УДК: 351.746:004.056; JEL classification: H11, H83, K24, L86 DOI: https://doi.org/10.36887/2524-0455-2026-3-26

НЕКРЯЧ Анастасія Іванівна, Доктор політичних наук, професор, професор кафедри міжнародних відносин та політичного консалтингу, Інститут права та суспільних відносин, ЗВО «Відкритий міжнародний університет розвитку людини «Україна», https://orcid.org/0000-0001-5058-4145
КИРИЧЕНКО Ганна Володимирівна, Кандидат наук з державного управління, доцент кафедри міжнародних відносин та політичного консалтингу, Інститут права та суспільних відносин, ЗВО «Відкритий міжнародний університет розвитку людини «Україна», https://orcid.org/0000-0003-1067-8758

МЕХАНІЗМИ РЕГУЛЮВАННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В СИСТЕМІ НАЦІОНАЛЬНОЇ БЕЗПЕКИ В УМОВАХ РОЗВИТКУ ІНФОРМАЦІЙНОГО СУСПІЛЬСТВА

Некряч А. І., Кириченко Г. В. Механізми регулювання інформаційної безпеки в системі національної безпеки в умовах розвитку інформаційного суспільства.

У статті проаналізовано теоретичні та практичні засади державного регулювання інформаційної безпеки як складової забезпечення національної безпеки в умовах розвитку інформаційного суспільства. Проаналізовано нормативно-правові засади державної політики у сфері інформаційної та кібербезпеки, а також сучасні міжнародні підходи до захисту інформаційного простору. Розкрито сутність інформаційної безпеки як багатокомпонентної системи, визначено її основні складові та обґрунтовано необхідність застосування системного і ризик-орієнтованого підходів до державного регулювання. Особливу увагу приділено використанню сучасних цифрових технологій, зокрема системного моделювання, цифрових двійників, штучного інтелекту та машинного навчання, які сприяють підвищенню ефективності управління інформаційними ризиками, забезпеченню стійкості критичної інформаційної інфраструктури та підтриманню процесу прийняття управлінських рішень. Обґрунтовано, що вдосконалення механізмів державного регулювання інформаційної безпеки має здійснюватися шляхом розвитку правових, організаційних та технологічних інструментів, гармонізації національного законодавства з європейськими стандартами, зміцнення системи управління інформаційними ризиками та підвищення кіберстійкості держави. Реалізація зазначених напрямів сприятиме зміцненню національної безпеки України та ефективному функціонуванню системи публічного управління в умовах цифрової трансформації.

This is an Open Access article distributed under the terms of the Creative Commons CC-BY 4.0

© *НЕКРЯЧ Анастасія Іванівна, КИРИЧЕНКО Ганна Володимирівна*, 2026

Ключові слова: *публічне управління, державне регулювання, інформаційна безпека, національна безпека, інформаційне суспільство, кібербезпека, інформаційні загрози, інформаційні ризики, критична інформаційна інфраструктура, механізми державного управління, ризик-орієнтоване управління, нормативно-правове регулювання, кіберстійкість, цифрові технології, системне моделювання.*

Постановка проблеми у загальному вигляді. Розвиток інформаційного суспільства, активна цифровізація публічного управління та широке використання інформаційно-комунікаційних технологій істотно підвищили роль інформаційної безпеки у забезпеченні національної безпеки держави. Інформаційний простір став одним із ключових середовищ реалізації національних інтересів, а його захист — одним із пріоритетних напрямів державної політики. Водночас стрімкий розвиток цифрових технологій супроводжується появою нових інформаційних загроз, зокрема кібератак, інформаційно-психологічних операцій, поширення дезінформації, несанкціонованого втручання в інформаційно-комунікаційні системи та посягань на критичну інформаційну інфраструктуру.

В умовах повномасштабної збройної агресії проти України проблема забезпечення інформаційної безпеки набуває особливої актуальності, оскільки інформаційний простір став одним із ключових об'єктів гібридного протиборства. Це зумовлює необхідність удосконалення механізмів державного регулювання, розвитку ризик-орієнтованого підходу до управління інформаційною безпекою, посилення міжвідомчої взаємодії та адаптації національної системи захисту інформації до сучасних європейських стандартів.

Вирішення зазначених проблем має важливе наукове й практичне значення, оскільки спрямоване на підвищення ефективності публічного управління у сфері інформаційної безпеки, зміцнення стійкості критичної інформаційної інфраструктури, удосконалення правового механізму захисту інформаційних ресурсів та забезпечення належного рівня національної безпеки України в умовах розвитку інформаційного суспільства.

Аналіз останніх досліджень і публікацій. Проблематика механізмів регулювання інформаційної безпеки активно досліджується у вітчизняній і зарубіжній науці у контексті національної безпеки, цифрової трансформації та розвитку інформаційного суспільства. Нормативно-правову основу функціонування системи інформаційної безпеки України становлять Конституція України, закони України у сфері національної, інформаційної та кібербезпеки, а також Стратегія кібербезпеки України [1–6].

