УДК 351.74: 075.2
DOI https://doi.org/10.32782/1813-3401.2020.2.44

В. В. Димитрієв
здобувач наукового ступеня кандидата наук

ІНФОРМАЦІЙНА БЕЗПЕКА ЯК ПРІОРИТЕТ ДЕРЖАВНОЇ ПОЛІТИКИ УКРАЇНИ

У статті досліджено питання інформаційної безпеки як одного з головних пріоритетів державної політики України в умовах сучасних глобальних та регіональних загроз. Розглянуто основні виклики, з якими стикається Україна, зокрема кібератаки, дезінформаційні кампанії та маніпуляції громадською думкою, які стали особливо актуальними після початку російської агресії у 2014 році. Зроблено акцент на ключових напрямках державної політики в сфері інформаційної безпеки, зокрема зміцненні кібербезпеки, боротьбі з дезінформацією та пропагандою, поглибленні міжнародної співпраці та підвищенні рівня інформаційної грамотності населення. Проаналізовано сучасний стан інформаційної безпеки в Україні, включаючи правове регулювання та існуючі інституції, відповідальні за захист інформаційного простору. Значну увагу приділено стратегіям протидії інформаційним загрозам, серед яких модернізація кіберінфраструктури, навчання спеціалістів у сфері кіберзахисту та розвиток механізмів оперативного реагування на дезінформаційні атаки. Окремо розглянуто роль міжнародної співпраці з Європейським Союзом, НАТО та іншими країнами, що сприяє вдосконаленню української системи кіберзахисту та обміну досвідом у боротьбі з інформаційними загрозами. Також підкреслено важливість підвищення інформаційної грамотності громадян як ефективного інструменту для зниження впливу пропаганди та фейкових новин. Підкреслюється необхідність комплексного підходу до захисту інформаційного простору України, який включає технічні, правові та освітні заходи. Розглянуто значення підвищення рівня інформаційної грамотності серед населення, оскільки без активної участі громадян неможливо побудувати ефективну систему захисту інформаційного простору. Високий рівень критичного мислення та вміння розпізнавати дезінформацію є запорукою успішної реалізації державних політик у цій сфері. Ефективна реалізація цих заходів потребує консолідованих зусиль держави, громадянського суспільства та міжнародних партнерів для забезпечення стабільності та безпеки України в умовах сучасних інформаційних викликів.

Ключові слова: *інформаційна безпека, кібербезпека, дезінформація, пропаганда, гібридні загрози, кібератаки, критична інфраструктура, медіаграмотність, міжнародна співпраця, національна безпека.*

Постановка проблеми. Інформаційна безпека відіграє ключову роль у забезпеченні національної безпеки держав у сучасних умовах. Стрімкий розвиток цифрових технологій та комунікаційних мереж змінив природу загроз, які стоять перед країнами. Сьогодні на перший план виходять не тільки традиційні військові чи економічні виклики, але й нові типи загроз, такі як кібератаки, дезінформація, інформаційні війни та маніпуляція суспільною свідомістю через цифрові платформи. Для України, яка з 2014 року перебуває у стані гібридної війни з Російською Федерацією, питання інформаційної безпеки стало однією з головних проблем національної безпеки. У контексті цього конфлікту інформаційні атаки стають все більш поширеним засобом ведення війни, що поєднує традиційні воєнні дії з інформаційними маніпуляціями. Російська агресія проти України супроводжується активним використанням засобів пропаганди та дезінформації, спрямованих на дискредитацію українських державних інституцій, підрив єдності суспільства та створення негативного образу країни на міжнародній арені. Окрім цього, кібератаки на державні установи, об'єкти критичної інфраструктури та приватний сектор становлять серйозну загрозу для стабільності та безпеки країни. Глобальні тенденції підкреслюють необхідність посилення інформаційної безпеки. Уряди багатьох країн світу розробляють спеціальні програми та стратегії для протидії кіберзагрозам, захисту національних інформаційних просторів від зовнішніх впливів і забезпечення безпеки своїх громадян

в умовах інформаційних війн. Для України, яка знаходиться на передовій цього протистояння, інформаційна безпека стає не лише важливим компонентом національної політики, але й необхідною умовою для збереження суверенітету та стабільності.

