УДК 004.056.53:006.03:351.86
JEL D80, O32, H12
DOI 10.32782/2786-765X/2025-9-4

Босак І.М.
аспірант кафедри теоретичної та прикладної економіки,
Інститут адміністрування, державного управління та професійного розвитку
Національного університету «Львівська політехніка»
ORCID: https://orcid.org/0009-0000-7880-9043

ІНФОРМАЦІЙНА БЕЗПЕКА УКРАЇНИ: ЗАГРОЗИ ТА МЕТОДИ ПРОТИДІЇ

Стаття присвячена дослідженню сучасних викликів та загроз інформаційної безпеки держави та методів їх протидії. У сучасному світі, де електронні технології стають необхідністю для забезпечення ефективності функцій державного управління, питання інформаційної безпеки є ключовим та актуальним. У статті комплексно досліджуються типи та види реальних і потенційних інформаційних загроз національній безпеці. Особливу увагу приділено методам захисту інформаційного суверенітету, протидії широкомасштабним інформаційним впливам, війнам та операціям. За результатами дослідження впроваджено розроблені рекомендації щодо формування стратегічних напрямів державної політики у сфері забезпечення інформаційної безпеки України. Ефективна реалізація основних принципів та завдань безпеки в інформаційній сфері досягається чітким виконанням обов'язків, покладених на кожного суб'єкта окремо та забезпеченням високого рівня їх взаємодії як системи інформаційної безпеки в цілому. У статті розглядаються елементи державної системи управління інформаційною безпекою як ключового механізму забезпечення безпеки держави.

Ключові слова: публічне управління, інформаційна безпека, національний інформаційний простір; інформаційні загрози, інформаційні війни та операції, механізми протидії інформаційним загрозам.

Постановка проблеми. Розвиток сучасних інформаційних технологій визначає нові правила використання інформаційних систем, сприяючи переходу органів державної влади у цифрову сферу. Щодня державні установи, підприємства, об'єкти критичної інфраструктури та система життєзабезпечення піддаються потужним кібератакам із застосуванням передових інформаційних технологій. Це є частиною скоординованої інформаційної агресії проти України. Важливо приділяти особливу увагу захисту відповідних ресурсів органів виконавчої влади. Органи державної влади адаптуються до нових умов функціонування в інформаційному середовищі, враховуючи нові виклики, загрози та ризики. Зростання протиправного впливу на інформаційні ресурси в системі публічного управління вимагає запровадження додаткових заходів для забезпечення інформаційної безпеки.

Аналіз останніх досліджень і публікацій. Дослідженню теоретико-методологічних засад національної безпеки присвячено наукові роботи відомих вітчизняних науковців. Інформаційну складову національної безпеки досліджували такі вчені, як Є. Кравець [9], О. Данільян [3], О. Додонов [4], В. Горбулін [4], Д. Ланде [4], С. Кавун [7], В. Носов [7], О. Манжай [7], Б. Кормич [8], В. Ліпкан [11], О. Литвиненко [12], В. Лизанчук [10], Н. Нижник [13], Г. Ситник [13], В. Білоус [13], В. Остроухов [14, 15], В. Петрик [14], М. Присяжнюк [14] та інші. Забезпечення та розвиток інформаційної безпеки держави було і є важливим предметом дослідження як вітчизняних, так і закордонних науковців. Не достатньо дослідженими залишаються загрози інформаційній безпеці держави в умовах сучасних викликів та методи їх протидії

Мета статті. Метою є дослідження сучасних загроз інформаційній безпеці держави під час війни, їх впливу на національну безпеку та стратегії їх подолання.

Виклад основного матеріалу дослідження. Забезпечення інформаційної безпеки обумовлено не тільки інтересами держави, але і інтересами людини в контексті забезпечення її прав та свобод. Основою сучасної інформаційної безпеки є цілісність даних, доступність інформації, конфіденційність та достовірність. Інформаційна безпека містить в собі не тільки нормативно-правову та політичну складову, але також інституційну сферу, що передбачає діяльність органів, які її забезпечують, а також використання програмно-технічних засобів.

