

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА»

ДИМИТРІЄВА ОКСАНА ІГОРІВНА

УДК 351

**ДЕРЖАВНА ПОЛІТИКА ЗАХИСТУ ДІТЕЙ У КІБЕРПРОСТОРІ ЯК
ПРІОРИТЕТ ГУМАНІТАРНОЇ БЕЗПЕКИ УКРАЇНИ**

25.00.05 – Державне управління у сфері державної безпеки
та охорони громадського порядку.

АВТОРЕФЕРАТ
дисертації на здобуття наукового ступеня
кандидата наук з державного управління

Житомир – 2025

Дисертацією є рукопис.

Робота виконана в Національному університеті цивільного захисту України.

Науковий керівник: доктор наук з державного правління, доцент,
ШПАК Юрій Валерійович,
Державний університет «Житомирська політехніка», професор кафедри національної безпеки, публічного управління та адміністрування.

Офіційні опоненти: доктор наук з державного управління, доцент,
ЯРОВОЙ Тихон Сергійович,
ЗВО «Університет трансформації майбутнього», професор кафедри бізнесу, адміністрування та права;

кандидат наук з державного управління,
ДОЛНЧЕНКО Ольга Михайлівна,
ПрАТ «ЗВО «Міжрегіональна Академія управління персоналом», доцент кафедри публічного адміністрування.

Захист відбудеться *27 грудня 2025 року о 13 годині* на засіданні спеціалізованої вченої ради Д 14.052.03 в Державному університеті «Житомирська політехніка» за адресою: 10005, м. Житомир, вул. Чуднівська, 103, конференц-зала (2-й поверх).

З дисертацією можна ознайомитись у бібліотеці Державного університету «Житомирська політехніка» за адресою: 10005, м. Житомир, вул. Чуднівська, 103.

Автореферат розісланий *26 листопада 2025 року*.

Учений секретар
спеціалізованої вченої ради

Л. В. Сергієнко

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

Актуальність теми. Сучасний етап розвитку суспільства супроводжується стрімкою цифровізацією усіх сфер життєдіяльності, що істотно змінює характер соціальних відносин, формує нові можливості, проте й генерує безпрецедентні ризики, особливо для найуразливіших верств населення – дітей. У кіберпросторі діти виступають активними споживачами, творцями контенту та учасниками соціальної взаємодії, але водночас вони стають мішенню для різноманітних кіберзагроз: від кібербулінгу, секстингу, грумінгу до експлуатації, шкідливого контенту та маніпулятивних технологій впливу на поведінку. З огляду на це, захист дітей у кіберпросторі постає не лише як технологічне або правове завдання, а як складова ширшої парадигми гуманітарної безпеки.

Особливої актуальності тема набуває в умовах повномасштабної війни та глибокі соціальні трансформації. Діти, які стали внутрішньо переміщеними особами, пережили втрату близьких або зруйновану інфраструктуру освіти, зазнають подвійного навантаження: інформаційного й емоційного. Цифрове середовище для них водночас виступає простором порятунку, комунікації та навчання, але й джерелом загроз, що поглиблюють травматичний досвід. У таких умовах держава зобов'язана формувати ефективну, гнучку й інноваційну політику захисту дітей у кіберпросторі, яка б не лише відповідала на виклики, а й була на крок попереду потенційних ризиків.

Теоретичною основою дисертаційного дослідження стали наукові праці дослідників, що охоплюють комплекс проблематики цифрової безпеки, захисту дітей у кіберпросторі, гуманітарної безпеки та державної політики в умовах цифровізації. Вагомий внесок у розкриття гуманітарного виміру безпеки зробили В.І. Горбулін, О. М. Литвиненко, М.С. Баюк, В.В. Максимець, які досліджують роль гуманітарних чинників у системі національної безпеки. Інституційні й правові аспекти захисту дітей у кіберпросторі розкриті у працях Т.М. Димитрієвої, Н.М. Крестовської, Н. Г. Волкової, Н.І. Коломоець, О.О. Безпаленко, Ю.В. Губаля, О.В. Дрозд, Ж. В. Петрочко, які розглядають питання реалізації прав дитини, інституційного супроводу політики захисту та гармонізації національного законодавства з міжнародними стандартами. Питання цифрової трансформації публічного управління та національної кібербезпеки в контексті суспільних інституцій досліджували В.В. Євдокимов, Д.О. Грицишен, Л.В. Сергієнко, Т.В. Барановська, А.В. Антонов, Н.В. Васильєва, Д.І. Даник, Ю.Г. Даник, Н.В. Дацій, І.О. Драган, П.М. Воробієнко, Б.М. Кормич, Є.М. Котух, Б. В. Корнієнко, Д.О. Ланде, С.О. Гончар, А.П. Дикий, О.М. Долінченко, Д.І. Дубов, В.В. Ксендзук, Н.С. Орлова, О.М. Руденко, С.В. Свірко, І.В. Супрунова, Ю.В. Шпак, Т.С. Яровой. Теоретичне обґрунтування управлінських механізмів, стратегій і політик у сфері захисту дітей висвітлено у працях В.А. Василенка, В.А. Гришка, В.І. Гончаренка, С.О. Крука, О.С. Гордєєва, які формують методологічні рамки

для застосування сучасних форм публічного врядування, зокрема – у сфері соціального захисту, кібербезпеки, освіти та цифровізації.

Огляд зазначених досліджень дає підстави стверджувати, що хоча науковий інтерес до окремих аспектів цифрової трансформації, дитячої безпеки та управлінських механізмів є високим, проте відсутня інтегрована наукова концепція, яка б системно об'єднала інституційні, правові, гуманітарні, технологічні та комунікаційні компоненти політики державного захисту дітей у кіберпросторі. Саме ця прогалина і визначає наукову нішу, актуальність і новизну обраної теми дисертаційного дослідження.

Зв'язок роботи з науковими програмами, планами, темами. Дисертаційна робота виконана в межах НДР Національного університету цивільного захисту України за темою «Розробка механізмів державного управління соціально-економічною сферою та її галузями в контексті забезпечення безпеки українського суспільства» (ДР №0118U001007), в рамках запропоновано прикладні механізми публічної політики щодо попередження та реагування на цифрові загрози для дітей, які включають правове та інституційне забезпечення, впровадження цифрових інструментів раннього попередження загроз; здійснено концептуалізацію механізмів попередження цифрових загроз на рівні органів місцевого самоврядування, розроблено підходи до інституціоналізації міжвідомчої взаємодії у сфері гуманітарної та цифрової безпеки.

Мета та завдання дослідження. Метою дисертаційної роботи є наукове обґрунтування теоретико-концептуальних засад, інституційно-організаційних механізмів та стратегічних напрямів вдосконалення державної політики захисту дітей у кіберпросторі в умовах сучасних викликів гуманітарної безпеки, цифрової трансформації та збройного конфлікту.

Для реалізації зазначеної мети, необхідно виконати такі *завдання*:

- розкрити теоретико-концептуальні положення щодо формування державної політики захисту дітей у кіберпросторі;
- проаналізувати типологію та характер кіберзагроз для дітей, їх механізми впливу на фізичну, психоемоційну, інформаційну та соціальну безпеку дитини;
- оцінити сучасний стан державної політики в Україні щодо захисту дітей у кіберпросторі та виявити ключові проблеми цифрової безпеки дітей;
- здійснити порівняльний аналіз досвіду зарубіжних країн щодо стратегій і практик кіберзахисту дітей;
- обґрунтувати стратегічні пріоритети державної політики у сфері цифрової безпеки дітей в Україні;
- сформулювати концептуальні основи цифрової трансформації державної політики захисту дітей;
- обґрунтувати модель розгортання національної цифрової інфраструктури для забезпечення захисту дітей в онлайн-середовищі.