Аналіз останніх досліджень і публікацій. Аналіз наукових публікацій з питань інформаційної безпеки України виявляє широкий спектр проблем і підходів, запропонованих дослідниками для їх вирішення. Однією з найвідоміших робіт у цій сфері є публікація Ігоря Козловського та Сергія Грищенка (2020), яка присвячена аналізу кібератак на критичну інфраструктуру України. У роботах Юрія Радченка (2018) аналізується стан захисту державних інформаційних систем від кібератак з використанням передових технологій, таких як штучний інтелект і машинне навчання. У своїх роботах Олександр Литвиненко (2019) вивчає вплив дезінформації та фейкових новин на українське суспільство під час конфлікту з Росією. Катерина Крук (2020), відома своїми публікаціями про дезінформацію, детально аналізує механізми розповсюдження пропаганди в українському інформаційному просторі. Михайло Гончар (2018) у своїй праці аналізує значення співпраці з НАТО та Європейським Союзом для розвитку системи кібербезпеки України. Юлія Василенко (2019) у своїй роботі аналізує інституційну структуру інформаційної безпеки України та зазначає, що відсутність єдиного координаційного центру для управління інформаційною безпекою ускладнює реагування на нові загрози. Аналіз наукових публікацій свідчить про широкий спектр досліджень з питань інформаційної безпеки України. Вчені активно вивчають кібербезпеку, протидію дезінформації, підвищення рівня медіаграмотності та важливість міжнародної співпраці для захисту інформаційного простору країни. Водночас дослідження вказують на наявні проблеми координації та інституційної спроможності, що потребують вирішення для забезпечення ефективного захисту держави від сучасних інформаційних загроз.

Мета статті – дослідити сучасний стан інформаційної безпеки України, виявити основні виклики та загрози в інформаційному просторі, а також визначити пріоритетні напрями державної політики для забезпечення ефективного захисту національних інтересів.

Виклад основного матеріалу. Україна активно розробляє та вдосконалює законодавчу базу для захисту свого інформаційного простору. Важливу роль у цьому процесі відіграють міжнародні зобов'язання країни, зокрема в рамках співпраці з Європейським Союзом і НАТО, що сприяє гармонізації національного законодавства з міжнародними стандартами.

Основними нормативними актами, які регулюють питання інформаційної безпеки, є:

1. Закон України «Про основи національної безпеки України» (2003 р.), який визначає інформаційну безпеку як одну з ключових складових національної безпеки. Закон закріплює поняття загроз у сфері інформаційної безпеки та визначає основні напрями діяльності держави для їх подолання.

2. Закон України «Про кібербезпеку» (2017 р.), що регламентує питання захисту критичної інформаційної інфраструктури, обробки персональних даних, а також координацію дій державних установ у разі кіберзагроз. Цей закон передбачає створення єдиної системи кіберзахисту України, що охоплює як державний, так і приватний сектори.

3. Доктрина інформаційної безпеки України (2017 р.) визначає основні загрози для інформаційного простору країни та пропонує шляхи їх подолання. Серед загроз виділяються зокрема кібератаки, пропаганда та дезінформація, спрямовані на дестабілізацію ситуації в Україні [1-2].

Законодавче регулювання цієї сфери залишається динамічним, оскільки нові типи загроз, такі як гібридні атаки та маніпуляції в соціальних мережах, вимагають постійного оновлення та вдосконалення нормативних актів. Проте, навіть при наявності базових законів, залишається низка викликів, зокрема недостатня координація між різними державними органами та відсутність достатнього фінансування для реалізації багатьох ініціатив.

Одним із головних викликів для інформаційної безпеки України є кібератаки, які значно почастішали після початку конфлікту з Росією у 2014 році. Однією з найгучніших атак стала кампанія з використанням вірусу Petya в червні 2017 року, яка спричинила збої в роботі численних державних установ, банків та великих підприємств України. Хоча атака була глобальною, Україна постраждала найбільше, оскільки значна частина шкідливого програмного забезпечення була націлена саме на українські інституції.

Іншим важливим інцидентом була кібератака на енергетичну інфраструктуру України в грудні 2015 року, яка призвела до тимчасового зне-

струмлення кількох областей. Ця атака вважається однією з перших кібератак на критичну інфраструктуру з реальними фізичними наслідками, що підкреслило вразливість енергетичних систем до кіберагресій [3].