Загрози національній безпеці України – явища, тенденції і чинники, що унеможливлюють чи ускладнюють або можуть унеможливити чи ускладнити реалізацію національних інтересів та збереження національних цінностей України [5]. Інформаційна загроза – потенційно

або реально негативні явища, тенденції і чинники інформаційного впливу на людину, суспільство і державу, що застосовуються в інформаційній сфері з метою унеможливлення чи ускладнення реалізації національних інтересів та збереження національних цінностей України і можуть прямо чи опосередковано завдати шкоди інтересам держави, її національній безпеці та обороні [6];

Відповідно до чинного законодавства слід виділити наступні загрози інформаційній безпеці України:

– Інформаційний вплив на національну безпеку: російська федерація активно проводить інформаційні операції, які мають на меті підрив національної безпеки України, знищення української ідентичності та державності, а також дестабілізацію внутрішньої ситуації через пропаганду і маніпуляції. Відсутність чіткої відповіді на ці загрози створює вразливість для країни.

Інформаційне домінування на окупованих територіях: на тимчасово окупованих територіях росія контролює медіа і придушує свободу слова, створюючи альтернативні, маніпулятивні наративи. Це сприяє поширенню пропаганди та знищенню незалежних засобів масової інформації, що може серйозно вплинути на сприйняття реальності місцевим населенням.

– Деструктивна пропаганда і дезінформація: російська федерація активно поширює дезінформацію як на внутрішньому, так і на міжнародному рівні, з метою підриву соціальної стійкості в Україні. Відсутність ефективної системи реагування на такі загрози знижує здатність держави боротися з дезінформаційними кампаніями.

– Неврегульованість інформаційної діяльності та захисту журналістів: відсутність належного правового регулювання в інформаційній сфері призводить до зловживань і втручання в роботу журналістів, що може спричинити погрози та насильство щодо них. Це обмежує свободу преси і здатність журналістів виконувати свою роль у суспільстві.

– Несформованість системи стратегічних комунікацій в Україні: в нашій державі не вдалося створити ефективну систему стратегічних комунікацій, що ускладнює координацію заходів між різними державними органами для протидії інформаційним загрозам. Це знижує ефективність комунікації та планування інформаційних стратегій для захисту національних інтересів.

– Маніпуляція свідомістю громадян щодо європейської та євро-атлантичної інтеграції: Росія також активно поширює дезінформацію, спрямовану на послаблення підтримки євроатлантичної інтеграції України, що може призвести до політичної дестабілізації та уповільнення реформ в країні.

– Доступ до інформації на місцевому рівні: низька якість доступу до інформації, зокрема через обмежений доступ до Інтернету і політичну заангажованість місцевих медіа, створює інформаційну нерівність. Це обмежує можливості громадян отримувати об'єктивну та достовірну інформацію.

– Недостатній рівень медіаграмотності та інформаційної культури: відсутність належної медіаграмотності у суспільстві робить громадян вразливими до маніпуляцій, що дозволяє ефективно проводити інформаційні операції, які підривають стійкість населення і його сприйняття реальності.

Ключовими заходами щодо забезпечення ефективної діяльності у сфері державного управління інформаційною безпекою є розробка показників для оцінки ефективності систем захисту інформаційної безпеки держави, а також моніторинг і ідентифікація появи дестабілізуючих факторів та загроз. Важливою складовою є організація проведення фундаментальних та прикладних наукових досліджень у галузі забезпечення інформаційної безпеки. Крім того, необхідно розробити відповідну нормативно-правову базу для належного захисту інформації. Останнім важливим етапом є протистояння загрозі інформаційної війни, що стає все більш актуальним у сучасному світі [9, с. 1235].

Механізм забезпечення інформаційної безпеки є невід'ємною складовою в процесі реалізації національної безпеки. Серед ключових напрямів, які має виконувати механізм забезпечення інформаційної безпеки варто відзначити наступні:

– виявлення внутрішніх та зовнішніх загроз інформаційній безпеці держави;

– визначення індикаторів інформаційної безпеки та їх порівняння нормативними показниками;

– формування та реалізація системи моніторингу, яка включає: спостереження, збір, обробку, збереження та аналіз інформації щодо стану інформаційної безпеки держави;

– розробка заходів, спрямованих на забезпечення стабільності у сфері інформаційної безпеки держави [2, с. 39–46].

Механізми захисту інформаційної безпеки України можна розділити на два рівні – законодавчий та адміністративний. Найважливіше на законодавчому рівні – створити механізм, що дозволяє узгодити процес розробки законів з реаліями і прогресом інформаційних технологій.

