

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ АЕРОКОСМІЧНИЙ УНІВЕРСИТЕТ «ХАРКІВСЬКИЙ
АВІАЦІЙНИЙ ІНСТИТУТ»

УДК 351.851:378.1(477)

НОВАК Валерій Миколайович



**МЕХАНІЗМИ ІНФОРМАЦІЙНИХ КОМУНІКАЦІЙ СУЧАСНОГО
СУСПІЛЬСТВА**

25.00.02 – механізми державного управління

АВТОРЕФЕРАТ

дисертації на здобуття наукового ступеня
кандидата наук з державного управління

Харків – 2026

Дисертацією є рукопис.

Робота виконана у Національному університеті цивільного захисту України.

Науковий керівник

доктор наук з державного управління, професор,
заслужений працівник освіти і науки України
ДОМБРОВСЬКА Світлана Миколаївна,
Національний аерокосмічний університет «ХАІ»,
проректор з наукової роботи

Офіційні опоненти:

доктор наук з державного управління, професор
ЩЕПАНСЬКИЙ Едуард Валерійович,
Хмельницький університет управління та права
імені Леоніда Юзькова, завідувач кафедри
публічного управління та адміністрування

доктор наук з державного управління, професор
БСЛАЙ Сергій Вікторович,
Національна академія Національної гвардії
України, начальник центру організації та
координації наукової та інноваційної діяльності

Захист відбудеться «06» травня 2026 р. об 14.00 годині на засіданні спеціалізованої вченої ради Д 64.062.09 Національного аерокосмічного університету «Харківський авіаційний інститут» за адресою: 61070, м. Харків, вул. Вадима Манька 17.

З дисертацією можна ознайомитись в науково-технічній бібліотеці Національного аерокосмічного університету «Харківський авіаційний інститут» за адресою: 61070, м. Харків, вул. Вадима Манька 17.

Автореферат розісланий «06 » квітня 2026 р.

Учений секретар
спеціалізованої вченої ради



Надія КАРПЕКО

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

Актуальність дисертаційного дослідження обумовлена сетевізацією поширення інформації в сучасному суспільстві. Однією з основних його характеристик є активна експансія мережевих інформаційних технологій, що неминуче супроводжується становленням нових форм соціальності та засобів життєдіяльності, зокрема комунікації, як квінтесенція, суті людської взаємодії. Найбільш яскравим проявом впровадження цих технологій є мережа Інтернет, яка нині суттєво змінює характер комунікацій. Виникли небачені раніше форми мережевої комунікації, які якісно змінюють форми суспільної комунікації і являють собою соціокультурні новації, здатні впливати на життєві світи індивідів і функціональність суспільства в цілому. Формується нова комунікаційна культура, в якій людина, маючи доступ до новітніх технологій, стає актором, що впливає не лише на свою життєдіяльність, а й на розвиток структур та функцій суспільства. У зв'язку з цим і з теоретичної, і з практичної точки зору важливим є розгляд вразливостей сучасних комунікацій, включаючи як уразливості у вигляді наростання дисфункціональної складності Інтернету, так і вразливості індивідуальних і колективних акторів, що діють у мережі.

Як джерело нових уразливостей суспільства розглядається сама природа складних систем, які набувають властивостей саморефлексії. Комунікаційні новації багато в чому пов'язані з технічним розвитком, при цьому вразливості комунікацій виявляють себе найбільш значуще саме в умовах мережевого суспільства з підвищеним значенням інформації, і життєдіяльність людини залежить від необхідності її відбору. Особливо важливо проаналізувати вплив уразливостей мережевих комунікацій на формування спільностей для людей у контексті знаходження гуманних способів співіснування індивідів.

Інформація, маючи безліч значень, кардинально змінюючи форму і канали доставки, втрачає статус орієнтовних відомостей і стає джерелом небезпеки. Антонімічною опозицією безпеки є загроза, тому реальність інформаційної безпеки зумовлена реальністю інформаційних загроз.

Декларовані стратегічні завдання забезпечення інформаційної безпеки дітей гостро потребують якнайшвидшого вирішення та впровадження ефективних комплексних механізмів управління, адекватних викликам інформаційної ери. Трагічні події останніх років пов'язуються фахівцями з негативним впливом інформації на особистість та свідчать про соціальне значення інформаційної безпеки.

Значний внесок у розвиток знань у сфері інформаційного суспільства зробили такі вчені, як Д. Белл, А. Берг, З. Бжезинський, Д. Блюменау, Е. Брандман, П. Браун, Н. Вінер, М. Кастельс, Б. Ківі, Е. Масуда, Д. Тапскотт, Е. Тоффлер, Ф. Уебстер, Г. Хакен, Ю. Харари, К. Шеннон та ін.

Різним аспектам механізмів інформаційних комунікацій сучасного суспільства присвятили свої праці українські автори, серед яких можна виділити Л. Антонову, О. Валевську, О. Власюка, В. Голобуцького, В. Горбуліна, А. Гуза, С. Белая, О. Данільяна, А. Дегтяря, Ю. Древалю, С. Домбровську, В. Ковальчук, Б. Кормич, В. Костюка, О. Кохановського,

О. Крюкова, В. Ліпкана, С. Луценка, О. Радченко, Я. Романовського, О. Сенченко, В. Степанова, В. Торічного, В. Тогобицьку, В. Шведун, Е. Щепанського та інших.

У той же час категорії, закономірності, принципи, методи, концепції, моделі, системи, класифікація у сфері інформаційного забезпечення безпеки сучасного суспільства практично не розроблені. Дослідники зосереджують увагу переважно на окремих проблемах, а питання перетворення України на ефективну державу з точки зору інформаційної безпеки ще не стало предметом всебічного науково-практичного вивчення, що, у свою чергу, потребує системного аналізу ролі та місця інформаційного забезпечення в державному управлінні інформаційною безпекою як частини забезпечення національної безпеки.

Зв'язок роботи з науковими програмами, планами, темами. Дисертацію виконано в межах науково-дослідної роботи «Розробка наукових основ державного управління у сфері безпеки ринку соціально-економічних послуг України з точки зору цивільного захисту» (державний реєстраційний номер 0112U002587), що розробляється Національним університетом цивільного захисту України. Конкретно дисертантом проаналізовано заходи вдосконалення механізмів інформаційних комунікацій сучасного суспільства.

Мета і завдання роботи. Метою дисертаційної роботи є обґрунтування теоретичних засад та розробка практичних рекомендацій щодо удосконалення механізмів інформаційних комунікацій сучасного суспільства.

