сектор і державні інформаційні ресурси, необхідно створити національну кібернетичну стратегію, яка передбачає: Інвестиції в сучасні технології: впровадження передових систем захисту від кібератак, використання штучного інтелекту для виявлення та нейтралізації загроз. Підготовка фахівців: розвиток освітніх програм для

підготовки висококваліфікованих спеціалістів у сфері кібербезпеки та постійне підвищення кваліфікації кадрів. Міжвідомча координація: створення єдиної платформи для координації дій між державними установами, приватним сектором та міжнародними партнерами в разі кіберінцидентів. Розробка законодавчих актів: вдосконалення законодавчої бази для регулювання діяльності у сфері кібербезпеки та визначення відповідальності за порушення інформаційної безпеки.

2. Боротьба з фейковими новинами та дезінформацією. У боротьбі з дезінформацією та фейковими новинами важливо створити комплексну систему моніторингу та реагування на інформаційні загрози. Основними елементами цієї стратегії мають стати: Моніторинг інформаційного простору: використання технологій штучного інтелекту та великих даних (Big Data) для виявлення фейкових новин та дезінформаційних кампаній у реальному часі. Створення Центру протидії дезінформації: організація спеціалізованого державного центру, який координуватиме зусилля з нейтралізації інформаційних атак, проведення контрkamпаній та інформування населення про маніпуляції. Розвиток медіаграмотності: впровадження освітніх програм для підвищення критичного мислення серед населення, що допоможе громадянам розпізнавати фейкову інформацію та маніпуляції в медіапросторі. Співпраця з соціальними мережами та медіаплатформами: укладення угод із провідними технологічними компаніями щодо оперативного видалення дезінформаційного контенту та блокування облікових записів, пов'язаних із поширенням фейкових новин.

3. Підтримка цифрової трансформації та інновацій. Цифрова трансформація економіки є ключовою складовою для розвитку конкурентоспроможності України у глобальному масштабі. Вона передбачає всебічне впровадження новітніх технологій, автоматизацію процесів і розвиток інноваційного потенціалу держави. Основні заходи в цьому напрямку включають: Розвиток інфраструктури: забезпечення доступу до високошвидкісного Інтернету у всіх регіонах України, включаючи віддалені райони, щоб подолати цифровий розрив та забезпечити рівні можливості для всіх громадян. Інтеграція цифрових технологій у державне управління: впровадження електронного урядування (e-governance) для підвищення

ефективності надання державних послуг, скорочення бюрократичних бар'єрів та покращення прозорості державних процесів. Підтримка стартапів та IT-сектора: створення сприятливого середовища для розвитку технологічних компаній та інноваційних проєктів, зокрема через надання грантів, податкових пільг та створення технопарків. Розвиток штучного інтелекту та великих даних: підтримка досліджень та розробок у галузі штучного інтелекту, машинного навчання, аналітики даних для створення інноваційних продуктів та сервісів.

4. Міжнародна співпраця та інтеграція у глобальні інформаційні мережі. Міжнародна співпраця є важливим елементом для ефективного протистояння глобальним викликам, що стоять перед інформаційною політикою України. Це включає розвиток стратегічних партнерств з країнами та організаціями, які мають досвід у сфері інформаційної безпеки та кібернетичного захисту. Основні аспекти міжнародної співпраці включають: Інтеграція в європейські та глобальні інформаційні мережі: активна участь у програмах Європейського Союзу та НАТО, які спрямовані на посилення кібербезпеки та розвиток спільних механізмів захисту від гібридних загроз. Участь у міжнародних ініціативах та обміні досвідом: регулярне проведення міжнародних конференцій, форумів та навчань з кібербезпеки для обміну знаннями, передовими технологіями та кращими практиками. Співпраця з глобальними технологічними компаніями: партнерство з провідними світовими компаніями у галузі інформаційних технологій для забезпечення доступу до новітніх розробок та підвищення рівня захисту національного кіберпростору.

5. Регулювання та гармонізація законодавства у сфері інформаційної безпеки. Для забезпечення ефективної інформаційної політики важливим є вдосконалення законодавчої бази, яка повинна відповідати сучасним викликам і бути гармонізованою з європейськими стандартами. Це передбачає: Розробку нормативних актів для захисту персональних даних: забезпечення прав громадян на конфіденційність та захист їхньої приватної інформації відповідно до міжнародних стандартів, таких як GDPR. Удосконалення правових механізмів: посилення відповідальності за кібератаки, інформаційні злочини та поширення дезінформації, що включає запровадження суворіших санкцій за порушення у цій сфері. Створення

стандартів безпеки для цифрових платформ: розробка чітких вимог і рекомендацій щодо захисту даних, кібербезпеки та етичного використання штучного інтелекту.

Стратегічні напрями розвитку інформаційної політики України повинні бути орієнтовані на забезпечення національної кібербезпеки, підвищення стійкості до дезінформації, розвиток цифрової економіки та активну інтеграцію у міжнародні інформаційні мережі. Реалізація цих напрямів створить фундамент для стабільного економічного розвитку, підвищить конкурентоспроможність країни на глобальній арені та зміцнить національну безпеку в умовах сучасних інформаційних загроз.

