

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА»

Кваліфікаційна наукова
праця на правах рукопису

ДИМИТРІЄВА ОКСАНА ІГОРІВНА

УДК 351

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

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

Подається на здобуття наукового ступеня
кандидата наук з державного управління

Дисертація містить результати власних досліджень. Використання ідей,
результатів і текстів інших авторів мають посилання на відповідне джерело

_____ О. І. Димитрієва

Науковий керівник:
Шпак Юрій Валерійович
доктор наук з державного управління, доцент

Житомир – 2025

АНОТАЦІЯ

Димитрієва О.І. Державна політика захисту дітей у кіберпросторі як пріоритет гуманітарної безпеки України. – Кваліфікаційна наукова праця на правах рукопису.

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.

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.

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, ІТ-сферою та міжнародними організаціями [4, 20, 54].

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 межах дослідження було чітко 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. Це зумовлює не лише багатогранність об'єкта дослідження, а й потребу у формуванні інноваційного міждисциплінарного концепту, який би включав у себе такі складові: суб'єктно-об'єктну взаємодію, що передбачає включення дитини не лише як об'єкта захисту, а як активного учасника процесу цифрової взаємодії та користувача цифрових послуг; нормативно-ціннісні орієнтири, які визначають пріоритетність прав дитини в цифровій політиці; цифрові інструменти управління, включаючи електронне урядування, алгоритмічне регулювання, кіберінфраструктурні механізми; механізми контролю та моніторингу загроз, що базуються на сучасних аналітичних, правових та технічних засобах оцінки ризиків.

Проведена міждисциплінарна декомпозиція цього концепту дозволила обґрунтувати необхідність інтеграції знань і підходів із таких галузей, як кібербезпека (захист від технічних та інформаційних загроз), педагогіка (формування цифрової компетентності дітей), соціологія дитинства (вивчення поведінкових патернів у кіберпросторі), психологія (оцінка емоційного та ментального впливу цифрових технологій), інформаційне право (правове регулювання даних, приватності та прав дітей), а також цифрове врядування (архітектура управління цифровими процесами на макро- та мезорівнях). Такий міждисциплінарний підхід забезпечує не лише глибше розуміння об'єкта дослідження, але й сприяє формуванню ефективних, адаптивних та сталих управлінських рішень у сфері цифрової безпеки дітей.

У процесі дослідження було виокремлено методологічні основи, які забезпечують наукову обґрунтованість і цілісність підходу до аналізу та моделювання управлінських рішень у цій сфері. До таких підходів, зокрема, віднесено: системний підхід, що дає змогу бачити цифрову безпеку дітей у

контексті єдиної системи національної безпеки; структурно-функціональний підхід, який акцентує увагу на взаємозв'язках між суб'єктами, функціях і ролях державних інституцій; компаративний підхід, що дозволяє порівнювати національні і міжнародні практики; прогностичний підхід, орієнтований на визначення майбутніх викликів і розробку превентивних стратегій. Застосування цих підходів у сукупності забезпечує всебічне й гнучке дослідження, адаптоване до стрімких трансформацій цифрового середовища.

У результаті всебічного аналізу було 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.

Класифікація загроз, проведена у розділі, засвідчила, що їх природа є багатоспоровою: 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.

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.

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 межах проведеного дослідження 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. Ці загрози включають кібербулінг, сексуальну експлуатацію, деструктивний контент, втручання в приватність, ігрову залежність, а також використання персональних даних дітей у зловмисних цілях. Такий комплексний підхід дав змогу розробити класифікацію загроз з урахуванням вікових, поведінкових та соціокультурних особливостей дітей, а також визначити ключові наслідки кожного з типів впливу.

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 IT-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.

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). 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.

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

ABSTRACT

Dymytrieva O.I. State policy of child protection in cyberspace as a priority of humanitarian security of Ukraine. – Qualification scientific work in the form of a manuscript.

Thesis for a PhD degree in Public Administration, specialty 25.00.02 – Mechanisms of the Public Administration. – Zhytomyr Polytechnic State University, Zhytomyr, 2025.

As a result of the research, a holistic theoretical and conceptual basis was formed for understanding humanitarian security as a systemic category, integral to the architectonics of national security of Ukraine. The definition of humanitarian security was 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. In this context, humanitarian security was conceptualized as a multi-vector and multi-level category that is integrated into the political-legal, educational-cultural, socio-informational and demographic spaces of national security.

Thanks to a comprehensive interdisciplinary approach, the structure of humanitarian security was clarified, which includes the following key components: cultural-value, which ensures the preservation of cultural heritage, national identity

and the formation of stable social guidelines; educational and intellectual, which guarantees access to quality education, the development of critical thinking, digital literacy and human capital; information and communication, which regulates safe interaction in the information environment, protection from disinformation, manipulation and cyber threats; legal, which forms legal safeguards and mechanisms for the implementation of human rights in the humanitarian space; psychological and behavioral, which is related to the security of the mental and emotional state of the individual, in particular in conditions of military, information and digital threats; socio-demographic, aimed at maintaining the stability and viability of society through the formation of a safe environment for the development of children, youth, vulnerable groups of the population.

Special attention is paid to the definition of children's digital security as a priority area of humanitarian security, which is critical for the long-term stability of society. This direction is considered not only through the prism of threats, but also as a condition for ensuring future national development - taking into account technological, social, mental and institutional determinants. The thesis is formulated on the need to consider the child as both an object and a subject of the state policy of digital security, which involves strengthening their participation, awareness and digital capabilities.

Based on the analysis, 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. This model reflects the need for a new humanitarian paradigm aimed at forming a safe educational and information environment, developing critical digital thinking, ethical self-awareness and institutional protection of the rights of the child.

A deep interdisciplinary analysis of scientific and applied approaches to the formation of state administration policy in the field of child protection was carried out, which allowed us to identify the main theoretical models that determine modern guidelines in this area. The following key paradigms are summarized and systematized: regulatory, institutional, governance approach, network management,

rights-based approach, integration and multisectoral approach, as well as the theory of management decisions and rational choice.

The regulatory approach made it possible to substantiate the importance of a clear legislative basis as a frame that sets the boundaries of state policy in the field of child protection. However, it is in combination with the institutional approach that the multidimensional role of institutions - formal and informal - in the implementation of state regulation is revealed, especially in the digital environment. Governance and network models turned out to be the most relevant to modern conditions, since they allow us to see management not as a hierarchical vertical, but as an interactive and flexible system of interaction between various stakeholders - the state, civil society, family, educational institutions, IT-sphere and international organizations [4, 20, 54].

The study pays special attention to the network approach, which is gaining special significance in the context of digital transformation. It was established that this management model is the most adaptive and effective in the context of protecting children in the digital environment. It involves the creation of partnership alliances between government agencies, business, parents, teachers, technology companies and children themselves as active security actors. This approach ensures not only the implementation of the principle of subsidiarity, but also the mobilization of resources, rapid adaptation to changes, openness to innovations and technological solutions. At the same time, the concept of a rights-based approach, which focuses on the priority of children's rights, allows us to move from declarative protection to the practical implementation of legal norms in the public administration system. This means a change of focus from the "object of protection" to the "subject of policy", from duty to partnership, from paternalistic control to support and self-realization child protection. Synthesized with this, the child-centered approach contributes to the formation of a new ethical paradigm in management, where the main criteria for effectiveness are not only results, but also processes of participation, trust, inclusion and equal access to the digital environment.

The emphasis is also placed on an integrative and multi-sectoral approach, which allows for the coordination of policy goals and instruments between sectors - education, healthcare, social protection, digital transformation, justice, etc. In such a

context, child protection ceases to be the competence of only a separate authority, but acquires the features of a single public political project at the national level. The theory of rational choice and management decisions has provided a methodological framework for analyzing the effectiveness of management models, their adaptability to changes, the ability to respond to risks and choose the optimal mechanisms for implementing policies in the field of digital safety for children.

The study clearly outlined that state management of children's digital security constitutes a new research category that is being formed at the intersection of several key areas - public administration, digital technologies, human rights, security studies and humanitarian security. This determines not only the multifaceted nature of the research object, but also the need to form an innovative interdisciplinary concept that would include the following components: subject-object interaction, which involves the inclusion of the child not only as an object of protection, but also as an active participant in the process of digital interaction and a user of digital services; normative and value guidelines that determine the priority of children's rights in digital policy; digital management tools, including e-government, algorithmic regulation, cyber infrastructure mechanisms; mechanisms for controlling and monitoring threats based on modern analytical, legal and technical means of risk assessment.

The interdisciplinary decomposition of this concept made it possible to substantiate the need to integrate knowledge and approaches from such areas as cybersecurity (protection against technical and information threats), pedagogy (formation of children's digital competence), sociology of childhood (study of behavioral patterns in the digital environment), psychology (assessment of the emotional and mental impact of digital technologies), information law (legal regulation of data, privacy and children's rights), as well as digital governance (architecture of digital process management at macro and meso levels). Such an interdisciplinary approach provides not only a deeper understanding of the object of research, but also contributes to the formation of effective, adaptive and sustainable management decisions in the field of children's digital safety.

In the process of research, methodological foundations were identified that ensure the scientific validity and integrity of the approach to the analysis and modeling of management decisions in this area. Such approaches include, in particular: a systemic approach that allows us to see children's digital safety in the context of a unified national security system; a structural-functional approach that focuses on the relationships between actors, functions and roles of state institutions; a comparative approach that allows us to compare national and international practices; a prognostic approach focused on identifying future challenges and developing preventive strategies. The use of these approaches in combination provides a comprehensive and flexible study adapted to the rapid transformations of the digital environment. As a result of a comprehensive analysis, it was found that the modern digital environment creates both unique opportunities for the development of the child and unprecedented threats to his safety, health, rights and dignity. Ukrainian children – as full participants in the online space – are increasingly exposed to cyber threats such as cyberbullying, online grooming, sexual exploitation, the spread of harmful content, digital addiction, disinformation and mind manipulation. In addition, in the context of a full-scale war against Ukraine, threats in cyberspace have become even more widespread and complex, in particular through the use of information attacks by the aggressor to demoralize the population, recruit minors, spread panic or pro-Russian narratives.

The classification of threats carried out in the section showed that their nature is multi-layered: technical, social, psychological and political. Accordingly, their impact on the child is multidimensional: from violation of privacy and emotional well-being to threats to physical safety, development or even life. Children from vulnerable groups suffer the most – those who are evacuated, under occupation, without parental supervision or with special educational needs. In this context, a comprehensive state policy that combines technological solutions, legal regulation, institutional mechanisms, as well as preventive and educational work is extremely important.

An analysis of the current regulatory framework of Ukraine has shown that the state has already created a basis for legislative support for the protection of children

in the digital environment –this includes, in particular, the Law of Ukraine "On the Protection of Childhood", the Law "On the Basic Principles of Ensuring Cybersecurity in Ukraine", the National Strategy for the Protection of Children in the Digital Environment and other acts. However, in practice, the legislation does not ensure proper implementation due to the lack of specific implementation mechanisms, interagency coordination, clearly defined responsible bodies and stable financing of relevant programs.

The institutional system for the protection of children in the digital environment is fragmented. Powers are dispersed between the Ministry of Education and Science, the Ministry of Digital, cyber police, social services, educational institutions, and public organizations, but there is no single coordination center or national structure that would ensure a systematic approach. At the same time, the practice of a number of countries (in particular, Poland, Estonia, South Korea) demonstrates the effectiveness of specialized state agencies or centers that are exclusively engaged in the protection of children's rights in the digital environment, conduct monitoring, coordinate interagency actions and develop recommendations for educators, parents and technology companies.

The following problems of policy implementation in Ukraine were separately identified: lack of systematic prevention, lack of digital literacy in schools, low level of technological protection of the educational environment, lack of coordination of actions in cases of cyber incidents, as well as lack of effective monitoring. All this leads to a situation where child protection in the digital space is mainly declarative, and children are often left alone with threats, having neither the necessary knowledge nor effective support.

The problems are significantly exacerbated in war conditions, when many institutions have lost or limited their functionality, and the load on digital communication channels is only increasing. The lack of specialized response platforms, insufficient number of qualified personnel in the field of cybersecurity, weak protection of critical infrastructure and digital education systems - all this makes the system vulnerable to attacks and failures.

In general, the state policy in the field of digital protection of children in Ukraine needs a reboot and systemic modernization. It is necessary to create a holistic model with clear coordination, consolidation of responsibility, broad involvement of stakeholders - in particular, IT business, civil society, international partners. It is also necessary to develop new approaches to monitoring, implement pilot projects, train specialists, adapt educational content to digital reality.

Therefore, only a combination of legislative initiatives, technological solutions, educational programs and intersectoral cooperation will allow creating an effective, sustainable and truly humane system for protecting children in cyberspace - one that will be able to adequately respond not only to current threats, but also to the challenges of the future.

As part of the study, a comprehensive analysis of the state administration system in the field of protecting children in the digital environment 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 problem and practical approaches to its solution. It was determined that the threats facing children in the digital space are multidimensional, covering psychological, social, legal, technical and humanitarian aspects. These threats include cyberbullying, sexual exploitation, destructive content, privacy invasion, gaming addiction, and the use of children's personal data for malicious purposes. Such a comprehensive approach made it possible to develop a classification of threats taking into account the age, behavioral and socio-cultural characteristics of children, as well as to identify the key consequences of each type of impact.

The existing institutional and regulatory framework in Ukraine regulating the protection of children in the digital environment was analyzed. It was found that it is fragmented, 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 have been collected and systematized. The need for harmonization of Ukrainian legislation with

EU standards and the Council of Europe Convention on Cybercrime has been substantiated.

Strategic guidelines for the transformation of the state child protection policy in the digital space have been proposed, which cover priority areas: prevention of threats and increasing digital literacy; development of technological infrastructure of cyber protection; improvement of institutional interaction; advanced training of specialists; involvement of children in policy-making processes. Special attention has been 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 administration in the field of child protection have been developed, based on the principles of service orientation, interdepartmental integration, openness, use the emergence 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 with the involvement of artificial intelligence tools and automated filtering systems is justified.

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. The tabular model allows you to systematize measures in the logic of "goal - task - tools - performers - result", which is the basis for the development of program-targeted strategies at the national and regional levels. 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

the current empirical base (surveys, case studies, cyber incident data). Thus, based on the generalized results, a scientifically substantiated proposal has been formed to create a holistic model of state management of children's digital safety, combining preventive, regulatory, institutional and technological components within the framework of the modern humanitarian security paradigm.

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

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 засідчують 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.).

ЗМІСТ

Вступ	21
РОЗДІЛ 1. ТЕОРЕТИКО-КОНЦЕПТУАЛЬНІ ЗАСАДИ ЗАХИСТУ ДІТЕЙ У КІБЕРПРОСТОРІ ЯК КОМПОНЕНТА ГУМАНІТАРНОЇ БЕЗПЕКИ	28
1.1. Поняття, сутність та структура гуманітарної безпеки в системі національної безпеки України	28
1.2. Теоретичні підходи до формування державної політики захисту дітей	53
1.3. Концептуальні засади дослідження державної політики у сфері цифрової безпеки дітей	77
Висновки до розділу 1	90
РОЗДІЛ 2. АНАЛІЗ СТАНУ РЕАЛІЗАЦІЇ ДЕРЖАВНОЇ ПОЛІТИКИ ЗАХИСТУ ДІТЕЙ У КІБЕРПРОСТОРІ В УКРАЇНІ	95
2.1. Сучасні загрози дітям у кіберпросторі та їх вплив на безпеку дитини	95
2.2. Аналіз інституційного та правового забезпечення захисту дітей у кіберпросторі	114
2.3. Практика реалізації державної політики захисту дітей у кіберпросторі	133
Висновки до розділу 2	148
РОЗДІЛ 3. ШЛЯХИ ВДОСКОНАЛЕННЯ ДЕРЖАВНОЇ ПОЛІТИКИ ЗАХИСТУ ДІТЕЙ У КІБЕРПРОСТОРІ В КОНТЕКСТІ ГУМАНІТАРНОЇ БЕЗПЕКИ	151
3.1. Стратегічні пріоритети державної політики захисту дітей у кіберпросторі	151
3.2. Запровадження ефективних механізмів попередження та реагування на кіберзагрози	170
3.3. Цифрова трансформація державної політики у сфері захисту дітей	189
Висновки до розділу 3	201
ВИСНОВКИ	204
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ	207
ДОДАТКИ	220

ВСТУП

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. Коломоєць, 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;

- напрями 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.

РОЗДІЛ 1. ТЕОРЕТИКО-КОНЦЕПТУАЛЬНІ ЗАСАДИ ЗАХИСТУ ДІТЕЙ У КІБЕРПРОСТОРІ ЯК КОМПОНЕНТА ГУМАНІТАРНОЇ БЕЗПЕКИ

1.1. Поняття, сутність та структура гуманітарної безпеки в системі національної безпеки України

У сучасному глобалізованому світі, який стрімко трансформується під впливом інформаційно-комунікаційних технологій, цифровізації, гібридних загроз та широкомасштабної війни, поняття безпеки набуває нового змісту та розширюється за межі традиційно військово-політичного трактування. Особливої актуальності набуває гуманітарна безпека як ключовий компонент національної безпеки, що безпосередньо стосується захисту прав людини, збереження культурної ідентичності, забезпечення доступу до якісної освіти, інформації, духовних цінностей, а також формування стійкої до зовнішніх впливів соціогуманітарної сфери.

З огляду на безпрецедентні виклики, з якими стикається Україна – збройна агресія, масове переміщення населення, руйнування інфраструктури, кібератаки на інформаційний простір, цифрова залежність дітей і молоді, поширення фейкових наративів та маніпуляцій у соціальних мережах – питання гуманітарної безпеки постає як надзвичайно актуальне. Гуманітарна сфера дедалі частіше стає ціллю ворожих інформаційно-психологічних операцій, що мають на меті дестабілізувати суспільство, посіяти недовіру до інституцій держави, зруйнувати національну ідентичність, вплинути на свідомість молодого покоління. Саме тому аналіз концепту гуманітарної безпеки, її сутності, ролі та структури є необхідним методологічним етапом дослідження ефективного державної політики у сфері захисту вразливих груп, передусім – дітей, у кіберпросторі.

Особливо важливо в цьому контексті розглядати гуманітарну безпеку не лише як напрям політики безпеки, а як системний інституційно-управлінський механізм, що забезпечує сталий розвиток особистості, збереження ціннісного

потенціалу нації, запобігання девіантній поведінці та цифровій дезадаптації молоді. Такий підхід вимагає глибокого теоретичного осмислення понятійного апарату, уточнення структурних елементів гуманітарної безпеки, а також їхньої інтеграції в загальну систему національної безпеки України.

Понятійно-категоріальний апарат сучасної науки про безпеку постійно трансформується під впливом нових загроз та глобальних викликів. Однією з таких новітніх категорій, що набуває стратегічного значення у вітчизняному й світовому науковому дискурсі, є гуманітарна безпека. У широкому розумінні цей термін відображає ступінь захищеності особистості, суспільства та держави від загроз у гуманітарній сфері – зокрема в галузях освіти, культури, духовності, інформації, мови, прав людини, ідентичності та соціальної згуртованості. Водночас в умовах цифрової епохи гуманітарна безпека дедалі більше охоплює нові сфери – кіберпростір, цифрову етику, безпечне середовище для дітей в онлайн-просторі.

Аналіз наукової літератури свідчить про багатозначність та багатовимірність тлумачення поняття гуманітарної безпеки. У працях М. І. Баюка гуманітарна безпека розглядається як складова державної безпеки, яка охоплює духовно-культурну сферу, ціннісні орієнтири суспільства, освітній простір, інформаційно-комунікаційне середовище, а також гарантії реалізації прав і свобод особистості [7]. Автор акцентує увагу на тому, що гуманітарна безпека визначається не лише відсутністю загроз, а й наявністю умов для гармонійного розвитку особистості, зокрема дітей як стратегічного ресурсу майбутнього.

В. Горбулін та О. Литвиненко у своїй монографії підкреслюють, що гуманітарна безпека має визначальне значення для формування національної ідентичності та національної ідеї, що в умовах гібридної війни стає не лише культурним чи моральним імперативом, а й питанням виживання держави [23]. Автори наполягають, що загрози в гуманітарному просторі – зокрема розмивання культурних кодів, деструктивні інформаційні кампанії, маніпулювання свідомістю через цифрові технології – є формами м'якої сили, здатними викликати стратегічну дестабілізацію.

У свою чергу, Євсюков О. трактує гуманітарну безпеку як «складову частину державної політики, спрямовану на захист духовного, культурного, морального та інтелектуального потенціалу суспільства від внутрішніх і зовнішніх загроз» [40, с. 24]. Таким чином, гуманітарна безпека – це не лише захисний механізм, але й інструмент довгострокового розвитку, який базується на гармонізації стосунків між державою, громадянським суспільством та людиною як центральною фігурою безпекової парадигми.

Визначальним чинником у розумінні гуманітарної безпеки є її антропоцентричний характер. У центрі концепції гуманітарної безпеки знаходиться людина, її гідність, потреби та права, а не лише інституційні чи державні інтереси. Це відповідає загальносвітовому підходу, запропонованому Програмою розвитку ООН, яка трактує human security як «безпеку особистості в умовах загроз насильства, злиднів, нестабільності, хвороб, а також політичного чи інформаційного тиску». У вітчизняному контексті така парадигма має особливу актуальність, враховуючи масштабні гуманітарні виклики, що виникли внаслідок російської агресії та окупації частини територій України.

Крім того, гуманітарна безпека інтегрує в собі принципи інформаційної, соціальної, психологічної, правової та освітньої безпеки, які в комплексі формують простір, у якому людина може реалізувати свій потенціал без загрози деградації, маніпуляції чи дискримінації. Особливої важливості це набуває щодо дітей, які перебувають у стані активного соціального формування та найбільш уразливі до впливів агресивного інформаційного контенту.

Невід’ємною складовою категоріального аналізу є розмежування гуманітарної безпеки від суміжних понять. Наприклад, соціальна безпека зосереджується на матеріальних умовах життя (доходи, зайнятість, доступ до соціальних послуг), тоді як гуманітарна безпека охоплює нематеріальні, ціннісно-культурні та правові аспекти розвитку особистості. Інформаційна безпека, в свою чергу, є структурним елементом гуманітарної безпеки, який забезпечує людині право на доступ до правдивої, об’єктивної та безпечної інформації [50], [55].

Особливу увагу заслуговує інституційне осмислення гуманітарної безпеки. За Круком С. І., гуманітарна безпека має розглядатися як інтегральний об'єкт державного управління, що вимагає узгодження політик у сфері освіти, культури, інформації, прав людини та цифрової трансформації [60], [61]. У такому контексті гуманітарна безпека виступає не лише предметом безпекової стратегії, а й функцією державної політики сталого розвитку.

Таким чином, проведений категоріальний аналіз дозволяє дійти висновку, що гуманітарна безпека – це багатовимірне, міждисциплінарне поняття, яке включає: захист особистісних прав та свобод; збереження культурної ідентичності; створення сприятливого духовного та інформаційного середовища; забезпечення психоемоційного благополуччя; підтримку сталого розвитку інтелектуального та освітнього потенціалу.

Для повноцінного розуміння сутності гуманітарної безпеки як складної міждисциплінарної категорії необхідним є аналіз основних наукових підходів до її визначення. У сучасному науковому дискурсі спостерігається множинність трактувань цього поняття, що обумовлена різними дослідницькими парадигмами, національними підходами та безпековими контекстами. Зведена у таблицю компаративна характеристика ключових підходів дозволяє систематизувати та порівняти позиції провідних вітчизняних і міжнародних авторів, виявити спільні риси та унікальні акценти в розумінні гуманітарної безпеки (табл.1.1).

Проведений аналіз дозволяє стверджувати, що незважаючи на різницю в акцентах (інформаційний, культурний, правозахисний, освітній тощо), всі автори погоджуються з ключовим положенням: гуманітарна безпека є людиноцентричною і становить базовий елемент стійкості держави в умовах сучасних загроз. Найбільш комплексними є ті підходи, які інтегрують ціннісну, інформаційно-комунікаційну та правову складову безпеки, а також враховують вразливість соціальних груп – зокрема дітей – у кіберпросторі.

Враховуючи сучасні реалії, до переліку ключових векторів гуманітарної безпеки необхідно додати цифрову безпеку дітей, як підгрупи, що одночасно є активними споживачами цифрового контенту та найбільш незахищеними від

кіберзагроз. Цей аспект гуманітарної безпеки потребує подальшого глибокого аналізу та розвитку управлінських механізмів реагування на цифрові ризики.

Таблиця 1.1

Теоретичні підходи до визначення гуманітарної безпеки

Автор / Джерело	Підхід до визначення гуманітарної безпеки	Ключові акценти
М. Баюк [7]	Гуманітарна безпека як система збереження духовного, культурного та освітнього потенціалу	Духовність, культура, освіта, захист гуманітарного простору
В. Горбулін, О. Литвиненко [23]	Гуманітарна безпека як ціннісна основа національної ідентичності та державної стійкості	Національна ідея, протидія культурній експансії, гібридним загрозам
О. Євсюков [40]	Політика захисту морального, інформаційного, освітнього середовища людини від зовнішніх і внутрішніх загроз	Людиноцентричність, захист інтелектуального потенціалу
Крук С. І. [60], [61]	Гуманітарна безпека як об'єкт державної політики з міжвідомчою інтеграцією	Державна політика, координація сфер: освіта, культура, права людини
Програма розвитку ООН	Human Security — безпека особистості в усіх сферах життєдіяльності	Антропоцентризм, свобода від страху й потреб, індивідуальні права
Авторська інтерпретація	Стан захищеності особистості та суспільства в духовній, культурній, інформаційній, моральній, освітній сферах	Інтеграція безпеки прав людини, цифрових ризиків і національного культурного ядра

Джерело: [7;23;40;60-61]

Сучасна парадигма національної безпеки дедалі більше тяжіє до інтегрального, міждисциплінарного підходу, що визнає необхідність охоплення не лише військово-політичних чи економічних факторів, але й гуманітарних. Такий підхід відповідає міжнародним тенденціям у сфері безпеки, а також внутрішньодержавним потребам України, яка перебуває у складному безпековому середовищі, зумовленому зовнішньою агресією, гібридними впливами, культурною експансією та інформаційними війнами. У цьому контексті гуманітарна безпека постає як одна з ключових підсистем національної безпеки, що забезпечує збереження духовного, освітнього, культурного, морального, інформаційного та психологічного потенціалу нації.

Закон України «Про національну безпеку» № 2469-VIII від 21 червня 2018 року закріплює системний підхід до безпеки, вказуючи на необхідність захисту національних інтересів у всіх сферах суспільного життя, включно з гуманітарною, культурною та інформаційною [92]. Водночас Національна стратегія національної безпеки України «Безпека людини – безпека країни» (2020) наголошує на пріоритетності захисту прав і свобод людини, розвитку

інклюзивного середовища, духовної консолідації нації, що прямо виводить гуманітарну безпеку в центр сучасної безпекової доктрини держави.

Гуманітарна безпека в системі національної безпеки України виконує функціональну роль інтегратора, що поєднує та узгоджує різні політики – освітню, культурну, інформаційну, правозахисну, молодіжну та сімейну. Як підкреслюють В. Горбулін та О. Литвиненко, саме гуманітарна безпека визначає «ціннісну архітектуру» української державності й здатність держави до самозбереження як суб'єкта міжнародного права та історичного розвитку [23].

Особливістю гуманітарної безпеки є її превентивний і довгостроковий характер. Якщо воєнна безпека реагує на загрози, що вже стали реальністю, то гуманітарна безпека формує умови для недопущення глибокої кризи у свідомості, ідентичності, ціннісній системі нації. У періоди воєнних або соціальних катаклізмів, як нині в Україні, саме гуманітарна сфера зазнає перших атак – у вигляді пропаганди, дезінформації, маніпуляції свідомістю, інформаційного терору, підриву довіри до держави. Як зазначає Євсюков О., гуманітарна безпека є тим рубежем, на якому вирішується майбутнє державності в умовах стратегічного тиску [40].

Ураховуючи виклики гібридної війни, особливого значення набуває інформаційно-комунікаційний сегмент гуманітарної безпеки. Цей компонент охоплює такі завдання як захист від ворожих інформаційно-психологічних операцій, забезпечення кібербезпеки громадян (особливо дітей), розвиток національного інформаційного простору, підтримка якісної журналістики та фактчекінгу. Відсутність ефективної інформаційної політики може призвести до розмиття ідентичності, зневіри в демократичні інститути, поляризації суспільства, що вже частково спостерігалось в Україні на окремих етапах історії [55], [56].