Важливу роль у формуванні сучасних підходів до державного регулювання інформаційної безпеки відіграють міжнародні нормативні документи, зокрема Directive (EU) 2022/2555 (NIS2), Cybersecurity Act та міжнародний стандарт ISO/IEC 27001:2022, які визначають сучасні вимоги до управління кіберризиками, захисту інформаційних систем і забезпечення стійкості критичної інформаційної інфраструктури [7–9].

Окремі аспекти правового забезпечення інформаційної безпеки, удосконалення законодавства, захисту критичної інфраструктури та управління інформаційними ризиками висвітлено у працях О. Головка, М. Кравченка, І. Погребицького, В. Романюка, В. Горулька, Р. Черниша, М. Чеховської, А. Давидюка, В. Зубка, M. Brunner, A. Abedi та інших дослідників [11–17]. Питання державного регулювання інформаційної безпеки як складової забезпечення національної безпеки розглядають О. І. Пархоменко-Куцевіл та Г. Д. Радзівілов [18; 19].

Формулювання цілей статті (постановка завдання). Попри значний науковий доробок у сфері інформаційної та національної безпеки, низка аспектів механізмів регулювання інформаційної безпеки потребує подальшого наукового осмислення. Насамперед це стосується формування комплексного механізму державного регулювання, який би поєднував правові, організаційні, інституційні та технологічні інструменти забезпечення інформаційної безпеки в умовах розвитку інформаційного суспільства. Недостатньо дослідженими залишаються питання впровадження ризик-орієнтованого підходу, використання сучасних цифрових технологій і методів моделювання у процесі прийняття управлінських рішень, а також гармонізації національної системи інформаційної безпеки з європейськими стандартами. Це зумовлює необхідність подальшого вдосконалення теоретичних і практичних засад державного регулювання інформаційної безпеки як складової забезпечення національної безпеки України.

Метою статті є комплексне дослідження механізмів державного регулювання інформаційної безпеки як складової забезпечення національної безпеки в умовах розвитку інформаційного суспільства, визначення сучасних інформаційних загроз і ризиків, аналіз особливостей функціонування системи інформаційної безпеки держави, а також обґрунтування пріоритетних напрямів удосконалення механізмів державного регулювання на основі системного й ризик-орієнтованого підходів, сучасних цифрових технологій та європейських стандартів у сфері інформаційної і кібербезпеки.

Виклад основного матеріалу дослідження. Формування інформаційного суспільства докорінно змінило

значення інформації у функціонуванні держави, економіки та суспільних відносин. На сучасному етапі інформація виступає не лише засобом комунікації, а й стратегічним ресурсом, від ефективного використання та захисту якого залежить результативність державного управління, рівень економічної конкурентоспроможності, стабільність суспільно-політичної системи та забезпечення національних інтересів. За таких умов інформаційна безпека набуває статусу одного з ключових напрямів державної політики, що охоплює комплекс правових, організаційних, інституційних, технологічних і управлінських заходів. Відповідно до Закону України «Про національну безпеку України» [4] забезпечення інформаційної безпеки є складовою системи національної безпеки та спрямоване на захист державного суверенітету, конституційного ладу й інших національних інтересів від внутрішніх і зовнішніх загроз.

У сучасних наукових дослідженнях державне регулювання інформаційної безпеки трактується як система взаємопов'язаних правових, організаційних, економічних і адміністративних інструментів, за допомогою яких держава забезпечує належний рівень створення, використання, оброблення, поширення та захисту інформації. Такий підхід відповідає концепції сучасного публічного управління, відповідно до якої функції держави не обмежуються нормативним регулюванням і контролем, а передбачають координацію взаємодії органів державної влади, органів місцевого самоврядування, суб'єктів господарювання, громадянського суспільства та міжнародних партнерів з метою формування безпечного інформаційного простору. Результативність державного регулювання визначається не лише досконалістю нормативно-правової бази, а й спроможністю органів публічної влади оперативно адаптуватися до технологічних змін, імплементувати міжнародні стандарти та використовувати сучасні цифрові інструменти.

Концептуальною основою державного регулювання інформаційної безпеки є принципи верховенства права, законності, системності, комплексності, превентивності, пропорційності та ризик-орієнтованого управління. Їх практична реалізація передбачає комплекс заходів, спрямованих на запобігання інформаційним загрозам, захист державних інформаційних ресурсів, розвиток критичної інформаційної інфраструктури, підвищення рівня кіберстійкості та формування інформаційної культури населення. Важливого значення набуває ризик-орієнтований підхід, який забезпечує можливість своєчасної ідентифікації потенційних загроз, прогнозування їх наслідків та впровадження превентивних управлінських рішень ще до виникнення кризових ситуацій.