Досягнення визначеної мети зумовило необхідність вирішення таких завдань:

охарактеризувати сутність та вразливість нових форм комунікації інформаційного суспільства;

систематизувати зарубіжний досвід регулювання обігу інформації з метою захисту дітей в сучасному суспільстві;

оцінити організаційний механізм інформаційних комунікацій сучасного суспільства;

окреслити методичні основи формування механізмів управління інформаційною безпекою дітей;

визначити напрями управління ризиками інформаційних комунікацій сучасного суспільства;

обґрунтувати стратегічні напрями удосконалення механізмів інформаційних комунікацій сучасного суспільства.

Об'єкт дослідження – державна інформаційна політика.

Предмет дослідження – механізми інформаційних комунікацій сучасного суспільства.

Методи дослідження. Методологічну основу роботи становлять загальнонаукові прийоми досліджень і спеціальні методи, що ґрунтуються на сучасних наукових засадах управлінської, економічної і споріднених з ними наук. В основу методології дослідження було покладено системний підхід, методологічна специфіка якого визначається тим, що він орієнтує дослідження на розкриття цілісності об'єкта і механізмів, що її забезпечують, на виділення

різноманітних типів зв'язків складного об'єкта і зведення їх у єдину теоретичну картину.

Автором використано низку наукових методів, зокрема: гіпотетико-дедуктивний метод формування методології дисертаційного дослідження, який дав змогу сформулювати гіпотезу дослідження, побудувати евристичні моделі формування механізмів інформаційних комунікацій сучасного суспільства.

Дедуктивний доказ висунутої гіпотези дослідження не тільки підтвердив правильність формування його методології, справедливність висновків, а й дав можливість також висунути й верифікувати практичні рекомендації з удосконалення досліджуваного об'єкта, а також:

провести структурно-функціональний аналіз, сутність якого полягає у виділенні елементів системи інформаційних комунікацій сучасного суспільства;

визначити ряд порівняльних методів, що надали можливість аналізу стандартів і механізмів інформаційних комунікацій сучасного суспільства;

впровадити: статистичний метод, що дав змогу розкрити реальні й точні факти стану досліджуваного об'єкта;

прогностичний метод, за допомогою якого визначено більш віддалені перспективи його розвитку;

теоретико-концептуальний метод, що визначив напрям дослідження, втілений в аналізі функцій, структури та параметрів об'єкта, та дав змогу позначити, осмислити, описати та порівняти роль механізмів інформаційних комунікацій сучасного суспільства, уточнити їх функції в діяльності кожної з підсистем, оцінити результати управлінського впливу, виявити перспективи й механізми.

Інформаційну базу дисертаційного дослідження становили нормативно-правові акти, праці зарубіжних і вітчизняних учених, Інтернет-ресурси, статистична інформація Державної служби статистики України та інших центральних органів виконавчої влади.

Наукова новизна одержаних результатів полягає у вирішенні наукового завдання щодо розвитку теоретичних засад та обґрунтуванні науково-прикладних рекомендацій щодо удосконалення механізмів інформаційних комунікацій сучасного суспільства.

Найсуттєвіші результати дисертаційного дослідження, які містять наукову новизну, полягають у тому, що:

вперше:

запропоновано модель управління інформаційною безпекою, що включає в себе основні елементи системи управління, які взаємодіють на основі рівневого принципу прийняття та реалізації управлінського рішення, процесного підходу до комунікації, виявлених факторів ризикової поведінки та типів ризику, де модель орієнтована на синхронізацію ресурсів суб'єктів управління з активізацією управлінського потенціалу соціальних інститутів юридичної відповідальності, експертизи та громадянської участі для оптимізації соціальних ризиків через узгодження спрямованості та швидкості

управлінського впливу;

удосконалено:

особливості впливу медіа-технологій на систему управління інформаційною безпекою, що полягає як у розширенні зони ризику, так і у зміні управлінських ресурсів суб'єктів управління, через особливості, які зумовлені безальтернативністю використання медіа-технологій, емансипацією інформаційних потоків, темпоральним скороченням презентації та споживання інформаційного сигналу (контенту), доступністю інформації, доместикацією медіа-технологій, а також розширенням технологічних можливостей контролю, комунікацій суб'єктів керування та агрегування ними даних;

управління інформаційною безпекою, як цілеспрямованого впливу соціальних інститутів на фактори ризикової поведінки для зниження ймовірності шкоди від інформації щодо здоров'я та розвитку цієї соціальної спільноти, специфіка управлінського впливу якого обумовлена типом ризику, що визначає необхідні управлінські ресурси, статусом суб'єкта ризикової поведінки, що вказує на рівень управлінського рішення, функціоналом соціального інституту як суб'єкта управління, де закладено уявлення про суб'єкт-об'єктну природу ризикової поведінки та її фактори; типологія ризиків, що включає інституційні ризики; рівневий принцип розробки та реалізації управлінських рішень;

набуло подальшого розвитку:

універсальні компоненти світових практик забезпечення інформаційної безпеки: змістовний (ціннісний, світоглядний) та процедурний (технології оцінки інформації та обмеження її обігу з метою захисту дітей), де разом з цими компонентами виділено закономірності динаміки затребуваності ресурсів соціальних інститутів;

управлінський потенціал інституту громадянської активності, що полягає у можливостях моніторингу, збору та обробки громадської думки з метою конкретизації критеріїв шкоди, виявлення та формування соціального консенсусу щодо них та щодо технологій оцінки шкоди, а також з метою соціального масштабування уваги до проблем інформаційної безпеки, до якої відносяться гнучкість організації, оперативність реакції, висока затребуваність технологічних можливостей комунікування та інтеграції форм активності, стійкість мотивів представників інституту перед деформацією.

Практичне значення одержаних результатів. Основні положення й висновки дисертації можуть використовуватися фахівцями під час написання підручників і навчальних посібників, створення навчально-методичної літератури; в роботі органів державної влади та у процесі удосконалення механізмів інформаційних комунікацій сучасного суспільства.

Теоретичні та практичні напрацювання автора дисертаційного дослідження використано в роботі Міністерства енергетики України (довідка про впровадження №25/1.1-10.1 -20906 від 10.12.2025).

Змістовні пропозиції автора дослідження використано в практичній діяльності Департаменту державного контролю у сфері захисту інформації та

кіберзихисту ДДК Адміністрації Держспецзв'язку (довідка про впровадження від 06.01.2026, №11/04/01-22/2026/1Д)

Особистий внесок здобувача. Основні положення й висновки дисертації можуть використовуватися фахівцями під час написання підручників і навчальних посібників, створення навчально-методичної літератури; в роботі органів державної влади та у процесі удосконалення механізмів інформаційних комунікацій сучасного суспільства.