Об'єкт дослідження – державна політика забезпечення прав та безпеки дітей у кіберпросторі в умовах гуманітарних загроз і цифрової трансформації.

Предмет дослідження – механізми формування та реалізації державної політики захисту дітей у кіберпросторі як пріоритет гуманітарної безпеки України.

Методи дослідження. Методологічною основою дисертаційного дослідження став комплекс загальнонаукових, спеціальних і міждисциплінарних методів, які дозволили забезпечити цілісне, системне та обґрунтоване розкриття проблеми державної політики у сфері захисту дітей у кіберпросторі в контексті гуманітарної безпеки. У процесі дослідження було використано дискурсивно-аналітичний метод для систематизації наукових підходів до цифрової безпеки, прав дитини та кіберзагроз, що дозволило виявити основні теоретичні школи та акценти сучасної наукової думки. Системно-структурний підхід було застосовано для розкриття взаємозв'язків між правовими, організаційними, технологічними та освітніми елементами державної політики у сфері забезпечення кібербезпеки дітей. Контент-аналіз нормативно-правових актів, стратегічних документів, звітів міжнародних організацій, національних програм та публічної інформації дозволив виявити змістовні, процедурні та змістовні прогалини в українській системі захисту дітей. Порівняльний аналіз використовувався для зіставлення досвіду України з практиками Польщі, Естонії та Південної Кореї, що надало змогу окреслити ефективні моделі політики та інституційної взаємодії. Функціональний аналіз дав змогу визначити компетенції, функції та взаємозв'язки між суб'єктами публічного управління, освітньої сфери, правоохоронної системи та ІТ-сектора. Метод експертного оцінювання застосовувався для ідентифікації практичних викликів у реалізації політики, слабких місць у технологічному забезпеченні та реагуванні на кіберінциденти. Прогностичний метод було використано для формування стратегічних орієнтирів та пропозицій щодо цифрової трансформації системи захисту дітей. Моделювання та візуалізація використовувалися для створення структурних схем, інтерактивних матриць, таблиць пріоритетів і механізмів політики, що дозволили представити складні процеси у доступній формі. Комплексне використання зазначених методів дало змогу забезпечити високий рівень наукової обґрунтованості положень дисертаційної роботи, досягнення поставленої мети та вирішення ключових завдань дослідження.

Використання технологій штучного інтелекту. Технології штучного інтелекту (ChatGPT) використовувалися для: 1) пошукових цілей під час вивчення досвіду реалізації державної політики у сфері захисту дітей у кіберпросторі, правового регулювання цифрової безпеки неповнолітніх, механізмів державного нагляду та міжвідомчої координації в країнах Європейського Союзу та провідних міжнародних організаціях; результати запитів містили посилання на офіційні веб-ресурси урядових структур, уповноважених органів із захисту прав дітей, національних центрів кібербезпеки, а також міжнародні нормативно-правові акти та політичні документи (зокрема, документи ООН, Європейської комісії, Ради Європи, ЮНІСЕФ); 2) попереднього перекладу іноземних нормативно-правових актів,

стратегій, аналітичних документів і рекомендацій, що стосуються безпечного цифрового середовища для дітей, з англійської мови на українську. Технології штучного інтелекту не використовувалися для генерування авторського тексту дисертації.

Наукова новизна одержаних результатів. Основні положення дослідження, що характеризують наукову новизну одержаних результатів і виносяться на захист, полягають у наступному:

удосконалено:

- наукові підходи до формування державної політики захисту дітей у кіберпросторі шляхом обґрунтування її концептуальної моделі в контексті гуманітарної безпеки, які враховують багаторівневу архітектуру цифрових загроз, специфіку вікових груп, мультиакторність системи забезпечення безпеки та потребу в інтеграції етичних, правових і технологічних елементів, що дало змогу концептуалізувати цифрову безпеку дітей як складову загальнонаціональної гуманітарної політики;

- типологію загроз для дітей у кіберпросторі, яка враховує не лише правову, а й психологічну, соціокультурну, інформаційну та когнітивну природу впливів, та передбачає їх класифікацію за критеріями інтенсивності впливу, характеру шкоди, джерела походження загроз і способу дії, що створює основу для таргетованих управлінських інтервенцій і системи раннього попередження;

- механізми моніторингу, виявлення та реагування на цифрові загрози для дітей, зокрема запропоновано запровадження Національного порталу безпеки дітей у мережі, використання алгоритмів штучного інтелекту для виявлення ризикового контенту, залучення громадських платформ для інцидентного звітування, що дає змогу підвищити ефективність реагування на загрози та створити оперативну цифрову інфраструктуру;

набуло подальшого розвитку:

- понятійно-категоріальний апарат науки державного управління на основі уточнення сутності «державної політики у сфері цифрової безпеки дітей», що дало змогу трактувати цей феномен як міждисциплінарну категорію, що поєднує гуманітарно-правову, управлінську, інформаційну та соціальну площини; «цифрова вразливість дитини», як підвищеної ймовірності того, що дитина зазнає шкоди в цифровому середовищі через недостатній рівень захисту, цифрової грамотності, емоційної зрілості або соціальної підтримки; «гуманітарна кібербезпека», як напряму державної політики, що зосереджений на захисті прав, свобод і добробуту людини в цифровому середовищі, з особливим акцентом на вразливі групи населення, зокрема дітей; «дитиноцентрична цифрова політика», як підходу до формування цифрової політики, який ставить на перше місце інтереси, безпеку та розвиток дитини, забезпечуючи її участь у цифровому середовищі на умовах захищеності, рівності та підтримки;

- інституційна модель державної політики у сфері цифрової безпеки дітей, яка охоплює центральні органи виконавчої влади, місцеве самоврядування, освітні установи, громадські організації, ІТ-сектор та

міжнародні інституції як взаємопов'язані елементи, що дає змогу забезпечити координацію дій на різних рівнях управління, реалізувати інтегровану державну політику в умовах цифрової трансформації суспільства;

- напями нормативно-правового забезпечення державної політики захисту дітей у кіберпросторі, які включають розробку спеціального Закону України «Про захист дітей у кіберпросторі», що визначатиме правові механізми запобігання цифровим загрозам для дітей, гармонізацію національного законодавства із законодавством ЄС, зокрема положеннями Регламенту ЄС про цифрові послуги (DSA) та Загального регламенту про захист даних (GDPR), оновлення Кримінального кодексу України щодо відповідальності за кіберзлочини проти дітей, посилення правового регулювання діяльності онлайн-платформ у частині контенту, доступного для неповнолітніх а також забезпечення цифрових прав дитини як складової гуманітарної безпеки;

- модель цифрового партнерства між державою, громадянським суспільством та бізнес-структурами з метою підвищення ефективності реалізації державної політики захисту дітей у кіберпросторі, яка передбачає створення національної платформи співпраці, що забезпечить прозору взаємодію між BigTech-компаніями, освітніми установами та регуляторами.