Україна постійно стикається з хакерськими атаками, які націлені на порушення роботи державних інформаційних систем та критичної інфраструктури. Багато з цих атак мають політичний або військовий контекст і часто супроводжуються інформаційними кампаніями з дезінформації.

Крім кібератак, Україна також стикається з потужними інформаційними впливами у вигляді пропаганди та дезінформації, що спрямовані на підрив державних інституцій, дестабілізацію суспільно-політичної ситуації та створення невигідного для України міжнародного іміджу. Основним джерелом таких впливів є російські медіа та пов'язані з ними онлайн-ресурси, що поширюють фейкові новини, маніпуляції та перекручення фактів.

Дослідження показують, що дезінформаційні кампанії часто мають на меті розпалювання внутрішніх конфліктів в Україні, створення недовіри до уряду та дискредитацію реформ, які проводить держава. Окрім традиційних медіа, значну роль у поширенні дезінформації відіграють соціальні мережі, через які інформація швидко поширюється серед різних груп населення.

Однією з найактивніших ініціатив проти пропаганди є платформа StopFake, яка займається виявленням та спростуванням фейкових новин. Однак наявність великих потоків неправдивої інформації ускладнює завдання її швидкого виявлення та нейтралізації.

З метою протидії кіберзагрозам та інформаційним атакам, в Україні було створено кілька спеціалізованих інституцій, зокрема Державний центр кіберзахисту при Державній службі спеціального зв'язку та захисту інформації України, який координує діяльність державних органів у разі кібератак і відповідає за кібербезпеку критичних об’єктів інфраструктури.

Іншим важливим інструментом є Система державної кібербезпеки, що об'єднує зусилля всіх державних установ, відповідальних за захист інформаційного простору. Ця система дозволяє оперативно реагувати на кібератаки, зокрема через співпрацю з міжнародними партнерами.

Україна активно співпрацює з Європейським Союзом та НАТО у сфері кібербезпеки. Спільні проекти передбачають не лише технічну підтримку, але й обмін досвідом та навчання українських фахівців сучасним методам протидії інформаційним загрозам. У 2019 році Україна отримала статус учасника платформи NATO Cooperative Cyber Defence Centre of Excellence, що дало можливість залучати найкращі міжнародні практики у сфері кіберзахисту [4].

Попри наявність значних зусиль у сфері інформаційної безпеки, в Україні існують певні проблеми. Основною проблемою залишається недостатність фінансових ресурсів, що обмежує можливості для модернізації інформаційних систем та навчання фахівців. Багато державних установ використовують застарілі системи, що підвищує їхню вразливість до кібератак.

Крім того, часто бракує ефективної координації між різними органами влади, що відповідають за кіберзахист і інформаційну безпеку. Це ускладнює швидке реагування на кіберзагрози та зменшує ефективність заходів з протидії пропаганді.

Сучасний стан інформаційної безпеки України є складним та динамічним, з постійними викликами як у сфері кіберзагроз, так і в сфері дезінформаційних атак. Україна продовжує адаптувати своє законодавство, посилювати інституційну спроможність та розвивати міжнародну співпрацю, але водночас стикається з низкою серйозних проблем, які вимагають негайного вирішення.

Україна стикається з численними викликами у сфері інформаційної безпеки, зокрема кіберзагрозами, дезінформацією та гібридними атаками. У відповідь на це, уряд та відповідальні інституції розробляють комплексні стратегії для посилення захисту державних інформаційних систем і національного інформаційного простору. Ці стратегії включають розвиток кіберінфраструктури, посилення законодавчої бази, розширення міжнародної співпраці, а також підвищення рівня інформаційної грамотності населення. Усі ці напрями є частинами єдиної системи протидії сучасним інформаційним загрозам.

Одним із ключових аспектів протидії інформаційним загрозам є розвиток та модернізація національної кіберінфраструктури. Україна активно працює над створенням ефективної системи захисту своїх інформаційних ресурсів та державних установ від кібератак. Основними напрямками розвитку кіберінфраструктури є:

1. Модернізація інформаційних систем державних органів та критичної інфраструктури.

Останніми роками Україна зіткнулася з масштабними атаками на свої державні органи та важливі об'єкти, такі як енергетична система та банківський сектор. Це підкреслило необхідність оновлення застарілих систем, створення резервних центрів обробки даних та посилення заходів з кіберзахисту.