Апробація результатів дисертації. Основні положення й результати дисертації доповідались і обговорювались на конференціях, конгресах і семінарах, зокрема: Міжнародній науково-практичній інтернет-конференції «Публічне управління у сфері цивільного захисту: освіта, наука, практика» (м. Черкаси, 2025 р.); Міжнародній науково-практичній конференції «Розвиток компетентності в публічному секторі: європейські стандарти та перспективи» (м. Івано-Франківськ, 2025 р.); III Всеукраїнській науково-практичній інтернет-конференції «Теорія і практика розвитку туризму: досвід, проблеми, інновації» (м. Черкаси, 2025 р.), IX Міжнародній науково-практичній конференції «Теоретико-практичні засади управління, економіки та природокористування: аспекти реінтеграції Криму в господарський комплекс України (м. Київ, 2025 р.)

Публікації. Основні положення дисертаційної роботи опубліковано в 10 наукових працях, із них: 1 колективна монографія, 5 статей в наукових фахових виданнях, з яких 2 статті в закордонному науковому виданні за напрямком дослідження, 4 тези доповідей на конференціях. Загальний обсяг публікацій автора за темою дослідження – 5,85 др. арк.

Структура та обсяг дисертації. Робота складається зі вступу, трьох розділів, висновків, списку використаних джерел, додатків. Загальний обсяг дисертації 206 сторінок. Обсяг основного тексту становить 182 сторінки. Список використаних джерел включає 192 найменування.

ОСНОВНИЙ ЗМІСТ РОБОТИ

У **вступі** обґрунтовано актуальність досліджуваної теми та розкрито ступінь її розробленості; сформульовано мету, завдання, об'єкт, предмет і методи дослідження; визначено зв'язок дисертаційної роботи з тематикою наукових досліджень Національного університету цивільного захисту України; представлено наукову новизну; показано теоретичну та практичну значимість отриманих результатів, наведено відомості щодо їхньої апробації.

У **першому розділі** – *«Теоретичні основи механізмів інформаційних комунікацій сучасного суспільства»* – охарактеризовано динаміку розвитку амбівалентних тенденцій для комунікації, визначено сутність нових форм комунікації інформаційного суспільства та специфіку ризиків та уразливостей мережевих систем.

Визначено, що в умовах мережевізації та динаміки суспільства, зовнішній контроль і регулювання ресурсних потоків ускладнюються, та призводить до системних «нормальних» аварій, але при цьому зростає роль самої людини в матриці інформаційних потоків і мереж. Так, мережі

виступають чинником трансформації значимості, ролі людини як актора у конструюванні та реалізації комунікації.

Тенденції останніх сприяють появі нових форм комунікацій. В епоху поширення мережі Інтернет з'являється новий тип комунікацій: мережеві комунікації, найбільш поширеною формою яких є масові самокомунікації. Вони сприяють появі автономних комунікаційних каналів, що потенційно досягають масової аудиторії, які вільно і самостійно створюються будь-якими індивідуальними акторами у віртуальному просторі.

Нові форми комунікації амбівалентні: з одного боку, є продовженням і новим виміром традиційно сформованих форм суспільної комунікації, а з іншого, – являють собою соціокультурні новації, здатні по-новому впливати на якість життя індивіда, функціональність суспільства і його інститутів. Отримують апробацію гнучкі горизонтальні зв'язки, що релятивують колишні комунікаційні структури, які виходять з-під централізованої координації. Логіка складних систем: мережеві комунікації відрізняються нелінійністю, відсутністю центру та ієрархії. Так, мережа Інтернет у сучасному суспільстві поступово перетворюється на простір поширення нових комунікативних практик, що формують адекватні їм культурні зразки взаємодій, та вплинути на динаміку суспільства, що створює характерний стиль життя.

На тлі такої плюралізації соціетальних форм та образів людської життєдіяльності та формального послаблення функціональності «традиційних» медіа, виникає потреба у нових формах соціальної взаємодії. Йде постійний пошук зміцнення соціальної спільності, також затребувані нові способи розв'язання задач гуманістичного напрямку, зростає і необхідність нових методів самоідентифікації та ідентифікації у процесі комунікацій.

Проаналізовані нами контекст та природа розвитку мережевих комунікацій дозволяють висунути положення про те, що загалом мережеві комунікації амбівалентні. Їхні функціональні прояви досить легко визначаються, але насправді вони можуть сприяти виникненню вразливостей, які є дисфункціональними для соціальних відносин.

При всіх перевагах, мережеві комунікації, основним засобом яких є текст, та аудіовізуальні продукти, які можуть стати технічним способом продовження встановлених соціальних зв'язків або способом відтворення ділових відносин, нетворкінгу, але виникають явища, які дозволяють припустити, що глибокі емоційні контакти та відносини, невербальні комунікації. Крім того, в мінливому світі агенти соціалізації іманентні, і процес адаптації до соціальної реальності, як і раніше, відбувається значною мірою поза мережевими комунікаціями.

Більше того, складається така картина: чим більше інтерактивності, тим складніше навчитися адаптації. Мережеві комунікації виглядають як доступніші в порівнянні зі звичними взаємодіями, але виявляється, що під ілюзорною легкістю ховаються нові латентні вразливості для розуміння життєвих світів один одного. Наприклад, бачимо, що свобода самовираження у мережевих комунікаціях і відсутність бар'єрів не збільшують рівень толерантності у суспільстві.

Головне, що ми з'ясували: уразливості мережевих комунікацій, що ускладнюються, будучи новим типом «нормальних аварій», проявляють себе як уразливості у вигляді наростання дисфункціональної складності Інтернету, так і як уразливості індивідуальних та колективних факторів мережі.

Вразливості мережевих комунікацій вимагають постійного моніторингу та аналізу, що, з одного боку, представляється дуже складним завданням, адже такі властивості, які виявляють їх «симптоми» – глобальні ризики в сучасному соціумі – як справакалізованість, незліченність, поява безлічі інсценованих ризиків, висновки, служать лише невеликими сигналами змін, що відбуваються саме в даний момент і можуть швидко втрачати свою актуальність. З іншого боку, фіксованість мережевих комунікацій на цифрових носіях надає дослідникам безпрецедентну можливість доступу до експресії внутрішнього світу та спільного життя користувачів. В цілому, визначення природних властивостей основних вразливостей, що проявляють себе, можуть допомогти створити алгоритм, яким можна дотримуватися при моніторингу і класифікації нових вразливостей мережевих комунікацій, що розуміються через призму збільшеної складності сетевізованого світу, побудованого в результаті взаємодії ресурсних і просторових потоків різного напрямку.