Слід зазначити, що у період повномасштабної збройної агресії РФ гуманітарна безпека стала об'єктом цілеспрямованого руйнування. Російські пропагандистські стратегії системно атакують освітню, культурну, мовну політику України, дискредитують національні цінності, поширюють фейки через соціальні мережі. За даними Держспецзв'язку та Центру стратегічних

комунікацій, лише у 2022–2023 роках було зафіксовано понад 2500 випадків інформаційних атак, з яких значна частина була спрямована на дітей і молодь [10], [11].

У цьому контексті актуалізується теза про те, що гуманітарна безпека – це платформа для національної єдності та внутрішньої стійкості. Захищене інформаційне, культурне й освітнє середовище сприяє консолідації суспільства, зміцненню національної ідентичності, утвердженню демократичних цінностей та довіри до держави. Саме тому держава має системно інституціоналізувати цей напрям – шляхом ухвалення спеціальних стратегій, створення відповідальних інституцій, міжвідомчої координації дій і реалізації профілактичних політик.

Гуманітарна безпека також тісно пов'язана із питаннями соціальної стійкості. За висновками експертів Національного інституту стратегічних досліджень, у кризових умовах саме гуманітарна сфера першою реагує на виклики та стає джерелом довіри до держави, що є критичним фактором легітимності публічного управління [6], [19].

Окремо варто наголосити на специфіці гуманітарної безпеки дітей, як центрального елементу майбутнього соціального капіталу нації. В умовах цифрової трансформації та постійної присутності дітей у кіберпросторі, гуманітарна безпека для цієї категорії громадян повинна охоплювати комплексне забезпечення: цифрової грамотності, захисту психоемоційного стану, доступу до безпечного контенту, правового захисту від цифрових загроз (кібербулінг, грумінг, маніпуляції, ігрова залежність тощо). Як підкреслює О. Димитрієва, саме діти мають стати фокусною групою гуманітарної безпеки, адже вони є і найбільш уразливими, і найперспективнішими суб'єктами цифрового суспільства [35].

У системі національної безпеки України гуманітарна складова виконує низку функцій, які мають ключове значення для збереження соціальної стійкості, ідентичності та прав людини в умовах внутрішніх і зовнішніх загроз. Представлена таблиця узагальнює основні функції гуманітарної безпеки та відповідні загрози, що актуалізують її значення як стратегічного напрямку

державної політики. Такий формат дозволяє виявити зв'язок між потенціалом гуманітарної безпеки й національною стійкістю у воєнний та поствоєнний періоди (табл. 1.2).

Таблиця 1.2.

Роль гуманітарної безпеки в системі національної безпеки України

Функція гуманітарної безпеки	Зміст	Наслідки і значення для нацбезпеки
Ціннісно-консолідуюча	Формування національної ідентичності, культурної єдності, патріотизму	Забезпечення внутрішньої єдності, стійкість до зовнішніх впливів
Інформаційно-захисна	Протидія дезінформації, пропаганді, захист у цифровому просторі	Запобігання когнітивному впливу та підризу демократичного устрою
Психоемоційно-стабілізуюча	Підтримка психічного здоров'я, боротьба з тривожністю, страхами, пов'язаними з війною, соціальною нестабільністю	Суспільна стійкість, зниження рівня тривожності та агресії
Освітньо-інтелектуальна	Забезпечення доступу до якісної освіти, критичного мислення, цифрової грамотності	Підготовка до протидії інформаційним загрозам, формування кадрового потенціалу
Правозахисна	Гарантії реалізації прав і свобод, зокрема прав дітей в інформаційному просторі	Посилення легітимності державної політики, дотримання міжнародних стандартів
Превентивна	Виявлення і нейтралізація загроз до того, як вони стануть масовими	Зниження рівня конфліктності, профілактика соціальних криз
Інституційно-управлінська	Координація дій державних органів у сфері гуманітарної політики	Забезпечення системності, міжвідомчої взаємодії, ефективності управлінських рішень

Джерело: систематизовано автором

Визначені функції гуманітарної безпеки є критично важливими для збереження цілісності українського суспільства, попередження внутрішніх конфліктів, посилення міжнародної суб'єктності держави. Особливої ваги набувають інформаційно-захисна та освітньо-інтелектуальна функції, оскільки саме в інформаційному середовищі реалізується більшість сучасних гібридних загроз. Водночас зростає потреба у формалізації гуманітарної безпеки як окремого напрямку державної безпекової політики – із чіткими індикаторами, суб'єктами та координаційними механізмами.

Отже, гуманітарна безпека є не лише невід'ємною частиною національної безпеки України, а й стратегічною умовою її стійкості, суб'єктності, культурної самодостатності та європейського майбутнього. Інтеграція гуманітарної безпеки

в національній політиці має передбачати комплексність, міжвідомчу взаємодію, орієнтацію на права людини та пріоритет захисту дітей у кіберпросторі. Її ігнорування чи недооцінка несе загрозу не лише культурній деградації, а й політичній нестабільності та втраті національної ідентичності в умовах інтенсивного інформаційного тиску (рис. 1.1).



Рис. 1.1. Зміст інтеграції гуманітарної безпеки в національну політику

Джерело: побудовано автором

Гуманітарна безпека, як складова національної безпеки, є системним соціальним явищем, що охоплює весь спектр життєдіяльності людини в гуманітарному просторі – від освіти та культури до моральних цінностей, інформаційного середовища та психологічної стійкості особистості. Її зміст полягає у створенні та підтриманні умов, за яких гарантовано захист людини, соціуму та держави від загроз, що можуть підірвати гуманітарний потенціал,

ціннісні орієнтири, національну ідентичність, духовність і здатність суспільства до стабільного розвитку.

На відміну від інших типів безпеки (військової, економічної, екологічної), гуманітарна безпека має людиноцентричну природу і тісно пов'язана з реалізацією базових прав і свобод людини, насамперед – права на освіту, інформацію, культурну самореалізацію, свободу думки, світогляду, релігії, мови та захист гідності. Вона формується на основі фундаментальних цінностей, зафіксованих у Загальній декларації прав людини [41], Конвенції про права дитини [104], Конституції України [49], а також у низці національних стратегічних документів.

Зміст гуманітарної безпеки розкривається через її цілі, завдання, об'єкти захисту, загрози, а також механізми реалізації. Основною ціллю гуманітарної безпеки є створення сприятливого соціокультурного та інформаційного середовища, в якому особистість має змогу повноцінно розвиватися, реалізовувати свій потенціал, бути захищеною від деструктивних впливів, дискримінації та дегуманізації. Зокрема, йдеться про: збереження національної ідентичності в умовах глобалізації; забезпечення духовної, моральної та культурної стабільності суспільства; формування світоглядної стійкості до маніпуляцій, пропаганди, дезінформації; гарантування права кожної дитини на безпечне та повноцінне інформаційне середовище.

До ключових завдань гуманітарної безпеки належать:

1. Інституційний захист гуманітарного простору – формування та функціонування ефективної системи державної політики в сфері культури, освіти, інформаційної політики та прав людини.

2. Протидія загрозам гуманітарного характеру, зокрема деструктивним інформаційним кампаніям, нав'язуванню чужих культурних кодів, мовній дискримінації, фальсифікації історії.

3. Освітня просвіта та медіаграмотність – забезпечення знань і навичок, необхідних для критичного сприйняття інформації, розпізнавання фейків, розуміння прав у кіберпросторі.

4. Психосоціальний захист особистості – зменшення психологічного тиску та травматизації, особливо серед дітей, унаслідок впливу інформаційного або воєнного середовища.

Гуманітарна безпека орієнтується на захист: людини як центральної фігури безпекової політики (зокрема її психоемоційного стану, свободи думки, культурної самореалізації); соціальних груп, що є вразливими до гуманітарних загроз (діти, молодь, літні люди, внутрішньо переміщені особи); суспільства в цілому, як носія культурного коду та колективної ідентичності; гуманітарної інфраструктури – закладів освіти, культури, засобів масової інформації, цифрових платформ.

У сучасних умовах Україна стикається з низкою комплексних загроз, які мають гуманітарну природу або безпосередньо впливають на гуманітарну сферу: інформаційно-психологічний тиск і когнітивні війни; масове поширення дезінформації та пропаганди; спроби ревізії історичної пам'яті та підміни національних цінностей; мовна, культурна або релігійна дискримінація; розширення кіберзагроз, спрямованих на дітей (кібербулінг, грумінг, деструктивні онлайн-спільноти); витіснення національного культурного продукту з інформаційного простору; психологічна травматизація населення внаслідок війни.

Загрози гуманітарній безпеці часто є латентними, складно діагностованими та діють у довгостроковій перспективі, поступово підриваючи духовні основи суспільства. Це ускладнює їх своєчасне виявлення та ефективне реагування.

Зміст гуманітарної безпеки розкривається також через механізми її практичного втілення. До них належать:

- нормативно-правове забезпечення – розробка і вдосконалення законодавства щодо прав людини, свободи слова, захисту дітей у кіберпросторі;
- інституційне управління – діяльність Міністерства освіти і науки, Міністерства культури, Держкомтелерадіо, Мінцифри, Національної ради з питань телебачення і радіомовлення, правоохоронних і правозахисних органів;

- державна політика – прийняття стратегій, програм, концепцій у сфері інформаційної, освітньої та культурної безпеки;
- громадсько-державне партнерство – залучення громадських організацій, експертних центрів, освітян і батьківської спільноти до формування безпечного гуманітарного середовища;
- міжнародна співпраця – імплементація міжнародних стандартів у сфері прав людини, захисту дітей, цифрової безпеки;
- цифрові інструменти – створення онлайн-платформ, гарячих ліній, освітніх застосунків, систем фільтрації контенту.

Таким чином, зміст гуманітарної безпеки охоплює весь спектр заходів, спрямованих на забезпечення гідного, вільного, безпечного та ціннісно насиченого життя людини в гуманітарному просторі держави. У сучасному безпековому ландшафті України вона виступає не лише як відповідь на гуманітарні загрози, а як стратегічний напрям формування суспільної стійкості, інтелектуального потенціалу та ціннісного суверенітету нації. Особливої уваги вона потребує в умовах цифровізації суспільства, що підсилює вразливість окремих категорій населення, зокрема дітей, до нових типів загроз, що формуються у віртуальному середовищі.

Поняття гуманітарної безпеки, як було показано в попередніх підпунктах, є складною, багаторівневою категорією, яка інтегрує низку взаємопов'язаних сфер життєдіяльності людини та суспільства. Водночас для ефективної реалізації політики гуманітарної безпеки у державному управлінні необхідним є її концептуальне структурування – тобто виокремлення основних функціонально-змістовних компонентів, що формують її системну основу. Такий підхід дозволяє не лише визначити сферу відповідальності інституцій, але й чітко встановити механізми реагування на специфічні загрози.

У межах проведеного аналізу наукових джерел [7], [23], [40], [55], [60] і стратегічних документів (у т.ч. Національної стратегії національної безпеки України, Стратегії розвитку інформаційного суспільства, Національної стратегії захисту дітей в цифровому середовищі на 2021–2026 роки) обґрунтовано, що

гуманітарна безпека складається з щонайменше шести взаємопов'язаних компонентів, які утворюють цілісну систему.

1. Культурно-ціннісний компонент гуманітарної безпеки. Культурно-ціннісний компонент є базовим, фундаментальним елементом гуманітарної безпеки, оскільки саме культура й система національних цінностей формують ідентичність, світогляд, поведінкові орієнтири та суспільну згуртованість. У найширшому розумінні цей компонент включає не лише охорону матеріальної та нематеріальної культурної спадщини, а й збереження та розвиток національної мови, традицій, символів, історичної пам'яті, духовності, етичних норм і ціннісних установок, що забезпечують безперервність і самобутність українського соціокультурного простору.

У контексті національної безпеки культура виступає не лише об'єктом захисту, а й стратегічним ресурсом, який може слугувати основою для формування патріотизму, стійкості до зовнішніх впливів, зміцнення соціального капіталу. Культурно-ціннісна безпека забезпечує духовну цілісність нації, захищає від культурної експансії, глобалізаційного тиску, мовної асиміляції та цілеспрямованої ідеологічної деструкції.

Особливу загрозу в українських реаліях становить культурна війна, що ведеться проти України як держави з власною історією, традиціями, мовою і моделлю цивілізаційного розвитку. Деструктивні інформаційно-пропагандистські впливи ззовні спрямовані на підрив української культурної ідентичності, спотворення історичних фактів, дискредитацію видатних національних діячів, руйнування традиційних сімейних і духовно-моральних цінностей. Саме тому культурно-ціннісний компонент гуманітарної безпеки має розглядатися не лише в оборонному, а й у проактивному вимірі Національної стратегії захисту дітей в цифровому середовищі на 2021–2026 роки як сфера, що вимагає інвестування, підтримки та стратегічного розвитку.

Важливим аспектом у межах цього компоненту є мовна безпека, яка безпосередньо пов'язана з культурною стійкістю. Державна мова відіграє роль не лише засобу комунікації, а й чинника національної ідентифікації, носія історичної пам'яті, засобу мислення та культурної передачі поколінь.

Поширення мови агресора в українському публічному просторі, зокрема в медіа, на цифрових платформах і в освіті, створює додаткові ризики для інформаційної, культурної та ціннісної безпеки держави.

Культурно-ціннісний компонент також включає історичну політику, яка покликана формувати об'єктивну, науково вивірену національну пам'ять, засновану на правді, героїзмі, трагізмі й досвіді боротьби за державність. Спотворення історії, зокрема у шкільній освіті чи популярній культурі, може спричинити ідентифікаційні зсуви, особливо серед молоді, що часто є цільовою аудиторією для ідеологічного впливу ворожих сил.

Крім того, складовою цього компоненту є духовно-моральний вимір гуманітарної безпеки. Йдеться про захист моральних норм, етичних стандартів, сімейних цінностей, релігійної свободи – як фундаменту соціального порядку. Зниження морального рівня суспільства, легалізація агресії, вульгаризація культурного простору, нормалізація насильства у ЗМІ, кіно та соціальних мережах — усе це послаблює культурний імунітет нації.

Культурно-ціннісний компонент набуває особливої значущості у зв'язку з цифровізацією гуманітарного простору. Національна культура дедалі частіше стає об'єктом конкуренції у кіберпросторі, де домінують глобальні інформаційні платформи з чужими ціннісними орієнтирами. Відсутність якісного українського цифрового контенту, мультимедійної продукції, освітніх платформ та онлайн-бібліотек створює вакуум, який заповнюється зовнішніми культурними моделями, часто несумісними з національними традиціями.

Держава має забезпечити розвиток та просування українського культурного продукту в інформаційному просторі – через підтримку книговидавництва, сучасного кіно, музики, театрів, цифрових музеїв, освітніх ініціатив, фестивалів. Спроможність культури до саморепрезентації у світі є індикатором гуманітарної спроможності держави. У цьому сенсі культурна дипломатія та підтримка українських митців за кордоном також є інструментами гуманітарної безпеки.

Важливо також усвідомлювати, що культурно-ціннісний компонент має міжпоколінний характер. Тобто, він передається з покоління в покоління,

зберігає спадковість національного досвіду та формує морально-етичний ґрунт для подальшого розвитку. Тому культурна безпека – це водночас і безпека майбутнього, а не лише захист теперішнього.

Таким чином, культурно-ціннісний компонент гуманітарної безпеки забезпечує збереження і розвиток основ національної ідентичності, культурної спадщини, мови, історичної пам'яті та духовно-моральних орієнтирів. Його належна реалізація створює умови для соціальної згуртованості, міжетнічного діалогу, протидії культурній експансії та збереження цивілізаційної суб'єктності українського народу. У сучасних умовах війни та цифрової трансформації саме цей компонент потребує системної підтримки як на рівні державної політики, так і на рівні місцевих громад, закладів освіти, культури та медіа.

2. Освітньо-інтелектуальний компонент гуманітарної безпеки. Освітньо-інтелектуальний компонент гуманітарної безпеки відіграє системоутворюючу роль у формуванні людського капіталу, забезпеченні соціальної мобільності, відтворенні національної ідентичності та підвищенні рівня стійкості суспільства до внутрішніх і зовнішніх загроз. У межах гуманітарної безпеки цей компонент охоплює як базові функції освітньої системи (забезпечення доступу до знань, виховання, формування навичок), так і ширші завдання – формування світогляду, критичного мислення, інформаційної гігієни, а також здатності особистості до адаптації у складних суспільно-політичних умовах.

Освіта є стратегічним ресурсом, що безпосередньо впливає на стан національної безпеки через інтелектуалізацію населення, зниження рівня вразливості до маніпуляцій, радикалізації, пропаганди. Слабкість системи освіти, особливо в регіонах з високим рівнем соціальної маргіналізації, створює передумови для ідеологічного впливу ззовні, поширення фейкової інформації, зниження довіри до інституцій, що загрожує політичній стабільності та цілісності держави.

У цьому контексті освітньо-інтелектуальний компонент можна розглядати як захисний механізм, який забезпечує когнітивну безпеку – здатність особистості критично осмислювати реальність, відрізнити правду від

маніпуляції, відстоювати демократичні цінності, національні інтереси та ідентичність. Особливо це актуально в умовах гібридної війни, коли об'єктами атак стають не лише інфраструктура чи збройні сили, а й свідомість громадян, зокрема молоді.

Іншою важливою складовою цього компоненту є науково-інтелектуальний потенціал держави. Від рівня інвестицій в науку, інновації, технічну освіту залежить не лише економічна конкурентоспроможність, а й спроможність держави формувати власні наративи, виробляти ідеї, розвивати стратегічне мислення. Ослаблення академічної сфери, витік мізків, деградація гуманітарних наук і підміна їхньої функції ідеологією – усе це створює ризики для довготривалого виживання національної культурно-інформаційної екосистеми.

Доступ до якісної освіти – ще один ключовий параметр гуманітарної безпеки. Освітня нерівність, відсутність цифрової інфраструктури в сільських громадах, виключення дітей з вразливих категорій (ВПО, діти з особливими освітніми потребами, сироти) з якісного освітнього процесу спричиняє довготривалі наслідки. Це не лише знижує рівень соціальної справедливості, а й формує нові зони напруги, які в майбутньому можуть проявитися у вигляді протестного потенціалу або асоціальної поведінки.

Особливу увагу в межах цього компоненту заслуговує цифрова освіта та інформаційна грамотність. В умовах повномасштабного вторгнення та перенесення значної частини освітніх процесів у цифровий простір, зросла актуальність формування в учнів, студентів і вчителів навичок цифрової безпеки, захисту персональних даних, розпізнавання кіберзагроз. Саме через освітню сферу має реалізовуватися політика держави з профілактики кібербулінгу, онлайн-залежностей, маніпулятивного впливу цифрових платформ на поведінку дітей та підлітків.

Окремим напрямом є виховання у сфері національної безпеки та обороноздатності, зокрема через впровадження курсів з основ безпеки, цифрової гігієни, критичного мислення, а також предметів, що формують історичну обізнаність, національну ідентичність, повагу до прав людини та

демократичних інституцій. Освітнє середовище в такому випадку виступає простором формування культури безпеки та відповідального громадянства.

Крім формальної освіти, суттєвий внесок у зміцнення гуманітарної безпеки відіграє неформальна освіта, громадянська просвіта, культурні проекти та інформаційні кампанії. Держава повинна сприяти активній взаємодії з громадянським суспільством, підтримці молодіжних та освітніх ініціатив, реалізації довготривалих національних програм просвітницького характеру.

Насамкінець, до освітньо-інтелектуального компоненту варто віднести здатність нації до самонавчання, гнучкості мислення, інноваційності. У сучасному світі це визначає не лише рівень економічного розвитку, а й спроможність національної системи безпеки адекватно відповідати на нетипові та швидкоплинні виклики.

Освітньо-інтелектуальний компонент гуманітарної безпеки – це не просто галузь політики, а основа життєстійкості нації. Його ефективне функціонування формує освічене, стійке до маніпуляцій, морально зріле та патріотично орієнтоване суспільство. В умовах воєнних загроз, інформаційних атак та соціальної нестабільності саме інтелектуально підготовлене суспільство є найкращою гарантією збереження державності, культурної ідентичності та демократичного розвитку. Тому інвестиції в освіту та інтелектуальний потенціал мають стати пріоритетом національної безпеки України.

3. Інформаційно-комунікаційний компонент гуманітарної безпеки. Інформаційно-комунікаційний компонент є одним із найбільш динамічних і чутливих сегментів гуманітарної безпеки, особливо в умовах гібридної війни та стрімкого розвитку цифрових технологій. Його сутність полягає у забезпеченні захисту інформаційного простору держави, формуванні інформаційного імунітету громадян, протидії дезінформації, пропаганді, інформаційно-психологічним операціям, а також гарантуванні права на доступ до достовірної інформації.

У межах гуманітарної безпеки інформаційно-комунікаційний компонент виконує кілька ключових функцій: по-перше, інформування громадськості про реальні загрози та події, що дозволяє формувати обґрунтовані оцінки ситуації й

запобігати панічним настроям; по-друге, забезпечення комунікації між державою та суспільством, зокрема у кризових ситуаціях; по-третє, протидія зовнішнім інформаційним впливам, які мають на меті розкол суспільства, підрив довіри до інституцій, деморалізацію населення, деструкцію національної ідентичності.

Особливої уваги потребує вплив соціальних мереж, месенджерів, блогерів, медіаплатформ та штучного інтелекту на формування суспільних настроїв і поведінкових моделей. Сучасний інформаційний простір характеризується високим рівнем маніпулятивності, що потребує від громадян високої медіаграмотності, вміння розрізняти фейкові джерела, виявляти пропаганду, аналізувати джерела інформації. Формування такої грамотності має стати частиною загальноосвітньої підготовки та державної просвітницької політики.

В умовах війни саме інформаційна безпека стає елементом не лише гуманітарної, а й національної оборони. Тому інформаційно-комунікаційний компонент включає: захист державних інформаційних ресурсів, безпеку критичної інформаційної інфраструктури, протидію кібератакам і кібертероризму, а також контроль за наративами, які формуються в публічному просторі (включаючи деструктивні меседжі, що підривають єдність, формують відчуття безнадії тощо).

Державні органи мають забезпечити прозору комунікацію з суспільством, уникаючи як надмірного оптимізму, так і мовчання у критичні моменти. Ефективні комунікації, засновані на принципах довіри, відкритості, оперативності та відповідальності, є основою гуманітарної стабільності.

Не менш важливим є розвиток державної гуманітарної інформаційної політики, що включає підтримку національного інформаційного продукту, державних медіа, освітнього контенту, цифрових платформ із просвітницьким спрямуванням, а також популяризацію українських цінностей та культурних кодів.

Таким чином, інформаційно-комунікаційний компонент – це не лише оборонний механізм, а й стратегічний інструмент формування ідентичності, довіри та стійкості суспільства до сучасних викликів.

4. Правовий компонент гуманітарної безпеки. Правовий компонент гуманітарної безпеки є основою функціонування всіх інших її складових, адже саме через правові норми відбувається регулювання, гарантування та захист прав і свобод людини, формування механізмів відповідальності та правосуддя, забезпечення верховенства права, що є наріжним каменем демократичної держави. Цей компонент передбачає: наявність належного правового забезпечення гуманітарної політики; створення та імплементацію інструментів захисту прав людини, зокрема дитини, у різних сферах (освіта, культура, інформація, кіберпростір); розвиток інституційного механізму, зокрема діяльність омбудсмена з прав людини і прав дитини, судових та правоохоронних органів, що забезпечують справедливість і правову безпеку.

Правовий компонент також передбачає гармонізацію українського законодавства з міжнародно-правовими стандартами, зокрема: Конвенцією про права дитини, Загальною декларацією прав людини, Європейською конвенцією з прав людини та Конвенцією про кіберзлочинність.

Особливу роль у цьому контексті відіграють механізми правового захисту в цифровому середовищі: захист персональних даних, забезпечення права на приватність, захист дітей від кібербулінгу, регламентація діяльності цифрових платформ тощо.

Слабкість правозастосування, правовий нігілізм, недовіра до судової системи, корупція, а також неефективність правових механізмів соціального захисту – усе це підриває гуманітарну безпеку, знижує рівень довіри до держави, стимулює соціальну дезінтеграцію.

Крім того, правовий компонент покликаний гарантувати: інклюзивність гуманітарної політики (захист вразливих груп, зокрема внутрішньо переміщених осіб, людей з інвалідністю, дітей-сиріт); публічність прийняття рішень (право на доступ до інформації, участь у прийнятті рішень);

відповідальність за порушення гуманітарних норм (військові злочини, злочини проти людяності, пропаганда насильства тощо).

У контексті воєнної агресії проти України правовий компонент гуманітарної безпеки набуває нового значення – як засіб міжнародно-правової протидії агресії, фіксації злочинів, захисту цивільного населення, документування порушень гуманітарного права та переслідування винних. Правова культура громадян, правова обізнаність і правовий захист у кризових ситуаціях є критично важливими для соціальної згуртованості та стійкості держави.

Отже, інформаційно-комунікаційний та правовий компоненти гуманітарної безпеки України – це ключові інструменти захисту людини як найвищої цінності демократичного суспільства. Перший відповідає за змістовне наповнення суспільної свідомості, стійкість до маніпуляцій, формування єдиного інформаційного простору. Другий – за юридичне забезпечення прав, свобод, відповідальності, справедливості. Обидва компоненти є не лише частиною гуманітарної сфери, а й опорою для державної політики в умовах гібридних загроз, війни та соціальних трансформацій.

5. Психологічно-поведінковий компонент гуманітарної безпеки охоплює сукупність психічних станів, поведінкових моделей, ціннісних орієнтацій та рівня емоційної стійкості населення, що безпосередньо впливають на спроможність суспільства протистояти загрозам, адаптуватися до криз і зберігати внутрішню згуртованість. У сучасних умовах, коли суспільство постійно перебуває під впливом стресових факторів (війна, втрати, вимушене переміщення, інформаційний тиск, соціальна нестабільність), психологічна складова гуманітарної безпеки набуває особливого значення.

Цей компонент охоплює два основні вектори: Індивідуальний рівень – психоемоційне здоров'я особистості, зокрема дітей і молоді; здатність до критичного мислення, психологічна стійкість до маніпуляцій, рівень тривожності, здатність до соціалізації; Колективний рівень – соціальні установки, морально-психологічний клімат у суспільстві, домінуючі поведінкові сценарії (наприклад, апатія, агресія, солідарність, мобілізація тощо).

Психологічна безпека особливо актуальна в умовах: гібридної агресії, яка активно експлуатує страхи, розгубленість, недовіру; поширення фейкових новин і пропаганди, які викликають паніку, зневіру в інститути влади, міжгрупову напругу; травматизації дітей унаслідок бойових дій, вимушеного переселення, втрати близьких, порушення звичного способу життя.

Ключовими загрозами в межах цього компоненту є: зниження рівня довіри до соціальних інститутів; поширення девіантної та деструктивної поведінки (особливо серед молоді); соціальна апатія, синдром емоційного вигорання; посттравматичні стани, депресії, панічні розлади; емоційна дезорієнтація, втрата ціннісних орієнтирів.

Забезпечення психологічно-поведінкової безпеки потребує впровадження системної державної політики в галузі психічного здоров'я, включаючи: розвиток мережі психологічної допомоги та кризового консультування; інтеграцію психосоціальної підтримки в освітній процес; психологічну реабілітацію ветеранів, переселенців, дітей, постраждалих від війни; державні програми з формування емоційного інтелекту та стресостійкості у школах.

Особливу увагу слід приділяти поведінковим патернам, що формуються під впливом цифрового середовища. Наприклад, діти, які зазнали кібербулінгу, можуть проявляти агресію, самоізоляцію, тривожність, що вимагає раннього виявлення і психокорекційної роботи. Формування здорової поведінкової культури – через сім'ю, школу, медіа – є довгостроковим завданням державної політики у сфері гуманітарної безпеки.

6. Соціально-демографічний компонент гуманітарної безпеки розкриває важливість сталого розвитку людського потенціалу, збереження демографічної рівноваги, соціальної справедливості та інтеграції різних груп населення в єдиний безпечний соціокультурний простір. Він визначає рівень соціальної стійкості суспільства, його спроможність підтримувати внутрішню єдність, забезпечувати рівні можливості, попереджувати соціальні конфлікти.

Цей компонент особливо критичний для України в контексті: тривалої демографічної кризи (зменшення чисельності населення, старіння, еміграція); вимушеної міграції внаслідок війни (внутрішньо переміщені особи, біженці,

втрата домівок і засобів до існування); погіршення соціальної мобільності; порушення міжпоколінного та міжрегіонального балансу.

Соціально-демографічна небезпека проявляється у: депопуляції (скорочення чисельності населення, зменшення народжуваності); трудовій міграції молоді, «відтоку мізків»; маргіналізації вразливих груп (люди з інвалідністю, самотні особи, багатодітні родини, діти-сироти); поглибленні соціальної нерівності; зростанні регіональних диспропорцій.