Практичне значення одержаних результатів полягає в обґрунтуванні інституційних, нормативно-правових, організаційно-управлінських та цифрових засад державної політики у сфері захисту дітей у кіберпросторі в контексті гуманітарної безпеки. Так, оригінальні методики та практичні рекомендації, що містяться в дисертаційній роботі, використано в діяльності: Чернігівського інституту інформації, бізнесу і права ЗВО «Міжнародний науково-технічний університет імені академіка Юрія Бугая» у навчальній та науковій діяльності (довідка про впровадження від 9 липня 2024 року № 186/24); Громадської організації «Освітній компас» при розробці заходів щодо розвитку інформаційної сфери в Україні (довідка про впровадження від 25 грудня 2024 року № 05/24); Міністерства культури та стратегічної комунікації при аналізі цифрових засад державної політики у сфері захисту дітей (довідка про впровадження від 3 лютого 2025 року № 20/14.25/1); Народного депутата Верховної Ради України при розробці та вдосконаленні нормативно-правових актів, формуванні державної стратегії цифрової безпеки дітей (довідка про впровадження від 25 серпня 2025 року № 110д9/10-2025/196113); Офісу генерального прокурора (довідка про впровадження від 3 вересня 2025 року № 24/1/1-691 вих. 25) взято до уваги удосконалений методичний підхід, який дає змогу визначити залежність між рівнем кіберзагроз та ефективністю державної політики у сфері захисту дітей у цифровому середовищі.

Особистий внесок здобувача. Наукові положення, висновки та рекомендації, що виносяться на захист, одержані автором особисто. Обсяг особистого внеску автора в роботах, опублікованих у співавторстві, наведено в переліку опублікованих праць.

Апробація результатів дослідження. Основні ідеї, положення, висновки дисертаційної роботи були оприлюднені на науково-практичних конференціях,

зокрема, за міжнародною участю та всеукраїнських: «Розвиток української держави в умовах активізації євроінтеграційних процесів» (Київ, 2016), «Актуальні питання цивільного права та права інтелектуальної власності» (Київ, 2015), «Роль юриспруденції у формуванні сучасного суспільства» (Київ, 2017), «Актуальні проблеми розвитку правової держави і громадянського суспільства» (Київ, 2017), «Роль юриспруденції у формуванні сучасного суспільства» (Київ, 2016).

Публікації. Основні результати дослідження висвітлено в 12 наукових працях, з яких: 6 статей у наукових фахових виданнях з державного управління, 1 зарубіжна публікація, 5 тез у матеріалах науково-комунікативних заходів. Загальний обсяг публікацій становить 4,4 друк. арк.

Структура і обсяг дисертації. Дисертація складається зі вступу, трьох розділів, висновків, списку використаних джерел. Основний обсяг дисертації становить 177 сторінок друкованого тексту. Робота містить 13 таблиць, 3 рисунки. Список використаних джерел налічує 161 найменувань.

ОСНОВНИЙ ЗМІСТ РОБОТИ

У **вступі** обґрунтовано актуальність теми дослідження, визначено стан її наукової розробки, розкрито зв'язок з науковими програмами, планами, темами, визначено мету, завдання, об'єкт, предмет і методи дослідження, наукову новизну та практичне значення отриманих результатів, наведено відомості про їх апробацію.

У першому розділі **«Теоретико-концептуальні засади захисту дітей у кіберпросторі як компонента гуманітарної безпеки»** досліджено зміст та структуру гуманітарної безпеки в системі національної безпеки України; визначено концептуальні засади дослідження державної політики цифрової безпеки дітей; систематизовано теоретичні підходи до формування державної політики захисту дітей.

У результаті проведеного дослідження було сформовано цілісне теоретико-концептуальне підґрунтя для розуміння гуманітарної безпеки як системної категорії, невід'ємної від архітекτονіки національної безпеки України. Здійснено уточнення дефініції гуманітарної безпеки, яка розглядається не лише як інструмент захисту особистості, а як динамічна, ціннісно зорієнтована підсистема, що покликана забезпечувати стійкий розвиток соціокультурного середовища, захист прав і свобод людини, збереження ідентичності, інтелектуального, освітнього та морального потенціалу населення. У цьому контексті гуманітарна безпека була концептуалізована як багатовекторна та багаторівнева категорія, що інтегрується у політико-правовий, освітньо-культурний, соціоінформаційний і демографічний простори національної безпеки.

Завдяки комплексному міждисциплінарному підходу уточнено структуру гуманітарної безпеки, яка включає такі ключові компоненти: культурно-ціннісний, що забезпечує збереження культурної спадщини, національної

ідентичності та формування стійких суспільних орієнтирів; освітньо-інтелектуальний, який гарантує доступ до якісної освіти, розвиток критичного мислення, цифрової грамотності та людського капіталу; інформаційно-комунікаційний, що регулює безпечну взаємодію в інформаційному середовищі, захист від дезінформації, маніпуляцій і кіберзагроз; правовий, який формує правові запобіжники і механізми реалізації прав людини у гуманітарному просторі; психологічно-поведінковий, що пов'язаний із безпекою ментального та емоційного стану особистості, зокрема в умовах воєнних, інформаційних і цифрових загроз; соціально-демографічний, спрямований на підтримання стабільності та життєздатності соціуму через формування безпечного середовища для розвитку дітей, молоді, вразливих груп населення.

Окрему увагу приділено визначенню цифрової безпеки дітей як пріоритетного напрямку гуманітарної безпеки, який має критичне значення для довгострокової стабільності суспільства. Цей напрямок розглядається не лише через призму загроз, а й як умова забезпечення майбутнього національного розвитку – з урахуванням технологічних, соціальних, ментальних та інституційних детермінант. Сформульовано тезу про необхідність розглядати дитину як одночасно об'єкт і суб'єкт державної політики цифрової безпеки, що передбачає посилення її участі, інформованості та цифрової спроможності.

На основі здійсненого аналізу запропоновано модель інтеграції гуманітарної безпеки до системи національної безпеки України, яка враховує виклики цифрової трансформації, гібридних загроз, культурної поляризації та демографічної нестабільності. Ця модель відображає необхідність нової гуманітарної парадигми, що має на меті формування безпечного освітньо-інформаційного середовища, розвиток критичного цифрового мислення, етичної самосвідомості та інституційного захисту прав дитини (табл. 1).

Здійснено глибокий міждисциплінарний аналіз наукових і прикладних підходів до формування політики державної політики у сфері захисту дітей, що дозволило виявити основні теоретичні моделі, які визначають сучасні орієнтири у цій сфері. Узагальнено й систематизовано такі ключові парадигми: нормативно-правовий, інституційний, governance-підхід, мережеве управління, rights-based підхід, інтеграційний і мультисекторальний підхід, а також теорія управлінських рішень і раціонального вибору.

Нормативно-правовий підхід дав змогу обґрунтувати важливість чіткої законодавчої основи як фрейму, що задає межі державної політики у сфері захисту дітей. Проте саме у поєднанні з інституційним підходом розкривається багатовимірна роль інститутів – формальних і неформальних – у реалізації державного регулювання, особливо в умовах цифрового середовища. Governance- і мережеві моделі виявилися найбільш релевантними до умов сучасності, оскільки вони дозволяють бачити управління не як ієрархічну вертикаль, а як інтерактивну й гнучку систему взаємодії між різними стейкхолдерами – державою, громадянським суспільством, сім'єю, освітніми закладами, IT-сферою та міжнародними організаціями.