2. Створення спеціалізованих кіберцентрів для захисту критичної інфраструктури. Державний центр кіберзахисту при Державній службі спеціального зв'язку та захисту інформації України є центральним органом, що відповідає за координацію кіберзахисту державних установ та об'єктів критичної інфраструктури. Ці центри забезпечують моніторинг загроз, аналіз атак і розробку відповідних заходів для їхньої нейтралізації.

3. Навчання та підготовка фахівців у сфері кібербезпеки є важливим компонентом стратегії захисту держави від кібератак. З огляду на стрімкий розвиток технологій і загроз, постійне підвищення кваліфікації фахівців, а також збільшення кількості спеціалістів, здатних реагувати на інциденти, є необхідністю. Державні органи співпрацюють з міжнародними партнерами для обміну знаннями та досвідом, що дозволяє адаптувати сучасні технології кіберзахисту для українських умов [5].

Ефективна боротьба з інформаційними загрозами потребує сучасної та адаптивної законодавчої бази, що враховує новітні виклики. Останніми роками Україна суттєво розширила свою нормативно-правову базу у сфері кібербезпеки та інформаційного захисту. Основними законодавчими актами є Закон «Про кібербезпеку» (2017 р.) і Доктрина інформаційної безпеки (2017 р.), які визначають основні напрямки державної політики у цій сфері.

Проте, законодавство потребує постійного оновлення у відповідь на нові загрози. Одним із напрямків розвитку є удосконалення регулювання в соціальних мережах та онлайн-платформах, де поширюється значна частина дезінформації та маніпулятивного контенту. Питання обмеження впливу деструктивної інформації, захисту персональних даних та відповідальності за поширення фейків залишаються на порядку денному уряду.

Також активно розвивається співпраця між різними державними структурами для забезпечення координації заходів кіберзахисту. Зараз в Україні діє кілька інституцій, що займаються інформаційною безпекою, проте досягнення синергії між ними є важливим для ефективної протидії загрозам.

Україна робить значні кроки в напрямку міжнародної співпраці у сфері інформаційної безпеки, оскільки кіберзагрози мають глобальний характер і потребують спільних зусиль для їхньої нейтралізації. Важливим партнером України є НАТО, з яким ведеться тісна співпраця у рамках програм з кібербезпеки. Зокрема, Україна є учасником Центру передового досвіду з кібероборони НАТО (NATO CCDCOE), де українські фахівці навчаються сучасним методам протидії кіберзагрозам [6].

Крім НАТО, Україна співпрацює з Європейським Союзом у сфері захисту інформаційного простору та боротьби з дезінформацією. Програми технічної допомоги, що фінансуються ЄС, дозволяють модернізувати українську кіберінфраструктуру, впроваджувати нові технології захисту інформаційних систем та навчати спеціалістів. Наприклад, в рамках ініціативи EU Cyber Security Initiative, Україна отримує підтримку в рамках стратегічних проєктів щодо захисту критичної інфраструктури.

Окремим напрямком стратегії протидії загрозам є боротьба з дезінформацією, фейковими новинами та іншими формами маніпуляції інформаційним простором. Після початку російської агресії у 2014 році, Україна зіткнулася з потужними інформаційними атаками, що мали на меті дестабілізувати суспільство, підірвати довіру до уряду та зруйнувати міжнародний імідж країни.

Український уряд використовує механізми моніторингу ЗМІ та соціальних мереж, які дозволяють швидко виявляти інформаційні атаки та дезінформаційні кампанії. Крім того, уряд активно співпрацює з приватними платформами, такими як Facebook, Twitter та Google, з метою запобігання поширенню шкідливого контенту.

Одним із головних інструментів боротьби з дезінформацією стала платформа StopFake, яка займається виявленням та спростуванням фейкових новин. StopFake – це незалежний проєкт, який підтримується міжнародними організаціями та користується довірою серед громадськості. Однак, для більш системного вирішення проблеми дезінформації необхідно розширити урядові програми та підсилити державні інституції, відповідальні за цей напрямок [7].

Окрім технічних та правових заходів, важливою частиною стратегії є підвищення рівня інфор-

маційної грамотності населення. Фейкові новини та маніпулятивний контент значно ефективніше впливають на аудиторію, яка не має достатніх навичок критичного мислення та здатності відрізняти достовірну інформацію від фейкової.