Найвразливішою категорією залишаються діти, особливо ті, що опинилися в умовах війни або окупації. Згідно з даними міжнародних організацій, мільйони українських дітей зазнали впливу воєнних дій, порушення права на освіту, безпеку, здоров'я, житло. Це створює довгострокову загрозу гуманітарній безпеці через втрату освіченого, здорового, соціально адаптованого покоління.

Реалізація соціально-демографічного компоненту вимагає: політики з підтримки народжуваності (матеріальна допомога, соціальні послуги, житлові програми); забезпечення реінтеграції внутрішньо переміщених осіб; доступу до якісної медицини, освіти, соціального страхування; інклюзивних програм для вразливих груп; реабілітаційних програм для дітей, які постраждали від війни або насильства.

Важливу роль відіграє і державна статистика, яка має забезпечувати актуальні, достовірні, деталізовані демографічні дані, на основі яких приймаються управлінські рішення.

Психологічно-поведінковий та соціально-демографічний компоненти є основоположними для формування цілісної моделі гуманітарної безпеки. Перший визначає внутрішню емоційну стабільність, рівень свідомості, здатність до консолідації. Другий – соціальний баланс, сталість розвитку, відтворення людського потенціалу. Їх інтеграція в державну політику має стати пріоритетом у повоєнній стратегії гуманітарного відновлення України.

У процесі дослідження гуманітарної безпеки як ключового напрямку забезпечення національної безпеки України виникає необхідність її структурного осмислення. Гуманітарна безпека є багатовимірною категорією,

що охоплює широкий спектр сфер суспільного життя, пов'язаних із захистом і розвитком людського потенціалу, збереженням національної ідентичності, гарантуванням прав і свобод людини в умовах внутрішніх і зовнішніх викликів. Для кращого розуміння її змісту та функціонального наповнення доцільним є розмежування ключових структурних компонентів гуманітарної безпеки. У представленій таблиці систематизовано основні компоненти цієї категорії, подано їх коротку змістову характеристику, функціональні призначення, а також проаналізовано потенційні загрози, що можуть порушити безпековий баланс у відповідних сферах. Такий підхід дозволяє комплексно охопити всі напрями гуманітарної політики держави та забезпечити цілісність управлінських рішень у сфері захисту людини, особливо вразливих груп населення, зокрема дітей (табл. 1.3).

Таблиця 1.3.

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

Аналіз структурних компонентів гуманітарної безпеки засвідчив її комплексний, міждисциплінарний характер та високий ступінь взаємозалежності між окремими елементами. Жоден із представлених компонентів – чи то культурно-ціннісний, чи освітньо-інтелектуальний, інформаційний, правовий, психологічний чи соціально-демографічний – не може функціонувати ізольовано. Їх ефективна взаємодія формує надійний гуманітарний щит держави, який захищає суспільство від зовнішнього впливу, деструктивної інформації, соціальної дезінтеграції, порушення прав людини та руйнування національної свідомості. Водночас загрози, що виникають в одному з компонентів, мають тенденцію до поширення на інші сфери, що вимагає від органів державної влади скоординованої, системної політики у сфері гуманітарної безпеки. Представлена таблиця може слугувати аналітичним інструментом для розробки стратегій реагування, оцінки ризиків і формування міжвідомчих програм захисту гуманітарного простору України.

Підсумовуючи слід зазначити, що гуманітарна безпека посідає ключове місце в ієрархії національної безпеки, оскільки вона стосується безпосередньо захисту людини як центральної цінності державної політики. У сучасних умовах, зокрема в період повномасштабної воєнної агресії проти України, гуманітарна безпека постає не лише як складова, а як пріоритетна стратегічна категорія, що об'єднує культурну, освітню, інформаційну, правову, психологічну та соціально-демографічну сфери.

Проведений категоріальний аналіз дозволив конкретизувати зміст поняття «гуманітарна безпека» через призму сучасних викликів, які виникають в умовах цифровізації, глобалізації, воєнно-політичної нестабільності та кризових соціальних трансформацій. Визначено, що гуманітарна безпека – це стан гарантованого захисту базових прав, свобод і гідності людини від загроз, що виникають у культурній, освітній, психологічній, соціальній, інформаційній і правовій площинах. Особлива увага приділяється безпеці дітей як найвразливішої соціальної категорії.

Структурний аналіз гуманітарної безпеки дав змогу виокремити її шість ключових компонентів: культурно-ціннісний, освітньо-інтелектуальний, інформаційно-комунікаційний, правовий, психологічно-поведінковий та соціально-демографічний. Кожен із них виконує специфічну функцію у зміцненні суспільної стійкості, збереженні національної ідентичності, формуванні здатності до протидії гібридним загрозам та забезпеченні гармонійного розвитку особистості.

Таким чином, гуманітарна безпека в системі національної безпеки України виступає як комплексна категорія, що синтезує у собі не лише інституційно-правові підходи, а й ціннісно-світоглядні орієнтири розвитку держави. Її ефективна інтеграція в державну політику можлива лише за умови міжгалузевої взаємодії, міжвідомчої координації та сталого діалогу між державою, громадянським суспільством і міжнародною спільнотою.

1.2. Теоретичні підходи до формування державної політики захисту дітей

Формування ефективної політики державної політики у сфері захисту дітей постає сьогодні як одне з найактуальніших завдань гуманітарної безпеки України. Це зумовлено як внутрішніми трансформаційними процесами, так і зовнішніми викликами: гібридною війною, гуманітарними катастрофами, загрозами в кіберпросторі, посиленням цифрової залежності молодого покоління та загальним зростанням вразливості дітей до інформаційних, соціальних і психологічних ризиків. У таких умовах необхідність чіткого, науково обґрунтованого підходу до розробки та впровадження політики захисту дітей набуває стратегічного значення.

На сучасному етапі розвитку державної політики спостерігається переосмислення традиційних механізмів і моделей політики, що стосуються дітей як особливої соціально-демографічної групи. З одного боку, держава зобов'язана забезпечити реалізацію прав дитини відповідно до Конституції України [49], міжнародних конвенцій, зокрема Конвенції ООН про права

дитини [47], а також низки галузевих законів, зокрема Законів України «Про охорону дитинства» [95], «Про освіту», «Про соціальні послуги» та інших. З іншого боку, виклики XXI століття – динаміка соціальних ризиків, кіберзлочинність, діджиталізація освіти й дозвілля, трансформація сімейного середовища – вимагають модернізації політики та управлінських стратегій із урахуванням нових теоретико-методологічних орієнтирів.

Захист прав дитини в сучасних умовах не може бути зведений до суто адміністративних чи правових заходів – він має базуватися на комплексному баченні дитини як суб'єкта прав, носія людської гідності та ключового елементу соціального капіталу нації. Саме тому в основі сучасного державно-управлінського підходу мають лежати не лише юридичні імперативи, а й гуманітарні, ціннісні, інституційні, соціологічні й інформаційні підходи.

У межах даного підрозділу розглядатимуться ключові теоретичні підходи до формування політики державної політики у сфері захисту дітей, що включають: нормативно-правовий, інституційний, мережевий (governance), rights-based (орієнтований на права дитини), інтеграційний та мультисекторальний. Розкриття змісту кожного з них дозволяє сформулювати глибоке наукове підґрунтя для розуміння природи та механізмів сучасної державної політики у сфері захисту дітей, а також обґрунтувати концептуальну модель її реалізації в українському контексті.

Таким чином, теоретичне осмислення проблеми є першоосновою для розробки цілісної, ефективної та адаптивної політики державної політики у сфері захисту дітей як одного з ключових пріоритетів гуманітарної безпеки України (рис. 1.2).

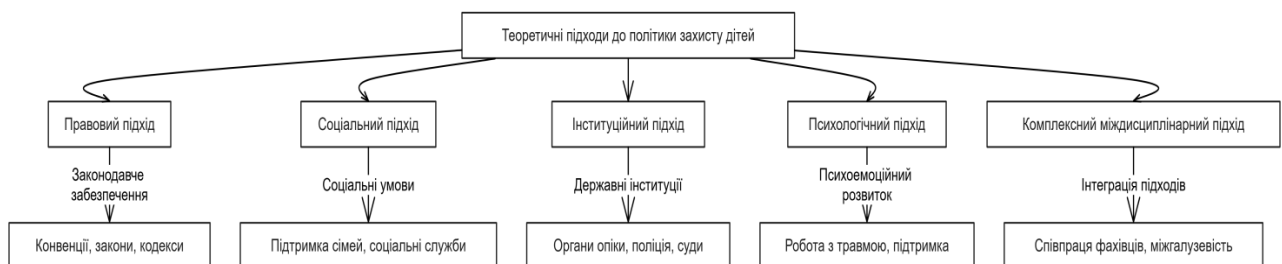


Рис. 1.2. Структура підходів до формування політики захисту дітей

Джерело: побудовано автором

Нормативно-правовий підхід є базовою та визначальною теоретико-методологічною основою у формуванні політики державної політики у сфері захисту дітей. Його сутність полягає в тому, що саме через систему правових норм, законодавчих актів, міжнародних договорів і підзаконних рішень держава визначає рамки, механізми, принципи та гарантії реалізації прав дитини, а також відповідальність органів влади за їхнє дотримання. У межах цього підходу дитина розглядається не як об'єкт опіки, а як повноправний суб'єкт права, носій невід'ємних прав і свобод, які держава зобов'язана гарантувати, охороняти й відновлювати у випадку їх порушення.

Нормативно-правовий підхід спирається на розуміння того, що правова держава може ефективно функціонувати лише тоді, коли права дитини інтегровані в загальну систему національного законодавства та є невід'ємною частиною конституційного ладу. Конституція України (статті 3, 52, 53) визначає людину, її життя, честь, гідність і безпеку найвищою соціальною цінністю, а також покладає на державу обов'язок охороняти права дітей, створювати умови для їхнього розвитку, освіти та соціального захисту [49]. Ця норма задає правову основу для всієї політики державної політики у сфері дитинства, формуючи правовий фундамент для подальшого розгортання інституційних і соціальних механізмів.

Важливе місце у нормативно-правовій парадигмі займають міжнародні стандарти, насамперед Конвенція ООН про права дитини (1989 р.) [47], ратифікована Україною в 1991 році. Конвенція визначає ключові принципи політики щодо дітей – пріоритет найкращих інтересів дитини, рівність прав, недискримінацію, участь дитини у прийнятті рішень, що її стосуються. У контексті державної політики це означає, що будь-яка політика чи програма має бути оцінена через призму впливу на права дитини. Водночас міжнародно-правова система створює обов'язок держави гармонізувати національне законодавство з цими принципами, що є невід'ємною складовою правового суверенітету України як демократичної та правової держави.

На національному рівні ключовим нормативним документом є Закон України «Про охорону дитинства» [95], який визначає основні засади державної політики щодо забезпечення прав, свобод і законних інтересів дітей. Закон закріплює обов'язки держави, батьків і суспільства у сфері захисту дітей, формує основи міжвідомчої взаємодії та встановлює відповідальність за порушення дитячих прав. Разом із ним важливу роль відіграють такі акти, як Закон України «Про основні засади забезпечення кібербезпеки України» [93], який поширює сферу правового захисту дітей на цифрове середовище, а також закони «Про освіту», «Про соціальні послуги», «Про запобігання та протидію домашньому насильству», «Про захист персональних даних» [91], що визначають спеціальні механізми правового реагування у відповідних сферах.

Особливе значення має Національна стратегія захисту дітей у кіберпросторі на 2021–2026 роки [80], схвалена урядом України, яка є прикладом практичної реалізації нормативно-правового підходу. Вона спрямована на створення безпечного цифрового простору, формування державних стандартів інформаційної безпеки дітей, розвиток кіберграмотності, запровадження ефективних процедур реагування на кібербулінг і сексуальну експлуатацію дітей онлайн. Водночас зазначений документ підкреслює потребу у вдосконаленні міжгалузевого законодавства, що регулює діяльність державних органів у цій сфері.

Важливо, що нормативно-правовий підхід передбачає не лише ухвалення законів, а й формування інституційного механізму їх реалізації. Йдеться про діяльність служб у справах дітей, центрів соціальних служб, Національної поліції, прокуратури, Міністерства освіти і науки, Міністерства соціальної політики, Уповноваженого Президента з прав дитини, а також місцевих органів влади. Усі ці інституції діють у межах законодавчо визначених повноважень, що забезпечує системність і підзвітність політики.

Водночас практика державної політики показує, що сам по собі нормативно-правовий підхід не гарантує ефективності політики. Проблеми виникають тоді, коли норми не підкріплені реальними ресурсами, механізмами контролю та моніторингу виконання. Як зауважує Бакуменко В. [3], державне

управління є дієвим лише тоді, коли нормативна база поєднується з аналітичними, організаційними та поведінковими механізмами. Тобто правове регулювання має не лише визначати обов'язки, але й створювати умови для їх реалізації.

Крім того, в українському контексті особливої уваги потребує адаптація законодавства до сучасних цифрових реалій. Зокрема, необхідно враховувати міжнародні стандарти щодо захисту персональних даних дітей (GDPR [145]), регламентацію діяльності інтернет-платформ і провайдерів контенту, питання етичного використання даних у сфері освіти та медицини. У цьому аспекті нормативно-правовий підхід переходить у сферу кібергуманітарної безпеки, де йдеться про забезпечення права дитини на цифрову приватність, свободу від онлайн-насильства та доступ до безпечного контенту.

Отже, нормативно-правовий підхід формує юридичний каркас державної політики у сфері захисту дітей, забезпечуючи визначеність, легітимність і відповідальність. Він задає рамки для функціонування інших підходів – інституційного, мережевого, інтеграційного – та створює підґрунтя для реалізації принципів верховенства права, прозорості, підзвітності та соціальної справедливості. Проте для забезпечення його ефективності необхідна постійна гармонізація законодавства з міжнародними стандартами, оновлення правових норм відповідно до нових типів загроз і забезпечення практичної реалізації ухвалених законів через дієві механізми контролю, моніторингу та оцінювання.

У результаті нормативно-правовий підхід можна розглядати як стрижневий елемент системи державної політики у сфері захисту дітей, який перетворює гуманітарні цінності та суспільні очікування на конкретні правові норми, що гарантують безпеку, розвиток і добробут кожної дитини в Україні.

Інституційний підхід є одним із базових напрямів сучасної теорії державної політики та виступає важливою методологічною основою формування ефективної політики у сфері захисту дітей. Його сутність полягає у розгляді системи захисту прав дитини як мережі взаємопов'язаних інститутів, що мають певну структуру, функції, ресурси, повноваження, правила взаємодії та відповідальність за результати своєї діяльності. На відміну від нормативно-

правового підходу, який визначає «що» має бути зроблено, інституційний підхід відповідає на запитання «хто» і «як» забезпечує реалізацію політики, якими засобами, механізмами та управлінськими інструментами.

У класичному розумінні, інститути – це стійкі соціально-правові структури, що забезпечують виконання певних суспільно важливих функцій і підтримують стабільність системи державної політики [24], [60]. У сфері захисту дітей до таких інститутів належать: органи державної влади (законодавчі, виконавчі, судові), уповноважені установи та служби у справах дітей, освітні, медичні, соціальні заклади, правоохоронні органи, інститути громадянського суспільства (громадські організації, благодійні фонди, правозахисні об'єднання), міжнародні організації, що діють на території України (ЮНІСЕФ, Save the Children, ECPAT International тощо).

Інституційний підхід дозволяє аналізувати не лише формальну структуру системи захисту дітей, а й якість управлінських зв'язків, комунікацій та взаємодії між цими інститутами. У сучасних умовах ефективність політики визначається не лише кількістю органів, що нею займаються, а й ступенем їхньої координації, узгодженості дій та спільної відповідальності. Як зауважує В. Горбулін [21], у складних системах національної безпеки, до яких належить і гуманітарна сфера, результат досягається лише за наявності міжінституційної синергії, коли діяльність різних структур підпорядковується єдиній стратегічній меті.

У контексті України інституційний підхід розкривається через багаторівневу систему суб'єктів державної політики у сфері захисту дітей. Центральним координатором виступає Міністерство соціальної політики України, яке реалізує державну політику у сфері сім'ї, дітей та молоді, забезпечує нормативно-правове регулювання і координацію міжвідомчих програм. Поруч із ним діють:

1. Служби у справах дітей, які на місцевому рівні забезпечують облік, супровід, влаштування дітей у складних життєвих обставинах, реалізацію соціальних програм.

2. Уповноважений Президента України з прав дитини, який виконує функції нагляду, представництва та захисту інтересів дітей у державних органах, ініціює законодавчі зміни, проводить моніторинг дотримання прав дитини [16], [42].

3. Міністерство освіти і науки України, яке забезпечує освітній компонент захисту дітей, зокрема безпечне освітнє середовище та профілактику насильства у школах.

4. Національна поліція, що реалізує функції запобігання злочинам проти дітей, протидії насильству, кіберзлочинам і експлуатації неповнолітніх [11].

5. Міністерство цифрової трансформації, яке відповідає за реалізацію Національної стратегії захисту дітей у кіберпросторі[80].

Важливою складовою інституційного підходу є інституціоналізація механізмів взаємодії між державою та громадянським суспільством. Згідно з підходом, розробленим Т. Безверхнюк [8], партнерські мережі, координаційні ради, міжвідомчі групи є ефективною інституційною формою реалізації політики у складних гуманітарних сферах. У сфері захисту дітей це проявляється через спільні ініціативи державних органів і неурядових організацій – наприклад, програми з протидії торгівлі дітьми, кібербулінгу, сексуальній експлуатації, а також створення дитячих омбудсервісів і гарячих ліній.

Важливим аспектом інституційного підходу є оцінка спроможності інститутів, тобто здатності виконувати покладені функції ефективно, прозоро, з урахуванням потреб дітей. За теорією В. Бакуменка [2], [3], ефективність державної політики визначається наявністю чітко визначених функцій, процедур, кадрового потенціалу та інституційної пам'яті. На жаль, українська практика свідчить про низку проблем: кадровий дефіцит у службах у справах дітей, перевантаження соціальних працівників, брак фінансування, фрагментарність міжвідомчих комунікацій. Ці фактори знижують дієвість політики навіть за наявності розвиненої нормативної бази.

З позицій інституційного підходу ефективна політика захисту дітей повинна спиратися на такі принципи: Чіткий розподіл повноважень і відповідальності між суб'єктами. Координація дій і міжвідомча взаємодія на горизонтальному та вертикальному рівнях. Підзвітність і прозорість діяльності інститутів – як державних, так і громадських. Ресурсна забезпеченість, включно з фінансами, кадрами, технічною базою, аналітичними інструментами. Стійкість і гнучкість інституцій, їх здатність адаптуватися до нових викликів (зокрема цифрових, соціальних, воєнних).

Сучасний інституційний підхід також передбачає інтеграцію цифрових інститутів у систему державного управління. В умовах діджиталізації захист дітей дедалі частіше здійснюється через електронні сервіси, бази даних, цифрові платформи моніторингу та реагування на випадки порушення прав дитини. Як зазначає Є. Котух [55], формування цифрової екосистеми кібербезпеки у публічному секторі потребує нового типу інституцій – гібридних структур, які поєднують правові, інформаційні та технологічні інструменти. Таким чином, інституційна архітектура політики захисту дітей в Україні має розвиватися у напрямі «цифрового гуманітарного управління», що передбачає єдині стандарти взаємодії між державними та недержавними суб'єктами у кіберпросторі.

Не менш важливим є аспект інституційної культури – норм, цінностей, етичних стандартів, що визначають поведінку представників державних структур, які працюють із дітьми. Без формування гуманістичної культури державної політики будь-які інституційні реформи залишатимуться формальними. Як підкреслює С. Крук [61], інституційна стійкість державної політики базується не лише на нормативно-організаційних елементах, а й на соціально-моральних цінностях, які забезпечують довіру громадян до держави.

Отже, інституційний підхід до формування політики державної політики у сфері захисту дітей є системоутворювальним, оскільки забезпечує узгоджене функціонування всіх суб'єктів політики, створює механізми координації, партнерства та спільної відповідальності. Його ефективна реалізація можлива лише за умови розвитку інституційної спроможності, децентралізації

управління, прозорості процесів прийняття рішень і підзвітності державних органів перед суспільством.

Таким чином, інституційний підхід формує практичну основу гуманітарної державної політики, перетворюючи правові норми та політичні декларації на реальні інституційні механізми, що здатні гарантувати кожній дитині в Україні безпеку, розвиток і захист її прав у відповідності до принципів демократичного врядування.

У контексті сучасного державного управління, особливо в таких чутливих та соціально орієнтованих сферах, як захист прав і свобод дітей, дедалі більшої ваги набуває мережевий підхід (Governance). Він виходить за межі класичної ієрархічної моделі управління, заснованої виключно на вертикальному підпорядкуванні, і фокусується на горизонтальній взаємодії, партнерстві, співуправлінні та координації між усіма зацікавленими сторонами. Цей підхід є надзвичайно актуальним в умовах плюралізму суб'єктів, цифровізації, глобалізації та підвищених соціальних очікувань щодо якості публічних послуг, зокрема у сфері дитячої безпеки.

На відміну від традиційної моделі «government» (влада як керівництво), концепція «governance» визначає управління як мережу міждержавних, міжінституційних та міжсекторних зв'язків, у межах яких відбувається ухвалення рішень, реалізація політики, розподіл ресурсів та відповідальності. Управління у цій моделі – це спільне вироблення рішень (co-governance), в якому беруть участь не лише державні інституції, а й представники громадянського суспільства, бізнесу, наукових кіл, міжнародних організацій, а також самі бенефіціари – у нашому випадку, діти та їхні батьки.

Цей підхід особливо ефективний у багатофакторних і складних соціальних середовищах, де традиційні вертикалі управління виявляються надто інерційними та негнучкими. У сфері захисту дітей це означає, що жодна державна структура самотійно не здатна повноцінно гарантувати безпеку, права і розвиток дитини без тісної кооперації з іншими суб'єктами (табл. 1.4).

У сфері захисту дітей мережевий підхід реалізується через створення партнерських форматів, таких як: міжвідомчі робочі групи при органах влади;

платформи співпраці держави та НУО; електронні сервіси (e-Health, e-Social, «Дія») як інструменти участі; цифрові платформи сповіщення про випадки насильства або порушення прав дітей; програми за підтримки міжнародних партнерів (ЮНІСЕФ, ЕСРАТ, Ради Європи) у тісній співпраці з українськими міністерствами [80], [10], [33].

Таблиця 1.4

Ключові ознаки Governance-підходу в державному управлінні

№	Ознака	Зміст	Прояв у сфері захисту дітей
1	Мережева взаємодія	Управління не централізоване, а розподілене між державою, бізнесом, громадськістю, наукою	Співпраця МОН, Мінцифри, громадських організацій, IT-компаній у створенні онлайн-платформ
2	Публічно-приватне партнерство (PPP)	Спільна реалізація політики державою та недержавними акторами	Спільні кампанії держави та компаній (Google, Meta, UNICEF) проти онлайн-насильства
3	Горизонтальність управління	Відсутність ієрархії, рішення приймаються колективно, на засадах діалогу	Консультативні ради при міністерствах із залученням громадськості та експертів
4	Децентралізація рішень	Уповноваження регіонів, громад, закладів освіти приймати рішення в межах політики	Надання школам автономії у впровадженні політик цифрової безпеки дітей
5	Участь зацікавлених сторін (stakeholders)	Всі дотичні групи беруть участь у формуванні політики	Включення в обговорення політики батьків, дітей, вчителів, IT-фахівців
6	Прозорість та підзвітність	Управління відкрито для громадськості, передбачає зворотний зв'язок	Регулярні звіти, онлайн-опитування, платформи оцінки ефективності програм
7	Гнучкість і адаптивність	Можливість швидко реагувати на виклики, змінювати політики	Адаптація програм після появи нових кіберзагроз чи цифрових платформ
8	Інноваційність та цифровізація	Застосування сучасних технологій у процесі управління	Використання чат-ботів, мобільних додатків, аналітики великих даних
9	Міждисциплінарність	Залучення різних сфер знань: право, соціологія, IT, педагогіка, психологія	Командна робота юристів, освітян, кіберполіції, психологів над спільними проектами
10	Координаційні механізми	Наявність постійно діючих міжвідомчих та міжсекторальних структур	Координаційні ради з безпеки дітей у кіберпросторі на рівні Кабміну та ОДА

Джерело: систематизовано автором [35;42]

Одним із прикладів реалізації governance-підходу є Національна стратегія захисту дітей в цифровому середовищі на 2021–2026 роки, яка базується на партнерстві держави, індустріальних компаній (оператори зв'язку, платформи контенту), освітян, батьківських спільнот і самих дітей. Документ передбачає спільну відповідальність за кіберзахист дітей і створення безпечного цифрового середовища [80].

Також у рамках мережевого підходу громадські організації стають повноправними суб'єктами реалізації політики. Зокрема, ГО «Ла Страда», «Save the Children», «Українська мережа за права дитини» здійснюють тренінги,

адвокацію, супровід дітей у складних життєвих обставинах. Згідно з дослідженнями Т. Семигіної [104], саме партнерська модель є найбільш ефективною для впровадження міжнародних стандартів захисту прав дитини, зокрема положень Конвенції ООН про права дитини.

У сучасному світі особливе місце в реалізації governance-підходу займають інформаційно-комунікаційні технології, які слугують одночасно і середовищем, і інструментом управління. Йдеться про: платформу «е-Малютко» – як приклад сервісу, що об'єднує декілька державних функцій (реєстрація народження, оформлення допомоги тощо); інформаційні системи моніторингу дітей в СЖО (складних життєвих обставинах); електронні консультації та платформи зворотного зв'язку з громадськістю.

У публічному управлінні, за словами Є. Котуха [54], нова цифрова архітектура держави вимагає змін не лише у формах подання послуг, але і в моделях врядування, в яких зникає розрив між управлінцем і громадянином, а рішення виробляються на засадах колективного інтелекту (crowdsourcing).

Попри переваги, застосування мережевої моделі має низку системних викликів: низький рівень довіри до органів влади з боку громадян; відсутність сталої інфраструктури взаємодії між державою і громадськістю; формальне залучення НУО до консультацій і прийняття рішень; цифрова нерівність і недостатній рівень цифрової грамотності серед певних категорій населення; брак фахівців у сфері цифрового управління.

Водночас, згідно з дослідженнями DQ Institute (2020) та EU Kids Online (2020) [134], мережеве управління є найефективнішою моделлю для боротьби з новітніми викликами, зокрема у сфері цифрової безпеки дітей, оскільки дозволяє об'єднати ресурси, знання та інструменти різних акторів.

Мережевий підхід (governance) є сучасною, гнучкою та адаптивною моделлю управління, яка забезпечує комплексну реалізацію політики захисту дітей, особливо в умовах цифрового середовища, гібридних загроз і швидких соціальних трансформацій. Він орієнтований на спільне вироблення рішень, багатосторонню участь, інституційну та технологічну відкритість, і є ключовим

для побудови інклюзивної гуманітарної безпеки, в основі якої лежить реальне забезпечення прав та безпеки кожної дитини.

Реалізація governance-моделі в Україні потребує політичної волі, розвитку партнерської інфраструктури, цифрової трансформації та зміни управлінської культури в бік прозорості, співучасті та довіри.

Мережевий підхід у державному управлінні, що базується на принципах горизонтальної координації, партнерства та співучасті, знаходить особливо плідне застосування у сфері захисту дітей. Це зумовлено складністю й багатогранністю викликів, які стоять перед сучасним суспільством: від соціальної нерівності, насильства, занедбаності до новітніх цифрових загроз, таких як кібербулінг, онлайн-грумінг, експлуатація в Інтернеті тощо. У таких умовах забезпечення прав і безпеки дитини не може залишатися виключною функцією органів державної влади – воно стає спільною справою держави, громадянського суспільства, приватного сектору, міжнародних партнерів, батьків і самих дітей.

Застосування мережевого підходу (governance) у сфері захисту дітей передбачає створення інституційно-організаційної системи багаторівневої взаємодії, у якій кожен суб'єкт – від міністерства до місцевого закладу освіти чи громадської ініціативи – виконує свою функцію, координуючи дії з іншими учасниками мережі. Це дозволяє підвищити ефективність заходів захисту, знизити дублювання функцій, оперативніше реагувати на загрози та формувати політику, орієнтовану на реальні потреби дитини, а не на формальні інструкції.

1. Платформи багатосекторальної взаємодії. Один із найбільш яскравих прикладів реалізації мережевого підходу – Національна стратегія захисту дітей в цифровому середовищі на 2021–2026 роки, яка впроваджується в Україні на основі партнерства між: державними органами (Міністерство цифрової трансформації, МВС, МОЗ, МОН, Мінсоцполітики); громадськими організаціями (ГО «Ла Страда-Україна», «Батьки за вакцинацію», «Stop Sexting»); міжнародними інституціями (ЮНІСЕФ, ОБСЄ, ЄС, СОЕ); приватним сектором (мобільні оператори, ІТ-компанії, платформи соцмереж, Google Україна, TikTok).