В ході дослідження, констатовано, що деякі амбівалентні наслідки урбанізації, що ускладнюють мережеві комунікації, є фактором як кращих, так і погіршення вирішення даних проблем.

Перше. Ще сильніше загострюється проблема співіснування людини з природою та довкіллям, ускладнюються соціальні комунікативні завдання екологічного виховання та економії невідновлюваних ресурсів. Мережеві комунікації в такому контексті стають одними з вирішальних факторів створення та розвитку векторів інвазіоменталістської поведінки, його роль у вирішенні екологічних питань значно зростає. Нові форми мережевої консолідації мають суттєвий потенціал впливу на реалізацію завдань інвайроменталістського стибу, але можуть стати платформою для розвитку інсценованих ситуацій ризикофобій.

Друге. Зростає загроза індивідуалізації людей та соціальної атомізації. Індивіди, проживаючи в одній локальності, можуть не перетинатися, існувати в різних соціокультурних світах або занурюватись у віртуальну реальність. Зрештою, може народжуватися суспільство «мережевого індивідуалізму». Поява і розвиток «чистих відносин» широко оцінюються як гігантський крок інтерпретовано як свободу від обмежень особистого вибору, до яких призводять усі зобов'язання. На відміну від громад, мережі поєднані між собою індивідуально, так само індивідуально змішуються і «розбираються», і покладаються на бажання індивіда їх зберегти як єдину, хоч і хитку, підставу.

Четверте. Як наслідок, невирішена проблема непристосованості до мультикультуралізму локальних співтовариств, веде до спонтанних зіткнень представників різних культур, зростання недовіри один до одного та роз'єднаності соціуму, розривах у соціальних комунікаціях – що легше реалізується в умовах саме експансії мережевих комун.

П'яте. Слідом за руйнуванням глибоких емоційних стійких зв'язків, які

не можуть бути компенсовані мережевими комунікаціями, через міграцію з рідних малих міст і сіл до мегаполісів і раннім (до повноліття) відривом від сім'ї виникає травматизація особистості, ускладнюється самоідентифікація членів соціуму.

З цього випливає, що міське життя сприяє інтенсифікації числа комунікацій та соціальних контактів, але характер соціальних зв'язків ускладнюється. Незважаючи на технічне вдосконалення засобів комунікації, а також зростання доступності інформації та збільшення швидкості обміну нею, ці процеси не обов'язково сприяють розвитку соціальної спільності, впливаючи на якість спілкування амбівалентно, можуть бути фактором послаблення стійких відносин. У таких умовах мережеві комунікації можуть стати як джерелом покращення ситуації, фактором адаптації комунікації до урбанізації, так і нести у собі латентні ризики.

В другому розділі – *«Аналіз механізмів інформаційних комунікацій сучасного суспільства»* – окреслено методичні основи механізмів інформаційних комунікацій сучасного суспільства, систематизовано зарубіжний досвід регулювання обігу інформації з метою захисту дітей в сучасному суспільстві, оцінено організаційний механізм інформаційних комунікацій сучасного суспільства.

Нами визначено, що ресурсність інституту юридичної відповідальності залежить від соціальних уявлень про норму та девіацію та їхнє втілення на рівні доктринального та концептуального обґрунтування, а також застосування санкції на рівні розповсюдження інформації. Зниження ресурсності даного інституту детермінується розбіжністю морфології мережного простору поширення інформації з механізмом дії санкції (межами правового регулювання), необхідністю балансування між захистом (і гарантуванням) двох благ – здоров'я та інформаційної свободи, а також лабільністю мотивів представників інституту.

Ресурсність інституту експертизи полягає у затребуваності наукового обґрунтування шкоди для застосування юридичної санкції, в організації залучення наукової оцінки інформації на рівні створення, розповсюдження та доступу до інформації. Тому зниження ресурсності інституту експертизи прямо пропорційне значенню наукової діагностики шкоди від інформації та її ймовірності (ризик), а також дефектам порядку (інституціоналізації) експертизи як умов уразливості мотивів експертів.

Ресурсність інституту громадянської активності полягає у можливостях солідаризації соціальних груп («жертв ризику») щодо визнаних загроз щодо дітей, в усвідомленні недоліків інституту юридичної відповідальності, можливостях, що забезпечуються розвитком комунікативних технологій, а також у стійкості мотивів представників цього інституту. Ресурси інституту громадянської активності реалізуються на таких рівнях прийняття управлінського рішення як рівень доктринального обґрунтування (суспільне обговорення законопроектів), рівень створення та розповсюдження інформації, рівень доступу до інформації (моніторинг обігу інформації).

В цілому, аналіз практик соціальних інститутів, що мають функції

мінімізації ризиків шкоди від інформації для здоров'я та розвитку дітей, дозволяє визначити фактори ресурсності суб'єктів управління і виявити їхній потенціал на кожному з чотирьох рівнів прийняття управлінського рішення, що виділяються нами.

Виявлено, що ефективність цих функцій розглянуто та залежить від сили та стійкості мотивів їх представників. Визначено диференціацію управлінського потенціалу суб'єктів на різних етапах комунікативного акту та зв'язок зі ступенем формалізації відносин учасників усередині кожного етапу. Чим більш формалізовані ці відносини, тим більше ресурсів виявляє суб'єкт управління з найвищим ступенем інституціалізації (нормованості, організаційності). Наприклад, на рівні розповсюдження контенту як найбільш нормованого більшу ефективність виявляє інститут юридичної відповідальності. І, навпаки, лише на рівні споживання інформації цей інститут виявляє низьку ресурсність.

Таким чином, дослідження досвіду захисту дітей від шкідливого контенту через поєднання ризикологічного, інституційного та ресурсного підходів відкриває можливості для опису технології управління контентними ризиками. Представлений емпіричний аналіз практик мінімізації контентних ризиків, що утворюють одну з двох складових системи управління інформаційною безпекою, потребує доповнення відповідним аналізом форматних ризиків та можливостей їхньої мінімізації.

Соціалізаційний та екологічний підходи надали можливість визначити зміст поняття захищеності, благополуччя та безпеки дітей, а також підійти до типології шкоди від інформації та виділити контентний та форматний типи шкоди від інформації. Іншими словами, ці підходи уточнили розуміння об'єкта та мети управління інформаційною безпекою. Аналіз даних підходів допоміг сформулювати загальний принцип – принцип психофізіологічних універсальї розвитку, що диференціюють заходи безпеки відповідно до вікової періодизації фізіологічного розвитку.