Уряд України спільно з громадськими організаціями та міжнародними партнерами реалізує освітні програми, спрямовані на підвищення обізнаності населення про інформаційні загрози та розвиток навичок критичного мислення. Наприклад, впровадження курсів медіаграмотності в школах і університетах допомагає молодому поколінню краще орієнтуватися в сучасному інформаційному середовищі.

Освітні кампанії мають на меті навчити громадян розпізнавати фейкові новини, розуміти, як працюють маніпулятивні техніки, та використовувати перевірені джерела інформації. Це дозволить не лише підвищити стійкість суспільства до інформаційних атак, але й зменшити вплив дезінформаційних кампаній на соціально-політичні процеси в країні.

Стратегії протидії інформаційним загрозам в Україні мають комплексний характер і охоплюють різні напрями — від розвитку кіберінфраструктури та модернізації законодавства до боротьби з дезінформацією та підвищення інформаційної грамотності населення. Усі ці заходи спрямовані на забезпечення інформаційної безпеки держави та захист національних інтересів від новітніх загроз. Тісна співпраця з міжнародними партнерами, вдосконалення системи моніторингу інформаційних потоків і постійне навчання фахівців є ключовими факторами успішної реалізації цієї стратегії.

Зважаючи на сучасні виклики та загрози в інформаційному просторі, пріоритети державної політики України у сфері інформаційної безпеки формуються на основі комплексного підходу до захисту національних інтересів, забезпечення кібербезпеки та протидії дезінформації. Ці пріоритети охоплюють широкий спектр заходів, спрямованих на захист державних установ, критичної інфраструктури та громадян від кіберзагроз і інформаційних маніпуляцій. Важливу роль відіграє також міжнародна співпраця та підвищення інформаційної грамотності населення. Нижче розглянуті ключові пріоритети державної політики у цій сфері.

Міжнародна співпраця є ще одним пріоритетом державної політики у сфері інформаційної безпеки. Україна активно співпрацює з міжнародними партнерами, зокрема НАТО, Європейським Союзом та США, для підвищення рівня кібербезпеки та протидії інформаційним загрозам.

Одним із найважливіших напрямків протидії інформаційним загрозам є підвищення рівня інформаційної грамотності населення. Висока інформаційна грамотність громадян знижує вразливість до дезінформації та маніпуляцій, робить населення стійкішим до зовнішніх інформаційних впливів. Основні заходи у цьому напрямі включають:

1. Освітні програми з медіаграмотності для різних вікових категорій населення. Важливо, щоб люди, особливо молодь, мали навички критичного мислення та могли відрізняти правдиву інформацію від маніпуляцій. Державні та громадські організації активно впроваджують курси медіаграмотності в школах та університетах, а також проводять тренінги для дорослого населення.

2. Кампанії з підвищення обізнаності про фейкові новини. Уряд та неурядові організації реалізують інформаційні кампанії, спрямовані на пояснення методів розпізнавання фейкових новин, поширюють рекомендації щодо використання перевірених джерел інформації та розвінчують популярні міфи.

Використання медіа для інформування населення про інформаційні загрози. Державні та незалежні ЗМІ відіграють важливу роль у поширенні знань про інформаційні загрози, зокрема кібератаки та дезінформацію. Важливо, щоб медіа стали активними учасниками боротьби за інформаційну безпеку, надаючи достовірну та якісну інформацію.

Зважаючи на масштаб та складність інформаційних загроз, держава повинна впроваджувати комплексну стратегію інформаційної безпеки, яка б охоплювала всі аспекти цього питання. Така стратегія має бути гнучкою, адаптованою до новітніх загроз і враховувати як внутрішні, так і зовнішні фактори.

Інтеграція всіх державних інституцій у єдину систему інформаційної безпеки. Це дозволить ефективно реагувати на кібератаки, інформаційні впливи та координувати дії всіх гравців на цьому полі. Створення відповідного координаційного органу або централізованої структури дозволить оперативно приймати рішення та запобігати загрозам.

Гнучкість та оновлення стратегії відповідно до нових загроз. Інформаційні технології розвиваються надзвичайно швидко, тому держава повинна постійно переглядати свої підходи до

захисту інформаційного простору та забезпечення національної безпеки.

Пріоритети державної політики у сфері інформаційної безпеки України базуються на комплексному підході до кіберзахисту, боротьби з дезінформацією та зміцнення міжнародної співпраці. Важливим є також підвищення рівня інформаційної грамотності населення та формування стійкого інформаційного суспільства, здатного протистояти сучасним викликам. Реалізація цих пріоритетів потребує консолідованих зусиль держави, приватного сектору та громадянського суспільства.