Теоретичне обґрунтування державного регулювання інформаційної безпеки нерозривно пов’язане з визначенням її місця в системі національної безпеки. Цифровізація державного управління, активне впровадження електронного урядування, хмарних сервісів, технологій штучного інтелекту, великих даних та цифрових платформ суттєво підвищили залежність діяльності органів державної влади від стабільного функціонування інформаційної інфраструктури. За цих умов інформаційний простір перетворюється на самостійну сферу реалізації національних інтересів, а інформаційні ресурси стають стратегічними об'єктами захисту поряд із територіальною цілісністю, економічною безпекою та обороноздатністю держави. Саме тому інформаційна безпека сьогодні розглядається як міжгалузевий напрям державної політики, що забезпечує стійкість функціонування системи публічного управління та сталий розвиток держави.

Ключовим елементом реалізації державної політики є правовий механізм забезпечення інформаційної безпеки, який охоплює сукупність нормативно-правових актів, державних інституцій, організаційних процедур і механізмів управління. Його основу становлять Конституція України, закони України у сфері інформаційної, кібернетичної та національної безпеки, а також стратегічні документи, що визначають напрями цифрової трансформації держави [1-6]. Разом із тим сучасні виклики актуалізують необхідність подальшого вдосконалення нормативно-правового забезпечення, чіткого розмежування повноважень суб'єктів сектору безпеки, посилення міжвідомчої взаємодії та гармонізації українського законодавства з правом Європейського Союзу.

Одним із пріоритетних напрямів модернізації державного регулювання є імплементація положень Директиви (ЄС) 2022/2555 (NIS2), яка встановлює сучасні вимоги до управління кіберризиками, функціонування мережевих та інформаційних систем, захисту критичної інфраструктури та відповідальності суб'єктів, що забезпечують функціонування життєво важливих секторів [7]. На відміну від попередніх підходів, зазначена директива ґрунтується на принципах безперервного управління ризиками, обов'язкового інформування про кіберінциденти, відповідальності керівництва за стан кібербезпеки та розвитку міжсекторальної співпраці. Для України імплементація цих положень є важливою складовою адаптації національної системи інформаційної безпеки до європейських стандартів.

В умовах повномасштабної війни проти України питання забезпечення інформаційної безпеки набуло особливої актуальності. Поряд із технічними атаками на державні інформаційні системи активно застосовуються інформаційно-психологічні операції, спрямовані на дестабілізацію суспільної ситуації, підрив довіри до державних інституцій, поширення дезінформації та маніпулювання громадською думкою. За таких умов ефективне державне регулювання можливе лише за умови комплексного поєднання правових, організаційних, технологічних та інформаційних механізмів, а також посилення координації між суб'єктами сектору безпеки і оборони.

Важливим напрямом удосконалення державного регулювання є розвиток системи управління інформаційними ризиками. Такий підхід передбачає систематичне виявлення потенційних загроз, оцінювання рівня вразливості інформаційних ресурсів, прогнозування можливих наслідків кіберінцидентів і розроблення комплексу превентивних заходів. Саме принципи ризик-орієнтованого управління покладено в основу сучасної європейської політики кібербезпеки та положень Директиви NIS2, що передбачає безперервний моніторинг ризиків, підвищення стійкості інформаційної інфраструктури та вдосконалення механізмів реагування на кіберзагрози [7].

Однією з визначальних характеристик системи інформаційної безпеки є її нелінійність, яка проявляється у складному характері взаємозв'язків між окремими компонентами. Взаємодія технічних, організаційних і людських чинників може спричиняти наслідки, які неможливо повною мірою передбачити за допомогою традиційних аналітичних моделей.

Важливою властивістю системи інформаційної безпеки є її адаптивність, яка характеризує здатність своєчасно змінювати механізми функціонування відповідно до трансформацій зовнішнього середовища. Динамічний розвиток цифрових технологій, удосконалення способів здійснення кібератак, активізація інформаційно-психологічних операцій та поширення інших форм гібридних загроз потребують постійного оновлення механізмів регулювання інформаційної безпеки. Саме адаптивність забезпечує стійкість системи, її готовність до оперативного реагування на нові виклики та ефективного зниження рівня потенційних ризиків [12].

Поряд із цим система інформаційної безпеки має динамічний характер, що проявляється у безперервній трансформації її структури, функцій і механізмів під впливом цифровізації, розвитку інформаційно-комунікаційних технологій та зміни характеру сучасних інформаційних загроз. За таких умов ефективність функціонування механізмів регулювання значною мірою визначається здатністю органів публічної влади своєчасно

модернізувати інформаційні системи, удосконалювати нормативно-правове забезпечення та підтримувати належний рівень кіберстійкості державної інформаційної інфраструктури.