У межах цієї мережі кожен учасник виконує специфічну функцію: держава формує політику та забезпечує нормативно-правове підґрунтя [80], НУО надають сервіси підтримки, консультування та освіти, технологічні компанії впроваджують технічні рішення для блокування небажаного контенту або сповіщення про загрози.

2. Створення локальних міжвідомчих механізмів. Впровадження мережевого підходу на місцевому рівні передбачає створення координаційних рад, міжвідомчих груп та центрів безпеки дитини, у складі яких працюють: служби у справах дітей; центри соціальних служб; представники поліції (ювенальні інспектори, кіберполіція); освітяни та шкільні психологи; представники медичних закладів; громадські активісти.

Така взаємодія забезпечує оперативний обмін інформацією про вразливі випадки, спільне прийняття рішень щодо втручання в інтересах дитини, координацію профілактичної, реабілітаційної та просвітницької роботи. Застосування цієї моделі особливо актуальне у громадах, які приймають внутрішньо переміщених осіб, де діти часто перебувають у зоні підвищеного ризику.

3. Використання цифрових платформ як інструментів взаємодії. Цифрові інструменти відіграють ключову роль у побудові ефективної мережі управління. Платформи на кшталт: «е-Малятко» – об'єднує в один запит понад 10 послуг, пов'язаних із народженням дитини; «Дія» – надає сервіси для батьків і опікунів; «Національна платформа з безпеки дітей в інтернеті» – ресурс із навчальними матеріалами, формами зворотного зв'язку; боти у месенджерах, де можна анонімно повідомити про випадок насильства або загрозу.

Такі платформи не лише спрощують доступ до послуг, а й забезпечують зворотний зв'язок із громадянами, створюючи канали швидкої комунікації між державою і суспільством.

4. Залучення дітей до процесу ухвалення рішень. Одна з принципових ознак мережевого підходу – інклюзивність, тобто залучення самих дітей до процесів розробки, моніторингу й оцінки політик, що їх стосуються. Це

відповідає положенням Конвенції ООН про права дитини щодо врахування думки дитини [47], а також концепції «rights-based governance».

Прикладом такого залучення є: дитячі ради при органах місцевого самоврядування; дитячі омбудсмени; онлайн-опитування та фокус-групи; конкурси ідей щодо безпеки в інтернеті; участь у розробці освітніх програм про кібербезпеку (наприклад, з ініціативи Google Україна).

5. Взаємодія з міжнародними партнерами. Україна активно залучає досвід, експертизу та ресурси міжнародних інституцій у впровадження політик захисту дітей. Наприклад: програма ЮНІСЕФ «Спільно» забезпечує мобільні дитячі простори для дітей у кризових умовах; ЕСПАТ International підтримує боротьбу з експлуатацією дітей в інтернеті; Рада Європи впроваджує стандарти захисту дітей від сексуального насильства; EU Kids Online надає аналітику про поведінку дітей в цифровому середовищі [138]. Таке транскордонне партнерство є важливим ресурсом для посилення спроможності українських інституцій.

Таким чином, застосування мережевого підходу в сфері захисту дітей формує нову якість державної політики – інтегровану, відкриту, гнучку й орієнтовану на потреби дитини. Такий підхід дозволяє долати розрізненість між інституціями, розподіляти відповідальність, підвищувати ефективність реагування на загрози та формувати цілісну гуманітарну політику.

У сучасних умовах, коли загрози для дитини мають комплексний, часто цифровий або латентний характер, саме мережевий підхід стає єдиною можливою моделлю управління, здатною забезпечити сталу, системну й адаптивну політику державного захисту дітей.

У цифрову епоху, коли інформаційні технології проникають у всі сфери життя, цифрова складова мережевого управління набуває ключового значення у процесі забезпечення прав і безпеки дітей. Вона не лише доповнює традиційні інституційні механізми, а й створює нові канали комунікації, мобілізації ресурсів, ухвалення рішень і реагування на загрози, формуючи інноваційну екосистему для реалізації політики державного управління. Особливо актуально це в контексті захисту дітей у кіберпросторі – складової гуманітарної безпеки,

яка вимагає максимальної інтеграції цифрових інструментів на всіх рівнях управління.

1. Електронні сервіси як інструмент доступності і прозорості. Цифровізація державної політики у сфері захисту дітей починається з електронних сервісів, які дозволяють спростити доступ до адміністративних послуг для батьків, опікунів та підлітків. Наприклад: «єМалятко» об'єднує понад 10 послуг, пов'язаних із народженням дитини; «Дія» дає змогу отримати сертифікати, довідки, допомоги, включно з послугами захисту прав дитини; портали міністерств (МОН, Мінцифри, Мінсоцполітики) надають доступ до актуальної інформації та консультацій. Ці сервіси сприяють прозорості управління, зменшують корупційні ризики, забезпечують оперативність реагування та покращують інформованість громадян.

2. Цифрові платформи міжвідомчої взаємодії. Мережеве управління передбачає координацію дій різних структур, і цифрова складова тут виконує роль об'єднуючої інфраструктури. Успішним прикладом є: Національна платформа захисту дітей в цифровому середовищі, яка поєднує освітні, соціальні, медичні та правозахисні сервіси; системи електронного міжвідомчого документообігу між службами у справах дітей, поліцією, навчальними закладами, органами юстиції; електронні кейс-менеджмент системи, які дозволяють відслідковувати статус дитини, яка перебуває в складних життєвих обставинах. Завдяки цифровим технологіям реалізується швидкий і безпечний обмін даними, що особливо критично при роботі з конфіденційною інформацією щодо дітей.

3. Аналітика великих даних (Big Data) та штучний інтелект. Застосування аналітики великих даних та інструментів штучного інтелекту (AI) відкриває нові горизонти для моніторингу стану дитячого середовища. Це дозволяє: прогнозувати зони підвищених ризиків (наприклад, зростання кіберзагроз, насильства, депресії серед підлітків); виявляти приховані патерни негативних явищ (завдяки аналізу соціальних мереж, звернень на гарячі лінії, статистики злочинів); розробляти індивідуалізовані траєкторії підтримки для дітей у групах ризику.

Такий підхід вже реалізується у рамках Європейських хмарних платформ захисту дітей та частково імплементується в Україні через співпрацю з міжнародними структурами [138].

4. Освітньо-просвітницькі цифрові ресурси. Цифрова компонента є невіддільною частиною профілактики та просвіти у сфері захисту дітей. В Україні активно використовуються: платформи онлайн-освіти з безпеки в інтернеті (наприклад, «Stop Sexting», «Google: Безпека дітей»); інтерактивні уроки з цифрової грамотності для школярів; віртуальні курси для батьків і вчителів щодо розпізнавання ознак ризикованої поведінки в онлайні.

Це формує цифрову компетентність усіх учасників освітнього процесу та сприяє створенню безпечного освітнього середовища.

5. Цифровий зворотний зв'язок і участь громадян. Цифрова складова мережевого управління дозволяє не лише транслювати політики, а й отримувати зворотний зв'язок від суспільства: анонімні чат-боти для повідомлень про загрози (наприклад, «ReAction»); цифрові скриньки довіри в школах; онлайн-опитування дітей та батьків; мобільні додатки, які дозволяють оцінити рівень цифрової безпеки дитини вдома та в школі.

Це забезпечує участь користувача в політиці, що відповідає принципам демократичного, інклюзивного управління.

6. Захист персональних даних і кібербезпека. Цифровізація вимагає адекватного захисту персональних даних дітей, що в Україні забезпечується: нормами Закону України «Про захист персональних даних» [91]; імплементацією принципів GDPR [145]; розвитком інфраструктури кіберзахисту (зокрема, кіберполіції, CERT-UA, Уповноваженого з прав дитини); впровадженні стандартів безпеки в цифрових платформах, які взаємодіють з дітьми.

Цифрова складова мережевого управління у сфері захисту дітей є не лише технічним елементом, а стратегічним ресурсом нової моделі гуманітарної політики. Вона дозволяє поєднувати різнорівневі інституції в єдину систему реагування, спрощує доступ до послуг, формує цифрову культуру безпеки,

забезпечує захист прав дитини в інтернеті та офлайн-середовищі, а також створює нові можливості для участі громадян.

У сучасних умовах цифрова трансформація державної політики у сфері захисту дітей має бути пріоритетом не лише технічного, а ціннісного та стратегічного характеру, адже саме в інформаційному середовищі сьогодні формується майбутнє покоління нації.

У сучасному світі, де права людини визнані фундаментальною цінністю, підхід, орієнтований на права («rights-based approach»), виступає не просто як метод чи політична стратегія, а як світоглядна основа, на якій має будуватися державна політика в чутливих соціальних сферах. Однією з таких сфер є захист прав і безпеки дітей, де цей підхід є надзвичайно актуальним та ефективним у довгостроковій перспективі.

«Rights-based» підхід ґрунтується на міжнародних правових актах, насамперед на: Конвенції ООН про права дитини (1989), яка визнала дитину як самостійну особу з повним набором прав; Загальній декларації прав людини (1948) [41]; Європейській конвенції з прав людини [47]; міжнародних пактах ООН та регіональних інструментах захисту дітей.

На національному рівні основу правового підходу закладають Конституція України [49], Закон України «Про охорону дитинства» [95], Закон «Про забезпечення рівних прав і можливостей жінок і чоловіків», Сімейний кодекс та Цивільний кодекс України [109], а також Національна стратегія захисту дітей у кіберпросторі[80].

Підхід, орієнтований на права, базується на таких засадничих принципах: Верховенство права: дитина як суб'єкт, а не об'єкт політики; Недискримінація: рівний доступ до захисту всіх дітей незалежно від походження, статусу, віку, стану здоров'я; Участь дитини: дитина має право бути почутою, висловлювати свою думку та впливати на рішення, що її стосуються (принцип, закріплений у ст. 12 Конвенції ООН); Пріоритет найкращих інтересів дитини (ст. 3 Конвенції ООН; імплементовано в українське право через численні нормативно-правові акти [52; 84]); Підзвітність держави: органи влади несуть зобов'язання

забезпечити реалізацію прав дитини і можуть бути притягнуті до відповідальності в разі їх порушення.

На відміну від соціально-захисного підходу, який часто сприймає дитину як отримувача послуг або «об'єкт опіки», rights-based підхід визнає дитину як активного учасника суспільного життя, носія прав, гідності, свобод і потреб. Таким чином, змінюється акцент: із «піклування» – на «надання можливостей»; із «втручання» – на «партнерство з дитиною»; із «адміністративної моделі» – на «інклюзивну і права-орієнтовану політику».

Підхід, орієнтований на права дитини, поступово впроваджується в державну політику України через: діяльність Уповноваженого Президента з прав дитини [16]; створення служб у справах дітей на місцевому рівні; введення інклюзивних механізмів участі дітей у школах, громадах (шкільні ради, дитячі омбудсмени тощо); розробку національних стратегій, у яких дитина фігурує як пріоритетний суб'єкт (зокрема, у Стратегії з прав людини, Концепції реформування інтернатних закладів, Стратегії цифрової трансформації освіти); участь України у механізмах ЮНІСЕФ, Ради Європи, ОБСЄ щодо моніторингу дотримання прав дитини.

У контексті гуманітарної безпеки України, яка передбачає захист життя, гідності, цінностей і перспектив кожної людини, rights-based підхід дає змогу: створити справедливую систему раннього реагування на загрози (наси́льство, бу́лінг, експлуата́ція, викрадення, кібератаки); забезпечити інклюзію в освітньому, медичному, правовому середовищі; інтегрувати психологічну, інформаційну та правову підтримку для дітей, постраждалих від війни чи переміщених осіб; формувати культуру прав дитини у педагогів, батьків, державних службовців; гарантувати соціальну справедливість, що є основою стійкої та безпечної держави.

Попри стратегічне значення, rights-based підхід в Україні стикається з низкою бар'єрів: низький рівень правової обізнаності серед батьків та дітей; формалізм у діяльності органів опіки та правосуддя, які не завжди враховують думку дитини; недостатня міжвідомча взаємодія; обмеженість ресурсів для

реалізації права на освіту, охорону здоров'я, психологічну допомогу; не врегульованість цифрових прав дитини.

Таким чином, rights-based підхід є потужним концептуальним і практичним інструментом, що дозволяє будувати ціннісно-орієнтовану, підзвітну і справедливу політику державної політики у сфері захисту дітей. У фокусі цього підходу – не абстрактна дитина як категорія, а реальна дитина як особистість, громадянин, носій гідності та прав. Інтеграція rights-based парадигми у стратегії гуманітарної безпеки України є не лише етичною вимогою, а й необхідною умовою формування демократичного, гуманного та безпечного суспільства.

У сучасних умовах посилення складності суспільних відносин, зростання кількості транснаціональних і цифрових загроз, ефективна політика державної політики у сфері захисту дітей не може базуватися виключно на вертикальній моделі «держава – громадянин». Сучасні виклики потребують застосування інтеграційного та мультисекторального підходів, що дозволяють поєднати зусилля всіх залучених сторін – держави, громадянського суспільства, приватного сектору, міжнародних організацій, наукової спільноти та безпосередньо самих дітей.

Інтеграційний підхід передбачає розгляд захисту дитини як багатовимірного феномену, що вимагає комплексного об'єднання правових, соціальних, освітніх, інформаційних, психологічних та інституційних механізмів. Йдеться про формування єдиної політики, в межах якої забезпечується координація дій усіх державних органів та інтеграція функцій різних сфер – освіти, охорони здоров'я, соціального захисту, правосуддя, інформаційної безпеки тощо. Наприклад, питання кіберзахисту дітей не може бути вирішене винятково силами кіберполіції або освітніх установ. Воно потребує спільних дій Держспецзв'язку, Міністерства цифрової трансформації, МОН, Мінсоцполітики, омбудсмена, ІТ-компаній, громадських організацій та самих батьків [80; 10; 11; 34].

Мультисекторальний підхід (multisectoral approach) – це стратегія, згідно з якою: кожна галузь державної політики включається у процес розробки та

реалізації політики щодо дітей; міжгалузеві дії скоординовані та взаємодоповнюючі; нормативна база, фінансування, моніторинг та відповідальність розподіляються відповідно до функцій секторів; формується єдина платформа або інституційний механізм, який забезпечує системність і цілісність політики (національні стратегії, міжвідомчі комісії, платформи взаємодії тощо).

Прикладом такого підходу в Україні є Національна стратегія захисту дітей у кіберпросторі на 2021–2026 роки, яка об'єднує цифрову трансформацію, освіту, правосуддя, інформаційну безпеку, соціальні послуги і права дитини в єдину рамку [80].

В умовах війни, внутрішньої міграції, руйнування соціальної інфраструктури, загроз у кіберпросторі інтеграційний і мультисекторальний підходи стають не просто корисними – вони життєво необхідні для: формування єдиного безпекового простору для дітей; створення дієвих механізмів раннього виявлення та реагування на загрози; залучення міжнародних ресурсів на основі прозорості та партнерства; стабілізації соціальної тканини громади через залучення всіх стейкхолдерів до процесу захисту дітей.

Інтеграційний та мультисекторальний підходи є ключовими для формування сучасної, стійкої, ефективної політики державної політики у сфері захисту дітей. Вони дозволяють подолати міжвідомчу роз'єднаність, знизити ризики управлінської неузгодженості та побудувати систему, в якій кожна дитина – незалежно від місця проживання, сімейного статусу чи рівня цифрової грамотності – отримає захист і підтримку. У ширшому контексті, така модель політики є основою гуманітарної безпеки та сталого розвитку України як європейської соціальної держави.

Формування ефективної політики державної політики у сфері захисту дітей в умовах цифрових трансформацій, гібридних загроз та зростання вразливості дитячої аудиторії вимагає не лише інституційної спроможності та нормативної бази, а й використання сучасних теоретико-методологічних підходів до прийняття рішень. Одним з таких підходів є теорія управлінських рішень у поєднанні з теорією раціонального вибору, яка надає системний,

логічний і доказовий інструментарій для ухвалення оптимальних управлінських стратегій у складних умовах.

В основі цієї теорії – ідея, що ефективне державне управління ґрунтується на послідовності дій, що веде до досягнення цілей із врахуванням ресурсних обмежень, суспільних очікувань і прогнозів розвитку ситуації [2; 3; 14].

У контексті політики захисту дітей це означає, що будь-яке рішення – наприклад, запровадження національної програми цифрової безпеки, створення платформи електронного моніторингу випадків насильства над дітьми, чи прийняття нормативного акту – має проходити через структурований процес аналізу, що включає ідентифікацію проблеми, формулювання мети, вибір критеріїв ефективності та прогнозування наслідків [1; 69].

Теорія раціонального вибору базується на припущенні, що суб'єкти приймають рішення, зважуючи вигоди та витрати, орієнтуючись на максимізацію власної корисності. У сфері публічної політики ця модель трансформується: її адаптовано до потреб колективного вибору, де інтереси суспільства домінують над індивідуальними вигодами.

У сфері захисту дітей це дозволяє: оцінювати альтернативні стратегії втручання (наприклад, профілактика онлайн-загроз через освіту vs. посилення кіберконтролю); враховувати інтереси різних груп: державних органів, батьків, шкіл, IT-сектору, самих дітей; вибудовувати оптимальні варіанти партнерства – наприклад, державно-приватне партнерство у розробці програм фільтрації контенту чи психологічної підтримки [30; 123].

Таким чином, у центрі ухвалення рішень мають бути раціональні обґрунтування, які враховують: цілісність політики; ефективність розподілу ресурсів; довгострокові наслідки; ризики соціального неприйняття. На основі класичної моделі прийняття управлінського рішення (див. [2; 14]) можна виокремити такі етапи (табл. 1.5):

Усе це вимагає від державних органів поєднання раціональної логіки, етичних принципів і адаптивних механізмів, що є характерним для новітніх підходів до політики «evidence-based» та «child-sensitive policy». Теорія управлінських рішень та раціонального вибору надає наукове обґрунтування

для проектування й реалізації ефективної політики у сфері захисту дітей. Вона допомагає: структурувати процес прийняття рішень; уникнути політичного або емоційного волюнтаризму; забезпечити зваженість, прогнозованість і прозорість дій держави; підвищити довіру суспільства до інституцій захисту прав дитини.

Таблиця 1.5

Етапи прийняття державного рішення у сфері захисту дітей

Етап	Зміст	Приклад для сфери захисту дітей
Ідентифікація проблеми	Визначення реальної загрози	Зростання випадків кібербулінгу серед школярів
Збір інформації	Аналітика, моніторинг, експертиза	Дані Нацполіції, соціопитування, звіти МОН
Генерація альтернатив	Визначення можливих рішень	Освітня кампанія / технічний контроль / законодавча заборона
Оцінка альтернатив	Порівняння ефективності, вартості, ризиків	Аналіз вартості й потенціалу підтримки
Прийняття рішення	Вибір оптимального варіанту	Запуск інтерактивної освітньої платформи
Реалізація	Впровадження в життя	Розробка контенту, підготовка вчителів
Оцінка результатів	Зворотний зв'язок, коригування	Моніторинг кількості скарг, повторний аудит

Джерело: [18; 27]

Водночас ця теорія повинна застосовуватись у поєднанні з гуманітарними підходами, орієнтованими на права дитини, етичні стандарти та міжнародні норми, що забезпечить її реальну життєздатність у соціально чутливій сфері.

Аналіз сучасних теоретичних підходів до формування політики державної політики у сфері захисту дітей засвідчує багатовимірність і складність цієї проблематики. Державна політика у цій сфері вже давно вийшла за межі суто нормативного регулювання та потребує системного інтегрування гуманітарних, соціальних, цифрових, правових та управлінських компонентів, що визначає необхідність опори на комплексні наукові підходи (табл. 1.6).

Нормативно-правовий підхід є фундаментом системи захисту дітей, оскільки забезпечує закріплення базових прав і гарантій дитини в законодавстві. Однак він не є самодостатнім і має реалізовуватися в комплексі з інституційним та організаційним наповненням.

Підходи до формування політики державної політики у сфері захисту дітей

Підхід	Сутність	Ключові принципи	Механізми реалізації	Переваги	Обмеження
Нормативно-правовий	Формування політики через закони, підзаконні акти, стратегії	Законність, правова визначеність, захист прав	Прийняття законів, стратегій, програм, постанов, наказів	Юридична чіткість, підзвітність, формалізація зобов'язань	Часто декларативність без механізмів реалізації
Інституційний	Визначення структур, які реалізують політику	Розмежування повноважень, функціональна ефективність	Створення служб у справах дітей, комісій, департаментів, омбудсмена	Чіткий розподіл ролей, наявність відповідальних органів	Можливе дублювання функцій, слабка координація
Governance / мережевий	Побудова політики через співпрацю держави, громади, бізнесу, НУО	Партнерство, горизонтальність, децентралізація	Міжвідомчі ради, коаліції, державно-приватні ініціативи, платформи	Гнучкість, мобілізація ресурсів, інноваційність	Висока потреба у координації, залежність від ресурсів партнерів
Rights-based (орієнтований на права)	Спрямованість на реалізацію прав дитини як суб'єкта	Недискримінація, участь, найкращі інтереси дитини	Врахування думки дитини, правозахисний аудит, child-friendly justice	Ціннісність, правова обґрунтованість, справедливність	Потребує високого рівня обізнаності, часто ігнорується на практиці
Інтеграційний	Об'єднання всіх секторів політики (освіта, охорона здоров'я, правопорядок тощо)	Комплексність, міждисциплінарність, координація	Спільні програми, міжвідомчі плани, узгоджені стандарти	Узгодженість, системність, ефективність використання ресурсів	Потребує міжвідомчої волі та фінансування
Мультисекторальний	Включення всіх ключових галузей і суб'єктів в єдиний процес	Відповідальність, взаємодія, ефективність	Програми на стику освіти, медицини, ІТ, юстиції; міжсекторальний аудит	Виявлення прогалин, залучення нових партнерів, краща ефективність	Висока управлінська складність, потреба в постійній координації
Рационального вибору / управлінських рішень	Оцінювання рішень на основі вигод, витрат, ефекту	Максимізація користі, ефективність, альтернативність	Моделі аналізу рішень, KPI, оцінка політики, сценарне моделювання	Обґрунтованість, уникнення волюнтаризму, прозорість	Потреба в якісних даних, ризик технократизму
Доказової політики (evidence-based policy)	Рішення на основі даних, фактів, досліджень	Емпіричність, об'єктивність, відповідальність	Моніторинг, соціологія, аудит, аналітичні звіти	Підвищення якості рішень, підзвітність	Потреба в якісних системах даних, аналітичному персоналі
Адаптивний / гнучкий підхід	Політика, що здатна швидко змінюватись відповідно до викликів	Гнучкість, реагування, зворотний зв'язок	Регулярне оновлення стратегій, механізми пілотування, тестування	Актуальність, швидка реакція на нові загрози	Потребує постійного моніторингу, складно прогнозувати
Цифровий / технологічний підхід	Використання цифрових інструментів у розробці й реалізації політики	Автоматизація, доступність, прозорість, інновації	Е-сервіси, боти, мобільні додатки, платформи онлайн-консультування	Масовість, зручність, оперативність	Цифрова нерівність, залежність від ІТ-ресурсів

Джерело: систематизовано автором

Інституційний підхід дозволяє окреслити коло суб'єктів, наділених повноваженнями у сфері захисту дітей, їхню компетенцію, механізми координації та підзвітності. Його ефективність залежить від здатності інституцій до міжсекторальної взаємодії та інноваційного оновлення.

Мережевий (governance) підхід актуалізує взаємодію держави, громадянського суспільства, приватного сектору й міжнародних партнерів у режимі партнерства, горизонтальної відповідальності та відкритості. У сучасних умовах саме мережеві механізми сприяють мобілізації ресурсів і забезпеченню адресності заходів захисту.

Rights-based підхід формує ціннісне ядро політики, виводячи в центр її архітектури права дитини як автономного суб'єкта. Це дозволяє оцінювати ефективність державного втручання не лише за показниками результативності, а й з позицій справедливості, поваги до гідності та забезпечення «найкращих інтересів дитини».

Інтеграційний і мультисекторальний підхід передбачає комплексну взаємодію усіх сфер державної політики – освіти, охорони здоров'я, цифрової трансформації, соціального захисту, правопорядку – задля досягнення єдиного гуманітарного ефекту. Теорія управлінських рішень і раціонального вибору формалізує процес вироблення політики, дозволяє уникати ситуативності та політичного волюнтаризму, забезпечує її доказовість і стратегічну зваженість.

Отже, ефективна політика державної політики у сфері захисту дітей може бути сформована лише за умов поєднання зазначених теоретичних підходів. Вони не виключають, а доповнюють одне одного, створюючи підґрунтя для побудови системної, сталозабезпечувальної та чутливої до викликів сучасності моделі захисту дітей як ключового елементу гуманітарної безпеки України. У перспективі це дозволить не лише зміцнити механізми забезпечення прав дитини, а й сприяти формуванню соціально стійкого, ціннісно орієнтованого та відповідального громадянського суспільства.

1.3. Концептуальні засади дослідження державної політики у сфері цифрової безпеки дітей

У XXI столітті цифрова трансформація набула глобального характеру, охопивши всі сфери життєдіяльності людини – від економіки й управління до освіти, комунікації та дозвілля. Особливої уваги в цьому контексті заслуговує становище дитини, яка з раннього віку стає активним користувачем цифрових технологій, проте водночас залишається однією з найбільш вразливих соціальних груп у кіберпросторі. Цифрова безпека дітей в умовах поширення інтернет-залежності, кібербулінгу, онлайн-шахрайства, дезінформації, сексуальної експлуатації та інших загроз є ключовим викликом для національної гуманітарної політики, правового регулювання та механізмів державної політики [10; 28; 35].

Сучасні умови формування цифрової культури суспільства потребують не просто захисту дитини від загроз у кіберпросторі, а створення цілісної державної політики, яка забезпечуватиме права, свободи та інтереси дітей у кіберпросторі. Така політика має ґрунтуватися на концептуально вивірених підходах, що враховують не лише правові норми, але й особливості соціального, інституційного, технологічного та комунікаційного контексту сучасного суспільства.

У цьому підрозділі розглядаються ключові концептуальні засади дослідження державної політики у сфері цифрової безпеки дітей, що включають теоретико-методологічні підходи, аналітичні рамки, нормативно-правову базу, а також інституційно-функціональні особливості реалізації політики захисту прав дітей у кіберпросторі. Аналіз опирається на узагальнення наукових джерел [33; 34; 35; 37; 55], вітчизняних і міжнародних стратегічних документів [80; 93; 99], а також результатів досліджень у сфері інформаційної безпеки, кіберпростору та прав людини [50; 52; 112].

Особлива увага приділяється мультидисциплінарному характеру цифрової безпеки дітей, що вимагає інтеграції знань із суміжних наукових галузей – права, психології, педагогіки, соціології, інформаційних технологій та

державного управління. Такий підхід дозволяє сформувати системне бачення механізмів захисту дітей в умовах цифрової реальності та закласти підґрунтя для ефективного управлінського впливу.

Таким чином, концептуальні засади дослідження цифрової безпеки дітей у сфері державної політики визначають методологічну рамку для подальшого формування, реалізації та оцінювання державної політики, орієнтованої на безпеку та добробут дитини як пріоритет гуманітарної безпеки України.

Проблематика цифрової безпеки дітей, як об'єкта державного управління, перебуває на перетині кількох наукових дисциплін. Її розгляд не може обмежуватися виключно правовим чи технічним підходом, оскільки сам феномен кіберпростору – складний, динамічний і багаторівневий, з властивою йому гібридністю ризиків, що загрожують дитині як фізично, так і ментально, соціально та культурно. Отже, в основі ефективного управління цифровою безпекою дітей лежить міждисциплінарна концептуалізація, яка забезпечує системний та цілісний аналіз об'єкта управління.

Зокрема, публічне управління забезпечує інституційно-організаційну рамку для формування і реалізації державної політики у цій сфері, вивчаючи механізми координації між державними, громадськими та приватними суб'єктами [2; 4; 20; 61]. Юридична наука, в свою чергу, фокусується на правовому регулюванні, зокрема гарантуванні прав дитини в цифровому середовищі, механізмах адміністративно-правового захисту, а також імплементації міжнародних стандартів, таких як Конвенція про права дитини, Європейська конвенція з прав людини та Конвенція про кіберзлочинність [47; 48; 97; 104].

Психологія та педагогіка додають до цієї картини глибоке розуміння впливу цифрового контенту на психоемоційний стан, соціалізацію та освітні траєкторії дітей. Психологічні дослідження доводять зв'язок між цифровими ризиками та зниженням рівня безпеки дитини, що вимагає залучення профілактичних програм, освітніх інтервенцій та роботи з батьками [79; 84; 107].