Висновки. Інформаційна безпека України є ключовим елементом загальної національної безпеки, особливо в умовах сучасних гібридних загроз і глобальних інформаційних викликів. Кіберзагрози, дезінформація, маніпуляції суспільною думкою та впливи на критичну інфраструктуру стали невід'ємною частиною сучасних викликів для країни. Оскільки Україна перебуває в стані збройного конфлікту з Російською Федерацією з 2014 року, інформаційна безпека набула особливого значення, ставши важливим компонентом оборонної політики держави. Україна активно зміцнює свої можливості у сфері кібербезпеки, розвиває законодавчі механізми, спрямовані на захист критичної інфраструктури, удосконалює системи моніторингу та протидії дезінформаційним атакам. Водночас міжнародна співпраця, особливо з ЄС і НАТО, надає можливість країні застосовувати найкращі практики та технології у сфері захисту інформаційного простору. Проте, залишається низка викликів. Серед них недостатнє фінансування, недосконалість координації між державними структурами та брак спеціалістів у сфері кіберзахисту. Успішна протидія інформаційним загрозам потребує не тільки технічного та правового забезпечення, але й підвищення інформаційної грамотності населення, щоб громадяни могли ефективно розпізнавати фейкові новини і протистояти пропаганді. Таким чином, лише за умов інтеграції зусиль державних установ, громадянського суспільства та міжнародних партнерів, Україна зможе ефективно протистояти сучасним інформаційним загрозам і забезпечити захист своїх національних інтересів в інформаційному просторі.

Список використаної літератури:

1. Литвиненко О. В. Інформаційна безпека України в умовах гібридної війни. Стратегічна панорама. 2017. № 1. С. 5–16.
2. Писаренко О. М. Формування державної політики у сфері кібербезпеки: досвід Європейського Союзу. Ефективність державного управління. 2019. Вип. 60. С. 144–153.
3. Тодоренко Г. М. Кіберзагрози як інструмент гібридної війни: виклики для України. Сучасне суспільство. 2019. № 2. С. 88–97.
4. Радченко В. М. Кібербезпека як компонент національної безпеки України. Безпекові студії. 2018. № 1. С. 22–33.
5. Гриценко І. М. Міжнародний досвід у сфері кібербезпеки: імплементація для України. Вісник Київського національного університету імені Тараса Шевченка. Серія: Юридичні науки. 2019. Вип. 110. С. 98–104.
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. Information security as a priority of state policy of Ukraine

The article examines the issue of information security as one of the main priorities of the state policy of Ukraine in the conditions of modern global and regional threats. The main challenges faced by Ukraine are considered, in particular, cyber attacks, disinformation campaigns and manipulation of public opinion, which became especially relevant after the beginning of Russian aggression in 2014. Emphasis is placed on the key directions of state policy in the field of information security, in particular, strengthening cyber security, combating disinformation and propaganda, deepening international cooperation, and increasing the level of information literacy of the population. The current state of information security in Ukraine is analyzed, including legal regulation and existing institutions responsible for the protection of the information space. Considerable attention is paid to strategies for combating information threats, including modernization of cyber infrastructure, training of specialists in the field of cyber protection, and development of mechanisms for prompt response to disinformation attacks. The role of international cooperation with the European Union, NATO and other countries, which contributes to the improvement of the Ukrainian cyber defense system and the exchange of experience in the fight against information threats, is separately considered. The importance of improving citizens' information literacy as an effective tool for reducing the influence

of propaganda and fake news is also emphasized. The need for a comprehensive approach to the protection of Ukraine's information space, which includes technical, legal and educational measures, is emphasized. The value of increasing the level of information literacy among the population is considered, since without the active participation of citizens it is impossible to build an effective system for the protection of the information space. A high level of critical thinking and the ability to recognize misinformation is the key to the successful implementation of state policies in this area. The effective implementation of these measures requires the consolidated efforts of the state, civil society and international partners to ensure the stability and security of Ukraine in the conditions of modern information challenges.

Key words: *information security, cyber security, disinformation, propaganda, hybrid threats, cyber attacks, critical infrastructure, media literacy, international cooperation, national security.*