Ще однією характерною рисою системи є її стохастичність, зумовлена впливом численних випадкових і складно прогнозованих чинників. Це істотно ускладнює оцінювання можливих наслідків інформаційних інцидентів, кібератак і технічних збоїв. У зв'язку з цим традиційні підходи до управління доцільно доповнювати ризик-орієнтованими методами, які передбачають моделювання альтернативних сценаріїв розвитку подій, аналіз кризових ситуацій та оцінювання рівня вразливості інформаційних систем [19].

Вагоме місце у забезпеченні інформаційної безпеки посідає також і людський фактор. Незважаючи на стрімкий розвиток цифрових технологій, рівень захищеності інформаційних ресурсів значною мірою визначається професійною компетентністю персоналу, рівнем цифрової культури, дотриманням вимог інформаційної безпеки, готовністю діяти в умовах кризових ситуацій і здатністю приймати ефективні управлінські рішення. Поєднання сучасних технічних засобів захисту з належною організацією роботи персоналу істотно підвищує стійкість інформаційних систем і мінімізує ризики, пов'язані з людським фактором [10].

Таким чином, інформаційна безпека держави є складною відкритою системою, у якій технічні, правові, організаційні, інформаційні та кадрові компоненти функціонують як єдиний взаємопов'язаний механізм. Ефективність державного регулювання у цій сфері визначається здатністю забезпечувати адаптивність системи, своєчасно прогнозувати інформаційні ризики, підтримувати належний рівень захисту критичної інформаційної інфраструктури та оперативно реагувати на сучасні інформаційні загрози. Саме тому системний і ризик-орієнтований підходи є необхідною умовою зміцнення національної безпеки в умовах розвитку інформаційного суспільства.

Перспективним напрямом розвитку системи державного регулювання є використання технології цифрових двійників (Digital Twin), яка передбачає створення цифрової моделі інформаційної системи або окремого об'єкта критичної інфраструктури. Такі моделі дозволяють відтворювати особливості функціонування реальних систем, аналізувати різні сценарії розвитку подій, оцінювати наслідки потенційних кіберінцидентів, перевіряти ефективність механізмів захисту та виявляти критичні вразливості без втручання у роботу реальних інформаційних ресурсів. Їхнє використання сприяє підвищенню стійкості державної інформаційної інфраструктури та ефективності управління інформаційними ризиками [17].

Важливу роль у вдосконаленні механізму державного регулювання відіграють технології штучного інтелекту та машинного навчання, які забезпечують автоматизований аналіз великих масивів інформації, виявлення аномальної активності, прогнозування кіберзагроз і підтримку ухвалення управлінських рішень. Завдяки здатності швидко обробляти значні обсяги даних інтелектуальні алгоритми сприяють підвищенню ефективності реагування на інформаційні інциденти та оптимізації процесів управління інформаційною безпекою.

Поряд із цифровими технологіями важливе значення мають експертні методи оцінювання, які дозволяють використовувати практичний досвід фахівців для визначення вразливостей інформаційних систем, аналізу ефективності механізмів захисту та підготовки рекомендацій щодо їх удосконалення. Поєднання експертних оцінок із математичним моделюванням і сучасними аналітичними технологіями забезпечує більш об'єктивне оцінювання стану інформаційної безпеки та підвищує якість управлінських рішень.

Комплексне використання цифрових двійників, технологій штучного інтелекту, математичного моделювання та експертного аналізу створює підґрунтя для формування інтегрованих моделей державного регулювання інформаційної безпеки. Їхнє застосування дозволяє враховувати технічні, правові, організаційні та людські чинники, здійснювати багатоваріантне прогнозування розвитку подій і забезпечувати безперервне функціонування державних інформаційних ресурсів та критичної інформаційної інфраструктури в умовах постійного зростання інформаційних загроз.

З урахуванням складності сучасного інформаційного середовища особливого значення набуває системно-динамічне моделювання, яке дає змогу комплексно аналізувати процеси функціонування системи інформаційної безпеки. Його перевага полягає у можливості врахування нелінійності процесів, наявності зворотних зв'язків, взаємозалежності окремих компонентів, впливу зовнішніх чинників і часової динаміки розвитку загроз. На відміну від моделей, орієнтованих лише на окремі ризики або поведінку окремих суб'єктів, системно-динамічний підхід забезпечує цілісне бачення системи інформаційної безпеки та формує аналітичну основу для стратегічного планування її розвитку [19].

Доцільність застосування системного моделювання узгоджується з положеннями чинного законодавства України у сфері національної, інформаційної та кібербезпеки. Закони України «Про національну безпеку України», «Про захист інформації в інформаційно-комунікаційних системах», «Про основні засади забезпечення кібербезпеки України» та Стратегія кібербезпеки України визначають необхідність комплексного управління інформаційними ризиками, розвитку національної системи кібербезпеки та підвищення стійкості державної інформаційної інфраструктури [2-6]. Це підтверджує, що сучасні методи моделювання можуть виступати важливим інструментом реалізації державної політики у сфері інформаційної безпеки.