Інформаційні технології та кібербезпека, як прикладна галузь, забезпечують технічні інструменти контролю та моніторингу, аналізу великих даних (big data), розпізнавання загроз (threat detection), використання інтелектуальних систем на основі ШІ (AI) для виявлення кібербулінгу, спроб groomingu тощо [28; 30; 55; 66; 81].

Важливо, що останні дослідження акцентують на інформаційній безпеці як складовій гуманітарної безпеки, що зміщує фокус з традиційної безпекової парадигми (захист від технічних загроз) на ціннісно-антропоцентричну – захист прав і свобод дитини у кіберпросторі[7; 9; 35]. У цьому контексті формується підхід, орієнтований на права дитини («rights-based approach»), який інтегрує соціальну справедливість, етичні норми, нормативно-правові гарантії та управлінські механізми в єдину систему державного реагування.

Таким чином, міждисциплінарна природа концептуального осмислення цифрової безпеки дітей дозволяє сформувати інтегративну парадигму, в якій управлінські, правові, технічні, соціальні та гуманітарні елементи поєднуються для забезпечення комплексного захисту дитини як суб'єкта права, соціалізації і розвитку. Застосування такого підходу надає можливість для створення адаптивних, ефективних і орієнтованих на людину (human-centric) стратегій державної політики в цифрову епоху (табл. 1.7).

Методологічні положення дослідження державної політики у сфері цифрової безпеки дітей формують теоретико-інструментальну основу для аналізу, обґрунтування та проектування ефективної державної політики у цій галузі, що знаходиться на перетині гуманітарної, правової, управлінської, інформаційно-технологічної та соціальної проблематики. Цифрова безпека дітей є складовою ширшої системи національної безпеки, зокрема її гуманітарного сегменту, а також елементом політики захисту прав дитини в умовах цифрової трансформації суспільства.

З огляду на міждисциплінарний характер предмету, дослідження ґрунтується на комплексному застосуванні принципів і методів кількох наукових галузей. Методологія дослідження побудована на основі системного підходу, що дозволяє розглядати цифрову безпеку дітей як частину цілісної

структури управління суспільною безпекою в інформаційну епоху. Це дозволяє аналізувати взаємозв'язки між інституціями, механізмами, політиками та цифровими ризиками, що впливають на інтереси дитини.

Таблиця 1.7

Міждисциплінарний аналіз концептуальних основ цифрової безпеки дітей

Дисципліна / Галузь знань	Об'єкт дослідження	Концептуальний внесок	Ключові джерела
Публічне управління	Механізми державного регулювання, політики, управлінські рішення	Формування політик, управлінських стратегій, механізмів координації між секторами	[2], [4], [20], [61], [67]
Юриспруденція (право)	Права дитини, законодавче регулювання, судовий захист	Забезпечення правового захисту дитини, імплементація міжнародного права, нормативне забезпечення	[47], [48], [52], [97], [104]
Психологія	Психоемоційний стан, поведінка в інтернеті	Виявлення цифрових загроз: кібербулінг, залежність, психологічна травма	[79], [84], [107], [70]
Педагогіка / Освіта	Освітні практики, цифрова грамотність	Розвиток цифрових компетентностей дітей, просвіта батьків та вчителів щодо безпеки у кіберпросторі	[33], [34], [105]
Інформаційні технології / ІТ	Кіберпростір, цифрова інфраструктура	Розробка систем фільтрації, моніторингу, алгоритмів виявлення загроз, інструменти кіберзахисту	[28], [30], [55], [66], [81]
Соціологія / соціальна політика	Соціальні ризики, нерівність доступу, цифрова сегрегація	Аналіз цифрових викликів для різних груп дітей, створення інклюзивної безпечної цифрової екосистеми	[9], [33], [38]
Гуманітарні науки / філософія	Цінності, гуманітарна безпека, етика цифрового простору	Антропоцентризм, захист людської гідності в цифровому світі, філософія безпеки та культури	[7], [35], [142], [143]

Застосування інституціонального підходу дає змогу виявити основні суб'єкти управління (державні органи, освітні установи, правоохоронні структури, громадські організації, цифрові платформи) та оцінити ефективність їхньої взаємодії в умовах динамічного цифрового середовища. Управлінська взаємодія, як правило, відбувається в умовах поліцентричної моделі – мережевого врядування (governance), де держава не є єдиним актором, а співпрацює з приватним сектором, медіа, ІТ-компаніями, міжнародними організаціями [20], [67].

Окрему аналітичну вагу має нормативно-правовий підхід, що дозволяє оцінити відповідність національного законодавства міжнародним стандартам (зокрема, Конвенції ООН про права дитини [47], Конвенції про кіберзлочинність [48], Загальної декларації прав людини [41]) та виявити правові прогалини у сфері цифрового захисту дітей. Це передбачає також аналіз дієвості правозастосування, ефективності регуляторних інструментів, правового забезпечення цифрової грамотності та захисту персональних даних [91], [112].

Мережевий підхід (network-based governance), який включає концепції публічно-приватного партнерства, соціальних інновацій та спільного врядування, забезпечує методологічну платформу для дослідження нових форм взаємодії між державою та цифровим середовищем. Це дозволяє враховувати ризики, що виникають у результаті алгоритмічного управління, використання штучного інтелекту в модерації контенту, автоматизованого збору даних дітей у мережі [54], [66].

У контексті управлінських наук важливим є використання методології теорії управлінських рішень і раціонального вибору, яка дозволяє проаналізувати логіку, критерії, обмеження та наслідки прийняття державних рішень у сфері кібербезпеки дітей. Такий підхід акцентує увагу на пошуку балансу між інтересами дитини, вимогами безпеки, технічними можливостями та соціально-етичними нормами [2], [76].

У дослідженні також застосовано права́вий підхід «rights-based approach», що фокусується на забезпеченні найкращих інтересів дитини як головного критерію формування політики. Такий підхід передбачає залучення дітей як суб'єктів до оцінювання безпечності цифрового простору, розвиток процедур оскарження, створення механізмів участі дітей у прийнятті рішень щодо їх цифрової безпеки [52], [84].

Крім того, для емпіричного обґрунтування дослідження застосовуються методи контент-аналізу стратегічних і нормативних документів, порівняльний аналіз міжнародних практик, соціологічні опитування, статистичний аналіз даних про інциденти цифрової небезпеки серед дітей, а також експертне оцінювання ефективності існуючих політик.

Таким чином, методологічна основа дослідження характеризується інтегративністю, міждисциплінарністю та інноваційністю, що дозволяє адекватно оцінити динаміку ризиків цифрового середовища та забезпечити формування ефективної політики державної політики у сфері цифрової безпеки дітей.

Методологія дослідження цифрової безпеки дітей у контексті державної політики потребує комплексного, міждисциплінарного та системного підходу. Актуальність теми обумовлює необхідність переосмислення традиційних методологічних рамок на користь нових, гнучких, адаптивних моделей пізнання, які здатні враховувати як динамічні трансформації інформаційного середовища, так і зростаючі загрози цифровим правам дитини.

У межах дисертаційного дослідження запропоновано ґрунтуватися на поєднанні сучасної методології державного управління, теорії безпеки, інформаційної теорії, соціальних теорій ризику та інтердисциплінарних парадигм гуманітарної безпеки (табл. 1.8).

Таким чином, методологічна основа дослідження забезпечує комплексне, науково обґрунтоване бачення проблеми цифрової безпеки дітей як складової сучасного державної політики у сфері гуманітарної та національної безпеки. Обґрунтована методологія є передумовою для формування ефективної політики, орієнтованої на права дитини та виклики цифрової епохи.

У формуванні державної політики цифрової безпеки дітей стратегічні та концептуальні документи відіграють ключову роль, оскільки вони визначають пріоритети, завдання, інструменти та інституційну архітектуру державної політики у даній сфері. Розвиток цифрового середовища, посилення кіберзагроз і зростання вразливості дитячої аудиторії обумовлюють необхідність інтеграції захисту дітей у кіберпросторів загальнонаціональні стратегії безпеки, цифровізації, гуманітарної політики та соціального захисту.

Насамперед, важливо відзначити Закон України «Про основи національної безпеки» [92], у якому вперше системно задекларовано гуманітарну безпеку як структурну складову національної безпеки держави. Водночас у ньому цифрова безпека ще не окреслена як окрема категорія, що

свідчить про необхідність актуалізації стратегічного бачення з урахуванням цифрових трансформацій.

Таблиця 1.8

**Концептуальні положення дослідження державної політики у сфері
цифрової безпеки дітей**

Концептуальний підхід	Суть та зміст	Завдання в межах дослідження	Практичне значення
Системний підхід	Розгляд цифрової безпеки як частини загальної системи гуманітарної та національної безпеки	Виявлення взаємозв'язків між інституціями, політиками, інструментами управління	Забезпечує комплексний аналіз сфери цифрового захисту дітей
Інституціональний підхід	Аналіз суб'єктів управління, їх функцій, повноважень та взаємодії	Ідентифікація ключових акторів у сфері цифрової безпеки дітей	Визначає ефективну модель інституційної взаємодії
Нормативно-правовий підхід	Аналіз правових норм, стандартів, міжнародних та національних актів	Виявлення прогалин у законодавстві, відповідність міжнародним зобов'язанням	Сприяє вдосконаленню законодавчого поля у сфері цифрової безпеки
Мережевий (Governance) підхід	Управління як взаємодія мережі державних та недержавних суб'єктів	Дослідження механізмів публічно-приватного партнерства, громадської участі	Підвищує гнучкість і ефективність управлінських моделей
Підхід «rights-based»	Орієнтація на забезпечення прав дитини як основного суб'єкта політики	Визначення механізмів залучення дітей до процесів прийняття рішень, оцінки політик	Забезпечує реалізацію принципу «найкращих інтересів дитини»
Теорія управлінських рішень	Логіка, критерії, етапи прийняття рішень у сфері публічного управління	Вибір оптимальних рішень за обмежених ресурсів, в умовах ризику та цифрової невизначеності	Підвищує ефективність політик цифрової безпеки
Міждисциплінарний підхід	Залучення знань з права, ІТ, педагогіки, психології, соціології	Інтеграція багатогалузевих даних для створення цілісної моделі захисту	Враховує всі аспекти ризиків та потреб дитини у кіберпросторі
Порівняльно-аналітичний підхід	Вивчення міжнародного досвіду (ЄС, США, ООН, UNICEF, тощо)	Виявлення найкращих практик управління цифровою безпекою дітей	Дає змогу адаптувати ефективні моделі до українського контексту
Контент-аналіз / аналітика політик	Аналіз стратегічних документів, програм, звітів, законів	Виявлення тенденцій, прогалин, інструментів цифрової безпеки	Формує базу для доказового ухвалення державних рішень
Емпіричні методи (опитування, інтерв'ю, статистика)	Збір і аналіз даних про кіберінциденти, сприйняття загроз дітьми, думка батьків і педагогів	Підтвердження гіпотез, верифікація концепцій, оцінка ефективності впроваджених рішень	Дає змогу зробити науково обґрунтовані пропозиції щодо державної політики

Джерело: систематизовано автором

Вагомим кроком у напрямі консолідації зусиль держави стало ухвалення Національної стратегії у сфері прав людини (2015 р.) та оновленої Національної стратегії захисту дітей в цифровому середовищі на 2021–2026 роки [80], яка вперше на рівні державної політики чітко артикулювала проблематику цифрової безпеки дітей. Цей документ закладає підґрунтя для реалізації комплексного підходу до захисту дітей онлайн, включаючи: створення безпечного цифрового контенту; розвиток цифрової медіаграмотності серед дітей, батьків і педагогів; упровадження механізмів виявлення та блокування шкідливого контенту; формування міжвідомчої координації суб'єктів захисту дітей; підвищення рівня цифрової компетентності посадовців у сфері захисту дітей.

Окрім того, важливу методологічну роль відіграють Концепція розвитку цифрової економіки та суспільства України на 2018–2020 роки [99], яка заклала основи для побудови інформаційно-безпекової інфраструктури, а також Концепція розвитку електронного урядування в Україні [98], де відзначається необхідність цифрової інклюзії та рівного доступу до цифрових благ, зокрема для дітей і молоді.

Не менш важливою є Концепція забезпечення кібербезпеки України, затверджена Законом України «Про основні засади забезпечення кібербезпеки України» [93], яка орієнтована на створення єдиної системи кіберзахисту, включно із захистом дітей від кіберзлочинності, кібербулінгу, сексуальної експлуатації, втручання в приватність тощо. Згідно з цією Концепцією, цифрова безпека дітей трактується як частина національних інтересів у кіберпросторі, що створює передумови для інтеграції дитячого виміру у стратегічне планування у сфері безпеки.

На міжнародному рівні стратегічну базу формують:

1. Конвенція ООН про права дитини (1989) та Загальна декларація прав людини (1948), де підкреслюється право дитини на безпеку, приватність, доступ до інформації та захист від експлуатації [41; 47; 78].

2. Європейська стратегія «Better Internet for Kids» (BIK), яка фокусується на створенні безпечного цифрового простору для дітей у країнах ЄС.

3. Рекомендації Ради Європи, які зобов'язують держави-члени забезпечувати захист дітей від кіберзлочинності, відповідно до Конвенції про кіберзлочинність (Будапештська конвенція) [48].

У сукупності ці документи створюють стратегічну рамку, в межах якої здійснюється розробка, реалізація та моніторинг державної політики у сфері цифрової безпеки дітей. Проте їх реалізація потребує постійного оновлення та адаптації до нових загроз (deepfake, grooming, online radicalization тощо) і динаміки цифрової поведінки дітей.

У сучасних умовах цифрова безпека дітей потребує не лише декларативного, а інституційно-забезпеченого закріплення в стратегічних документах України, що передбачає: створення окремої підсистеми цифрового захисту дітей у системі кібербезпеки держави; закріплення індикаторів оцінки ефективності відповідної політики; розширення партнерських форматів з ІТ-сектором, громадськими організаціями та міжнародними інституціями [30; 38].

Таким чином, стратегічні та концептуальні документи відіграють ключову роль у формуванні цілісної державної політики щодо цифрової безпеки дітей, закладаючи нормативно-інституційний каркас і визначаючи вектори міжсекторальної координації. Подальший розвиток цієї сфери має базуватись на принципах дитиноцентризму, цифрової справедливості та гарантованого захисту цифрових прав дитини в контексті національних інтересів України.

Концепт державної політики у сфері цифрової безпеки дітей є складною багатовимірною конструкцією, що формується на перетині кількох міждисциплінарних площин: публічного управління, інформаційної безпеки, прав дитини, педагогіки, кіберпсихології та цифрової етики. Його формування відповідає сучасним трансформаціям гуманітарної безпеки, де дитина визнається не лише об'єктом захисту, а й повноправним суб'єктом цифрової взаємодії, потреби та інтереси якого мають бути стратегічним пріоритетом державної політики.

У науковому контексті концепт цифрової безпеки дітей включає в себе системне бачення процесів, механізмів і принципів, спрямованих на захист дітей від шкідливого впливу цифрового середовища та забезпечення умов для

безпечного, повноцінного і вільного користування інформаційно-комунікаційними технологіями (ІКТ). Водночас цей концепт охоплює не лише превентивні заходи, а й розвитковий потенціал дитини в цифровому середовищі, що відповідає правовій парадигмі «best interest of the child» (найкращі інтереси дитини) [84], [52].

Теоретичне осмислення концепту державної політики цифровою безпекою дітей ґрунтується на гуманітарно-центричному підході, згідно з яким безпека не обмежується захистом від фізичних чи інформаційних загроз, а охоплює цілісність особистості, право на ідентичність, інтелектуальний розвиток, психологічну стійкість, свободу думки й захист персональних даних.

У структурі цього концепту можна виокремити декілька ключових категоріальних блоків:

1. Суб'єктний блок – охоплює державні інституції (Міністерство цифрової трансформації, МОН, Національна поліція, Держспецзв'язку, суди, Служба у справах дітей), недержавні організації, цифрові платформи, родини, педагогів і самих дітей як активних учасників процесу формування політики безпеки [37], [46].

2. Регулятивно-нормативний блок – включає міжнародні (Конвенція ООН про права дитини, GDPR, Конвенція про кіберзлочинність) та національні документи (Закон України «Про основні засади забезпечення кібербезпеки», Національна стратегія захисту дітей у кіберпросторі) [80], [93], [97].

3. Інструментальний блок – охоплює практичні механізми реалізації політики, зокрема цифрові інструменти моніторингу, освітні програми з цифрової грамотності, правопросвітництво, електронні платформи підтримки дітей, національні реєстри кіберінцидентів та індикаторів ризику [35], [38], [33].

4. Ціннісно-етичний блок – визначає філософську основу концепту, яка орієнтована на повагу до гідності дитини, її автономії в цифровому середовищі, права на безпеку, приватність, участь та захист від експлуатації.

5. Міждисциплінарний блок – підкреслює теоретичну інтеграцію знань з кіберпсихології, інформаційного права, теорії публічного управління, цифрової педагогіки, інтернет-маркетингу та соціології дитинства [7], [40], [59].

Таким чином, теоретичне осмислення концепту дозволяє виявити його як фундаментальну модель, у межах якої можливо формувати ефективну, цілісну та інклюзивну державну політику. Він не лише окреслює предмет управлінського впливу, а й надає епістемологічне обґрунтування для подальшого наукового аналізу, методологічного проектування, а також практичної імплементації стратегій цифрової безпеки в інтересах дитини.

Цей концепт, з одного боку, вимагає постійного оновлення у відповідь на динаміку цифрових ризиків, а з іншого – забезпечує стратегічну стійкість управлінських рішень, спираючись на універсальні цінності прав людини та принципи належного врядування.

Сучасна цифрова епоха формує нову реальність функціонування соціуму, в якій цифровий простір стає не лише середовищем для комунікації та навчання, але й джерелом значних загроз, особливо для вразливих категорій населення – зокрема дітей. З огляду на стрімке зростання онлайн-активності серед неповнолітніх, питання забезпечення їхньої цифрової безпеки перетворюється на пріоритет державної політики в сфері гуманітарної безпеки, права та управління. При цьому цифрові трансформації мають подвійну природу: з одного боку – відкривають нові можливості для розвитку дитини, з іншого – значно підвищують ризики зловживань, маніпуляцій, агресії та психологічного насильства в онлайні.

Серед ключових викликів, що актуалізують потребу в переосмисленні підходів до державної політики у сфері цифрової безпеки дітей, варто виокремити наступні:

1. Кількісне зростання онлайн-загроз. За останні роки в Україні зафіксовано суттєве зростання інцидентів, пов'язаних із кібербулінгом, грумінгом, секстингом, залученням дітей до онлайн-шахрайств, витоком персональних даних та експлуатацією у кіберпросторі[10], [11], [128]. Згідно з даними Національної поліції України та МОН, понад 65% дітей стикаються з формами агресії в інтернеті до 16-річного віку [33], [79].

2. Розмитість меж між реальним і віртуальним середовищем для дітей. З раннього віку цифровий простір стає невіддільною частиною життя дитини:

соціалізація, навчання, дозвілля, комунікація – усе більше відбувається онлайн. У результаті ризику цифрового впливу мають не менш значущі наслідки, ніж загрози в офлайн-середовищі, впливаючи на психоемоційний, когнітивний і ціннісний розвиток особистості [7], [35], [80].

3. Швидкоплинність змін у кіберпросторі. Технології штучного інтелекту, доповненої реальності, блокчейн-систем, алгоритмів рекомендацій, deepfake-контенту тощо – створюють нові, раніше не існуючі, загрози. У таких умовах традиційні методи регулювання втрачають ефективність, а державна політика має бути адаптивною, гнучкою та випереджувальною [81], [148].

4. Дефіцит цифрових навичок у дорослих, відповідальних за захист дітей. Батьки, педагоги, соціальні працівники часто не володіють достатніми знаннями про алгоритми платформ, техніки маніпуляції, способи виявлення небезпек, що суттєво ускладнює реалізацію профілактичних та захисних заходів [32], [83], [105].

5. Інституційна фрагментація відповідальних суб'єктів. У сфері захисту дітей у кіберпросторі діє ціла низка державних та недержавних органів, проте їхня взаємодія недостатньо скоординована. Відсутність чіткого лідера, дублювання функцій, слабкий обмін інформацією – усе це знижує ефективність захисту та ускладнює комплексне реагування [34], [37], [106].

6. Неврегульованість багатьох аспектів на законодавчому рівні. Попри наявність Закону України «Про основні засади забезпечення кібербезпеки України» [93], низка аспектів цифрової безпеки дітей – як-от обробка персональних даних неповнолітніх, правові засади онлайн-згоди, відповідальність платформ – досі залишаються правовими прогалинами [36], [91], [112].

7. Посилення інформаційного впливу в умовах гібридної війни. Російська військова агресія супроводжується активною дезінформацією, пропагандою та психологічним тиском на українських дітей через цифрові канали. У цьому контексті питання цифрової безпеки перетворюється не лише на гуманітарне, а й на складову національної безпеки [21], [22], [23].

Урахування вищезазначених викликів вимагає перегляду підходів до державного управління: від реактивного (післяфактного) – до превентивного та проактивного; від ізольованого – до мережевого, що базується на партнерстві між державою, громадянським суспільством, міжнародними організаціями та цифровими платформами.

Таким чином, сучасні виклики цифрової епохи вимагають побудови нової управлінської парадигми, орієнтованої на цілісність, адаптивність, інноваційність і дитиноцентризм, де забезпечення цифрової безпеки дітей розглядається як стратегічний пріоритет державної політики в умовах інформаційного суспільства.

У межах підрозділу здійснено системний науковий аналіз концептуальних засад дослідження державної політики у сфері цифрової безпеки дітей, що дозволило сформулювати методологічну та категоріальну основу для подальшого опрацювання дослідницької проблематики.

Встановлено, що феномен цифрової безпеки дітей є складним, багаторівневим і міждисциплінарним явищем, що охоплює юридичні, соціальні, психологічні, інформаційні та управлінські аспекти. Його дослідження потребує застосування гнучкої комбінації підходів – системного, нормативно-правового, інституціонального, мережевого (governance), інтеграційного, rights-based та підходів публічного адміністрування, зокрема теорії управлінських рішень. Такий міждисциплінарний підхід дозволяє враховувати як специфіку державного управління, так і дитиноцентричну парадигму, орієнтовану на забезпечення найкращих інтересів дитини в цифровому середовищі.

Особливу увагу приділено стратегічним та концептуальним документам, що формують політику України у сфері цифрової безпеки – зокрема, Національній стратегії захисту дітей у кіберпросторі(2021–2026), Закону України «Про основні засади забезпечення кібербезпеки України», Концепції розвитку цифрової економіки, а також міжнародно-правовим актам — Конвенції про права дитини, Будапештській конвенції про кіберзлочинність тощо. Їхній зміст дозволив чітко окреслити нормативно-ціннісні рамки та стратегічні вектори дослідження.

Також окреслено концептуальні засади дослідження, серед яких ключову роль відіграють: системність, компаративність, правова і стратегічна верифікованість, а також використання кількісно-якісних методів аналізу. Виявлено, що для формування ефективної моделі державної політики у сфері цифрової безпеки дітей необхідна інтеграція зусиль різних секторів: державного, освітнього, громадського, ІТ-середовища та міжнародних інституцій.

Таким чином, результати дослідження заклали цілісну теоретико-концептуальну основу для подальших емпіричних і прикладних досліджень із розроблення механізмів державної політики, спрямованої на гарантування цифрової безпеки дітей як одного з ключових пріоритетів гуманітарної безпеки України.

Висновки до розділу 1

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 концептуальне 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.

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 багатовимірний 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, ІТ-сферою та міжнародними організаціями [4, 20, 54].

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 проекту 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 межах дослідження було чітко 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. Це зумовлює не лише багатогранність об'єкта дослідження, а й потребу у формуванні інноваційного міждисциплінарного концепту, який би включав у себе такі складові: суб'єктно-об'єктну взаємодію, що передбачає включення дитини не лише як об'єкта захисту, а як активного учасника процесу цифрової взаємодії та користувача цифрових послуг; нормативно-ціннісні орієнтири, які визначають пріоритетність прав дитини в цифровій політиці; цифрові інструменти управління, включаючи електронне урядування, алгоритмічне регулювання, кіберінфраструктурні механізми; механізми контролю та моніторингу загроз, що базуються на сучасних аналітичних, правових та технічних засобах оцінки ризиків.

Проведена міждисциплінарна декомпозиція цього концепту дозволила обґрунтувати необхідність інтеграції знань і підходів із таких галузей, як кібербезпека (захист від технічних та інформаційних загроз), педагогіка (формування цифрової компетентності дітей), соціологія дитинства (вивчення поведінкових патернів у кіберпросторі), психологія (оцінка емоційного та ментального впливу цифрових технологій), інформаційне право (правове регулювання даних, приватності та прав дітей), а також цифрове врядування (архітектура управління цифровими процесами на макро- та мезорівнях). Такий міждисциплінарний підхід забезпечує не лише глибше розуміння об'єкта дослідження, але й сприяє формуванню ефективних, адаптивних та сталих управлінських рішень у сфері цифрової безпеки дітей.

У процесі дослідження було виокремлено методологічні основи, які забезпечують наукову обґрунтованість і цілісність підходу до аналізу та моделювання управлінських рішень у цій сфері. До таких підходів, зокрема, віднесено: системний підхід, що дає змогу бачити цифрову безпеку дітей у контексті єдиної системи національної безпеки; структурно-функціональний підхід, який акцентує увагу на взаємозв'язках між суб'єктами, функціях і ролях державних інституцій; компаративний підхід, що дозволяє порівнювати національні і міжнародні практики; прогностичний підхід, орієнтований на визначення майбутніх викликів і розробку превентивних стратегій. Застосування цих підходів у сукупності забезпечує всебічне й гнучке дослідження, адаптоване до стрімких трансформацій цифрового середовища.

Особливе значення у концептуалізації проблематики має аналіз стратегічних документів, які визначають державну політику у сфері цифрового дитинства. Зокрема, ключовим документом визнано Національну стратегію захисту дітей у кіберпросторі на 2021–2026 роки, яка формалізує пріоритети, цілі та напрями державного реагування. Однак детальний аналіз її положень дозволив виявити суттєві розриви між стратегічними намірами та реальним рівнем їх імплементації. Недостатність інституційної координації, обмежене ресурсне забезпечення, фрагментарність нормативно-правової бази, відсутність чітких показників ефективності – ці чинники ускладнюють реалізацію цифрової політики щодо дітей. У зв'язку з цим актуалізується потреба в перегляді наявних концептуальних та процедурних рамок, посиленні інтеграційних механізмів, розширенні горизонтальних міжвідомчих зв'язків та формуванні системного міжсекторального підходу, що базується на принципах дітиноцентризму, відкритості та сталості.

РОЗДІЛ 2. АНАЛІЗ СТАНУ РЕАЛІЗАЦІЇ ДЕРЖАВНОЇ ПОЛІТИКИ ЗАХИСТУ ДІТЕЙ У КІБЕРПРОСТОРІ В УКРАЇНІ

2.1. Сучасні загрози дітям у кіберпросторі та їх вплив на безпеку дитини

Значне зростання цифровізації всіх сфер суспільного життя у ХХІ столітті призвело до того, що кіберпростір став не лише середовищем комунікації, навчання й дозвілля, але й полем нових ризиків, особливо небезпечних для дітей. У зв'язку з цим питання забезпечення кібербезпеки дитини виходить за межі суто технічної проблематики та набуває міждисциплінарного значення, охоплюючи соціальні, правові, психологічні й управлінські аспекти. Особливої актуальності ця тема набуває в контексті трансформації національної системи безпеки України в умовах гібридних загроз і збройного конфлікту, що супроводжується активною інформаційною війною, спрямованою, зокрема, на вразливі групи, серед яких діти займають особливе місце [12; 30; 35].

Сучасні дослідження свідчать, що діти є однією з найбільш незахищених категорій користувачів Інтернету. Через обмежений життєвий досвід, недостатню критичність сприйняття інформації, довірливість та підвищену емоційність вони стають легкою мішенню для зловмисників, маніпуляторів і кіберзлочинців [10; 11; 32]. Окрім технічних ризиків – таких як зараження пристроїв шкідливим програмним забезпеченням або витік персональних даних – віртуальне середовище несе також численні загрози психоемоційному стану дитини: кібербулінг, кібергрумінг, експозиція до небезпечного або травмуючого контенту, ігрова залежність тощо.

Загрози, які виникають у кіберпросторі, мають тенденцію до стрімкої еволюції, що потребує оперативної та адаптивної реакції з боку інституцій державного управління, освітніх закладів, родин і самих дітей. Відтак, постає нагальна потреба у розробці та впровадженні ефективних механізмів запобігання таким загрозам, їх виявлення, нейтралізації наслідків, а також формування культури безпечної поведінки в мережі.