Таблиця 1

Структурні компоненти гуманітарної безпеки

№	Компонент	Змістова характеристика	Основні функції	Потенційні загрози
1	Культурно-ціннісний	Система національних цінностей, традицій, мови, ідентичності	Формування національної єдності, патріотизму, міжкультурного діалогу	Культурна експансія, гібридна пропаганда, русифікація
2	Освітньо-інтелектуальний	Освіта, наука, інтелектуальний потенціал суспільства	Розвиток критичного мислення, технологічного суверенітету, просвітництва	Освітній занепад, відтік мізків, дезінформація
3	Інформаційно-комунікаційний	Стан та безпека інформаційного простору, цифрової культури	Захист від інформаційних атак, забезпечення доступу до правдивої інформації	Кіберпропаганда, фейки, кібербулінг, інформаційна війна
4	Правовий	Юридичні гарантії прав людини, захист вразливих груп (особливо дітей)	Забезпечення правового захисту, доступу до правосуддя	Порушення прав, недоступність правової допомоги
5	Психологічно-поведінковий	Психічна стійкість, емоційна культура, поведінкові моделі	Попередження девіантної поведінки, формування резильєнтності	Посттравматичні розлади, тривожність, агресія, апатія
6	Соціально-демографічний	Стан населення, міграція, відтворення людського капіталу	Демографічна стабільність, захист вразливих груп, соціальна інтеграція	Депопуляція, міграційна криза, маргіналізація

Джерело: систематизовано автором

Особливу увагу в дослідженні приділено мережевому підходу, який в умовах цифрової трансформації набуває особливої значущості. Установлено, що ця модель управління є найбільш адаптивною та ефективною в контексті захисту дітей у кіберпросторі. Вона передбачає створення партнерських альянсів між державними органами, бізнесом, батьками, педагогами, технологічними компаніями та самими дітьми як активними суб'єктами безпеки. Такий підхід забезпечує не лише реалізацію принципу субсидіарності, а й мобілізацію ресурсів, швидку адаптацію до змін, відкритість до інновацій та технологічних рішень.

Водночас концепція rights-based підходу, що орієнтується на пріоритетність прав дитини, дозволяє перейти від декларативного захисту до практичної імплементації правових норм у системі державного управління. Це означає зміну фокусу з «об'єкта захисту» на «суб'єкта політики», з обов'язку – на партнерство, з патерналістського контролю – на підтримку та самореалізацію дитини. Синтезований із цим, дитиноцентричний підхід сприяє формуванню нової етичної парадигми в управлінні, де основними критеріями ефективності виступають не лише результати, а й процеси участі, довіри, інклюзії та рівного доступу до цифрового середовища.

Також акцент зроблено на інтеграційно-мультисекторальному підході, який дозволяє узгодити цілі та інструменти політики між секторами – освітою, охороною здоров'я, соціальним захистом, цифровою трансформацією, юстицією тощо. У такому контексті захист дитини перестає бути компетенцією лише окремого органу влади, а набуває ознак єдиного публічного політичного проєкту на національному рівні. Теорія раціонального вибору та управлінських рішень надала методологічну рамку для аналізу ефективності управлінських моделей, їх адаптивності до змін, здатності реагувати на ризики й обирати оптимальні механізми реалізації політик у сфері цифрової безпеки дітей.

У другому розділі **«Аналіз стану реалізації державної політики захисту дітей у кіберпросторі в Україні»** здійснено комплексний аналіз загроз дітям у кіберпросторі та їхній вплив на безпеку дитини; оцінено особливості функціонування інституційного та правового забезпечення захисту дітей у кіберпросторі; визначено особливості реалізації політики захисту дітей у кіберпросторі: проблеми та виклики.

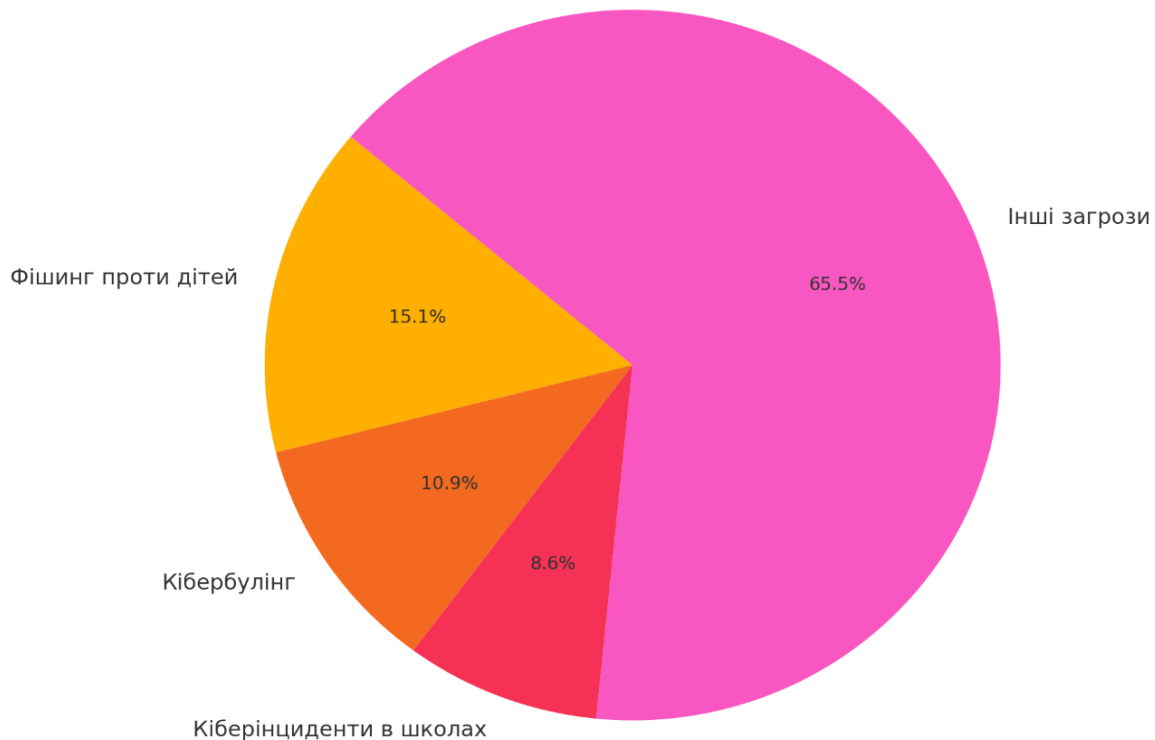
У результаті всебічного аналізу встановлено, що сучасне цифрове середовище створює як унікальні можливості для розвитку дитини, так і безпрецедентні загрози її безпеці, здоров'ю, правам та гідності. Українські діти – як повноцінні учасники онлайн-простору – зазнають зростаючого впливу таких кіберзагроз, як кібербулінг, онлайн-грумінг, сексуальна експлуатація, поширення шкідливого контенту, цифрова залежність, дезінформація та маніпуляції свідомістю. Окрім цього, в умовах повномасштабної війни проти України загрози у кіберпросторі набули ще більшого масштабу та складності, зокрема через використання інформаційних атак агресором для деморалізації населення, вербування неповнолітніх, поширення паніки чи проросійських наративів (рис.1).

Класифікація загроз захисту дітей у кіберпросторі, засвідчила, що їх природа є багатоплосковою: технічною, соціальною, психологічною та політичною. Відповідно, і їхній вплив на дитину є багатовимірним: від порушення приватності й емоційного благополуччя до загроз для фізичної безпеки, розвитку чи навіть життя. Найбільше страждають діти з вразливих груп – ті, хто знаходиться в евакуації, в окупації, без батьківського нагляду або з особливими освітніми потребами. У такому контексті надзвичайно важливою є комплексна державна політика, що поєднує технологічні рішення, правове регулювання, інституційні механізми, а також профілактичну й освітню роботу.

На тепловій карті зображено зміну інтенсивності основних типів кіберзагроз для дітей за період з 2021 по 2024 рік. Візуалізація дозволяє побачити, які загрози ставали все більш поширеними, та порівняти темпи їх зростання між собою (рис.2).