Важливим напрямом удосконалення сучасної державної політики у сфері інформаційної безпеки є впровадження проактивної моделі управління. Її основою є своєчасне виявлення потенційних загроз, прогнозування можливих сценаріїв розвитку подій та реалізація превентивних заходів, спрямованих на мінімізацію інформаційних ризиків ще до їх реалізації. Використання такого підходу сприяє підтриманню безперервного функціонування державних інформаційних систем, підвищенню їхньої стійкості до сучасних кіберзагроз і забезпеченню належного рівня захищеності в умовах стрімкої цифрової трансформації [15].

Реалізація проактивного підходу передбачає комплексне дослідження структури системи інформаційної безпеки, оцінювання взаємозв'язків між її основними складовими, аналіз факторів, що впливають на рівень захищеності інформаційних ресурсів, а також прогнозування можливих наслідків реалізації інформаційних загроз. Такий підхід створює науково-методичне підґрунтя для прийняття стратегічно обґрунтованих управлінських рішень, спрямованих на зміцнення захисту державних інформаційних ресурсів, підвищення стійкості критичної інформаційної інфраструктури та подальше вдосконалення механізмів державного регулювання інформаційної безпеки як важливої складової забезпечення національної безпеки в умовах розвитку інформаційного суспільства.

Висновки та перспективи подальших досліджень. За результатами проведеного дослідження встановлено, що в умовах розвитку інформаційного суспільства державне регулювання інформаційної безпеки набуває стратегічного значення як одна з ключових складових забезпечення національної безпеки України. Обґрунтовано, що ефективність державної політики у цій сфері визначається комплексним застосуванням правових, організаційних, інституційних, технологічних та управлінських механізмів, спрямованих на запобігання, своєчасне виявлення, оцінювання та мінімізацію сучасних інформаційних загроз і ризиків.

Дослідження засвідчило, що вдосконалення державного регулювання інформаційної безпеки потребує розвитку ризик-орієнтованого управління, посилення міжвідомчої координації, модернізації нормативно-правового забезпечення, зміцнення стійкості критичної інформаційної інфраструктури та активного впровадження сучасних цифрових технологій. Зокрема, використання системного моделювання, технології цифрових двійників, штучного інтелекту та прогнозної аналітики створює передумови для підвищення ефективності управлінських рішень, адаптивності державних інформаційних систем і їхньої здатності протидіяти сучасним викликам цифрового середовища.

Перспективними напрямками подальших наукових досліджень є удосконалення теоретико-методологічних засад державного регулювання інформаційної безпеки, розроблення сучасних моделей управління інформаційними ризиками, подальша гармонізація національного законодавства з європейськими вимогами у сфері кібербезпеки, зокрема положеннями Директиви (ЄС) 2022/2555 (NIS2), а також дослідження можливостей інтеграції технологій штучного інтелекту, цифрових двійників і прогнозного моделювання у діяльність органів публічної влади з метою підвищення рівня інформаційної та національної безпеки України.

Література.