Метою цього підрозділу є систематизація основних типів загроз, з якими стикаються діти у кіберпросторі, аналіз механізмів їхнього впливу на різні аспекти безпеки дитини, а також визначення ключових викликів для державної політики у сфері кіберзахисту дитинства. У межах розгляду особливу увагу буде приділено сучасним тенденціям поширення загроз, їхньому психологічному та соціальному впливу, а також специфіці українського контексту, обумовленого війною, цифровими трансформаціями й потребою в інтегрованому підході до протидії загрозам у кіберсередовищі.

У сучасному кіберпросторі кіберпростір для дітей виступає як простором можливостей, так і зоною ризику. З одного боку, він відкриває доступ до знань, інструментів самореалізації, соціалізації; з іншого – становить серйозну загрозу фізичній, психологічній, емоційній, соціальній і правовій безпеці дитини. З огляду на це, виникає необхідність у систематичному підході до класифікації цифрових загроз, що враховує не лише їхню природу, а й механізми впливу на дитячу аудиторію, особливості вікового розвитку та здатність до самозахисту.

Класифікація кіберзагроз для дітей, запропонована нижче, ґрунтується на міжгалузевому аналізі (інформаційна безпека, право, психологія, педагогіка, соціологія) і спирається на сучасні дослідження у сфері захисту прав дитини, цифрової політики та кібербезпеки [10; 32; 33; 35; 36; 38; 79; 138].

1. Контентно-орієнтовані загрози. Цей тип загроз пов'язаний із доступом дитини до шкідливого, неприйняттого або потенційно травматичного контенту. До таких належать: Порнографічні матеріали, зокрема дитяча порнографія (включно з «сексуалізованим» контентом, що не містить прямих зображень статевих органів, але є еротизованим). Сцени жорстокості, насильства, реальні або змодельовані відео, що можуть викликати психотравму. Контент, що пропагує суїцид, аутоагресію, харчові розлади (напр., «групи смерті», флешмоби на кшталт «Синій кит»). Інформація, яка популяризує наркотики, зброю, деструктивні культи тощо. Пропагандистські матеріали, фейки, що мають на меті вплив на політичні, етнічні чи релігійні переконання дитини.

Контентно-орієнтовані загрози найбільш поширені серед дітей середнього та старшого шкільного віку. Основна проблема полягає у неможливості дитини адекватно фільтрувати інформацію, а також у психологічному ефекті ідентифікації з героями, що може мати наслідком наслідувальну поведінку або посттравматичні стани [10; 32; 36].

2. Комунікаційні загрози. Цей блок охоплює ризики, що виникають у процесі цифрової взаємодії дитини з іншими користувачами, зокрема: Кібербулінг – систематичне цькування, переслідування, приниження дитини в онлайн-середовищі: через соціальні мережі, месенджери, відеоігри [11; 79]. Кібергрумінг – встановлення довіри до дитини з боку дорослого з метою її сексуальної експлуатації чи примусу до певної поведінки (від пересилання фото до реальних зустрічей) [32; 35]. Онлайн-харасмент, шантаж (сексторшн) – вимагання інтимного контенту, погрози щодо його оприлюднення. Онлайн-радикалізація – залучення до екстремістських груп через переконливу комунікацію.

Згідно з результатами досліджень проєкту EU Kids Online 2020, близько 28% українських дітей у віці 11–17 років стикалися з проявами кібербулінгу, і понад 6% повідомили про контакти з особами, які вдавали себе за когось іншого або намагалися зманіпулювати [138].

3. Загрози технічного характеру. Це загрози, пов'язані з функціонуванням пристроїв, додатків, інфраструктури: Шкідливе ПЗ, віруси, трояни, кейлогери – зараження пристрою з метою викрадення інформації, контролю або шантажу [44; 51; 81]. Фішинг та соціальна інженерія – отримання персональних даних або доступу до акаунтів через обман. Небезпечні додатки, посилення, онлайн-сервіси – під виглядом ігор, утиліт або освітніх платформ поширюється ПЗ, що виконує шпигунські або деструктивні функції. Загрози з боку IoT – «розумні іграшки» з підключенням до Інтернету можуть містити вразливості для витоку даних або бути використані для спостереження.

Ці загрози вимагають особливої уваги з боку батьків і технічного супроводу в освітніх закладах, адже дитина часто не усвідомлює природи

небезпеки – зокрема при завантаженні програм з неперевічених джерел або при підключенні до відкритих Wi-Fi-мереж [28; 30; 44; 55].

4. Особистісні та поведінкові ризики. До цієї групи належать загрози, що впливають на формування поведінкових моделей: Інтернет-залежність (ігрозалежність, залежність від соцмереж, відеоконтенту). Формування девіантної поведінки через контент або онлайн-спільноти. Сексуалізація або вульгаризація свідомості внаслідок впливу інфлюенсерів, блогерів із деструктивною поведінкою. Самоідентифікаційна криза, викликана віртуальним порівнянням із «ідеальними» образами (підвищення тривожності, зниження самооцінки, депресивні розлади).

У науковій літературі фіксується прямий зв'язок між рівнем залучення до віртуальних середовищ та розвитком психосоціальних розладів у підлітковому віці, зокрема – тривожності, порушень сну, гіперактивності, асоціальної поведінки [34; 35; 79].

5. Юридичні та репутаційні ризики. Ці загрози мають відстрочений, але стійкий ефект:

5.1. Порушення прав дитини, пов'язані з обробкою персональних даних без належної згоди (у т.ч. з порушенням GDPR і Закону України «Про захист персональних даних» №2297-VI) [91; 112; 145].

5.2. Створення цифрового дос'є дитини: непередбачені публікації батьків, вчителів, самих дітей (т. зв. «шерентинг») формують довгостроковий слід в Інтернеті, що може негативно вплинути на майбутнє дитини.

5.3. Кіберзлочинна відповідальність – залучення дітей до протиправної діяльності, зокрема участі у DDOS-атаках, зламі акаунтів, поширенні шкідливого ПЗ або фейкової інформації (іноді – несвідомо).

Законодавство України передбачає відповідальність за кіберзлочини, проте рівень обізнаності дітей і підлітків у цій сфері залишається недостатнім [46; 55; 93].

Таким чином, класифікація кіберзагроз для дітей дозволяє чітко структурувати ризики за їхньою природою, механізмами впливу та потенційними наслідками. Такий підхід є основою для формування ефективної

системи державної політики захисту дітей у кіберпросторі, що повинна поєднувати нормативно-правовий, технічний, освітній, психологічний і комунікативний компоненти [1; 14; 34; 35; 80]. Розуміння типології загроз є першочерговою умовою для подальшого проектування захисних механізмів, формування цифрової грамотності дітей, а також визначення стратегічних пріоритетів у державному управлінні кібербезпекою.

Серед усього спектра кіберзагроз для дітей особливе занепокоєння викликає доступ до небажаного або шкідливого цифрового контенту, який чинить прямий вплив на психоемоційний стан, моральний розвиток і соціальну поведінку дитини. Йдеться про візуальні, текстові або мультимедійні матеріали, які за своїм змістом є неприйнятними для осіб, які не досягли психологічної та емоційної зрілості.

Отже, небажаний та шкідливий контент у кіберпросторі становить системну загрозу безпеці дитини. Його багатфакторний вплив виявляється у трансформації мислення, поведінки, соціальних норм дитини, викликаючи ризики психологічного травмування, формування девіацій і порушення адаптації. Подолання цієї загрози можливе лише за умов інтегрованого підходу, що включає правову регламентацію, технічні бар'єри, інституційну відповідальність, освітні ініціативи та індивідуальну медіаграмотність [1; 14; 32; 35; 38; 80].

Проблематика кібербезпеки дитини в сучасному кіберпросторі має комплексний характер і вимагає не лише розгляду загроз як таких, але й ґрунтовного аналізу їх впливу на різні аспекти безпеки дитини. Оскільки безпека дитини – багатовимірна категорія, яка включає фізичну, психологічну, соціальну, правову та інформаційну складові [7; 23; 40], то й вплив цифрових ризиків необхідно оцінювати в цьому багатогранному контексті.

Цей графік ілюструє динаміку зростання основних кіберзагроз в Україні за період з 2021 по 2024 рік, з фокусом на інциденти, які безпосередньо або опосередковано впливають на дітей. На графіку представлено загальну кількість кібератак, інциденти в школах, а також специфічні загрози для дітей –

фішинг і кібербулінг. Дані змодельовано на основі відкритої статистики та аналітичних припущень (рис. 2.1).

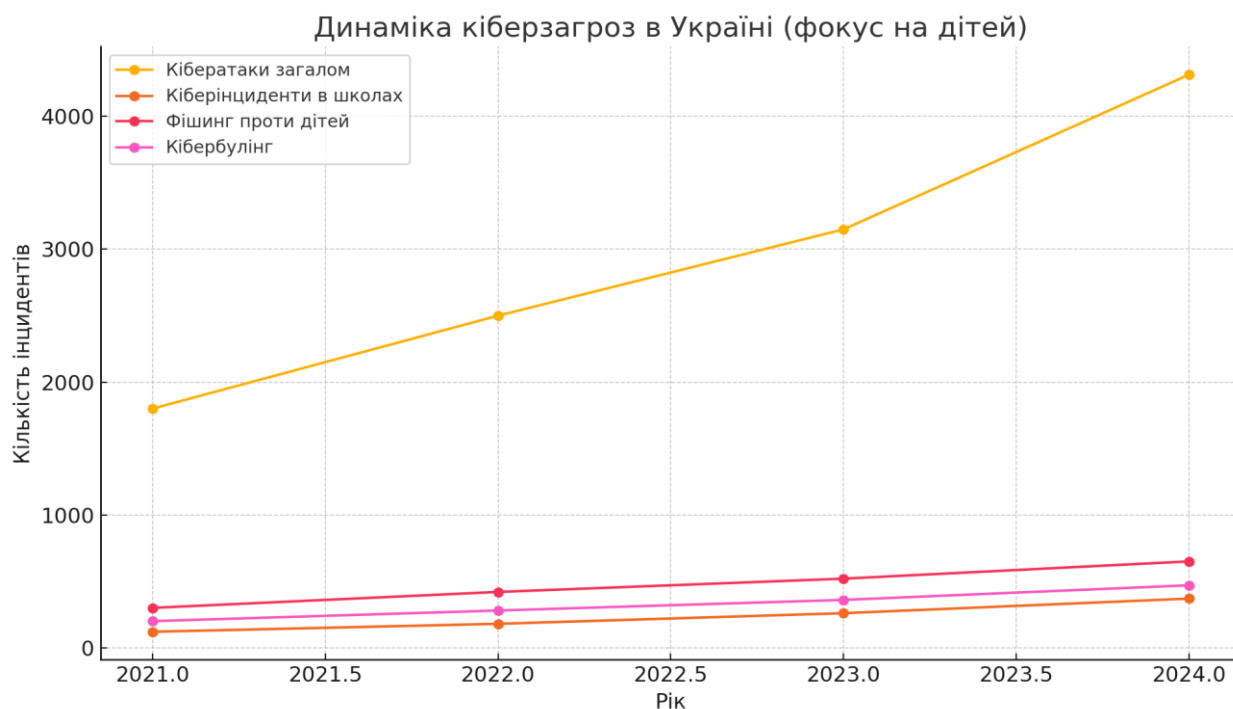


Рис. 2.1. Динаміка кіберзагроз в Україні (2021–2024)

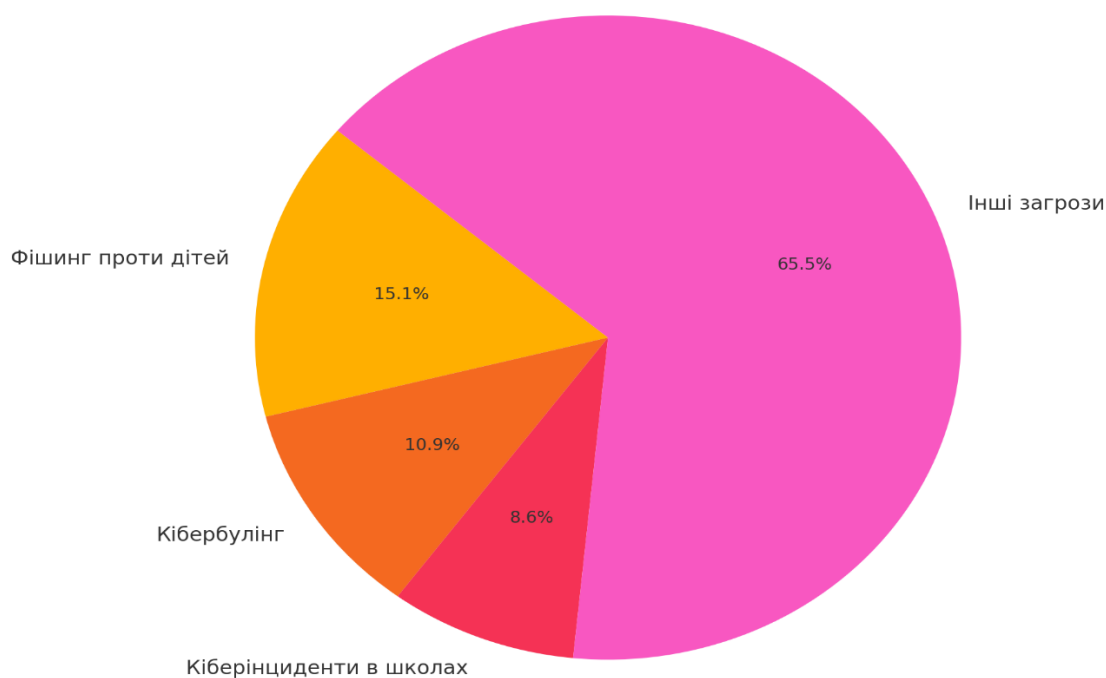
Джерело: [82-83]

Згідно з графіком, усі категорії загроз демонструють стабільне зростання, що свідчить про посилення кіберризиків у дитячому середовищі. Особливо тривожним є зростання кількості фішингових атак і кібербулінгу, що вказує на потребу в посиленні цифрової безпеки в школах та серед дітей.

Кругова діаграма демонструє співвідношення основних типів кіберзагроз, які вплинули на дітей в Україні у 2024 році. У візуалізації враховано фішинг, кібербулінг, шкільні кіберінциденти, а також інші види загроз, що не були деталізовані, але зафіксовані в загальній статистиці (2.2).

Найбільшу частку становлять інші кіберзагрози (які можуть включати шкідливе ПЗ, злом акаунтів, вимагання тощо), проте фішинг та кібербулінг разом охоплюють значну частину інцидентів, що безпосередньо стосуються дітей. Це підтверджує високий рівень вразливості дітей до соціальних інженерних атак і психологічного тиску в онлайн-середовищі.

Структура кіберзагроз для дітей в Україні у 2024 році

**Рис. 2.2. Структура кіберзагроз для дітей у 2024 році**

Джерело: [82-83]

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.2.3).

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.

Розглянемо, як кіберзагрози трансформуються у реальні ризики для безпеки дитини за основними вимірами її життєдіяльності.

1. Психологічна та емоційна безпека. Це один із найчутливіших вимірів, який найперше реагує на вплив кіберзагроз. Як показує практика, тривале або навіть короткочасне зіткнення дитини з негативним цифровим

досвідом (кібербулінг, харасмент, перегляд сцен насильства тощо) здатне викликати: підвищену тривожність, дратівливість, фобії, включно зі страхом користування цифровими засобами; депресивні симптоми, суїцидальні настрої, особливо серед підлітків, які є вразливими до соціальної оцінки; втрату самооцінки, особливо внаслідок кібербулінгу, порівняння з «ідеальними образами» у соцмережах, стигматизації або шантажу [11; 35; 79].

Низка психологічних досліджень підтверджує, що цифрові травми мають ефект накопичення, і за відсутності своєчасної підтримки (з боку сім'ї, школи, фахівців) можуть перейти в розлади адаптації та хронічні стани, що потребують медичного втручання [33; 34].

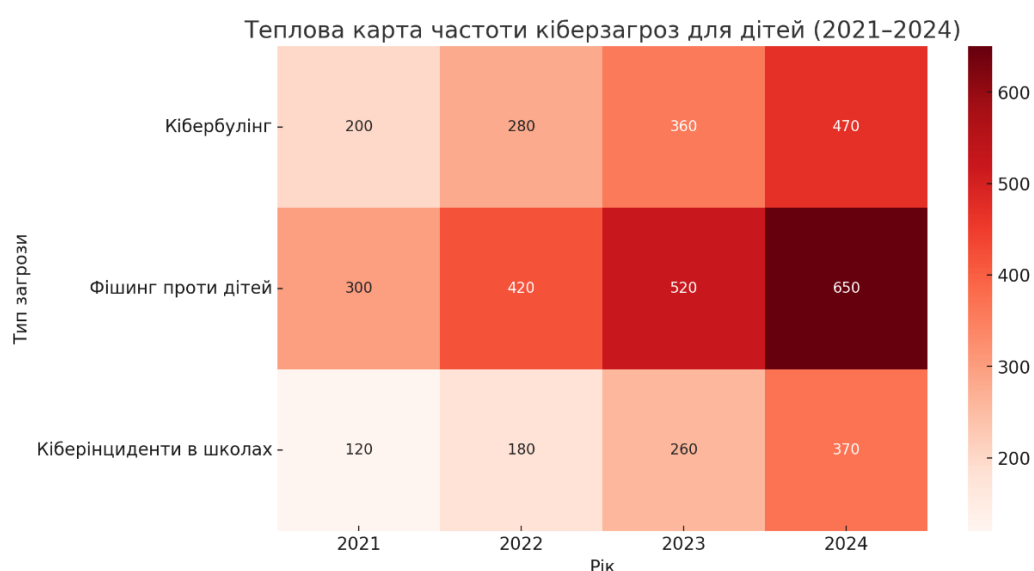


Рис. 2.3. Частота кіберзагроз для дітей (2021–2024)

Джерело: [82-83]

2. Соціальна безпека. Кіберзагрози мають істотний вплив на соціальну сферу життя дитини, особливо на: здатність до комунікації, яка порушується через ізоляцію, втрату довіри до оточення; стратегії поведінки у колективі – дитина, що зазнала кібербулінгу, часто переходить у позицію соціальної оборони або агресії; деформацію моделі соціалізації, коли основні взаємодії дитини відбуваються в онлайн-просторі за викривленими правилами, без етичних рамок.

У контексті війни та змішаного навчання, віддаленої освіти та зростання ролі цифрового середовища, дитина дедалі більше залежна від онлайн-

середовища як головного каналу соціальної взаємодії. Відтак, соціальна безпека напряду корелює з якістю та безпечністю цифрових контактів [9; 20; 30].

3. Фізична безпека. Хоч кіберзагрози спершу видаються нематеріальними, однак вони можуть мати реальні фізичні наслідки, зокрема: зустрічі з незнайомцями, які починаються в цифровому просторі (наприклад, унаслідок грумінгу), що може закінчитися викраденням, насильством або експлуатацією [10; 35; 32]; реалізація деструктивних флешмобів («синій кит», «повісься на виклик», «відключи дихання»), які становлять безпосередню загрозу життю та здоров'ю; залучення до незаконної діяльності (перенесення посилок, втягування у злочинні схеми), ініційоване через цифрові канали.

Крім того, довготривале перебування перед екранами та ігрова залежність викликають соматичні порушення: порушення сну, гіподинамію, мігрень, проблеми із зором – що також є складовими зниження фізичної безпеки [33; 34; 79].

4. Правова та інформаційна безпека. Цей вимір включає низку загроз, що стосуються:

- порушення прав дитини, передбачених законодавством України та міжнародними актами (Конвенція ООН про права дитини [47], Закон України «Про охорону дитинства» [95], GDPR [145]), через: збір, обробку та зберігання персональних даних без згоди; розголошення фото, відео, інтимної інформації;
- поширення матеріалів за участю дітей у порнографічних або небажаних формах. створення цифрового сліду дитини, який може переслідувати її у майбутньому (наприклад, через публікацію особистих даних у юному віці);
- використання дитини в кіберзлочинних схемах (наприклад, як «проксі-учасника» для переказу коштів або зламу акаунтів), що потенційно призводить до юридичних наслідків.

Відсутність цифрової обізнаності та правової грамотності серед дітей і підлітків суттєво збільшує ризик потрапляння у правову пастку або використання зловмисниками правових прогалин [91; 112; 46].

5. Культурно-ціннісна та гуманітарна безпека. Цифровий простір активно впливає на: формування ідентичності дитини, особливо в період підліткового самовизначення; сприйняття норм моралі, культури, цінностей, що можуть змінюватися під впливом ідеологічно забарвленого або комерційно спрямованого контенту; руйнування патріотичної, громадянської та національної самоідентифікації внаслідок дезінформації, впливу ворожих інформаційних кампаній.

Гуманітарна безпека як складова національної безпеки у сфері дитинства все частіше розглядається через призму інформаційної війни, в якій діти стають об'єктами м'якої сили, маніпуляцій та втрати критичного мислення [7; 27; 35; 60].

6. Цифрова та кібергігієнічна безпека. Цей вимір тісно пов'язаний із рівнем цифрової компетентності дитини та здатністю користуватись технологіями без шкоди: небезпека небезпечного онлайн-спілкування, фішингових атак, відкриття файлів без перевірки; відсутність паролів, шифрування, антивірусів – наслідок як браку навичок, так і недбальства; довіра до незнайомих ресурсів, додатків, платформ, реєстрація без верифікації.

Цифрова гігієна дитини формується переважно з боку школи та батьків – і її відсутність посилює всі інші загрози. Таким чином, кіберзагрози впливають на безпеку дитини не лінійно, а системно, охоплюючи щонайменше шість критично важливих вимірів: психологічний, соціальний, фізичний, правовий, гуманітарний та цифровий. Цей багатовимірний підхід дозволяє глибше зрозуміти природу впливу цифрових ризиків і краще обґрунтувати необхідність інтегрованої державної політики, орієнтованої не лише на реагування, але й на попередження та формування середовища стійкості дитини до кіберзагроз [1; 14; 30; 35; 38; 80].

Цей підхід потребує: впровадження системи оцінки ризиків для дітей у кіберпросторі; регулярного моніторингу проявів загроз та їх наслідків; інтеграції психологічного, правового та технічного супроводу в навчальний процес; залучення батьків, школи, державних інституцій та цифрових платформ до спільної відповідальності за безпеку дитини у кіберпросторі.

Особливістю сучасного етапу розвитку України є функціонування держави у воєнно-політичних умовах повномасштабної збройної агресії Російської Федерації, що триває з 2014 року і досягла свого апогею у 2022 році. У таких умовах питання безпеки набуває тотального характеру та охоплює не лише традиційні сфери національної безпеки – військову, енергетичну, економічну – але й гуманітарну, зокрема інформаційну й дитячу безпеку як стратегічно вразливі напрями. Війна змінила характер і масштаб загроз у кіберпросторі, вивівши кіберпростір на передній план гібридної війни, у межах якої діти стали цільовою групою як для прямих атак, так і для інформаційного впливу з боку противника.

Насамперед слід зазначити, що масова цифровізація освітнього процесу, спричинена карантинними обмеженнями під час пандемії COVID-19, а згодом і повномасштабною війною, суттєво розширила присутність дітей у кіберпросторі. За даними аналітичних звітів, понад 90% учнів шкільного віку в Україні щоденно користуються мережею Інтернет для навчання, спілкування та дозвілля. Така інтенсивність користування цифровими технологіями не супроводжувалася адекватною підготовкою до безпечного перебування в онлайн-середовищі, що призвело до суттєвого зростання ризиків цифрового характеру для дітей [10; 32; 34; 80].

Війна створила нові формати кіберзагроз, які раніше мали або локальний характер, або були рідкісними. Зокрема, до специфічних проявів цифрових ризиків в українських умовах належать наступні.

Цілеспрямовані інформаційні атаки проти дітей та молоді з боку ворожих сил, що мають на меті: поширення паніки, фейків, дезінформації («фейки про мобілізацію підлітків», «захоплення шкіл», «отруєння води», «обстріли з використанням дитячих координат»); психологічний тиск через месенджери, соціальні мережі та геймерські платформи; вплив на національну ідентичність дитини – зниження рівня довіри до державних інституцій, мілітаризація свідомості, романтизація ворожої армії [7; 23; 35].

Використання цифрових інструментів для збору інформації через дітей – ворог активно застосовує соціальну інженерію в ігрових додатках, чатах і

соціальних мережах для: визначення розташування об'єктів ЗСУ або критичної інфраструктури; отримання фото й відео з місць подій; виманювання геолокацій через "ігрові" платформи чи конкурси.

Це підтверджується численними повідомленнями СБУ та Кіберполіції України про спроби залучення дітей до розвідувальної діяльності, в тому числі шляхом фінансового стимулювання за пересилання координат чи фото техніки [11; 30; 55].

Кібербулінг на національному ґрунті: у соціальних мережах почастишали випадки цькування українських дітей з боку підконтрольних ворогу акаунтів, особливо – тих, хто опинився за кордоном, у тимчасовій міграції, або в тимчасово окупованих територіях. Такі дії мають на меті дискредитацію національної ідентичності, приниження гідності, викликання внутрішнього конфлікту між національною і особистою ідентичністю.

Посилення деструктивного контенту: в умовах війни значно зросла частка візуального контенту з елементами насильства, смерті, руйнувань, який стає доступним навіть наймолодшим користувачам через TikTok, Telegram, Instagram, YouTube. Такий контент травмує дитину, призводить до десенсибілізації, втрати чутливості до насильства, а іноді й до його наслідування в ігровій формі [35; 79; 138].

Нестача батьківського контролю через вимушену мобілізацію, розділення сімей, релокацію або перебування батьків за кордоном. У таких умовах дитина залишається сам на сам із цифровими загрозами, а спроби самостійного захисту без належних знань та навичок часто є неефективними.

Низький рівень психологічної стійкості через постійний стрес воєнного часу, що підсилює негативний вплив кіберзагроз. Травматичний досвід (втрати, евакуації, обстріли) послаблює психологічні бар'єри дитини, робить її більш вразливою до шантажу, погроз, грумінгу.

У цьому контексті варто звернути увагу на результати соціологічного дослідження, проведеного Національною школою суддів України у 2023 році, згідно з яким понад 42% українських дітей у віці 10–17 років заявили про переживання психологічного дискомфорту через онлайн-контент, пов'язаний із

війною; ще 17% стали об'єктами погроз чи вимагань у мережі саме після початку повномасштабної агресії.

Кіберзагрози для дітей в Україні набули системного характеру, маючи прояви у вигляді кібербулінгу, онлайн-грумінгу, залучення до небезпечних зустрічей, впливу деструктивного контенту, а також маніпуляцій у воєнний час. Основною небезпекою є те, що цифрова загроза часто має прихований, але довготривалий вплив, що проявляється не лише у порушенні психічного здоров'я, а й у соціальній дезадаптації та навіть у залученні до злочинної або ризикованої діяльності.

Особливу увагу слід звернути на перехід загроз із онлайн-середовища в реальне життя – випадки побоїв, знущань, самогубств або маніпуляцій із залученням до диверсійної діяльності є яскравим тому підтвердженням. Крім того, статистика свідчить про недостатню залученість дорослих (батьків, вчителів, фахівців) до своєчасного виявлення або запобігання таких ситуацій (табл. 2.1).

Нормативно-правова відповідь держави на ці виклики проявляється через низку ключових документів:

1. Національна стратегія захисту дітей у кіберпросторі на 2021–2026 роки, затверджена Кабінетом Міністрів України [80], яка прямо визнає вплив війни як чинник посилення вразливості дітей до цифрових загроз.

2. Закон України «Про основні засади забезпечення кібербезпеки України» №2163-VIII [93], що формує основу для протидії кіберзлочинам проти неповнолітніх.

3. Положення Концепції національної безпеки та її нових редакцій, що враховують інформаційно-психологічні загрози у сфері освіти та дитинства як складові гуманітарної безпеки [21; 22; 35].

Також важливу роль відіграють ініціативи громадянського суспільства, благодійних фондів, міжнародних організацій (UNICEF, Save the Children), які розробляють програми цифрової безпеки для дітей, у тому числі в умовах евакуації, вимушеного переселення чи перебування в окупації.