Серед основних напрямів, що визначили фундаментальні методологічні принципи, виділяються ризикологічний, інституційний та ресурсний підходи, які розкривають сутнісний зміст та характеристики елементів керуючої системи – суб'єктів управління та управлінських заходів. У цьому ризикологічний підхід визнається першорядним. Виділений у межах кожного підходу понятійний апарат і параметри, що підлягають виміру, дозволили підійти до формулювання цілісної концептуальної розробки, яка може трансформуватися в емпіричну методологію через формулювання ознак ефективності діяльності щодо зниження ймовірності шкоди інформації та їх подальший аналіз.

Так, ризикологічний підхід дозволив визначити принцип обліку поведінкової основи джерела загроз інформаційній безпеці дітей, факторності та альтернативності ризикової поведінки, ймовірності та ситуаційності загроз. Вимірюванню підлягають характеристики суб'єктів ризикової поведінки та фактори самої ризикової поведінки (мотиви та умови - обставини реалізації) як об'єкти управлінського впливу, які визначають ресурсомісткість ризику і,

відповідно, можуть вказати на суб'єкт управління, що володіє необхідними ресурсами.

Через інституційний підхід сформульовано принцип відповідності домінуючих функцій суб'єктів управління завданням захисту дітей від інформації як окремого випадку соціального захисту дітей, що реалізується соціальними інститутами, які мають «функції соціальних механізмів оптимізації ризиків». Емпіричному аналізу у разі можуть піддатися функції та дисфункції соціальних інститутів, як ресурсна основа своєї діяльності, з одного боку, і джерело інституційних ризиків, з іншого боку. Цей підхід також використано для класифікації управлінських рішень за рівневим принципом:

- 1) рівень інтерпретації інформаційної безпеки дітей – доктринального та концептуального обґрунтування інформаційної безпеки дітей;
- 2) рівень обігу інформації;
- 3) рівень організації доступу до інформації;
- 4) рівень споживання інформації.

Ресурсний підхід як логічний наслідок розгляду перших двох підходів визначає принцип обумовленості ефективності управлінського впливу ресурсністю соціального інституту як суб'єкта управління інформаційною безпекою дітей. У зв'язку з цим емпіричному аналізу підлягають конкретні управлінські ресурси кожного прийнятого, як суб'єкт управління, інституту, що вказують на його ресурсність – обсяг управлінського потенціалу, необхідного для впливу на конкретний ризик відповідного типу, тобто вказують на вектор управлінського впливу.

Гіпотетично стверджується, що рівень прийняття рішень, який відповідає функціям інституту та етапам інформаційно-комунікативного процесу, детермінує ресурсність суб'єкта стосовно конкретного ризику, вказуючи на збіг ресурсності інституту ресурсомісткості ризику – вектор управлінського впливу.

Однією із завдань емпіричного аналізу виступає розгляд даних чинників через призму впливу ними технологічного розвитку медіа комунікацій, включаючи реакцію соціальних інститутів на технологізацію ризиків, що має різні напрями впливу – розширення зони ризиків, зменшення чи збільшення ресурсності суб'єктів управління, трансформацію їх функцій.

Таким чином, концептуалізація управління інформаційною безпекою дітей полягає в описі механізму впливу на зниження ймовірності заподіяння інформацією шкоди здоров'ю та розвитку дітей через уявлення про фактори ризикової поведінки та можливості впливу на них інституційних суб'єктів, які мають функції з «оптимізації ризиків» та ресурсів, які володіють необхідними для кожного типу (контентного та форматного) ризику. Це розуміння управління через інтеграцію до єдиного комплексу сутнісних характеристик елементів системи управління.

В третьому розділі – *«Удосконалення механізмів інформаційних комунікацій сучасного суспільства»* – обґрунтовано методичні основи формування механізмів управління інформаційною безпекою дітей, визначено моделювання напрямів управління ризиками інформаційних комунікацій

сучасного суспільства, виокреслено стратегічні напрями удосконалення механізмів інформаційних комунікацій сучасного суспільства

Інформаційна безпека, коли стає багатовимірною, у суспільстві включає завдання задоволення потреб у інформації. Починає формуватись нова нерівність у доступі до джерел знань: з'являється проблема цифрової нерівності, доступу до оцифрованого знання. При цьому в інформаційному суспільстві безпека як суб'єкта, так і системи суспільства може залежати від наявності або відсутності відомостей і бути обумовленою «зростаючою швидкістю старіння інформації» та зростанням інтенсивності комунікацій. Так, мережеві комунікації впливають на вразливість суспільства, ускладнюючи вирішення традиційних завдань, ведуть до того, що соціальна нерівність набуває нової якості.

Вразливості мережевих комунікацій вимагають постійного моніторингу та аналізу, що, з одного боку, представляється дуже складним завданням, адже такі властивості, які виявляють їх «симптоми» – глобальні ризики в сучасному соціумі як справакалізованість, незліченність, поява безлічі інсценованих ризиків, що мають силу реальних висновки, служать лише невеликими сигналами змін, що відбуваються саме в даний момент і можуть швидко втрачати свою актуальність. З іншого боку, фіксованість мережевих комунікацій на цифрових носіях надає дослідникам безпрецедентну можливість доступу до експресії внутрішнього світу та спільного життя користувачів. В цілому, визначення природних властивостей основних вразливостей, що проявляють себе, можуть допомогти створити алгоритм, яким можна дотримуватися при моніторингу і класифікації нових вразливостей мережевих комунікацій, що розуміються через призму збільшеної складності сетевізованого світу, побудованого в результаті взаємодії ресурсних і просторових потоків різного штибу.

Проведене дослідження означило місце інформаційної безпеки дітей та дорослих у системі наукового знання та соціологічної думки, показало шлях вирішення проблеми, досягнення мети підвищення «якості дитинства» через гарантування захищеності дітей із застосуванням як відомих інструментів, так і нових механізмів, що інтегрують потужності суб'єктів керуючої системи, механізмів, адаптованих до природи гіпермережевої реальності

Вікова диференціація наслідків взаємодії людини з інформацією вказує на самостійне значення у порядку денного проблеми інформаційної безпеки, як забезпечення стійкості соціального порядку в умовах послаблення адміністративних засобів. Особливості завдань інформаційної безпеки дитячої групи полягають у специфіці мотиваційної сфери, залежності мотивів поведінки від властивостей ситуативності та імпульсивності, мотивів, що «швидко актуалізуються, негайно «спрацьовують» під впливом найближчої – внутрішньої або зовнішньої – безпосередньої дійсності» та «найближчої перспективи». Це і визначає проблему вразливості стану захищеності від загроз з боку медіатехнологій, що інтенсивно розвиваються. Сьогодні, як ніколи раніше, відчувається необхідність створення моделі забезпечення безпеки інформаційної політики (Рис.1).