1. ***Про інформацію.*** (1992). (Закон України № 2657-XII від 2 жовтня 1992 р.). https://zakon.rada.gov.ua/go/2657-12.
2. ***Про захист інформації в інформаційно-комунікаційних системах.*** (1994). (Закон України № 80/94-ВР від 5 липня 1994 р.). https://zakon.rada.gov.ua/go/80/94-вр.
3. ***Про основні засади забезпечення кібербезпеки України.*** (2017). (Закон України № 2163-VIII від 5 жовтня 2017 р.). https://zakon.rada.gov.ua/go/2163-19.
4. ***Про національну безпеку України.*** (2018). (Закон України № 2469-VIII від 21 червня 2018 р.). https://zakon.rada.gov.ua/go/2469-19.
5. ***Про критичну інфраструктуру.*** (2021). (Закон України № 1882-IX від 16 листопада 2021 р.). https://zakon.rada.gov.ua/go/1882-20.
6. ***Стратегія кібербезпеки України на 2021–2025 роки.*** (2021). (Рішення Ради національної безпеки і оборони України від 14 травня 2021 р., введене в дію Указом Президента України № 447/2021 від 26 серпня 2021 р.). https://www.president.gov.ua/documents/4472021-40013.
7. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS2). URL: https://eur-lex.europa.eu/eli/dir/2022/2555/oj.
8. Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 (Cybersecurity Act). URL: https://eur-lex.europa.eu/eli/reg/2019/881/oj.
9. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection — Information security management systems — Requirements. Geneva: ISO, 2022.
10. ***Abedi A., Gaudard L., Romerio F.*** Review of major approaches to analyze vulnerability in power systems. *Reliability Engineering & System Safety*. 2019. Vol. 183. P. 153–172. DOI: https://doi.org/10.1016/j.ress.2018.11.019.
11. ***Brunner M., Sauerwein C., Felderer M., Breu R.*** Risk Management Practices in Information Security: Exploring the Status Quo in the DACH Region. *arXiv*. 2020. DOI: https://doi.org/10.48550/arXiv.2003.07674.
12. ***Cali Ü., Catak F. Ö., Balogh Z. G., Ugarelli R., Jaatun M. G.*** Cyber-physical hardening of the digital water infrastructure. *Proceedings of the European Interdisciplinary Cybersecurity Conference*. 2023. DOI: https://doi.org/10.1145/3590777.3591408.
13. ***Chernysh R., Chekhovska M., Stoliarenko O., Lisovska O., Lyseiuk A.*** Ensuring information security of critical infrastructure objects as a component to guarantee Ukraine's national security. *Amazonia Investiga*. 2023. Vol. 12(67). P. 87–95. DOI: https://doi.org/10.34069/AI/2023.67.07.8.
14. ***Davydiuk A., Zubok V.*** Analytical review of the resilience of Ukraine's critical energy infrastructure to cyber threats in times of war. *Proceedings of the 15th International Conference on Cyber Conflict (CyCon)*. 2023. DOI: https://doi.org/10.23919/CyCon58705.2023.10181813.
15. ***Holovko O., Kravchenko O., Pogrebytskyi M., Romaniuk I.*** Ways to Improve Legal Regulation of Critical Infrastructure Information Networks Protection. *Social & Legal Studios*. 2025. Vol. 8(1). P. 70–81. DOI: https://doi.org/10.32518/sals1.2025.70.
16. ***Horulko V. V.*** Main directions of improving Ukrainian legislation on information security in war conditions. *Науковий вісник Ужгородського національного університету. Серія: Право*. 2025. № 88(2). С. 364–370. DOI: https://doi.org/10.24144/2307-3322.2025.88.2.49.
17. ***Yarovoy T., Koval Y., Kyrychenko A., Havrilechko Y., Moskalets I., & Sokol M.*** Utilization of digital technologies in the development of state policy on national security issues. *Multidisciplinary Science Journal*. 2024. Vol. 6. Article 2024ss0227. https://doi.org/10.31893/multiscience.2024ss0227.
18. ***Пархоменко-Куцевіл О. І.*** Проблеми забезпечення національної безпеки в умовах воєнного часу. *Науковий вісник Вінницької академії безперервної освіти. Серія «Екологія. Публічне управління та адміністрування»*. 2023. Вип. 3. С. 143–150. https://doi.org/10.32782/2786-5681-2023-3.19.
19. ***Радзівілов Г. Д.*** Модель державного регулювання інформаційної безпеки в контексті забезпечення національної безпеки держави. *Наукові перспективи*. 2025. № 11(65). С. 373–387. DOI: https://doi.org/10.52058/2708-7530-2025-11(65)-373-387.

References.

1. *Pro informatsiiu* [On Information] (Law of Ukraine No. 2657-XII of October 2, 1992). https://zakon.rada.gov.ua/go/2657-12.
2. *Pro zakhyst informatsii v informatsiino-komunikatsiinykh systemakh* [On Protection of Information in Information and Communication Systems] (Law of Ukraine No. 80/94-VR of July 5, 1994). https://zakon.rada.gov.ua/go/80/94-вр.
3. *Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy* [On the Basic Principles of Cybersecurity of Ukraine] (Law of Ukraine No. 2163-VIII of October 5, 2017). https://zakon.rada.gov.ua/go/2163-19.
4. *Pro natsionalnu bezpeku Ukrainy* [On National Security of Ukraine] (Law of Ukraine No. 2469-VIII of June 21, 2018). https://zakon.rada.gov.ua/go/2469-19.
5. *Pro krytychnu infrastrukturu* [On Critical Infrastructure] (Law of Ukraine No. 1882-IX of November 16, 2021). https://zakon.rada.gov.ua/go/1882-20.
6. *Stratehiia kiberbezpeky Ukrainy na 2021–2025 roky* [Cybersecurity Strategy of Ukraine for 2021–2025] (Decision of the National Security and Defense Council of Ukraine of May 14, 2021, enacted by Decree of the President of Ukraine No. 447/2021 of August 26, 2021). https://www.president.gov.ua/documents/4472021-40013.
7. *Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS2).* https://eur-lex.europa.eu/eli/dir/2022/2555/oj.
8. *Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 (Cybersecurity Act).* https://eur-lex.europa.eu/eli/reg/2019/881/oj.
9. *ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection — Information security management systems — Requirements.* Geneva: ISO, 2022.
10. ***Abedi, A.***, ***Gaudard, L.***, & ***Romerio, F.*** **(2019).** Review of major approaches to analyze vulnerability in power systems. *Reliability Engineering & System Safety*, 183, 153–172. https://doi.org/10.1016/j.ress.2018.11.019.
11. ***Brunner, M.***, ***Sauerwein, C.***, ***Felderer, M.***, & ***Breu, R.*** **(2020).** Risk Management Practices in Information Security: Exploring the Status Quo in the DACH Region. *arXiv*. https://doi.org/10.48550/arXiv.2003.07674.
12. ***Cali, Ü.***, ***Catak, F. Ö.***, ***Balogh, Z. G.***, ***Ugarelli, R.***, & ***Jaatun, M. G.*** **(2023).** Cyber-physical hardening of the digital water infrastructure. *Proceedings of the European Interdisciplinary Cybersecurity Conference*. https://doi.org/10.1145/3590777.3591408.
13. ***Chernysh, R.***, ***Chekhovska, M.***, ***Stoliarenko, O.***, ***Lisovska, O.***, & ***Lyseiuk, A.*** **(2023).** Ensuring information security of critical infrastructure objects as a component to guarantee Ukraine's national security. *Amazonia Investiga*, 12(67), 87–95. https://doi.org/10.34069/AI/2023.67.07.8.
14. ***Davydiuk, A.***, & ***Zubok, V.*** **(2023).** Analytical review of the resilience of Ukraine's critical energy infrastructure to cyber threats in times of war. *Proceedings of the 15th International Conference on Cyber Conflict (CyCon).* https://doi.org/10.23919/CyCon58705.2023.10181813.