Усі три категорії – фішинг, кібербулінг та інциденти в школах – демонструють стійке зростання за чотири роки. Найбільш інтенсивне зростання спостерігається у 2024 році, що може бути пов'язане з активізацією кіберзлочинців, зростанням онлайн-активності дітей та недостатнім рівнем цифрової грамотності.

Структура кіберзагроз для дітей в Україні у 2024 році

**Рис. 1. Структура кіберзагроз для дітей у 2024 році**

Джерело: Пам'ятка для батьків: «Діти. Інтернет. Мобільний зв'язок». URL: <https://mon.gov.ua/osvita-2/pozashkilna-osvita/vikhovna-robota-ta-zakhist-prav-ditini/bezpeka-ditey-v-interneti/pamyatka-dlya-batkiv-diti-internet-mobilniy-zvyazok>

Аналіз чинної нормативно-правової бази України показав, що в державі вже створено основу для законодавчого забезпечення захисту дітей у кіберпросторі— це, зокрема, Закон України «Про охорону дитинства», Закон «Про основні засади забезпечення кібербезпеки України», Національна стратегія захисту дітей у кіберпросторі та інші акти. Проте на практиці законодавство не забезпечує належної реалізації через відсутність конкретних механізмів впровадження, міжвідомчої координації, чітко визначених відповідальних органів та стабільного фінансування відповідних програм.

Інституційна система захисту дітей у кіберпросторі має фрагментарний характер. Повноваження розпорошені між МОН, Мінцифрою, кіберполіцією, соціальними службами, освітніми закладами, громадськими організаціями, проте відсутній єдиний координаційний центр або національна структура, яка б забезпечувала системний підхід. Водночас практика низки країн (зокрема Польщі, Естонії, Південної Кореї) демонструє ефективність спеціалізованих державних агенцій або центрів, які займаються винятково захистом прав дітей у кіберпросторі, проводять моніторинг, координують міжвідомчі дії та розробляють рекомендації для освітян, батьків і технологічних компаній.

Окремо були виокремлені проблеми реалізації політики в Україні: брак системної профілактики, відсутність цифрової просвіти у школах, низький рівень технологічного захисту освітнього середовища, неузгодженість дій у випадках кіберінцидентів, а також відсутність ефективного моніторингу. Усе це

призводить до ситуації, коли захист дитини у кіберпросторі є переважно декларативним, а діти часто залишаються сам на сам із загрозами, не маючи ані необхідних знань, ані ефективної підтримки.

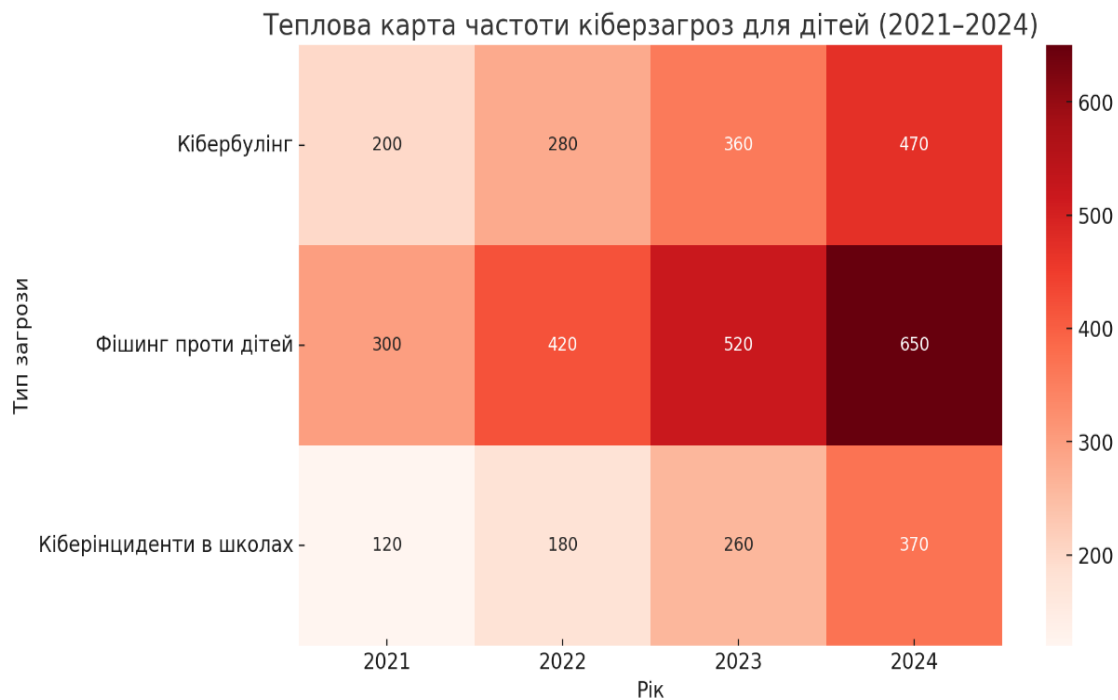


Рис. 2. Частота кіберзагроз для дітей (2021–2024)

Джерело: Пам'ятка для батьків: «Діти. Інтернет. Мобільний зв'язок». URL: <https://mon.gov.ua/osvita-2/pozashkilna-osvita/vikhovna-robota-ta-zakhist-prav-ditini/bezpeka-ditey-v-interneti/pamyatka-dlya-batkiv-diti-internet-mobilniy-zvyazok>

Проблеми значно загострюються в умовах війни, коли багато інституцій втратили або обмежили свою функціональність, а навантаження на цифрові канали комунікації лише зростає. Відсутність спеціалізованих платформ реагування, недостатня кількість кваліфікованих кадрів у сфері кібербезпеки, слабкий захист критичної інфраструктури та цифрових систем освіти – усе це робить систему вразливою до атак і збоїв.

Загалом, державна політика у сфері цифрового захисту дітей в Україні потребує перезавантаження та системної модернізації. Необхідно створити цілісну модель з чіткою координацією, закріпленням відповідальності, широким залученням стейкхолдерів – зокрема ІТ-бізнесу, громадянського суспільства, міжнародних партнерів. Також потрібна розробка нових підходів до моніторингу, впровадження пілотних проєктів, навчання фахівців, адаптація освітнього контенту до цифрової реальності.

Отже, лише поєднання законодавчих ініціатив, технологічних рішень, освітніх програм і міжсекторальної співпраці дозволить створити ефективну, стійку і справді гуманну систему захисту дітей у кіберпросторі – таку, що буде здатна адекватно реагувати не лише на сучасні загрози, але й на виклики майбутнього.

У третьому розділі **«Шляхи вдосконалення державної політики захисту дітей у кіберпросторі в контексті гуманітарної безпеки»** розроблено стратегічні пріоритети державної політики захисту дітей у кіберпросторі; обґрунтовано особливості імплементації ефективних механізмів попередження та реагування на кіберзагрози; сформовано комплекс практичних рекомендацій щодо цифрової трансформації державної політики у сфері захисту дітей.

Запропоновано стратегічні орієнтири трансформації політики державного захисту дітей у цифровому просторі, які охоплюють пріоритетні напрями: запобігання загрозам і підвищення цифрової грамотності; розвиток технологічної інфраструктури кіберзахисту; вдосконалення інституційної взаємодії; підвищення кваліфікації фахівців; залучення дітей до процесів вироблення політики. Окрему увагу приділено важливості формування цифрової культури безпеки на національному рівні, що передбачає включення безпекової тематики до освітніх програм усіх рівнів та підтримку медіаосвітніх ініціатив.