Закони не можуть випереджати життя, але важливо, щоб відставання не було занадто великим, що може спричинити послаблення інформаційної безпеки. Адміністративний механізм забезпечення інформаційної безпеки охоплює установи, діяльність яких спрямована на формування та реалізацію інформаційної безпеки. Головне на адміністративному рівні – сформувати програму заходів в галузі інформаційної безпеки та забезпечити її виконання, виділяючи необхідні ресурси і контролюючи поточний стан справ.

Інформаційний вплив може викликати численні негативні наслідки, такі як політичні протиріччя, погіршення стану громадського здоров'я та загроза національній безпеці. Наслідки інформаційних загроз в контексті національної безпеки становлять серйозну загрозу як внутрішній, так і зовнішній стабільності функціонування держави. Вплив інформаційних загроз на внутрішню стабільність функціонування держави є важливим аспектом, оскільки він може мати широкий спектр наслідків для суспільства та політичної ситуації. Інформаційні загрози можуть створювати штучні конфлікти та підкреслювати існуючі розбіжності між соціальними групами. Розповсюдження недостовірної інформації може активувати негативні стереотипи та сприяти виникненню ворожнечі. Такі загрози можуть викликати емоційні реакції, як-от обурення, страх чи невдоволення, що може призвести до масових протестів або громадянських рухів. Поява негативного настрою може поглибити напругу в суспільстві, а також бути спрямованою на підкриття політичних чи етнічних розбіжностей, поділяючи суспільство та створюючи конфлікти. Застосування маніпуляційних технік може створювати враження, що певні групи є «ворогами» або «іншими», сприяючи розділенню суспільства. Інформаційні загрози також можуть підривати довіру до влади, правоохоронних органів та інших інститутів, що може призвести до втрати легітимності та ефективності державних установ. Крім того, використання маніпуляційних технік може мати негативний вплив на психологічний стан населення, викликаючи стрес, невпевненість та загальне незадоволення.

Правове забезпечення інформаційної безпеки України зазвичай не відповідає сучасному розвитку інформаційних технологій. Саме тому боротьбу з інформаційними загрозами слід розпочати з реформування поточної нормативно-правової бази і виконати наступні кроки:

– удосконалення законодавства України у сфері забезпечення інформаційної безпеки з метою створенням спеціалізованих структур, що відповідають за безпеку в кіберпросторі;

– ухвалення нормативно-правових актів, що забезпечують реалізацію концепції електронного уряду, у тому числі надання державних послуг із використанням інформаційно-комунікаційних технологій, розвиток довіреного електронного документообігу на основі використання загальнодоступних інформаційно-телекомунікаційних мереж;

– законодавче закріплення переліку правопорушень та видів відповідальності в сфері інформаційної безпеки;

– вироблення спільної стратегії інформаційної безпеки і розвиток міждержавного співробітництва у зазначеній сфері.

Організацію протидії інформаційним загрозам, спрямованим проти національних інтересів держави у воєнній сфері, слід здійснювати у два етапи: підготовка та проведення заходів протидії. Підготовка охоплює планування заходів, організацію управління, взаємодії та ресурсного забезпечення, підготовку фахівців і структурних підрозділів, інформаційної інфраструктури, а також контроль за готовністю підрозділів до виконання поставлених завдань.

Планування заходів протидії інформаційним загрозам включає чотири етапи. Перший етап – оцінювання наявного стану інформаційної безпеки об'єкта, що забезпечується. Це передбачає виявлення вразливостей елементів інформаційної інфраструктури, аналіз морально-психологічного стану особового складу, виявлення та аналіз інформаційних загроз і джерел їх походження, прогнозування розвитку загроз та їхніх наслідків, а також аналіз результатів попереднього досвіду протидії. Також на цьому етапі здійснюється підготовка вихідних даних для планування: визначення мети протидії та конкретних завдань, необхідних сил і засобів, часу на підготовку та проведення заходів, ресурсів і зовнішніх умов, які можуть вплинути на ефективність дій.

Другий етап – вироблення та затвердження замислу проведення заходів протидії. Замисел повинен містити способи і терміни дій, визначення головного виконавця, склад сил і засобів, їх розподіл за завданнями та об'єктами, які є джерелами загроз; також враховується розташування джерел загроз, об'єкти, що потребують негайного реагування, порядок управління та взаємодії між учасниками, а також забезпечення ресурсами. Цей замисел є основою для розроблення плану дій.