Рис.1. Модель забезпечення безпеки інформаційної політики

Практична реалізація пропонованої моделі передбачає крім удосконалення нормативно-концептуальних основ інформаційної політики модернізацію порядку експертизи інформаційної продукції та реклами, реформування системи соціального захисту дитинства та профілактики бездоглядності у напрямку забезпечення права дітей на сприятливе інформаційне середовище (включаючи домашній простір) дефінітивних норм, що розкривають значення здатності учасника інформаційного обміну нести відповідальність та виконувати обов'язків, тобто так званої «інформаційної дієздатності» у контексті захисту від інформації.

У представленому дослідженні запропоновано бачення реалізації інформаційної безпеки у комплексному методологічному підході з опорою на соціально-управлінські концепції як процесу втілення виключно важливого результату – благополуччя дітей в умовах технологічно обумовленої несприятливої інформаційно-екологічної обстановки.

У роботі формулюється адаптація ресурсного потенціалу керуючої системи до сучасних технологічних викликів, та підхід до забезпечувальних механізмів, що орієнтуються на динаміку глобальних технологічних процесів, що забезпечують умови реалізації мотивів девіантної поведінки. Нами пропонується розвинути існуючі теорії та моделі забезпечення інформаційної безпеки, акцентуючи увагу на результатах наявної практики соціальних інститутів, що відображає їх управлінський потенціал та ступінь морфологічної тотожності нових ризиків. Ефективність вибудовування перешкод загрозам від інформації визначається їхньою симетрією, іншими словами, адекватністю реагування на загрози.

На основі аналізу природи інформаційного сигналу запропоновано класифікацію шкоди від інформації, рівневу типологізацію факторів ризикової поведінки, елементів системи контентної фільтрації.

Важливим є офіційне визнання публічного значення стану захищеності кожної дитини, гарантування такої захищеності будь-якій дитині, що вимагає демонополізації та деприватизації прийняття рішень у сфері захисту від шкідливої інформації. Пандемічний характер інформаційних загроз людству демонструє значення реакції на них з боку соціальних структур, виправдовує аналогію та застосування відповідної термінології боротьби з епідеміологічними ризиками як такої, що довела свою ефективність. Паралель з управлінням епідеміологічними ризиками дає змогу інтегрувати підходи до розбудови стратегій захисту від інформаційних загроз. Так, всі розглянуті нами процеси управління ризиками від інформації можна віднести або до бар'єрних засобів, або дистанціюванню від джерела шкоди, або до підвищення індивідуальної стійкості (імунітету), або до особистої гігієни та пропаганди особистої гігієни. Механізм передачі інфекції (девіації) уподібнюється до комунікативного ланцюга. Якщо враховувати таку аналогію, то стає очевидною обґрунтованість заборони на свободу індивідуального прийняття рішень щодо засобів захисту дітей від інформації (особливо в громадських місцях), виправданість нормативного закріплення вимог та зобов'язань щодо

застосування доступних заходів захисту кожної дитини від інформації, де б вона не перебувала (будинок чи громадський простір), оскільки природа інформаційної дії тягне за собою соціальні наслідки.

Опис гіпермережевої природи медіапростору вказує на необхідність відповідних досліджень з подальшим їх впровадженням у практику управління обігом інформації та в принципі інформаційної та соціальної політики. Ці завдання можна досягти, а дослідження, спрямовані на всебічне вивчення можливостей захисту від колишніх та нових загроз, виконують найважливіше завдання наукового обґрунтування управлінських та політичних рішень.

Представлений досвід наукового осмислення особливого типу зашумлення потребує подальших міждисциплінарних досліджень та застосування наявних засобів діагностики та оцінки. Медіазашумлення життєвого простору, потребує подальшого вивчення, що синтезує інструментарій різних галузей наукового знання, розробки трансдисциплінарної методології виявлення закономірностей та динаміки технологічного розвитку, їх впливу на стан індивідуальної та національної інформаційної безпеки як єдиного концепту інформаційно-технологічної безпеки людини.

ВИСНОВКИ

У дисертації наведено вирішення важливого наукового завдання з розвитку теоретичних засад та обґрунтування науково-прикладних рекомендацій щодо удосконалення механізмів інформаційних комунікацій сучасного суспільства.

За результатами проведеного дослідження обґрунтовано наступні висновки.

1. Охарактеризовано сутність та вразливість нових форм комунікації інформаційного суспільства. У результаті проведеного дисертаційного дослідження було здійснено узагальнення існуючих науково-теоретичних підходів до вивчення механізмів інформаційних комунікацій сучасного суспільства. Аналіз наукової літератури засвідчив еволюцію поглядів на роль комунікації в системі державного управління, починаючи від традиційних моделей інформування до сучасних концепцій інтерактивної взаємодії та електронної участі громадян. Виявлено, що цифровізація суттєво трансформує комунікаційний механізм, зумовлюючи появу нових каналів, інструментів та форм взаємодії між органами влади та суспільством.

2. Систематизовано зарубіжний досвід регулювання обігу інформації з метою захисту дітей в сучасному суспільстві. Виявлено універсальні компоненти світових практик забезпечення інформаційної безпеки дітей та дорослих: змістовний (ціннісний, світоглядний) та процедурний (технології оцінки інформації та обмеження її обігу з метою захисту дітей). У взаємозв'язку з цими компонентами виділено закономірності

динаміки затребуваності ресурсів соціальних інститутів.

Визначено необхідність подальшої гармонізації національного законодавства з європейськими стандартами у сфері інформаційної відкритості та захисту даних. Обґрунтовано важливість прийняття нових законодавчих актів та внесення змін до існуючих для врегулювання питань, пов'язаних з використанням соціальних мереж органами влади, захистом персональних даних в цифровому середовищі та протидією кіберзагрозам.

3. Оцінено організаційний механізм інформаційних комунікацій сучасного суспільства. Реалізація функцій суб'єктів управління та їх управлінський потенціал щодо конкретного ризику залежать від рівня прийняття управлінського рішення, типу ризику, ступеня їхньої інституціалізації (варіативності дій), особливостей соціально-правового зв'язку з суб'єктом ризикової поведінки, етапу комунікативного ланцюга, на якому проявляється ризикова поведінка. Серед джерел дисфункцій соціальних інститутів, суб'єктів управління, виділяються слабкий консенсус щодо соціального значення ризиків та критеріїв шкоди від інформації, вразливості порядку спадкоємності відповідальності за ризикову поведінку та недоліки організації контролю якості управлінських рішень, переважання екстенсивної стратегії мінімізації ризиків над інтенсивною, технологічно обумовленою емансипацією.