Розроблено концептуальні засади цифрової трансформації державної політики у сфері захисту дітей, що базуються на принципах сервісної орієнтації, міжвідомчої інтеграції, відкритості, використання великих даних (Big Data), інтелектуальних аналітичних систем та інклюзивності цифрових послуг. У цьому контексті обґрунтовано потребу у створенні єдиної національної платформи моніторингу та реагування на цифрові загрози дітям із залученням інструментів штучного інтелекту та автоматизованих систем фільтрації.

Запропоновано модель системи раннього попередження та реагування на кіберінциденти, яка включає компоненти виявлення, верифікації, фіксації, реагування та реабілітації. Вона орієнтована на мінімізацію часових лагів між виявленням загрози та реагуванням, інтеграцію даних між структурами освіти, кіберполіції, соціальних служб, НУО та технічних провайдерів. Висвітлено також роль громадянського суспільства, батьківських спільнот, та ІТ-бізнесу в оперативній реалізації заходів захисту. Запропоновано розгортання національної цифрової інфраструктури захисту дітей, з визначенням відповідальних інституцій, функціональних завдань, індикаторів оцінки ефективності та етапів реалізації. Таблична модель дозволяє систематизувати заходи в логіці «ціль – завдання – інструменти – виконавці – результат», що є основою для розробки програмно-цільових стратегій на національному та регіональному рівнях (табл. 2).

Доведено, що успішність державної політики у сфері цифрового захисту дітей безпосередньо залежить від наукового супроводження, міждисциплінарних досліджень, впровадження систем моніторингу ефективності, а також використання актуальної емпіричної бази (опитувань, кейс-аналізів, даних кіберінцидентів).

Таблиця 2

**Комплексна модель цифрової інфраструктури захисту дітей:
компоненти, функції, індикатори ефективності, відповідальні інституції**

№	Назва компоненту цифрової інфраструктури	Основна функція	Індикатори оцінки ефективності	Відповідальні інституції
1	Єдина національна платформа захисту дітей в інтернеті	Централізація інформації, координація дій, надання інструментів захисту	Кількість відвідувань, звернень, інтегрованих сервісів	Міністерство цифрової трансформації, Уповноважений Президента з прав дитини, МОН
2	Система штучного інтелекту для моніторингу онлайн-загроз	Виявлення шкідливого контенту, агресивних дій, потенційного кібербулінгу	Кількість виявлених загроз, точність, оперативність	Служба безпеки України, Кіберполіція, Державна служба спеціального зв'язку
3	Онлайн-чат-боти допомоги для дітей та батьків	Консультації в режимі 24/7 з правових, психологічних, цифрових питань	Кількість консультацій, позитивні оцінки, повторні звернення	Національна психологічна служба, Кіберполіція, НГО
4	Цифрові інструменти фільтрації контенту	Блокування порнографічного, насильницького, шахрайського контенту	Частка заблокованих ресурсів, охоплення шкіл, активність користувачів	Міністерство освіти і науки, провайдери інтернету, ІТ-компанії
5	Цілодобове кіберпатрулювання	Виявлення та реагування на кіберінциденти, залучення до відповідальності	Кількість порушень, швидкість реагування, зниження повторних випадків	Кіберполіція, Міністерство внутрішніх справ
6	Реєстр кіберінцидентів щодо дітей	Статистичний облік, аналітика інцидентів, прогнозування ризиків	Повнота даних, кількість кейсів, інтеграція з політикою	Національна поліція, Уповноважений з прав дитини, Центр громадського здоров'я
7	Освітньо-комунікаційна платформа для шкіл	Навчальні матеріали, тренінги з цифрової безпеки, тестування знань	Кількість шкіл, кількість пройдених курсів, результати опитувань	Міністерство освіти і науки, Інститут модернізації змісту освіти
8	Центр взаємодії з соцмережами та платформами	Оперативне реагування на скарги, видалення контенту, блокування	Кількість запитів, успішних видалень, час реагування	Кіберполіція, Національний центр кібербезпеки, приватні ІТ-компанії
9	Система попередження для батьків	Автоматичне сповіщення про ризики в цифровій поведінці дітей	Кількість повідомлень, рівень довіри, запобігання інцидентам	Мобільні оператори, розробники мобільного ПЗ, НЦК
10	Національна аналітична лабораторія цифрової безпеки дітей	Дослідження, формування рекомендацій, розробка стандартів	Кількість звітів, наукові публікації, вплив на політику	Академія педагогічних наук, Інститут кібербезпеки, НАН України

Джерело: побудовано автором

Таким чином, на основі узагальнених результатів сформовано науково обґрунтовану пропозицію щодо створення цілісної моделі державної політики цифровою безпекою дітей, що поєднує профілактичні, регуляторні, інституційні та технологічні компоненти в рамках сучасної гуманітарної парадигми безпеки.

ВИСНОВКИ

У дисертаційній роботі здійснено теоретичне узагальнення та запропоновано авторський підхід до розв'язання важливої наукової проблеми, що полягає у розробці теоретико-методологічних та практичних засад удосконалення державної політики захисту дітей у кіберпросторі в умовах сучасних викликів гуманітарної безпеки. Отримані результати проведеного дисертаційного дослідження дозволяють сформулювати такі висновки та пропозиції:

1. Розкрито теоретико-концептуальні засади формування державної політики захисту дітей у кіберпросторі. Обґрунтовано, що цифрове середовище є не лише засобом розвитку дитини, а й джерелом нових типів ризиків, що актуалізують гуманітарні виклики. Запропоновано авторське визначення державної політики захисту дітей у кіберпросторі як комплексної, міжгалузевої, ризик-орієнтованої діяльності публічної влади, спрямованої на нейтралізацію цифрових загроз через поєднання нормативно-правових, інституційних, освітньо-комунікаційних і технологічних механізмів. Наголошено на необхідності трансформації моделі державної політики: від фрагментарного реагування до системної профілактики кіберризиків з урахуванням принципів дитиноцентризму, інклюзії та діджитал-гуманізму.

2. Систематизовано типологію кіберзагроз для дітей та проаналізовано їхній вплив на ключові сфери безпеки дитини. Доведено, що сучасні загрози (кібербулінг, грумінг, секстинг, шкідливий контент, онлайн-насильство тощо) мають комплексну природу, впливаючи на фізичну, психоемоційну, інформаційну й соціальну безпеку дитини. Визначено основні механізми впливу: інформаційно-психологічне навантаження, цифрове переслідування, емоційна дестабілізація, технічна вразливість. Запропоновано класифікацію кіберзагроз за рівнем ризику, каналами проникнення та характером впливу, що створює підґрунтя для розробки адресної політики протидії.

3. Оцінено сучасний стан реалізації державної політики захисту дітей у цифровому середовищі в Україні. Проаналізовано національну нормативно-правову базу, інституційну спроможність, міжвідомчу взаємодію та наявні практики реагування на цифрові загрози. Встановлено фрагментарність державних ініціатив, брак єдиного координаційного центру, відсутність алгоритмів швидкого реагування, недостатнє врахування інтересів дитини при розробці цифрових регуляторних політик. Виявлено ключові проблеми: нормативна розрізненість, низька цифрова компетентність дорослого оточення дитини, інституційна інертність та слабкий рівень цифрової інфраструктури на місцевому рівні.