Третій етап – розроблення плану проведення заходів протидії. У плані визначаються послідовність, терміни і способи реалізації заходів, а також деталізується розподіл завдань між об'єктами протидії.

Четвертий, завершальний етап – доведення завдань до структурних підрозділів, які

залучаються до протидії. Це забезпечує своєчасність, оперативність та якісну підготовку до виконання завдань.

Загальне керівництво заходами протидії здійснює керівник об'єкта забезпечення інформаційної безпеки, а організацію управління – його заступник. Взаємодія між органами управління організовується з урахуванням завдань, розміщення об'єктів протидії, часу та способів дій. Ресурсне забезпечення охоплює фінансування, матеріальні засоби та залучення служб і установ. Підготовка фахівців і структурних підрозділів спрямована на досягнення необхідного рівня навченості та злагодженості. Підготовка інформаційної інфраструктури має на меті підвищення її захищеності від деструктивного інформаційно-технічного впливу. Контроль за готовністю до виконання заходів протидії здійснюється органом військового управління, відповідальним за інформаційну боротьбу.

Висновки. На основі проведеного дослідження можна зробити висновок, що в умовах цифровізації всіх сфер життя суспільства суттєво зросли виклики, загрози та ризики для інформаційної безпеки держави загалом. Серед найбільш актуальних загроз на сучасному етапі розвитку варто виокремити протиправний вплив на національні інформаційні ресурси, інформаційно-телекомунікаційні системи та критично важливу інфраструктуру, поширення недостовірної інформації з метою дезінформації населення, психологічний тиск на суспільство, спроби зовнішнього втручання в національний інформаційний простір та підрив основ функціонування державних інституцій. Усе це відбувається на тлі геополітичної нестабільності, збройної агресії та зростання міжнародної конкуренції в інформаційній сфері, що зумовлює необхідність переосмислення підходів до гарантування інформаційної безпеки як ключового елементу національної безпеки загалом.

Забезпечення ефективної інформаційної безпеки держави потребує впровадження комплексних і системних рішень. Насамперед, це вдосконалення нормативно-правового регулювання у сфері інформаційної та кібербезпеки відповідно до міжнародних стандартів. Важливу роль відіграє формування національної системи кіберзахисту з використанням сучасних технологій – таких як штучний інтелект, машинне навчання, блокчейн та автоматизовані системи виявлення загроз. Необхідним є також створення ефективної інфраструктури для моніторингу, прогнозування та реагування на інформаційні атаки, дезінформаційні кампанії та інші прояви інформаційного впливу.

Особливої уваги заслуговує розвиток людського потенціалу: підвищення цифрової грамотності населення, підготовка фахівців з інформаційної безпеки, а також посилення інформаційної культури в суспільстві. Важливим напрямом державної політики має бути підтримка наукових досліджень, інновацій та власних технологічних розробок у сфері захисту інформації. Водночас критично важливо налагоджувати міжнародне співробітництво, зокрема для створення міжнародно-правового режиму інформаційної безпеки, який би регламентував поведінку держав в інформаційному просторі, запобігав інформаційним конфліктам і сприяв ефективній взаємодії у сфері кіберзахисту.

Таким чином, лише системний, багаторівневий підхід до формування державної політики інформаційної безпеки, що поєднує правові, організаційні, технічні, освітні та міжнародні інструменти, дозволить Україні забезпечити надійний захист своїх національних інтересів, інформаційного суверенітету, стабільність функціонування державних інституцій і сталий розвиток у цифрову епоху.

Бібліографічний список

1. Боднар І. Інформаційна безпека як основа національної безпеки. *Механізм регулювання економіки*. 2014. № 1. С. 68–75.
2. Гончаренко О., Джангужин Р., Лисицин Е. Громадянський контроль і система національної безпеки. *Національна безпека України*. 2003. № 1. С. 39–46.
3. Данільян О. Г. [та ін.] Національна безпека України: сутність, структура та напрямки реалізації: навчальний посібник. Харків : Фоліо, 2002. 285 с.
4. Додонов О. Г., Горбулін В. П., Ланде Д. В. Інформаційні операції та безпека суспільства: загрози, протидія, моделювання: монографія. Київ : Інтертехнологія, 2009. 164 с.
5. Закон України «Про національну безпеку України» від 21 червня 2018 р. № 2469-VIII. URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text (дата звернення: 20.03.2025)
6. Закон України «Про основні засади забезпечення кібербезпеки України» від 5 жовтня 2017 р. № 685/2021. URL: https://zakon.rada.gov.ua/laws/show/685/2021#Text (дата звернення: 11.03.2025)
7. Кавун С. В., Носов В. В., Манжай О. В. Інформаційна безпека. Навчальний посібник. Ч. 2. Харків : Вид. ХНЕУ, 2018. 196 с.
8. Кормич Б. А. Організаційно-правові засади політики інформаційної безпеки України: Монографія. Одеса : Юридична література, 2003. 472 с.