4. Окреслено методичні основи формування механізмів управління інформаційною безпекою дітей. Змістовний (ціннісний, світоглядний) та процедурний (технології оцінки та обмеження обігу інформації) компоненти системи захисту дітей від ризиків, пов'язаних з інформацією, є універсальними для світових практик. Параметрами цих компонентів є: наявність спеціального законодавства щодо захисту дітей від шкідливого контенту; чіткість правового формулювання дефініцій шкідливого контенту та його асортимент; діапазон чутливих тем (уразливостей, «больових точок») в публічних дискусіях; визнання невідчужуваності права на вільний доступ до інформації; ступінь консенсусності щодо можливості обмеження інформаційних свобод на користь дітей. Особливості поєднання цих параметрів та ступінь прихильності населення до культурно-ціннісних універсалій дають підстави для рівневого розподілу світових систем забезпечення інформаційної безпеки дітей. Кожен із чотирьох рівнів передбачає різну затребуваність ресурсного потенціалу соціальних інститутів та його різні пропорції у технологіях мінімізації ризиків від інформації. Виявлено, що зниження прихильності населення до ціннісних орієнтирів тягне за собою зниження затребуваності ресурсів соціальних інститутів відповідно до ступеня їх інституціалізації в наступній послідовності: ресурси інституту сім'ї, ресурси інституту громадянської активності, ресурси інституту експертизи, ресурси інституту юридичної відповідальності.

5. Визначено напрями управління ризиками інформаційних комунікацій сучасного суспільства. Розвиток медіа-технологій виступає стимулом інтенсифікації процесів управління інформаційною безпекою,

оскільки одночасно сприяє реалізації ризикової поведінки та реалізації функцій соціальними інститутами як суб'єктами управління, збільшуючи їх ресурси та забезпечуючи новими технологічними засобами контролю, внутрішніх та зовнішніх комунікацій, збору та акумуляції даних. Технологізація ризиків полягає у можливостях надшвидкого, легкого та ефективного створення, поширення, доставки та споживання інформації, а також у нормативності та безальтернативності використання медіа-технологій, у посиленні варіативності поведінки.

6. Обґрунтовано стратегічні напрями удосконалення механізмів інформаційних комунікацій сучасного суспільства, через методологічні принципи побудови теоретичної концепції управління інформаційною безпекою які виходять з ризикологічного, інституційного та ресурсного підходів та представлені принципом урахування поведінкової основи джерела ризику, та альтернативності. Окреслено, що управління інформаційною безпекою сприймається як дія соціальних інститутів, які мають функцію мінімізації ризиків заподіяння інформацією шкоди здоров'ю та розвитку дітей та дорослих та впливають на фактори ризикової поведінки з метою зниження ймовірності шкоди від контенту інформації та формату її споживання через додаток. Ризик розуміється як результат поведінки суб'єктів на різних етапах інформаційно-комунікативного процесу (створення, розповсюдження, організації доступу та споживання інформації), що підвищує ймовірність заподіяння шкоди, пов'язаної з низькою якістю змісту інформації та/або режиму (формату) її споживання. Низька якість змісту інформації означає наявність шкідливого контенту, а низька якість формату споживання інформації – медіа-шумове навантаження, тобто фонове та вимушене споживання медіа сигналу.

СПИСОК ПУБЛІКАЦІЙ ЗДОБУВАЧА ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Наукові праці, в яких опубліковані основні наукові результати дисертації

Монографія

1. Формування дієвих механізмів публічного управління у сфері національної безпеки в умовах впливу цифрових технологій: Монографія: С.М. Домбровська, Н.М. Карпеко, С.Г. Порока, В.М. Новак: НАУ «ХАІ», 2026. 257с.

Особистий внесок: визначено сутність та вразливість нових форм комунікації інформаційного суспільства.

Статті у фахових наукових виданнях з державного управління:

2. Палюх В. В., Новак В. М. Вразливості інформаційних комунікацій в умовах гібридних загроз: механізми державної протидії. Вісник Національного університету цивільного захисту України. Серія: Державне

управління. 2025. Вип. 2(23). С. 102-107. URL: <http://repositsc.nuczu.edu.ua/bitstream/123456789/27296/1/14.pdf>

Особистий внесок: визначено вразливості інформаційних комунікацій в умовах гібридних загроз.

3. Новак В. М. Механізми державного протистояння вразливостям інформаційно-комунікаційних систем в умовах гібридної війни. Вісник Національного університету цивільного захисту України. Серія: Державне управління. 2023. Вип. 1(18). С. 364-374. URL: <http://repositsc.nuczu.edu.ua/bitstream/123456789/27837/1/Novak231%20%281%29.pdf>

4. Новак В. М. Трансформація механізмів соціальної консолідації в умовах розвитку мережових комунікацій. Вісник Національного університету цивільного захисту України. Серія: Державне управління. 2019. Вип. 2(11). С. 579-588. URL: <http://repositsc.nuczu.edu.ua/bitstream/123456789/27792/1/Novak.pdf>

5. Novak V., Burtovyi R. Resource potential of social institutions in the state information security management system in Ukraine. Public administration and state security aspects. 2025. Vol.2/2025. URL: <http://repositsc.nuczu.edu.ua/bitstream/123456789/27615/1/Novak.pdf>

Особистий внесок: визначено ресурсний потенціал соціальних установ у системі управління інформаційною безпекою держави в Україні

6. Novak V. Risks of information communications and mechanisms for their regulation under martial law conditions. Public administration and state security aspects. 2023. Vol.2/2023. URL: <http://repositsc.nuczu.edu.ua/bitstream/123456789/27745/1/NovakP232.pdf>

Наукові праці, які засвідчують апробацію матеріалів дисертації:

7. Новак В., Мамка О., Місюра А. Захист критичної інфраструктури України, як складова національної стійкості. Національна стійкість (резилієнтність) як ключовий елемент національної безпеки: архітектура, виклики та шляхи посилення : матеріали І-ї Міжнародної науково-практичної конференції (ІваноФранківськ, 27 листопада 2025 р.); за наук. ред. проф. І. І. Чудика, Д. І. Дзвінчука, І. П. Лопушинського; упоряд. доц. Л. С. Мосора. Івано-Франківськ : ІФНТУНГ, 2025. С.163-166

Особистий внесок: визначено ключові елементи національної безпеки.

8. Новак В. М. Державна політика захисту інформації. Матеріали міжнародної науково-практичної інтернет-конференції «Публічне управління у сфері цивільного захисту: освіта, наука, практика» м. Черкаси. 2025. С.110-112.