4. Проведено порівняльний аналіз зарубіжного досвіду стратегій та практик захисту дітей у кіберпросторі. Досліджено підходи країн ЄС, США, Канади, Скандинавських країн, Японії, Південної Кореї щодо формування національних стратегій, впровадження інноваційних моделей захисту (інтернет-омбудсмени, кіберпатрулі, онлайн-центри допомоги дітям, алгоритми модерації

контенту). Зроблено висновок, що найбільш ефективними є політики, які поєднують дитиноцентричність, цифрову інклюзію, превентивну освіту та технологічне реагування. Обґрунтовано можливість адаптації окремих практик з урахуванням національного правового та культурного контексту.

5. Обґрунтовано стратегічні пріоритети державної політики цифрової безпеки дітей в Україні. Запропоновано систему ключових орієнтирів: 1) розбудова системи державного моніторингу цифрових ризиків; 2) впровадження безпечного цифрового освітнього середовища; 3) розвиток цифрової грамотності всіх учасників освітнього процесу; 4) формування інституту цифрової довіри через залучення ІТ-бізнесу до публічно-приватного партнерства; 5) правове регулювання онлайн-платформ та змісту, доступного дітям; 6) підтримка сімей у цифровій адаптації. Акцент зроблено на пріоритеті прав дитини, міжсекторальній співпраці та технологічній інноваційності.

6. Сформульовано концептуальні засади цифрової трансформації державної політики захисту дітей. Аргументовано необхідність переходу до моделі інтегрованого цифрового управління, що передбачає створення єдиної платформи взаємодії всіх суб'єктів системи захисту дітей (освіта, охорона здоров'я, юстиція, поліція, соціальні служби). Запропоновано інституційні й технічні рішення щодо інтеграції державних реєстрів, запровадження цифрового кабінету дитини, створення автоматизованих систем виявлення загроз. Окреслено напрямки розвитку електронних сервісів і цифрових протоколів реагування, що забезпечують індивідуалізований, оперативний та прозорий захист.

7. Обґрунтовано модель національної цифрової інфраструктури захисту дітей у кіберпросторі. Розроблено концептуальну архітектуру цифрової інфраструктури, що охоплює: технологічну (штучний інтелект, Big Data, системи кіберпатрулювання), організаційну (Національний центр кібербезпеки дітей, регіональні підрозділи, гарячі лінії), комунікаційну (платформи цифрової підтримки, чат-боти, онлайн-консультації) та освітню (курси з цифрової гігієни, тренінги для вчителів і батьків) складові. Зроблено висновок, що лише синергія технологій, міжвідомчої координації та цифрової просвіти дозволить забезпечити стійкий захист дитини в умовах швидкоплинного цифрового середовища.

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Праці, які відображають основні наукові результати дисертації

Публікації у наукових фахових виданнях України з державного управління

1. Димитрієва О. І. Комунікаційні стратегії держави у сфері захисту дітей від цифрових загроз. *Держава та регіони*. 2022. № 2 (76). С.162-166 (0,5 друк. арк.).

2. Димитрієва О. І. Застосування технологічних інструментів у державному управлінні кібербезпекою дітей. *Держава та регіони*. 2023. №1(79). С. 180-185. (0,5 друк. арк.).

3. Димитрієва О.І. Механізми запобігання кіберзагрозам для дітей у системі гуманітарної безпеки України. *Право та державне управління*. 2023. №1. С. 426-431. (0,5 друк. арк.).

4. Димитрієва О.І. Нормативно-правове забезпечення кіберзахисту дітей в Україні. *Право та державне управління*. 2021. №2. С. 353-358. (0,5 друк. арк.).

5. Димитрієва О.І. Організаційно-функціональна модель державного управління кібербезпекою дітей. *Право та державне управління*. 2021. №4. С. 207-302. (0,5 друк. арк.).

6. Димитрієва О.І. Методичні підходи до оцінки ефективності державної політики щодо захисту дітей у цифровому середовищі. *Вчені записки Таврійського національного університету імені В. І. Вернадського*. 2023. Том 34 (73) №2. С.164-172. (0,5 друк. арк.).

Публікації в наукових виданнях іноземних держав за напрямом, з якого підготовлено дисертацію:

7. Dymytriieva Oksana State management of child protection in cyberspace: current challenges and prospects. *Global Prosperity*, 2023. 3(1). URL: <https://gprosperity.org/index.php/journal/article/view/173> (0,5 друк. арк.).

Праці, які засвідчують апробацію матеріалів дисертації

8. Димитрієва О.І. Міжнародний досвід державного управління кібербезпекою дітей. Збірник міжнародної науково-практичної конференції «Розвиток української держави в умовах активізації євроінтеграційних процесів». (Київ 19 лютого 2016 р.). МАУП, Київ. С.171-172 (0,2 друк. арк.).

9. Димитрієва О.І. Роль громадянського суспільства та приватного сектору у забезпеченні кібербезпеки дітей. Збірник Міжнародної науково-практичної конференції «Актуальні проблеми теорії держави і права» (28 березня 2018 року). Київ, 2018. С. 100-101. (0,2 друк. арк.).

10. Димитрієва О.І. Формування цифрової грамотності як елемента державної політики кіберзахисту дітей. Збірник Всеукраїнської науково-практичної конференції «Актуальні проблеми розвитку правової держави і громадянського суспільства» (28 березня 2017 року). Київ, 2017. С. 128-129.

11. Димитрієва О.І. Інформаційно-аналітичні системи моніторингу кіберзагроз у державному управлінні. Збірник V міжнародної науково-практичної конференції «Роль юриспруденції у формуванні сучасного суспільства». (Київ 6 жовтня 2017 р.). МАУП, Київ. С.174-175. (0,2 друк. арк.).

12. Димитрієва О.І. Кібербулінг як загроза гуманітарній безпеці: державна політика запобігання та реагування. Науково-практична конференція «Актуальні питання цивільного права та права інтелектуальної власності». (Київ 23 листопада 2015 р.). МАУП, Київ. С.73-74. (0,2 друк. арк.).

АНОТАЦІЯ

Димитрієва О. І. Державна політика захисту дітей у кіберпросторі як пріоритет гуманітарної безпеки України. – Рукопис.

Дисертація на здобуття наукового ступеня кандидата наук з державного управління за спеціальністю 25.00.05 – державне управління у сфері державної безпеки та охорони громадського порядку. – Державний університет «Житомирська політехніка». – Житомир, 2025.

Дисертація присвячена комплексному дослідженню державної політики захисту дітей у кіберпросторі як пріоритет гуманітарної безпеки України. Сформовано цілісне теоретико-концептуальне підґрунтя для розуміння гуманітарної безпеки як системної категорії, невід’ємної від архітекτονіки національної безпеки України.

Здійснено уточнення дефініції гуманітарної безпеки, яка розглядається не лише як інструмент захисту особистості, а як динамічна, ціннісно зорієнтована підсистема, що покликана забезпечувати стійкий розвиток соціокультурного середовища, захист прав і свобод людини, збереження ідентичності, інтелектуального, освітнього та морального потенціалу населення. Запропоновано модель інтеграції гуманітарної безпеки до системи національної безпеки України, яка враховує виклики цифрової трансформації, гібридних загроз, культурної поляризації та демографічної нестабільності. Здійснено глибокий міждисциплінарний аналіз наукових і прикладних підходів до формування політики державної політики у сфері захисту дітей, що дозволило виявити основні теоретичні моделі, які визначають сучасні орієнтири у цій сфері. Узагальнено й систематизовано такі ключові парадигми: нормативно-правовий, інституційний, governance-підхід, мережеве управління, rights-based підхід, інтеграційний і мультисекторальний підхід, а також теорія управлінських рішень і раціонального вибору. Окреслено, що державне управління цифровою безпекою дітей становить нову дослідницьку категорію, яка формується на перетині кількох ключових сфер – публічного адміністрування, цифрових технологій, прав людини, безпекознавства та гуманітарної безпеки.