9. Кравець Є. А. Інформаційна безпека держави. Київ : Українська енциклопедія, 1992.
10. Лизанчук В. В. Інформаційна безпека України: теорія і практика: підручник. Львів : ЛНУ ім. Івана Франка, 2017. 725 с.
11. Ліпкан В. А. Теоретичні основи та елементи національної безпеки України. Київ : КНТ, 2003. 599 с.
12. Литвиненко О. В. Інформаційні впливи та операції. Теоретико-аналітичні нариси: монографія. Київ : НІСД, 2003. 240 с.
13. Нижник Н. Р., Ситник Г. П., Білоус В. Т. Національна безпека України (методологічні аспекти, стан і тенденції розвитку): навчальний посібник. Ірпінь : Акад. ДПС України, 2000. 304 с.
14. Остроухов В. В., Петрик В. М., Присяжнюк М. М. та ін. Інформаційна безпека (соціально-правові аспекти): підручник. Київ : КНТ, 2010. 776 с.
15. Інформаційна безпека. Підручник. За ред. В. В. Остроухова. Київ : Видавництво Ліра-К, 2021. 412 с.

References

1. Bodnar I. (2014) Informatsiyna bezpeka yak osnova natsionalnoyi bezpeky [Information security as the basis of national security]. *Mekhanizm rehuliuvannya ekonomiky*, vol. 1, pp. 68–75.
2. Honcharenko O., Dzhanhuzhin R., Lysytsyn E. (2003) Hromadyanskyi kontrol i systema natsionalnoyi bezpeky [Civil control and the national security system]. *Natsional'na bezpeka Ukrainy*, vol. 1, pp. 39–46.
3. Danilyan O. H. [et al.] (2002) Natsionalna bezpeka Ukrainy: sutnist, struktura ta napryamky realizatsiyi: navchalnyi posibnyk [National Security of Ukraine: essence, structure, and directions of implementation: textbook]. Kharkiv: Folio, 285 p. (in Ukrainian)
4. Dodonov O. H., Horbulin V. P., Lande D. V. (2009) Informatsiyni operatsiyi ta bezpeka suspil'stva: zahrozy, protydiya, modelyuvannya: monohrafiya [Information operations and society security: threats, counteraction, modeling: monograph]. Kyiv: Intertekhnolohiya, 164 p. (in Ukrainian)
5. Zakon Ukrainy "Pro natsional'nu bezpeku Ukrainy" vid 21 chervnya 2018 r. № 2469-VIII [Law of Ukraine "On National Security of Ukraine" from June 21, 2018, No. 2469-VIII]. Available at: https://zakon.rada.gov.ua/laws/show/2469-19#Text (accessed: 20.03.2025)
6. Zakon Ukrainy "Pro osnovni zasady zabezpechennya kyberbezpeky Ukrainy" vid 5 zhovtnya 2017 r. № 685/2021 [Law of Ukraine "On the Basic Principles of Cybersecurity of Ukraine" from October 5, 2017, No. 685/2021]. Available at: https://zakon.rada.gov.ua/laws/show/685/2021#Text (accessed: 11.03.2025)
7. Kavun S. V., Nosov V. V., Manzhai O. V. (2018) Informatsiyna bezpeka. Navchal'nyi posibnyk. Ch. 2 [Information security. Textbook. Part 2]. Kharkiv: Vyd. KhNEU, 196 p. (in Ukrainian)
8. Kormych B. A. (2003) Orhanizatsiyno-pravovi zasady polityky informatsiynoyi bezpeky Ukrainy: Monohrafiya [Organizational and legal principles of information security policy of Ukraine: Monograph]. Odesa: Yurydychna literatura, 472 p. (in Ukrainian)
9. Kravets' Ye. A. (1992) Informatsiyna bezpeka derzhavy [Information security of the state]. Kyiv: Ukrayinska entsyklopediya. (in Ukrainian)
10. Lyzanchuk V. V. (2017) Informatsiyna bezpeka Ukrainy: teoryya i praktyka: pidruchnyk [Information security of Ukraine: theory and practice: textbook]. Lviv: LNU im. Ivana Franka, 725 p. (in Ukrainian)
11. Lipkan V. A. (2003) Teoretychni osnovy ta elementy natsional'noyi bezpeky Ukrainy [Theoretical foundations and elements of national security of Ukraine]. Kyiv: KNT, 599 p. (in Ukrainian)
12. Lytvynenko O. V. (2003) Informatsiyni vplyvy ta operatsiyi. Teoretyko-analitychni narysy: monohrafiya [Information influences and operations. Theoretical and analytical essays: monograph]. Kyiv: NISD, 240 p. (in Ukrainian)
13. Nyzhnyk N. R., Sytnyk H. P., Bilous V. T. (2000) Natsional'na bezpeka Ukrainy (metodolohichni aspekty, stan i tendentsiyi rozvytku): navchal'nyi posibnyk [National security of Ukraine (methodological aspects, state and development trends): textbook]. Irpin': Akad. DPS Ukrainy, 304 p. (in Ukrainian)
14. Ostroukhov V. V., Petrik V. M., Prysiazhniuk M. M. et al. (2010) Informatsiyna bezpeka (sotsial'no-pravovi aspekty): pidruchnyk [Information security (social and legal aspects): textbook]. Kyiv: KNT, 776 p. (in Ukrainian)
15. Informatsiyna bezpeka. Pidruchnyk. Za red. V. V. Ostroukhova. (2021) [Information security. Textbook. Edited by V. V. Ostroukhov]. Kyiv: Vydavnytstvo Lira-K, 412 p. (in Ukrainian)