9. Новак В. М. Інформаційна безпека суспільства в сучасних умовах. Теоретико-практичні засади управління, економіки та природокористування: аспекти реінтеграції Криму в господарський комплекс України : матеріали ІХ Міжнародної науково-практичної конференції (м. Київ, 11 листопада 2025

року) / упоряд. Д. В. Починок. Київ 2025. С.177-179.

10. Новак В. М. Інструментарій забезпечення цифрової безпеки суспільства. Збірник тез V Міжнародної науково-практичної конференції «Публічне управління в Україні: виклики сьогодення та глобальні імперативи». (м. Хмельницький, 19 лютого 2026 року). Хмельницький : Хмельницький університет управління та права імені Леоніда Юзькова, 2026. 200 с.

АНОТАЦІЯ

Новак В. М. Механізми інформаційних комунікацій сучасного суспільства.

Дисертація на здобуття наукового ступеня кандидата наук з державного управління за спеціальністю 25.00.02 – механізми державного управління. – Національний аерокосмічний університет «Харківський авіаційний інститут» – Харків, 2026.

У дослідженні запропоновано розв'язання актуального завдання з розвитку теоретичних засад та обґрунтування науково-прикладних рекомендацій щодо удосконалення механізмів інформаційних комунікацій сучасного суспільства.

Досягнення визначеної мети зумовило вирішення наступних завдань, а саме охарактеризовано сутність та вразливість нових форм комунікації інформаційного суспільства, та систематизовано зарубіжний досвід регулювання обігу інформації з метою захисту дітей в сучасному суспільстві. Надано оцінку організаційному механізму інформаційних комунікацій сучасного суспільства і окреслено методичні основи формування механізмів управління інформаційною безпекою дітей. Визначено напрями управління ризиками інформаційних комунікацій сучасного суспільства, та обґрунтовано стратегічні напрями удосконалення механізмів інформаційних комунікацій сучасного суспільства.

Об'єктом дослідження є державна інформаційна політика, а предметом дослідження виступають механізми інформаційних комунікацій сучасного суспільства.

Інформаційну базу дисертаційного дослідження становили нормативно-правові акти, праці зарубіжних і вітчизняних учених, Інтернет-ресурси, статистична інформація Державної служби статистики України та інших центральних органів виконавчої влади.

Наукова новизна одержаних результатів полягає у вирішенні наукового завдання щодо розвитку теоретичних засад та обґрунтуванні науково-прикладних рекомендацій щодо удосконалення механізмів інформаційних комунікацій сучасного суспільства.

Автором вперше: запропоновано модель управління інформаційною безпекою, що включає в себе основні елементи системи управління, які взаємодіють на основі рівневого принципу прийняття та реалізації

управлінського рішення, процесного підходу до комунікації, виявлених факторів ризикової поведінки та типів ризику, де модель орієнтована на синхронізацію ресурсів суб'єктів управління з активізацією управлінського потенціалу соціальних інститутів юридичної відповідальності, експертизи та громадянської участі для оптимізації соціальних ризиків через узгодження спрямованості та швидкості управлінського впливу;

Таки чином, у дисертації наведено вирішення важливого наукового завдання з розвитку теоретичних засад та обґрунтування науково-прикладних рекомендацій щодо удосконалення механізмів інформаційних комунікацій сучасного суспільства. За результатами проведеного дослідження зроблені обґрунтовані висновки.

Ключові слова: державне управління, механізми державного управління, механізми інформаційних комунікацій сучасного суспільства, організаційного механізму інформаційних комунікацій сучасного суспільства, управління ризиками інформаційних комунікацій.

ABSTRACT

Novak V. M. Mechanisms of Information Communications in Modern Society.

Dissertation for the degree of Doctor of Science in Public Administration, specialty 25.00.02 - Mechanisms of Public Administration. – National aerospace university "Kharkiv Aviation Institute" – Kharkiv, 2026.

Achieving the defined goal necessitated solving the following tasks: characterizing the essence and vulnerability of new forms of information society communication, and systematizing foreign experience in regulating information circulation to protect children in modern society. An assessment of the organizational mechanism of information communications in modern society is provided, and methodological foundations for forming mechanisms for managing children's information security are outlined. Directions for managing risks in information communications of modern society are defined, and strategic directions for improving the mechanisms of information communications in modern society are substantiated.

The information base of the dissertation research included regulatory legal acts, works by foreign and domestic scholars, Internet resources, statistical information from the State Statistics Service of Ukraine, and other central executive bodies.

The scientific novelty of the obtained results lies in solving the scientific problem of developing theoretical foundations and substantiating scientific and applied recommendations for improving the mechanisms of information communications in modern society.

For the first time, the author has: proposed an information security management model that includes the main elements of the management system,

interacting on the basis of a multi-level principle of managerial decision-making and implementation, a process approach to communication, identified factors of risky behavior and types of risk, where the model is oriented towards synchronizing the resources of management subjects with the activation of the managerial potential of social institutions of legal responsibility, expertise, and civic participation to optimize social risks through the alignment of the direction and speed of managerial influence.

The dissertation has improved: the features of media technologies' influence on the information security management system, which consists both in expanding the risk zone and in changing the managerial resources of management subjects, due to features caused by the lack of alternatives in using media technologies, the emancipation of information flows, the temporal reduction of information signal (content) presentation and consumption, information accessibility, domestication of media technologies, as well as the expansion of technological capabilities for control, communication among management subjects, and their data aggregation; and information security management as a purposeful influence of social institutions on factors of risky behavior to reduce the probability of harm from information regarding the health and development of this social community, the specificity of whose managerial influence is determined by the type of risk, which defines the necessary managerial resources, the status of the subject of risky behavior, which indicates the level of the managerial decision, the functionality of the social institution as a subject of management, where the understanding of the subject-object nature of risky behavior and its factors is embedded; the typology of risks, including institutional risks; and the multi-level principle of developing and implementing managerial decisions.

Thus, the dissertation presents a solution to an important scientific problem concerning the development of theoretical foundations and the substantiation of scientific and applied recommendations for improving the mechanisms of information communications in modern society. Based on the conducted research, substantiated conclusions have been drawn.

Keywords: public administration, public administration mechanisms, mechanisms of information communications in modern society, organizational mechanism of information communications in modern society, risk management of information communications.

Відповідальна за друк Домбровська С.М.

Підписано до друку 03.04.2026 р.
Формат 60x84 1/16. Обл.-вид. арк. 0,9.
Гарнітура Таймс. Тираж 100 прим.

Віддруковано з оригінал-макета в друкарні ФОП Леонов Д.С.
61023, м. Харків, вул. Весніна, 12, тел. (057) 717-28-80