Здійснено комплексний аналіз системи державної політики у сфері захисту дітей у кіберпросторі, що дало змогу сформулювати низку науково обґрунтованих положень і висновків, які відображають як теоретичне осмислення проблематики, так і практичні підходи до її вирішення. Визначено, що загрози, які постають перед дітьми у цифровому просторі, мають багатовимірний характер, охоплюючи психологічні, соціальні, правові, технічні та гуманітарні аспекти. Проаналізовано наявну інституційну та нормативно-правову базу в Україні, що регулює захист дітей у кіберпросторі. Встановлено, що вона носить фрагментарний характер, з відсутністю чіткої міжвідомчої координації, дублюванням функцій, недосконалістю процедур моніторингу та реагування. Водночас, зібрано та систематизовано ключові національні акти законодавства, міжнародні зобов’язання України та інституційні механізми, відповідальні за реалізацію політики захисту дітей. Обґрунтовано потребу в

гармонізації українського законодавства із стандартами ЄС та Конвенції Ради Європи про кіберзлочинність.

Запропоновано стратегічні орієнтири трансформації політики державного захисту дітей у цифровому просторі, які охоплюють пріоритетні напрями: запобігання загрозам і підвищення цифрової грамотності; розвиток технологічної інфраструктури кіберзахисту; вдосконалення інституційної взаємодії; підвищення кваліфікації фахівців; залучення дітей до процесів вироблення політики. Особливу увагу приділено важливості формування цифрової культури безпеки на національному рівні, що передбачає включення безпекової тематики до освітніх програм усіх рівнів та підтримку медіаосвітніх ініціатив.

Розроблено концептуальні засади цифрової трансформації державної політики у сфері захисту дітей, що базуються на принципах сервісної орієнтації, міжвідомчої інтеграції, відкритості, використання великих даних (Big Data), інтелектуальних аналітичних систем та інклюзивності цифрових послуг. У цьому контексті обґрунтовано потребу у створенні єдиної національної платформи моніторингу та реагування на цифрові загрози дітям із залученням інструментів штучного інтелекту та автоматизованих систем фільтрації.

Запропоновано модель системи раннього попередження та реагування на кіберінциденти, яка включає компоненти виявлення, верифікації, фіксації, реагування та реабілітації. Вона орієнтована на мінімізацію часових лагів між виявленням загрози та реагуванням, інтеграцію даних між структурами освіти, кіберполіції, соціальних служб, НУО та технічних провайдерів. Висвітлено також роль громадянського суспільства, батьківських спільнот, та ІТ-бізнесу в оперативній реалізації заходів захисту. Запропоновано розгортання національної цифрової інфраструктури захисту дітей, з визначенням відповідальних інституцій, функціональних завдань, індикаторів оцінки ефективності та етапів реалізації. Доведено, що успішність державної політики у сфері цифрового захисту дітей безпосередньо залежить від наукового супроводження, міждисциплінарних досліджень, впровадження систем моніторингу ефективності, а також використання актуальної емпіричної бази (опитувань, кейс-аналізів, даних кіберінцидентів).

Ключові слова: державна політика, державне управління, публічна політика, гуманітарна безпека, цифрова безпека дітей, кіберпростір, кіберзагрози, цифрова трансформація, права дитини, інформаційна безпека.

ANNOTATION

Dmytrieva O. I. State policy of child protection in cyberspace as a priority of humanitarian security of Ukraine. – Manuscript.

Thesis for a PhD degree in Public Administration, specialty 25.00.05 – State administration in the sphere of state security and public order protection. – Zhytomyr Polytechnic State University, Zhytomyr, 2025.

The dissertation is devoted to a comprehensive study of the state policy of child protection in cyberspace as a priority of humanitarian security of Ukraine. A

holistic theoretical and conceptual basis has been formed for understanding humanitarian security as a systemic category, integral to the architectonics of national security of Ukraine.

The definition of humanitarian security has been clarified, which is considered not only as a tool for protecting the individual, but as a dynamic, value-oriented subsystem designed to ensure the sustainable development of the socio-cultural environment, the protection of human rights and freedoms, the preservation of identity, intellectual, educational and moral potential of the population. A model of integration of humanitarian security into the national security system of Ukraine is proposed, which takes into account the challenges of digital transformation, hybrid threats, cultural polarization and demographic instability. A deep interdisciplinary analysis of scientific and applied approaches to the formation of state policy in the field of child protection has been carried out, which has allowed us to identify the main theoretical models that determine modern guidelines in this area. The following key paradigms have been summarized and systematized: regulatory, institutional, governance approach, network management, rights-based approach, integration and multisectoral approach, as well as the theory of managerial decisions and rational choice. It is outlined that state management of children's digital security constitutes a new research category that is formed at the intersection of several key areas – public administration, digital technologies, human rights, security studies and humanitarian security.

A comprehensive analysis of the state policy system in the field of child protection in cyberspace was carried out, which made it possible to formulate a number of scientifically sound provisions and conclusions that reflect both a theoretical understanding of the issue and practical approaches to its solution. It was determined that the threats facing children in digital space are multidimensional, covering psychological, social, legal, technical and humanitarian aspects. The existing institutional and regulatory framework in Ukraine that regulates the protection of children in cyberspace was analyzed. It was established that it is fragmentary, with a lack of clear interdepartmental coordination, duplication of functions, and imperfect monitoring and response procedures. At the same time, key national legislative acts, international obligations of Ukraine and institutional mechanisms responsible for the implementation of child protection policy were collected and systematized. The need for harmonization of Ukrainian legislation with EU standards and the Council of Europe Convention on Cybercrime is substantiated.

Strategic guidelines for the transformation of the state child protection policy in the digital space are proposed, which cover priority areas: prevention of threats and increasing digital literacy; development of technological infrastructure for cyber protection; improvement of institutional interaction; advanced training of specialists; involvement of children in policy-making processes. Special attention is paid to the importance of forming a digital security culture at the national level, which involves the inclusion of security topics in educational programs at all levels and support for media educational initiatives.

Conceptual principles for the digital transformation of state child protection policy are developed, based on the principles of service orientation, interagency integration, openness, use of big data (Big Data), intelligent analytical systems and inclusiveness of digital services. In this context, the need for creating a single national platform for monitoring and responding to digital threats to children is justified, involving artificial intelligence tools and automated filtering systems.

A model of an early warning and response system for cyber incidents is proposed, which includes components of detection, verification, fixation, response and rehabilitation. It is focused on minimizing time lags between threat detection and response, data integration between education structures, cyber police, social services, NGOs and technical providers. The role of civil society, parent communities and IT businesses in the operational implementation of protection measures is also highlighted. The deployment of a national digital infrastructure for child protection is proposed, with the definition of responsible institutions, functional tasks, indicators for assessing effectiveness and implementation stages. It has been proven that the success of state policy in the field of digital child protection directly depends on scientific support, interdisciplinary research, the implementation of efficiency monitoring systems, as well as the use of up-to-date information. empirical base (surveys, case studies, cyber incident data).

Key words: public policy, public administration, public policy, humanitarian security, digital security of children, cyberspace, cyber threats, digital transformation, children's rights, information security.

Формат 60x90 1/16 Папір друкарський.

Друк офсетний Гарнітура Time New Roman.

Ум. друк. арк. 0,9 Тираж 100.

Віддруковано з готових оригіналів-макетів автора
у Державному університеті «Житомирська політехніка» 10005,
Україна, м. Житомир, вул. Чуднівська, 103