15. ***Holovko, O., Kravchenko, O., Pohrebytskyi, M., & Romaniuk, I.* (2025).** Ways to Improve Legal Regulation of Critical Infrastructure Information Networks Protection. *Social & Legal Studios*, 8(1), 70–81. https://doi.org/10.32518/sals1.2025.70.

16. ***Horulko, V. V.* (2025).** Main directions of improving Ukrainian legislation on information security in war conditions. *Naukovyi visnyk Uzhhorodskoho natsionalnoho universytetu. Seriia: Pravo* [Uzhhorod National University Herald. Series: Law], 88(2), 364–370. https://doi.org/10.24144/2307-3322.2025.88.2.49.

17. ***Yarovoy, T., Koval, Y., Kyrychenko, A., Havrilechko, Y., Moskalets, I., & Sokol, M.* (2024).** Utilization of digital technologies in the development of state policy on national security issues. *Multidisciplinary Science Journal*, 6, Article 2024ss0227. https://doi.org/10.31893/multiscience.2024ss0227.

18. ***Parkhomenko-Kutsevil, O. I.* (2023).** Problemy zabezpechennia natsionalnoi bezpeky v umovakh voiennoho chasu [Problems of ensuring national security under martial law]. *Naukovyi visnyk Vinnytskoi akademii bezperervnoi osvity. Seriia «Ekolohiia. Publichne upravlinnia ta administruvannia»* [Scientific Bulletin of Vinnytsia Academy of Continuing Education. Series "Ecology. Public Administration and Management"], (3), 143–150. https://doi.org/10.32782/2786-5681-2023-3.19.

19. ***Radzivilov, H. D.* (2025).** Model derzhavnoho rehuliuvannia informatsiinoi bezpeky v konteksti zabezpechennia natsionalnoi bezpeky derzhavy [Model of state regulation of information security in the context of ensuring national security]. *Naukovi perspektyvy* [Scientific Perspectives], 11(65), 373–387. https://doi.org/10.52058/2708-7530-2025-11(65)-373-387.

Abstract.

Nekriach A., Kyrychenko H. Mechanisms of regulating information security in the national security system in the conditions of development of the information society.

The article analyzes the theoretical and practical principles of state regulation of information security as a component of ensuring national security in the context of the development of the information society. The regulatory and legal principles of state policy in the field of information and cybersecurity are analyzed, as well as modern international approaches to protecting the information space. The essence of information security as a multi-component system is revealed, its main components are identified, and the need to apply systemic and risk-oriented approaches to state regulation is substantiated. Particular attention is paid to the use of modern digital technologies, in particular system modeling, digital twins, artificial intelligence and machine learning, which contribute to increasing the efficiency of information risk management, ensuring the stability of critical information infrastructure and supporting the process of making managerial decisions. It is substantiated that the improvement of mechanisms for state regulation of information security should be carried out through the development of legal, organizational and technological instruments, harmonization of national legislation with European standards, strengthening the information risk management system and increasing the cyber resilience of the state. Implementing these measures will contribute to strengthening Ukraine's national security and the effective functioning of the public administration system in the context of digital transformation.