Стаття надійшла до редакції 16.03.2025

Ivan Bosak
Postgraduate Student of the Department of Theoretical and Applied Economics,
Institute of Administration, Public Administration and Professional Development
Lviv Polytechnic National University
ORCID: https://orcid.org/0009-0000-7880-9043

INFORMATION SECURITY OF UKRAINE: THREATS AND METHODS OF COUNTERACTION

Objective. The article aims to explore the modern challenges and threats to information security faced by government institutions and the state as a whole, with a focus on identifying and analyzing methods for counteracting these risks. In light of the growing reliance on digital technologies in the public administration sphere, the article investigates the evolving role of information security and its integration into national security strategies. The key objective is to outline the necessary actions for strengthening the state's cybersecurity defenses and proposing measures for improving the governance of information security. **Methods**. The study employs a combination of general scientific and specific scientific methods, including dialectical, formal-logical, inductive, and comparative-legal methods. The research also incorporates historical analysis and case studies of real-world cybersecurity incidents, enabling a thorough understanding of both theoretical and practical aspects of the field. The methodological approach involves an in-depth review of existing legislation, international practices in information security management, and the use of statistical data on cybersecurity threats. **Results.** The research highlights the growing threats to information security due to the digitalization of society, including unlawful interference with national information resources, misinformation, and external influence. These risks are compounded by geopolitical instability and international competition in the information space, underscoring the need for stronger security strategies. To address these challenges, Ukraine must improve its legal and regulatory frameworks, develop a national cybersecurity system using advanced technologies like AI and blockchain, and enhance infrastructure for monitoring and responding to cyber threats. Equally important is boosting digital literacy and training information security specialists. A comprehensive approach combining legal, technical, educational, and international measures will ensure the protection of national interests and stability in the digital age. **Scientific novelty.** The scientific novelty of the article rests in its approach to defining information security not just as a technical issue, but as an integral element of national defense and state policy. The study introduces new insights into the role of public authorities in ensuring information security and explores the intersection of cybersecurity with traditional areas of public administration, defense, and law. The article emphasizes the need for the development of advanced technologies to counter these emerging threats, highlighting the importance of staying ahead of rapidly changing cybersecurity challenges. **Practical significance.** The practical significance of the study lies in the recommendations for improving the information security policy of Ukraine. The article provides a detailed analysis of the threats to the national information security system and proposes practical steps to strengthen the security of state institutions. In particular, the steps to organize counteraction to information threats directed against the national interests of the State in the context of modern challenges are considered.

Keywords: public administration, information security, national information space; information threats, information wars and operations, mechanisms of information threats counteraction.