Приклади кіберзагроз для дітей в Україні (2020–2025)

№	Вид загрози	Опис ситуації / кейс	Рік	Наслідки / реакція	Джерело
1	Кібербулінг	Школярка зазнала фізичних побоїв від однокласниць, що знімали відео та поширили його онлайн.	2022	Психологічна травма; розгляд у суді (ст. 125 ККУ)	Projector.org.ua
2	Онлайн-грумінг	59% підлітків, які знайомились онлайн, погодились на зустріч; частина стали жертвами сексуального насильства.	2021	Травматичний досвід, ризик торгівлі дітьми	Focus.ua
3	Маніпуляція у воєнний час	Підлітки залучалися до збору даних, передавали фото, координати через месенджери.	2024–2025	2 загинули, 1 поранений, 103 затримано	UNICEF / uanews.net
4	Кібербулінг і суїцидальні наслідки	149 підліткових самогубств за півроку (2021); пов'язано з онлайн-погрозами, шантажем.	2021	Самогубства, психоемоційні розлади	HSA.org.ua
5	Контент сексуального характеру	Випадки поширення інтимних фото неповнолітніх серед однолітків або зловмисників.	2020–2024	Порушення справ за ст. 301–302 ККУ	Кіберполіція, Cyberpolice.gov.ua
6	Онлайн-ігрова залежність	Підлітки витрачали десятки тисяч гривень на ігрові платформи без відома батьків.	2023	Фінансові втрати, емоційна дестабілізація	Повідомлення батьків у ЗМІ, соцмережах
7	Псевдовиклики (Blue Whale, Момо)	Інтернет-групи підбурювали дітей до самопошкодження, участі в "челенджах"	2020–2022	Госпіталізації, поліцейські перевірки	ДСНС, МВС, ЗМІ

Джерело: систематизовано автором на основі Інтернет джерел

Окремої уваги заслуговує проблема тимчасово окупованих територій, де діти піддаються систематичному впливу пропагандистських платформ ворога (через доступ до російських освітніх онлайн-сервісів, блокування українських джерел інформації, насадження російської ідентичності), що є елементом інформаційного геноциду.

Таким чином, український контекст в умовах війни характеризується надзвичайно високим ступенем комплексної загрози для безпеки дитини в цифровому середовищі, яка поєднує загальнопоширені ризики з унікальними викликами воєнного часу. Ці умови зумовлюють необхідність формування спеціальних механізмів захисту дітей у кіберпросторі, які враховували б як технічні, так і соціальні, психологічні, правові та культурні аспекти.

У стратегічному плані така ситуація вимагає інституціонального переосмислення гуманітарної безпеки дітей як пріоритету державної політики в умовах війни та поствоєнного відновлення. Це передбачає запровадження інноваційних моделей державного управління, які поєднували б профілактику, моніторинг, правозахист, цифрову освіту, міжнародну кооперацію та психологічну реабілітацію дітей, які постраждали від дій у кіберпросторі [1; 35; 38; 80].

У сучасних умовах інтенсивної цифровізації, у тому числі прискореної війною, протидія загрозам у кіберпросторі, що спрямовані на дітей, потребує не фрагментарних або точкових заходів, а цілісної, системно скоординованої моделі дій – інтегрованого підходу. Цей підхід передбачає об'єднання зусиль усіх зацікавлених сторін – держави, освітніх установ, батьків, громадських організацій, бізнесу та самих дітей – для формування безпечного цифрового середовища. Проблема цифрових загроз є багатогранною за своєю сутністю, а отже, потребує міжсекторальної, міждисциплінарної та мультиагентної взаємодії в управлінні кібербезпекою дітей [35; 36; 38].

Інтегрований підхід у цій сфері передбачає поєднання правових, технічних, освітніх, соціальних і психологічних інструментів впливу. На практиці це означає, що лише наявність законодавчого регулювання або технологічних фільтрів не гарантує безпеки дитини в Інтернеті. Ефективна протидія загрозам можлива лише за умови, якщо: законодавство є актуальним, дієвим і виконуваним; технічні засоби захисту інтегровані у всі рівні доступу до цифрових платформ; освітнє середовище формує цифрову грамотність і навички самозахисту; родини мають доступ до ресурсів підтримки й поінформованості; держава забезпечує координацію та моніторинг ефективності застосовуваних заходів.

Зазначений підхід особливо важливий в умовах гібридної війни, що включає інформаційно-психологічні операції проти цивільного населення, зокрема дітей. Кіберпростір перетворився на простір впливу на свідомість, у якому ворог активно використовує соціальні мережі, месенджери, ігрові

платформи для деморалізації, викривлення цінностей, вербування та збору інформації [23; 30; 35].

У правовому аспекті інтегрований підхід реалізується через розробку єдиного нормативного середовища, що регулює: захист персональних даних дітей (Закон України «Про захист персональних даних» №2297-VI) [91]; забезпечення прав дітей на безпечне інформаційне середовище (Закон «Про охорону дитинства» №2402-III) [95]; кримінальну відповідальність за злочини проти дітей у кіберпросторі (ст. 301-1 ККУ – «Дитяча порнографія», ст. 156 – «Розбещення неповнолітніх» тощо).

Водночас практика показує, що законодавчі норми залишаються малоефективними без реального механізму впровадження, контролю й міжвідомчої координації. Саме тому ключовим інструментом реалізації інтегрованого підходу є система стратегічного управління, яка передбачає: створення цільових міжвідомчих груп за участі МВС, МОН, Держспецзв'язку, Уповноваженого з прав дитини; впровадження державних і регіональних програм кіберзахисту дітей, орієнтованих на профілактику, освіту, допомогу, реагування; інституціоналізацію цифрової гігієни в освітній політиці (інтеграція в шкільні програми обов'язкових курсів цифрової грамотності, протидії кібербулінгу, медіаграмотності); стимулювання ІТ-сектору до впровадження стандартів кіберетики, вікового маркування, інструментів батьківського контролю; підтримку громадських ініціатив та міжнародних проєктів у сфері захисту прав дитини в цифровому середовищі.

Важливу роль у реалізації інтегрованого підходу відіграє також система моніторингу й оцінювання ефективності державної політики. Зокрема, Димитрієва О. І. пропонує методичні підходи до визначення індикаторів ефективності заходів з кіберзахисту дітей, які охоплюють як кількісні (кількість повідомлень про загрози, рівень цифрової грамотності, кількість реалізованих кейсів допомоги), так і якісні (ступінь довіри до державних інституцій, задоволеність батьків і дітей тощо) параметри [38].

У міжнародній практиці приклади інтегрованого підходу спостерігаються в діяльності організацій, як-от EU Kids Online, UNICEF, Save the Children, a

також у національних стратегіях країн ЄС, Канади, Ізраїлю. Загальним у цих моделях є поєднання чотирьох компонентів: регулювання, освіта, технології, культура відповідальності.

Для України, з урахуванням актуального контексту війни, гуманітарної кризи, великої кількості внутрішньо переміщених осіб, зруйнованої інфраструктури, така модель набуває ще більшої актуальності, оскільки лише узгоджені дії здатні забезпечити стійкість дитячого середовища до цифрових загроз.

Окремо варто наголосити, що в межах інтегрованого підходу слід розглядати і підвищення ролі самих дітей як суб'єктів безпеки, а не лише як об'єктів захисту. Формування навичок критичного мислення, здатності до самоідентифікації, знання своїх прав у кіберпросторі – усе це має стати частиною інклюзивної освітньої та соціальної політики.

З огляду на динамічний розвиток цифрового середовища та активне занурення дітей у кіберпростір, важливо не лише ідентифікувати окремі види загроз, але й систематизувати їх відповідно до логіки причинно-наслідкових зв'язків. Побудована матриця «Тип загрози – Наслідок – Механізм впливу» дозволяє простежити, як конкретні цифрові загрози трансформуються у соціальні, психологічні або кримінальні наслідки для дітей. Такий підхід є надзвичайно важливим для практики державного управління, оскільки створює аналітичну базу для розробки адресних і профілактичних заходів, спрямованих на мінімізацію ризиків у кіберпросторі. Матриця структурована таким чином, аби відобразити три ключові компоненти кожної загрози: Її зміст і характер (тип); Ймовірний або зафіксований наслідок; Механізм реалізації впливу, який часто має прихований характер, але є ключем до виявлення загрози на ранньому етапі (табл. 2.2).

Проведений аналіз дозволяє зробити висновок, що кіберзагрози для дітей у кіберпросторі є ізольованими феноменами. Вони мають чітко структуровані механізми дії та прогнозовані наслідки, які змінюються залежно від віку, рівня цифрової грамотності, соціального оточення дитини та ступеня батьківського/інституційного контролю. Матриця демонструє, що найбільш

небезпечними є ті загрози, які мають повільний, кумулятивний вплив (наприклад, контент сексуального чи насильницького характеру), або ж реалізуються через маніпулятивну модель взаємодії (грумінг, кібербулінг, ІПСО).

Водночас матриця підкреслює необхідність перехідного управління – від реактивного до проактивного: державні структури, освітні заклади та батьки повинні фокусуватись не лише на боротьбі з наслідками, але й на превентивному виявленні механізмів впливу ще до того, як загроза реалізується в повному обсязі. У комплексі такий аналітичний інструмент сприяє формуванню ефективної, системної і дитиноцентричної політики у сфері цифрової безпеки.

Таблиця 2.2

Інтерактивна матриця: «Тип загрози – Наслідок – Механізм впливу»

Тип загрози	Потенційні наслідки	Механізм впливу
Кібербулінг	Психологічна травма, соціальна ізоляція	Повторювані образи, знущання, публічне приниження онлайн
Онлайн-грумінг	Сексуальне насильство, шантаж	Побудова довіри → маніпуляції → вимоги інтимного контенту
Sextortion / Sexting	Самогубство, залучення до криміналу	Виманювання інтимних фото → погрози → публічне викриття
Ігрова залежність	Втрата соціальних навичок, фінансові збитки	Механіки винагород / прокачки → прив'язаність → донати / кредити
Шкідливий контент	Депресія, страх, викривлене сприйняття реальності	Алгоритми рекомендацій → повторний перегляд → закріплення поведінки
Вербування (ІПСО)	Залучення до шпигунства, тероризму, дезінформації	Псевдопатріотичні меседжі → «гейміфікація» → передача даних

Джерело: систематизовано автором

Загалом, аналіз сучасних загроз дітям у кіберпросторі та їхнього впливу на безпеку дитини дозволяє зробити низку принципових висновків щодо природи, масштабів і системності цієї проблематики у сучасному українському та глобальному контексті. Встановлено, що цифрове середовище не є нейтральним простором – воно стає середовищем підвищеного ризику для дітей, оскільки поєднує низку потенційно небезпечних чинників: анонімність, надмірний інформаційний потік, нерегульований доступ до контенту,

комунікаційну відкритість і складність верифікації джерел. Діти, як найбільш вразлива соціальна група, не маючи достатніх життєвих, емоційних і когнітивних ресурсів, стають легкою мішенню для деструктивного впливу.

У межах підрозділу здійснено розширену класифікацію кіберзагроз для дітей, яка враховує не лише технічні, але й контентні, комунікаційні, соціальні, психологічні та правові фактори. Виявлено, що найбільш поширеними є загрози, пов'язані з доступом до шкідливого контенту, онлайн-комунікацією з потенційно небезпечними особами, кібербулінгом, технічними атаками на пристрої, шахрайством, а також негативним впливом соціальних мереж і відеоплатформ на формування поведінкових моделей дитини. Ці загрози, як доведено, чинять багатовекторний вплив на безпеку дитини – від емоційного і психологічного до соціального, фізичного, правового та культурного.

Окрему увагу приділено особливостям українського контексту, де ситуація ускладнюється умовами повномасштабної війни. Встановлено, що воєнна ситуація не лише підвищує частоту використання дітьми цифрових технологій (через дистанційне навчання, евакуацію, втрату традиційних форм дозвілля), але й активізує нові типи загроз – зокрема, цілеспрямовані інформаційно-психологічні атаки, спроби вербування через соціальні мережі, деструктивний контент, спрямований на деморалізацію та втрату національної ідентичності. В цих умовах безпека дитини в цифровому середовищі перетворюється на питання національної гуманітарної безпеки.

У підрозділі також обґрунтовано доцільність і безальтернативність інтегрованого підходу до протидії цифровим загрозам. Такий підхід передбачає системну взаємодію всіх суб'єктів – державних органів, освітніх установ, батьків, громадянського суспільства, ІТ-компаній – із поєднанням правових, освітніх, технічних та управлінських заходів. Зазначено, що фрагментарні заходи не можуть дати ефективного результату в умовах комплексного й динамічного характеру кіберзагроз. Саме тому важливо забезпечити інституційну взаємодію, розробку єдиної стратегії кіберзахисту дітей, постійне оновлення нормативної бази, впровадження цифрової освіти, а також розвиток системи моніторингу ризиків і оцінювання ефективності політики у цій сфері.

Отже, цифрові загрози дитинству є не просто технологічним викликом – вони становлять серйозну гуманітарну проблему, яка потребує комплексної відповіді на рівні державної політики, освіти, родинного середовища та громадянського суспільства. Своєчасне виявлення, превенція та адаптивне управління цифровими ризиками щодо дітей є однією з ключових передумов формування безпечного, сталого й інклюзивного цифрового майбутнього України.

2.2. Аналіз інституційного та правового забезпечення захисту дітей у кіберпросторі

У сучасному цифровому суспільстві, де процеси діджиталізації охоплюють майже всі сфери життєдіяльності, питання забезпечення безпеки дитини у віртуальному просторі набуває особливої ваги. З одного боку, інформаційно-комунікаційні технології відкривають нові можливості для розвитку, освіти, соціалізації та самореалізації дітей; з іншого – створюють численні загрози, здатні завдати шкоди психічному, емоційному, фізичному і правовому благополуччю неповнолітніх. У зв'язку з цим державне управління у сфері захисту дітей у кіберпросторі має ґрунтуватися на ефективній інституційній моделі, підкріпленій цілісною нормативно-правовою базою.

Наявні виклики у вигляді кібербулінгу, грумінгу, доступу до шкідливого контенту, порушення цифрової приватності, маніпулятивного впливу через соціальні мережі вимагають не лише технічного реагування, а й стратегічного підходу з боку держави. Інституційна система повинна забезпечувати превенцію, захист, реагування і реабілітацію з урахуванням вікових, психологічних, соціальних і технологічних чинників. Разом із цим нормативно-правове регулювання має бути достатньо гнучким і динамічним, щоб відповідати постійним змінам у кіберпросторі.

Проте аналіз вітчизняної практики вказує на наявність низки структурних та змістовних недоліків: фрагментарність законодавства, неузгодженість повноважень між інституціями, відсутність єдиного координаційного центру,

брак ресурсів для реалізації політик. Особливо загострилася ця проблема в умовах війни, коли ризики кіберзагроз для дітей зросли багаторазово, а інституційна спроможність держави зазнала додаткових викликів.

У цьому контексті даний підрозділ дисертації присвячено комплексному аналізу поточного стану інституційного та правового забезпечення захисту дітей у кіберпросторі України. Буде здійснено порівняльний огляд функцій ключових державних органів, розкрито основні прогалини чинного законодавства, проаналізовано механізми міжвідомчої взаємодії, розглянуто приклади кращих практик інших держав, а також сформульовано пропозиції щодо вдосконалення існуючої моделі з урахуванням міжнародних стандартів і сучасних викликів.

Система правового забезпечення захисту дітей у кіберпросторі України перебуває у стадії динамічного формування. Незважаючи на наявність окремих норм, що стосуються прав дітей у цифровому контексті, вітчизняна нормативно-правова база є розпорошеною та фрагментарною. Вона поєднує положення конституційного, адміністративного, інформаційного, кримінального, сімейного, освітнього та міжнародного права. Нижче розглядаються основні нормативні акти, які прямо або опосередковано регулюють питання безпеки дітей у цифровому просторі.

1. Конституційна та міжнародно-правова основа. Фундаментальні права дитини закріплено в Конституції України (ст. 3, 6, 32, 52), де гарантується захист честі, гідності, приватного життя, а також пріоритет прав дитини як найвищої соціальної цінності держави [49]. Конституційні норми є базовими при імплементації спеціального законодавства у сфері цифрової безпеки дітей.

Україна ратифікувала низку ключових міжнародних актів, зокрема: Конвенцію про права дитини (ООН, 1989) [104]; Європейську конвенцію з прав людини (1950) [47]; Конвенцію про кіберзлочинність (Будапешт, 2001) [48]; Європейську конвенцію про здійснення прав дітей [97].

Ці документи створюють обов'язок держави формувати національні механізми захисту дітей, у тому числі від загроз у віртуальному просторі, а також гармонізувати національне законодавство з європейськими стандартами.

2. Спеціальні закони України, що регламентують захист дітей. Серед найважливіших національних актів виділяються:

2.1. Закон України «Про охорону дитинства» [95] – закріплює права дитини на безпечне інформаційне середовище, захист від негативного контенту, маніпуляцій та експлуатації. Ст. 10-1 та 11 цього закону стосуються інформаційної безпеки та обов’язків держави щодо недопущення розповсюдження продукції, шкідливої для психіки дитини.

2.2. Закон України «Про основні засади забезпечення кібербезпеки України» [93] – створює правові основи функціонування системи кібербезпеки, включаючи захист держави, громадян і соціальних груп (включно з дітьми) від кіберзагроз. Закон визначає, що об’єкти критичної інформаційної інфраструктури мають розробляти системи захисту персональних даних, зокрема й дитячих.

2.3. Закон України «Про захист персональних даних» [91] – передбачає особливий правовий режим для обробки персональних даних дітей. Неповнолітні особи не можуть надавати згоду на обробку своїх даних без участі законних представників. Водночас, на практиці ці положення часто порушуються через відсутність технічних обмежень у кіберпросторі[112].

2.4. Закон України «Про освіту» та «Про повну загальну середню освіту» – визначають, що захист дитини в інформаційному просторі є обов’язковою складовою освітнього процесу. Запровадження елементів цифрової грамотності, кібергігієни, відповідального користування мережевими ресурсами має стати невід’ємною частиною навчальних програм.

2.5. Закон України «Про електронні комунікації» та суміжні з ним акти – встановлюють відповідальність операторів і провайдерів за передачу даних, вимоги до збереження та захисту інформації, механізми ідентифікації користувачів.

3. Стратегічні документи та національні програми. У 2021 році було ухвалено Національну стратегію захисту дітей у кіберпросторі на 2021–2026 роки [80], яка є першим комплексним політичним документом, орієнтованим виключно на безпеку дитини в цифровому контексті. Стратегія передбачає

реалізацію таких напрямів: забезпечення цифрової грамотності всіх учасників освітнього процесу; створення безпечної цифрової інфраструктури; запровадження механізмів моніторингу та реагування; адаптація законодавства до міжнародних стандартів.

Реалізація стратегії покладається на міжвідомчу співпрацю між Міністерством цифрової трансформації, Міністерством освіти і науки, Міністерством соціальної політики, Кіберполіцією, громадськими організаціями та міжнародними партнерами. Попри прогресивність положень, ефективність імплементації Стратегії залишається низькою через обмежене фінансування, кадровий дефіцит та слабку міжвідомчу координацію [35], [38].

4. Кримінально-правові аспекти. Кримінальний кодекс України містить низку норм, які можуть бути застосовані в контексті захисту дитини в Інтернеті. Серед них: ст. 301-1 (виготовлення, збут і розповсюдження дитячої порнографії); ст. 153, 156 (розбещення неповнолітніх); ст. 182 (порушення недоторканності приватного життя); ст. 161 (розпалювання ворожнечі, мова ворожнечі, що може поширюватися онлайн).

Крім того, чинне законодавство не містить окремої кваліфікації таких сучасних явищ, як грумінг, сексторшн, кіберпереслідування, що створює труднощі для правоохоронців та судової практики.

Аналіз нормативно-правової бази України свідчить про наявність важливих кроків на шляху до створення комплексної системи правового захисту дітей у кіберпросторі. Проте її ефективність знижується через: фрагментарність законодавства; нечітке розмежування повноважень між органами влади; відсутність правових норм, які враховують специфіку сучасних цифрових загроз; недостатній рівень інтеграції міжнародних стандартів.

З огляду на це, наступним етапом аналізу є розгляд інституційного механізму реалізації законодавства в сфері захисту дітей, а також оцінка дієвості існуючих державних структур у контексті реагування на цифрові виклики (табл. 2.3).

**Основні нормативно-правові акти України у сфері захисту дітей у
кіберпросторі**

№	Назва нормативного акта	Рік	Ключові положення	Сфера впливу
1	Конституція України [49]	1996	Гарантії прав дитини, захист приватності, гідності, свободи вираження поглядів	Загальні конституційні гарантії
2	Конвенція про права дитини [104]	1989 (ратифік. 1991)	Визначає право дитини на захист від усіх форм насильства, у т.ч. в онлайн-середовищі	Міжнародне право, права дитини
3	Закон «Про охорону дитинства» [95]	2001	Права дитини на безпечний інформаційний простір, захист від негативного контенту	Соціальна політика, інформаційна безпека
4	Закон «Про основні засади забезпечення кібербезпеки України» [93]	2017	Визначає суб'єктів, об'єкти, принципи та механізми кібербезпеки, зокрема захист дітей	Кібербезпека, державна політика
5	Закон «Про захист персональних даних» [91]	2010	Особливості обробки персональних даних дітей, згода законних представників	Приватність, персональні дані
6	Закон «Про освіту» / «Про загальну середню освіту»	2017 / 2020	Забезпечення цифрової грамотності, виховання кіберкультури у школах	Освіта, цифрова безпека
7	Кримінальний кодекс України	2001	Ст. 301-1, 153, 156, 182, 161 — передбачають відповідальність за злочини проти дітей в онлайн-середовищі	Кримінальне право
8	Національна стратегія захисту дітей у кіберпросторі(2021–2026) [80]	2021	Пріоритети державної політики: цифрова освіта, безпечна інфраструктура, реагування на загрози	Стратегія, міжвідомча взаємодія
9	Конвенція про кіберзлочинність (Будапештська) [48]	2001 (ратифік. 2005)	Міжнародна співпраця у боротьбі з кіберзлочинами, зокрема дитячою експлуатацією	Міжнародне право, кримінальне переслідування
10	Закон «Про електронні комунікації»	2021	Регламентує діяльність провайдерів, вимоги до безпеки інформаційних послуг	Цифрова інфраструктура

Аналіз наведеної таблиці демонструє, що в Україні вже створено законодавче підґрунтя для захисту дітей у кіберпросторі, яке включає як загальні норми (конституційні, міжнародні), так і спеціалізовані закони та стратегії. Водночас, комплексність законодавства потребує: кодифікації норм, що стосуються саме дітей у цифровому просторі; адаптації кримінального права

до новітніх форм кіберзагроз (наприклад, грумінгу, сексторшну, онлайн-мобінгу); посилення міжвідомчої координації у реалізації Національної стратегії.

Інституційна архітектура захисту дітей у кіберпросторів України представлена системою органів державної влади, незалежних інституцій, правоохоронних структур та недержавних партнерів. Незважаючи на численність суб'єктів, ефективність їхньої діяльності обмежується фрагментарністю повноважень, браком горизонтальної координації та відсутністю цілісної моделі міжвідомчої взаємодії. Сучасні виклики – від кібербулінгу до онлайн-експлуатації – потребують не лише формального поділу обов'язків, але й злагодженого функціонування інституцій у межах єдиного гуманітарного, правового та інформаційного поля.

1. Центральні органи виконавчої влади: функціональні ролі та виклики. Міністерство цифрової трансформації України відіграє провідну роль у реалізації політики цифровізації та розробці стратегій, зокрема у сфері безпеки дітей. Саме цей орган ініціював ухвалення Національної стратегії захисту дітей у кіберпросторі на 2021–2026 роки [80], яка стала основою формування системного підходу до цифрової безпеки неповнолітніх. Проте обмеженість виконавчих повноважень Мінцифри у сфері правопорядку ускладнює її повну реалізацію.

Міністерство освіти і науки України відповідальне за впровадження цифрової грамотності, виховання культури безпечної поведінки в Інтернеті, адаптацію освітніх програм до умов цифрового суспільства. В межах стратегії МОН зобов'язане інтегрувати в шкільну освіту обов'язкові курси з кібергігієни, однак у 2024 році їх покриття залишалося нерівномірним (лише 39% загальноосвітніх закладів мали окремі навчальні модулі з безпеки в Інтернеті) [34].

Міністерство соціальної політики України має мандат на захист прав дитини та координує діяльність служб у справах дітей. Проте цифрова компетентність соціальних працівників часто є недостатньою для протидії сучасним формам онлайн-загроз, таким як грумінг або сексторшн [35].

2. Правоохоронні структури: виявлення, розслідування, превенція. Департамент кіберполіції Національної поліції України є ключовим органом у боротьбі з кіберзлочинністю, включаючи злочини проти дітей. Підрозділи кіберполіції систематично викривають злочини, пов'язані з дитячою порнографією, шантажем та розповсюдженням шкідливого контенту. За даними департаменту, лише у 2023 році було відкрито понад 230 кримінальних проваджень, пов'язаних із сексуальною експлуатацією дітей в Інтернеті [11].

У межах проєкту «Безпечний Інтернет» кіберполіція проводить просвітницькі кампанії серед учнів, батьків і педагогів. Проте ефективність розслідувань залишається недостатньою через проблеми з кваліфікацією дій у правовому полі, відсутність належного судово-лінгвістичного аналізу повідомлень, а також технологічну перевагу правопорушників [12].

Офіс Генерального прокурора, а також органи досудового слідства залучаються до кримінальних проваджень, однак не мають спеціалізованих підрозділів з кіберзлочинів проти дітей, що ускладнює оперативне реагування.

3. Незалежні інституції: моніторинг і адвокація. Уповноважений Президента України з прав дитини здійснює моніторинг дотримання прав дітей, у тому числі в цифровому середовищі. Звіти Уповноваженого (2022–2023 рр.) фіксували збільшення скарг на онлайн-насильство, зокрема на залякування в соціальних мережах, втягнення в суїцидальні групи, шантаж фото- та відеоматеріалами [10].

Уповноважений Верховної Ради з прав людини веде окремий напрям діяльності з цифрових прав, включаючи персональні дані дітей, збирання інформації без згоди батьків, тощо. Інституція надає методичні рекомендації школам і батькам, а також реагує на звернення громадян щодо порушень [43].

4. Роль громадського сектору та міжнародних партнерів. Активну участь у реалізації державної політики беруть:

4.1. Громадські організації: ГО «Ла Страда», Stop Sexting, U-Report, Центр демократії та верховенства права тощо. Вони проводять тренінги, аналітику та розробку інформаційних кампаній.

4.2. Міжнародні структури: UNICEF, Save the Children, ECPAT International – постачають технічну допомогу, фінансування, методичну підтримку та проводять соціологічні дослідження [134].

Значна частина просвітницьких кампаній у закладах освіти, вебінарів та мобільних додатків із безпеки для дітей (наприклад, «ReThink», «Моя безпечна школа») була реалізована саме в межах державно-громадського партнерства (табл. 2.4).

Попри наявність широкої мережі інституцій, брак координації, дублювання функцій, а також нерівномірність ресурсного забезпечення призводять до фрагментарної реалізації державної політики у сфері цифрової безпеки дітей. Особливо актуальною є потреба: створення єдиного інтеграційного механізму з чітким розподілом повноважень; посилення цифрових компетентностей персоналу; налагодження постійного обміну даними між органами та структурами.

У контексті глобалізації, цифровізації та трансформації традиційних уявлень про безпеку, міжнародні норми та стандарти у сфері захисту прав дитини в цифровому середовищі набувають дедалі важливішого значення як орієнтири для побудови національної політики. Україна, як держава-учасниця низки міжнародних конвенцій та міжурядових угод, зобов'язана імплементувати основоположні принципи міжнародного права у своє внутрішнє законодавство, зокрема щодо захисту дітей від загроз, породжених цифровим середовищем.

Однією з ключових нормативно-правових засад міжнародного рівня є Конвенція ООН про права дитини (1989 р.), яка визнає право кожної дитини на захист від усіх форм експлуатації, насильства, посягань на честь і гідність, а також на доступ до безпечної інформації. У 2014 році до цієї Конвенції було прийнято Факультативний протокол про продаж дітей, дитячу проституцію та дитячу порнографію, який прямо стосується злочинів, що дедалі частіше відбуваються у цифровому просторі. Україна ратифікувала ці документи, що покладає на неї обов'язки щодо криміналізації відповідних діянь та створення інституційних механізмів протидії [47].