***Keywords**: public administration, state regulation, information security, national security, information society, cybersecurity, information threats, information risks, critical information infrastructure, mechanisms of public administration, risk-based management, regulatory and legal regulation, cyber resilience, digital technologies, system modeling.*

Стаття надійшла до редакції / Received 04.06.2026 Прийнята до друку / Accepted 22.06.2026 Опубліковано/ Published 08.08.2026

Бібліографічний опис статті:

Некряч А. І., Кириченко Г. В. Механізми регулювання інформаційної безпеки в системі національної безпеки в умовах розвитку інформаційного суспільства. Актуальні проблеми інноваційної економіки та права. 2026. № 3. С. 146-150.

Nekriach A., Kyrychenko H. Mechanisms of regulating information security in the national security system in the conditions of development of the information society. Actual problems of innovative economy and law. 2026. No. 3, pp. 146-150.

УДК: 005.8:338.43:351.82(477); JEL classification: Q16, Q18, O31, H83, M11 DOI: https://doi.org/10.36887/2524-0455-2026-3-27

ОХРІМЕНКО Андрій Валерійович, аспірант, Карпатський національний університет імені Василя Стефаника, кафедра публічного управління та адміністрування, https://orcid.org/0009-0005-8538-0093

АДАПТИВНИЙ ПРОЄКТНИЙ МЕНЕДЖМЕНТ У СИСТЕМІ ПУБЛІЧНОГО УПРАВЛІННЯ ІННОВАЦІЙНИМ РОЗВИТКОМ СІЛЬСЬКОГО ГОСПОДАРСТВА

This is an Open Access article distributed under the terms of the Creative Commons CC-BY 4.0

© *ОХРІМЕНКО Андрій Валерійович*, 2026

Охріменко А.В. Адаптивний проєктний менеджмент у системі публічного управління інноваційним розвитком сільського господарства.

У статті обґрунтовується роль адаптивного управління проєктами як організаційно-методичного інструменту реалізації державної інноваційної політики в сільському господарстві. Актуальність дослідження зумовлена необхідністю перетворення стратегічних пріоритетів аграрної політики на конкретні проєкти з визначеними цілями, ресурсами, термінами, відповідальними суб'єктами, процедурами управління ризиками та показниками ефективності. Мета статті – систематизувати теоретичні підходи до управління проєктами та розробити адаптивний підхід до їх застосування в державному управлінні інноваційним розвитком сільського господарства. Методологічна основа дослідження включає загальні наукові методи абстрагування, порівняння, систематизації, структурного й логічного аналізу, синтезу та концептуального моделювання. У дослідженні визначено ключові галузеві чинники, що модифікують класичну логіку управління проєктами в сільському господарстві: сезонність виробництва, залежність від природних і кліматичних умов, біологічні цикли, обмежений доступ до фінансових ресурсів, ризики воєнного стану, логістичні обмеження, забруднення земель, енергетична нестабільність та необхідність координації широкого кола зацікавлених сторін. Стверджується, що інноваційні проєкти в сільському господарстві потребують не лише традиційних інструментів планування, бюджетування та моніторингу, а й гнучкого сценарного планування, інтегрованого управління ризиками, цифрових платформ для взаємодії та механізмів зворотного зв'язку. Наукова новизна статті полягає в удосконаленні організаційно-методичного підходу до адаптації управління проєктами в сільському господарстві шляхом інтеграції зовнішніх викликів, галузевих особливостей, координації зацікавлених сторін, моніторингу та зворотного зв'язку між результатами проєктів і коригуванням рішень у сфері державного управління. Практичне значення отриманих результатів полягає в можливості використання запропонованого підходу державними органами, органами місцевого самоврядування, сільськогосподарськими підприємствами, фінансовими установами та консультаційними службами під час підготовки й реалізації інноваційних проєктів. Подальші дослідження повинні бути спрямовані на розробку кількісних показників для оцінки зрілості та ефективності управління проєктами в межах інноваційної політики у сфері сільського господарства.

***Ключові слова:** проєктний менеджмент, інноваційний розвиток, сільське господарство, публічне управління, державна політика, ризики, стейкхолдери.*

Постановка проблеми у загальному вигляді. Сучасний розвиток сільського господарства України відбувається в умовах поєднання воєнних, фінансових, технологічних, кліматичних та інституційних викликів. За таких обставин традиційні адміністративні підходи до реалізації державної аграрної політики не завжди забезпечують необхідну швидкість реагування, прозорість процедур, адресність ресурсів і вимірюваність результатів. Особливо це стосується інноваційного розвитку, де стратегічні орієнтири мають бути трансформовані у конкретні проєкти з визначеною метою, бюджетом, строками, відповідальними виконавцями та показниками ефективності.

Проєктний менеджмент у цьому контексті набуває системного значення, оскільки дає змогу поєднати стратегічне бачення з практичними механізмами його реалізації. У міжнародній практиці проєкт розглядається як тимчасова діяльність, орієнтована на створення цінності та досягнення унікального результату в межах установлених обмежень щодо строків, ресурсів, якості й ризиків [1]. Для публічного управління така логіка є важливою, адже вона дозволяє перейти від формального