Висновки. У результаті проведеного дослідження було визначено, що інформаційна політика України відіграє ключову роль у забезпеченні національної безпеки, соціальної стабільності та економічного розвитку в умовах глобальних викликів. Сучасний інформаційний простір став полем для ведення гібридних воєн, кібернетичних атак і дезінформаційних кампаній, які суттєво впливають на політичні процеси, суспільну думку та міжнародні відносини. В цих умовах Україні необхідно адаптувати свою інформаційну політику до нових реалій та активно розвивати стратегічні напрями, спрямовані на посилення кібербезпеки, протидію фейковим новинам, діджиталізацію та міжнародну співпрацю. Аналіз поточного стану інформаційної політики показав, що попри значний прогрес у створенні нормативно-правової бази та впровадженні заходів із захисту критичної інфраструктури, перед Україною все ще стоїть низка серйозних викликів. До них належать постійні кібератаки з боку агресорів, високий рівень дезінформації у медіапросторі та технологічна нерівність між регіонами. Ці фактори створюють значні загрози для стабільності суспільства та потребують системного підходу для їх вирішення. Основні стратегічні напрями розвитку інформаційної політики повинні включати створення надійної системи кібербезпеки, впровадження новітніх техноло-

гій для виявлення та нейтралізації інформаційних загроз, активне просування медіаграмотності серед населення та підтримку інноваційних технологій. Особлива увага має бути приділена міжнародному співробітництву, що дозволить Україні інтегруватись у глобальні інформаційні мережі та запозичити передовий досвід у сфері інформаційної безпеки. Загалом, лише за умови реалізації комплексної та адаптивної інформаційної політики Україна зможе стати стійкою до зовнішніх інформаційних впливів, забезпечити розвиток цифрової економіки та ефективно інтегруватись у світове інформаційне суспільство. Це не тільки сприятиме підвищенню рівня національної безпеки, але й створить нові можливості для економічного зростання, соціального прогресу та зміцнення міжнародної позиції України на глобальній арені.

Список використаної літератури:

1. Шульга О. І., Мельник Л. М. Забезпечення інформаційної безпеки України: сучасні виклики та шляхи вирішення. Інформаційні технології та кібербезпека. 2020. Т. 18. № 2. С. 112–120. DOI: 10.32620/ITKB.2020.18.2.12.
2. Шабунін С. М., Ємельянова О. В. Протидія російській дезінформації: аналіз стратегій та механізмів впливу. Журнал соціальних комунікацій. 2019. № 4. С. 38–45.
3. Офіційний сайт Міністерства цифрової трансформації України. URL: <https://thedigital.gov.ua>
4. Грицай В. М., Карпенко О. В. Цифрова трансформація державного управління в Україні: перспективи та виклики. Вісник економічної науки України. 2021. № 3. С. 55–62.
5. Тодоренко Г. М. Кіберзагрози як інструмент гібридної війни: виклики для України. Сучасне суспільство. 2019. № 2. С. 88–97.
6. Мельник А. П. Інформаційна безпека України: проблеми та шляхи їх вирішення. Економіка та безпека держави. 2019. № 6. С. 41–49.
7. Кравченко П. М. Кіберзахист критичної інфраструктури України: міжнародний досвід та національні пріоритети. Вісник державної служби та місцевого самоврядування. 2018. Вип. 4. С. 99–106.

Dimitriev V. V. Strategic directions of the development of Ukraine's information policy in the context of global challenges

The article examines the strategic directions of the development of Ukraine's information policy in the context of modern global challenges, such as digitalization, cyber security, information attacks, disinformation and hybrid threats. The development of information policy is considered as one of the key factors determining the country's ability to ensure national security, society's resilience to informational influence, and competitiveness in the global information environment. The current state of Ukraine's information space is analyzed, which requires strengthening of cyber security and protection of critical infrastructure, countering disinformation and fake news, as well as active digi-

talization of the economy. The article highlights the main global threats that Ukraine faces, such as cyber attacks and information manipulation used in hybrid warfare. Four main strategic directions for the development of Ukraine's information policy are proposed: strengthening cyber security and protection of critical information systems, fighting fake news, supporting the digital transformation of the economy and society, as well as expanding international cooperation and integration into global information networks. Attention is paid to the importance of international cooperation for the purpose of sharing experience, technologies and joint response to the latest information threats. The specified strategic directions of information policy development will not only contribute to the increase of national security, but will also create conditions for Ukraine's active involvement in global information processes, contributing to its integration into the global digital economy. This, in turn, will allow Ukraine to strengthen its position in the international arena and reduce dependence on external informational influences. Special attention in the article is paid to the issue of cyber security, which in modern conditions is a key component of national security. Cyberspace is becoming a field for conducting military operations of a new generation, which requires the development of effective defense mechanisms and a strategy for rapid response to cyber threats. The experience of recent years shows that Ukraine is at the forefront of cyber conflicts, and the development of a national cyber strategy is extremely important to minimize risks in this area. It was concluded that the implementation of these strategic directions is a necessary condition for effectively countering modern challenges, ensuring information security and building a competitive information ecosystem in Ukraine. The development of innovation and digitalization is considered a key factor for ensuring sustainable economic development and social stability of the state.

Key words: *information policy, cyber security, fake news, hybrid threats, digitalization, Ukraine.*