Інституційні механізми захисту дітей у кіберпросторі України

№	Інституція	Основні функції	Інструменти та механізми	Основні виклики
1	Міністерство цифрової трансформації України	Формування стратегій, політика цифровізації, захист цифрових прав	- Національна стратегія захисту дітей у кіберпросторі	- Брак виконавчих повноважень
			- Інформаційні кампанії	- Обмежені ресурси для контролю виконання
			- Цифрова освіта	
2	Міністерство освіти і науки України	Освітня політика, інтеграція цифрової безпеки в навчальні програми	- Впровадження курсів з кібергігієни	- Нерівномірне впровадження
			- Методичні рекомендації	- Недостатня кваліфікація педагогів
			- Програми для вчителів	
3	Міністерство соціальної політики України	Соціальний захист дітей, координація служб у справах дітей	- Робота з вразливими категоріями	- Низький рівень цифрової підготовки кадрів
			- Підтримка сімей	- Недостатній моніторинг
			- Соціальна профілактика	
4	Кіберполіція України	Виявлення та розслідування кіберзлочинів проти дітей	- Кримінальні провадження	- Високе навантаження
			- Профілактика	- Брак технологічних ресурсів
			- Онлайн-платформи скарг	- Юридичні прогалини
5	Уповноважений Президента України з прав дитини	Моніторинг дотримання прав дитини, зокрема в Інтернеті	- Розгляд скарг	- Обмеженість впливу
			- Рекомендації органам влади	- Залежність від політичної волі
			- Публічні звіти	
6	Омбудсман з прав людини (ВРУ)	Захист цифрових прав, захист персональних даних	- Перевірки скарг	- Недостатнє регламентування прав дітей у цифровому просторі
			- Адвокація	
			- Інформаційні кампанії	
7	Громадські організації (Ла Страда, Stop Sexting, U-Report тощо)	Просвіта, правозахист, допомога потерпілим	- Тренінги	- Нестійке фінансування
			- Гарячі лінії	- Залежність від грантової підтримки
			- Психологічна та юридична підтримка	
8	Міжнародні організації (UNICEF, Save the Children, ECPAT)	Методична допомога, дослідження, фінансування проєктів	- Міжнародні програми	- Недостатня інтеграція з національною системою
			- Технічна підтримка	
			- Аналітика і моніторинг	

Джерело: систематизовано автором

Особливу роль у формуванні стандартів цифрової безпеки дітей відіграє Європейський Союз. Так, Директива ЄС 2011/93/EU передбачає обов'язкове запровадження ефективних кримінальних санкцій за сексуальне насильство над дітьми та поширення дитячої порнографії через Інтернет. Окрім цього, Європейський парламент розробив Європейську стратегію з ефективнішого

використання Інтернету дітьми (Better Internet for Kids), яка визначає базові принципи: освіта, самозахист, батьківський контроль та регулювання діяльності провайдерів. Україна орієнтується на ці стандарти при розробці національних стратегічних документів, зокрема Національної стратегії захисту дітей у кіберпросторі на 2021–2026 роки [80].

Також важливими є положення Конвенції Ради Європи про кіберзлочинність (Будапештська конвенція, 2001 р.), яка є першим міжнародно-правовим інструментом, спрямованим на боротьбу з кіберзлочинністю, включаючи кіберзлочини проти дітей, такі як грумінг, кібербулінг, секстинг тощо [48]. Україна є її повноправним учасником, що створює зобов'язання адаптувати внутрішнє законодавство до положень цієї Конвенції, зокрема щодо збереження електронних доказів, доступу до інформаційних систем та транскордонного співробітництва.

Іншою важливою рамкою є Загальна декларація прав людини (1948 р.) та Міжнародний пакт про громадянські і політичні права (1966 р.), які гарантують право кожного на приватне життя, свободу вираження поглядів та захист від свавільного втручання. У цифрову епоху ці норми набувають нового виміру – як права на захист персональних даних, свободу онлайн-висловлювань та кібербезпеку. Вони стають базисом для розробки стандартів регулювання цифрових платформ, соціальних мереж і провайдерів інтернет-послуг, що все частіше мають вплив на інформаційне середовище, в якому зростають діти.

Крім нормативно-правових актів, важливим орієнтиром виступають документи міжнародних організацій, таких як UNICEF, ECPAT International, OECD, ITU. Зокрема, UNICEF у своїй доповіді «Children in a Digital World» (2017) сформулював глобальні рекомендації для урядів: інвестувати в цифрову грамотність дітей, створювати безпечні цифрові середовища, забезпечити підтримку жертв онлайн-насилюства, а також гарантувати баланс між правом на інформацію і правом на захист [134]. Ці принципи активно враховуються в національних стратегіях, зокрема у впровадженні українських ініціатив з розвитку цифрової освіти.

Окремо варто згадати General Data Protection Regulation (GDPR) Європейського Союзу, який хоч і не має прямої юрисдикції в Україні, однак встановлює глобальний стандарт захисту персональних даних, включаючи дані дітей. Україна поступово гармонізує своє законодавство з вимогами GDPR, зокрема через Закон «Про захист персональних даних» №2297-VI [91] та роз'яснення Уповноваженого Верховної Ради з прав людини щодо обробки даних неповнолітніх [112].

Таким чином, міжнародні зобов'язання виступають не лише зовнішнім стимулом, але і внутрішнім ресурсом розвитку національної системи правового та інституційного захисту дітей у кіберпросторі. Імплементация цих стандартів є ключовою умовою інтеграції України у загальноєвропейський безпековий та правозахисний простір. Водночас вимагає глибокої адаптації до українських соціокультурних реалій, умов війни та трансформацій державного управління.

Незважаючи на значні зусилля держави, громадянського суспільства та міжнародних партнерів у побудові системи захисту дітей у цифровому просторі, українська модель містить суттєві слабкі місця. Ці недоліки обмежують дієвість правового, інституційного й практичного забезпечення безпеки дітей онлайн. Виділимо основні проблеми, прогалини та виклики, які нині стоять на шляху до формування повноцінної захисної системи.

1. Фрагментарність нормативно-правового регулювання. Перша фундаментальна проблема полягає у тому, що нормативно-правова база захисту дітей у кіберпросторі розпорошеною і недостатньо спеціалізованою. Хоча існують закони, які містять положення про права дитини або захист персональних даних, відсутній єдиний спеціалізований закон «про кіберзахист дітей», який би системно регламентував усі ключові аспекти (грумінг, кібербулінг, сексторшн тощо). Це ускладнює правозастосування, оскільки суди та правоохоронні органи змушені “перекидатися” між різними законами й інтерпретаціями.

Крім того, термінологічний апарат у нормативних документах часто не відповідає сучасним викликам – поняття «онлайн-наси́льство», «грумінг», «сексуальне шантажування» не мають усталеного визначення або взагалі

відсутні в основних законах. Це створює правову невизначеність у процесі кваліфікації злочинів.

Також міжнародні стандарти, такі як GDPR (щодо обробки даних дітей), часто не повною мірою імплементуються в українське законодавство або реалізуються декларативно, без механізмів контролю чи санкцій.

2. Розпорошеність інституцій та неузгодженість повноважень. Хоча в Україні залучено багато інституцій до питань цифрової безпеки дітей – Мінцифри, МОН, соціальні служби, кіберполіція, Уповноважений з прав дитини тощо – їхні повноваження часто перетинаються, а сфери відповідальності недостатньо чітко окреслені. Це породжує дублювання функцій, пробіли у покритті відповідальності та зволікання в реагуванні.

Відсутність єдиного координуючого органу або координаційної структури з повною відповідальністю за захист дітей в Інтернеті суттєво послаблює міжвідомчу співпрацю. Без такої лінії відповідальності практично неможливо оперативно мобілізувати ресурси чи забезпечити узгоджений алгоритм реагування на кіберінциденти з дітьми.

3. Обмеженість кадрового та технічного потенціалу. На практичному рівні багато установ, відповідальних за захист дітей, стикаються з дефіцитом підготовлених фахівців із цифрової безпеки. Наприклад, педагоги мають обмежені знання щодо розпізнання кібербулінгу чи грумінгу, соціальні служби не оснащені інструментами аналізу цифрового ризику, а правоохоронці часто не мають достатньої компетенції в кіберрозслідуваннях.

Технічна база багатьох регіональних структур, шкіл чи місцевих центрів уразлива – відсутність сучасних систем фільтрації, антивірусного захисту, засобів моніторингу й журналювання подій створює «слабкі ланки» в системі, якими охоче користуються зловмисники.

4. Недостатній рівень просвітництва та цифрової грамотності. Батьки, опікуни та багато вчителів недостатньо обізнані з ризиками цифрового середовища, їхніми проявами та способами реагування. Часто діти стикаються з онлайн-загрозами, не повідомивши про це дорослим через страх, сором або

невіру в ефективність захисту. Низький рівень знань серед дорослих значно знижує шанси на раннє виявлення інцидентів і своєчасне втручання.

Освітня система в багатьох регіонах не забезпечує системного курсу з кібербезпеки – замість цього уроки з безпеки часто включаються епізодично або факультативно, що не формує сталий рівень знань.

5. Обмеженість моніторингу та механізмів реагування. За відсутності єдиного реєстру інцидентів та централізованої системи повідомлень про кіберзагрози щодо дітей, багато випадків залишаються невідфіксованими. Діти часто не звертаються зі скаргами або повідомлення обробляються з затримками.

Механізми реагування не завжди мають стандартизовані процедури. Наприклад, у багатьох випадках адміністрації платформ чи соцмереж не зобов'язані оперативно реагувати на звернення дітей або батьків, а правоохоронці не мають чіткого алгоритму співпраці з ІТ-компаніями щодо вилучення шкідливого контенту.

6. Географічна та соціальна нерівність. Діти, що проживають у сільській місцевості, віддалених або прифронтових районах, мають менший доступ до якісного інтернету, тренінгів, освітніх ініціатив або ресурсів захисту. В умовах війни ці регіони особливо вразливі до дезінформації та цифрової ізоляції. Крім того, внутрішньо переміщені діти та ті, що опинилися в умовах тимчасової окупації, часто не мають жодної системи підтримки чи доступу до безпечних цифрових ресурсів.

7. Військово-інформаційний виклик. Повномасштабна війна додала новий рівень загроз: використання дітей як інструментів інформаційної боротьби, вербування через цифрові канали, поширення матеріалів бойових дій чи пропаганди, психологічний тиск через месенджери. Ці нові форми маніпуляцій часто виходять за межі традиційного законодавства й регуляторних підходів, що вимагає гнучких і адаптивних механізмів реагування.

У підсумку, українська система захисту дітей у кіберпросторістикається з комплексом взаємопов'язаних проблем: від законодавчої фрагментарності і недостатньої координації інституцій до браку ресурсів, неготовності місцевих структур і особливостей війни. Подолання цих викликів вимагає стратегічної

реформи – формування єдиного координуючого центру, впровадження спеціалізованого законодавства, підвищення цифрової грамотності на всіх рівнях та активацію системи моніторингу й реагування.

В умовах динамічного розвитку цифрових технологій та зростання ризиків у кіберпросторі необхідною умовою ефективного захисту дітей є системна трансформація існуючої інституційної моделі. Сучасна ситуація в Україні демонструє наявність інституційного потенціалу, проте він фрагментарний, недостатньо скоординований і потребує осучаснення відповідно до міжнародних стандартів, таких як «Keeping Children Safe in the Digital Environment» (ЄС), «Guidelines for Industry on Child Online Protection» (ITU, UNICEF), а також до реалій гібридної війни. Нижче подано ключові стратегічні та операційні рекомендації, а також актуальні пілотні ініціативи, що можуть бути масштабовані на національному рівні.

1. Створення національного координуючого органу з питань цифрової безпеки дітей. Рекомендується запровадити єдиний координаційний центр (Центр цифрової безпеки дітей) у структурі Кабінету Міністрів або Міністерства цифрової трансформації. Такий центр має стати точкою перетину політик, рішень та відповідальності, забезпечуючи: стратегічне планування, координацію дій між міністерствами, службами, правоохоронними органами; збір та аналіз інцидентів; взаємодію з платформами, провайдерами, ІТ-компаніями; інформаційно-просвітницьку роботу. Фінансування може здійснюватись у змішаному форматі – державно-приватне партнерство із залученням донорської підтримки.

2. Вдосконалення нормативно-правової бази. Необхідно розробити та ухвалити спеціальний Закон України «Про захист дітей у кіберпросторі», який системно врегулює: поняття онлайн-насильства (грумінг, сексторшн, кіберсталкінг); повноваження відповідних органів; відповідальність онлайн-платформ; зобов'язання операторів/провайдерів щодо фільтрації, зберігання та передачі даних у випадках порушень; захист персональних даних дітей відповідно до стандартів GDPR [145].

Паралельно слід внести зміни до Закону України «Про охорону дитинства» [95], «Про основні засади забезпечення кібербезпеки України» [93] та Кримінального кодексу щодо кваліфікації цифрових злочинів проти дітей.

3. Розбудова системи освіти з цифрової безпеки. Рекомендовано ввести обов'язковий предмет «Цифрова безпека та медіаграмотність» у шкільну програму з 5 класу, інтегруючи: практичні кейси розпізнавання загроз; алгоритми реагування; етичне користування цифровими технологіями.

Також необхідно передбачити сертифіковану підготовку для вчителів, соціальних працівників, ювенальних поліціантів, із залученням онлайн-платформ, які вже існують в Україні (наприклад, CyberPanda, StopSexting, Prometheus, «Дія.Цифрова освіта»).

4. Запровадження Національної платформи онлайн-скарг і реагування. Створення інтерактивного порталу типу “Безпечний Інтернет для дітей” з можливістю: анонімного повідомлення про інциденти; отримання допомоги від юриста чи психолога в режимі онлайн; верифікації контенту; звернення до кіберполіції та наглядових органів.

Платформа має функціонувати цілодобово та включати функції швидкого реагування через інтеграцію з чат-ботами, соцмережами та месенджерами.

5. Вдосконалення міжвідомчої взаємодії. Необхідно затвердити єдиний міжвідомчий протокол реагування на кіберзагрози для дітей, що включає: чіткий алгоритм дій кожного суб'єкта (МОН, поліція, школа, соцслужби); часові рамки реагування; механізм обміну даними з урахуванням законодавства про персональні дані [91]. Такий протокол має пройти обов'язкове тестування у пілотних регіонах з подальшим масштабуванням.

6. Розширення інституційної участі громадського сектору. Громадські організації відіграють вирішальну роль у просвіті, моніторингу, адвокації. Слід формалізувати механізми участі ГО у політичних процесах через: підписання меморандумів про співпрацю; фінансування з державного бюджету на конкурсній основі; залучення експертів ГО до експертиз законопроектів.

Інституційна модель захисту дітей у кіберпросторі України повинна бути переосмислена через призму системного, інтегрованого та мультиакторного

підходу. Це означає не лише вдосконалення законодавства, а й розбудову сучасної архітектури координації, освіти, технологічного моніторингу, а також – ефективної комунікації з дітьми, батьками та платформами. Пілотні ініціативи, що вже реалізуються в Україні, засвідчують потенціал для масштабування та служать основою для нової моделі кіберзахисту, орієнтованої на потреби дитини, її права та цифрову гідність (табл. 2.5).

Таблиця 2.5

Приклади пілотних проєктів в Україні

Назва проєкту	Реалізатор	Цільова аудиторія	Формат	Стан
«Кіберпес» (CyberPanda)	Нацполіція + МОН	Учні 5–9 класів	Онлайн-гра з кібербезпеки	Активно реалізується
Stop Sexting	ГО «Ла Страда – Україна»	Діти, підлітки, батьки	Просвітницькі кампанії, чат-бот	Масштабовано
U-Report Ukraine	UNICEF	Молодь 14–25 років	Опитування, поради, кейси	Діє з 2017 року
«Дія.Цифрова освіта»	Мінцифра	Всі вікові групи	Освітні відео, тести	Постійне оновлення
Google Family Link кампанія	Google + МОН	Батьки, учні	Налаштування безпечного користування пристроєм	Часткова підтримка

Джерело: [65]

У сучасних умовах цифровізації всі сфери суспільного життя зазнають трансформацій, що, з одного боку, створює нові можливості для розвитку, навчання та самореалізації, а з іншого – породжує низку викликів, особливо вразливих для найменш захищених категорій населення, зокрема дітей. Забезпечення цифрової безпеки неповнолітніх в Україні набуває особливої актуальності в умовах воєнного стану, динамічного розвитку інформаційних технологій, високого рівня дезінформації, кібербулінгу та зростання кіберзлочинності. Попри наявність інституційних і правових механізмів, українська система захисту дітей у кіберпросторі залишається фрагментарною та недостатньо адаптованою до новітніх загроз. Саме тому виникає потреба у

глибокому порівняльному аналізі кращих світових практик, що успішно впроваджуються в інших країнах, з метою критичного осмислення можливостей їх адаптації до національного контексту.

У цьому зв'язку надзвичайно корисним є аналіз моделей, що діють у таких країнах, як Польща, Естонія та Південна Корея – держав, які, попри різні соціокультурні та геополітичні обставини, демонструють ефективність у впровадженні механізмів цифрового захисту дітей. Польща, як країна ЄС, орієнтована на гармонізацію із загальноєвропейськими стандартами, Естонія є піонером електронного врядування та цифрової трансформації освіти, а Південна Корея – приклад високотехнологічної держави з досвідом застосування жорстких регуляторних заходів щодо неповнолітніх в онлайні. Кожна з цих моделей несе у собі як переваги, так і певні ризики, які є цінними для розуміння шляхів удосконалення української інституційної та нормативно-правової системи у сфері захисту дітей.

Таким чином, подальший порівняльний аналіз дозволить не лише окреслити успішні практики, а й зосередити увагу на адаптивних підходах, які потенційно можуть бути інтегровані в українську стратегію цифрової безпеки дітей – із урахуванням культурних, соціальних та безпекових чинників.

Порівняльний аналіз міжнародного досвіду у сфері захисту дітей у кіберпросторі є важливим аналітичним інструментом для вдосконалення національної політики в Україні. У контексті стрімкого розвитку інформаційно-комунікаційних технологій та глобалізації цифрового простору, країни по-різному реагують на нові загрози для дітей: хтось робить акцент на освітньо-просвітницьких підходах, інші – на нормативно-правових або технологічних обмеженнях. У цьому підрозділі увагу зосереджено на трьох країнах – Польщі, Естонії та Південній Кореї, які обрали різні, але ефективні моделі забезпечення цифрової безпеки неповнолітніх.

Польща демонструє збалансований підхід, у якому поєднуються законодавче регулювання, інституційна підтримка та громадянська активність. Одним із ключових елементів польської моделі є діяльність Центру безпечного Інтернету (Safer Internet Centre), який функціонує у межах загальноєвропейської

ініціативи «Better Internet for Kids». Центр координує інформаційно-просвітницьку діяльність, забезпечує функціонування гарячої лінії для дітей і батьків (номер 116 111), а також платформи для скарг на шкідливий контент (Dyżurnet.pl). Крім того, Польща впроваджує регуляторні ініціативи, що передбачають вікову верифікацію користувачів, підвищення відповідальності провайдерів за доступ дітей до небажаного контенту, а також посилення контролю за онлайн-матеріалами, що імітують сексуальне зловживання щодо дітей. Такий комплексний підхід створює умови для ефективної превенції та реагування на цифрові загрози.

Естонія – одна з найцифровізованіших країн Європи – обрала модель, у центрі якої перебуває освіта, саморегулювання та партнерство між державою, громадянським суспільством і приватним сектором. Естонський уряд інтегрує питання цифрової безпеки дітей у національні стратегії розвитку освіти, молодіжної політики та внутрішньої безпеки. Наприклад, питання протидії онлайн-сексуальному насильству є окремим напрямом Плану внутрішньої безпеки Естонії на 2025–2028 роки. Особливістю естонського підходу є відмова від жорстких державних обмежень (зокрема, вікових бар'єрів для завантаження мобільних додатків), натомість основну відповідальність за цифрову безпеку дітей покладено на батьків, школи та самих дітей – шляхом розвитку їх цифрової грамотності. Це вказує на довіру до громадянської спроможності суспільства і високий рівень цифрової культури.

Південна Корея застосовує більш директивну модель, із сильним державним втручанням у регулювання цифрового середовища. Уряд країни намагався впровадити мобільний застосунок «Smart Sheriff», обов'язковий для встановлення на телефони всіх користувачів віком до 19 років. Він надавав батькам повний доступ до інформації про дії дитини в мережі, дозволяв блокувати сайти, додатки та фіксувати інші дії. Хоча цей додаток і було пізніше відкликано через проблеми із безпекою та порушенням приватності, він свідчить про активну спробу державного регулювання на технологічному рівні. Іншим прикладом є скасований у 2021 році «закон про вимикання ігор» (shutdown law), який забороняв особам до 16 років користуватися онлайн-іграми

у нічний час. Попри спірність таких заходів, вони засвідчують готовність уряду жорстко втручатися в цифрове середовище задля безпеки дітей, навіть ціною зменшення їх цифрових свобод.

Аналіз цих трьох моделей дозволяє окреслити як спільні риси (наявність спеціалізованих інституцій, законодавча база, міжнародна співпраця), так і ключові відмінності. Польща забезпечує комплексність завдяки інтеграції громадянського, публічного та правового секторів; Естонія – акцентує на цифровій грамотності та інституційному партнерстві; Південна Корея – практикує технологічне регулювання та адміністративний контроль. Ці моделі мають і позитивні, і суперечливі сторони: польський підхід – інституційно збалансований, але потребує стійкого фінансування; естонський – демократичний, але потребує високого рівня цифрової свідомості; південнокорейський – технологічно просунутий, але викликає занепокоєння з точки зору приватності та прав дитини.

Для України, яка перебуває у стані війни та проходить трансформацію цифрової безпеки, доцільно інтегрувати елементи всіх трьох моделей. Зокрема, від Польщі – інституційну організацію та гарячі лінії, від Естонії – освітній підхід і включення безпеки дітей у стратегії цифрового розвитку, а від Південної Кореї – розробку інноваційних технологічних інструментів контролю, але з дотриманням правових і етичних стандартів. Такий синтез дозволить не лише підвищити ефективність національної системи, а й сприятиме побудові безпечного, етичного і сприятливого цифрового середовища для українських дітей.

2.3. Практика реалізації державної політики захисту дітей у кіберпросторі

У сучасному суспільстві, де цифрові технології стрімко інтегруються в усі сфери життя, питання безпеки дітей у кіберпросторі набуває особливої ваги. У цифрову епоху дитина – не лише користувач інформаційних систем, а й

потенційний об'єкт численних загроз: від кібербулінгу та секстингу до маніпуляцій, пов'язаних із залученням до небезпечних онлайн-спільнот чи впливом ворожої пропаганди. Такий стан речей вимагає чіткої, науково обґрунтованої та ефективної політики держави, здатної не лише формально декларувати пріоритети, а й реалізовувати конкретні заходи щодо захисту дітей у кіберпросторі.

Однак ефективна політика неможлива без практичної реалізації – системної, міжсекторальної, орієнтованої на конкретні результати. Саме практика впровадження заходів державної, регіональної та місцевої політики у сфері цифрової безпеки дітей є ключовим індикатором зрілості та дієздатності управлінських рішень. З іншого боку, реальні дії часто стикаються з низкою об'єктивних і суб'єктивних труднощів: обмеженість фінансових ресурсів, недостатня кваліфікація кадрів, розрив між стратегією й виконавчою дисципліною, фрагментарність міжвідомчої взаємодії тощо.

Окрім того, унікальність українського контексту полягає в тому, що реалізація політики захисту дітей у кіберпросторі відбувається в умовах війни, що значно ускладнює не лише забезпечення базових потреб дитини, але й посилює ризики кіберзагроз, які набувають нових форм та масштабів.

Тому в межах цього підрозділу доцільним є аналіз практичних аспектів реалізації політики захисту дітей у кіберпросторі: від державних ініціатив та механізмів до участі недержавних інституцій, шкільних програм, технологічної інфраструктури, а також реальних прикладів і статистичних даних, що відображають результати цієї діяльності. Такий аналіз дозволяє виявити ключові проблеми, виклики, бар'єри, а також сформулювати підґрунтя для напрацювання конструктивних рекомендацій і напрямів подальшого вдосконалення політики.

Профілактика та просвітницька діяльність у сфері захисту дітей у кіберпросторі виступає ключовим напрямом державної політики, адже саме вона формує первинний бар'єр протидії загрозам, виховує критичне мислення, навички цифрової гігієни та відповідального користування інтернетом серед дітей, підлітків, батьків і педагогів. Враховуючи стрімке зростання ризиків у

кіберпросторі, саме превентивні заходи можуть стати ефективним інструментом попередження кібербулінгу, грумінгу, сексуальної експлуатації, маніпуляцій і деструктивного впливу [10], [32], [34].

В Україні за останні роки було реалізовано низку національних кампаній, спрямованих на підвищення цифрової обізнаності дітей. Зокрема, у рамках Національної стратегії захисту дітей в цифровому середовищі на 2021–2026 роки [80] було впроваджено:

- онлайн-платформи для навчання цифровій безпеці («Stop Sexting», «Безпека дітей в інтернеті», «#Не_ведись» тощо);
- цифрові уроки для школярів, у тому числі інтерактивні відеоуроки на базі YouTube-каналів і партнерських ресурсів;
- кампанії в соціальних мережах, спрямовані на протидію онлайн-грумінгу, кібербулінгу та поширенню фейкової інформації;
- пілотні проекти в школах, у рамках яких діти проходили навчання щодо безпечного спілкування в Інтернеті, роботи з особистими даними, повідомлення про ризики тощо [33], [34], [36].

Активну роль у просвітницькій діяльності відіграють міжнародні організації (UNICEF, Save the Children, ECPAT International), а також громадські ініціативи («Ла Страда – Україна», «Ukrainian Child Rights Network»). Вони реалізують: курси з медіаграмотності; тренінги для вчителів; розробку мобільних додатків з безпеки (наприклад, «ReThink»); брошури, методички, рекомендації для батьків, школярів, соціальних працівників [32], [79].

Згідно з даними Міністерства цифрової трансформації, за 2023 рік у рамках платформи «Дія.Цифрова освіта» понад 300 тисяч українських школярів та 60 тисяч освітян пройшли онлайн-курси з основ кібербезпеки та захисту персональних даних.

На рівні МОН, Державної служби якості освіти, Кіберполіції впроваджуються накази й методичні рекомендації щодо проведення класних годин на тему «Безпечний Інтернет», тематичних тижнів цифрової безпеки, тренінгів для педагогів. Водночас, участь освітніх закладів у таких заходах є часто факультативною, залежить від ініціативності адміністрацій та окремих

учителів. За даними Уповноваженого Верховної Ради з прав людини, лише 34 % шкіл мають постійно діючі програми з цифрової безпеки [10].

Незважаючи на позитивні зрушення, залишаються численні проблеми:

1. Фрагментарність і відсутність системності. Багато програм мають разовий характер або реалізуються як пілотні проєкти без масштабування на загальнодержавному рівні.

2. Низький рівень цифрової компетентності вчителів. За результатами опитування 2023 року, лише 18 % педагогів мають достатній рівень знань для проведення уроків із кібербезпеки без додаткової підготовки [34].

3. Недостатня адаптація матеріалів до віку дітей. Часто діти молодшого шкільного віку не розуміють змісту повідомлень, що створює ризик неефективного засвоєння інформації.

4. Відсутність обов'язкової складової у навчальних програмах. Предмет «Цифрова безпека» досі не введено як окремий курс або інтегрований модуль у навчальні плани (табл. 2.6).

Профілактика та просвітницька діяльність є фундаментом національної політики у сфері захисту дітей у кіберпросторі. Ефективність цього напряму значною мірою визначає рівень цифрової безпеки дітей у середньостроковій перспективі. Тому вкрай важливо зробити цей компонент системним, обов'язковим, масштабованим і професійно забезпеченим. Особливу увагу слід приділяти підготовці вчителів, розробці вікових програм, залученню батьків та інтеграції цифрової безпеки у всі освітні рівні – від початкової школи до профільної старшої.

Без якісної превенції держава ризикує втратити ключовий захисний рубіж у боротьбі з кіберзлочинністю та негативними інформаційними впливами на дітей.

У сучасних умовах функціонування цифрового середовища, ефективно реагування на кіберінциденти, що зачіпають дітей, є не лише питанням технологічної готовності, а й важливим елементом національної гуманітарної безпеки [28], [35], [51]. Швидкість, координація та скоординованість дій між

інституціями – критично важливі чинники, які визначають, чи отримає дитина своєчасний захист, а зловмисник – належне покарання.

Кіберінциденти, пов'язані з дітьми, можуть охоплювати широкий спектр порушень – від інтернет-грумінгу, кібербулінгу, розповсюдження інтимних матеріалів без згоди (сексторшену) до фінансових шахрайств, пов'язаних з онлайн-іграми. У випадках з українськими дітьми, особливо в умовах війни, зросла кількість інцидентів, пов'язаних із ворожою пропагандою, залученням у кіберактивізм, або використанням неповнолітніх як інструментів у гібридних інформаційних атаках [34], [55].

Таблиця 2.6

Виклики цифрової безпеки дітей в умовах війни

№	Категорія виклику	Конкретний прояв / приклад	Потенційні наслідки для дитини	Можливі заходи реагування
1	Кіберзагрози з боку агресора	Пропаганда, фейкові новини, психологічні атаки в соцмережах	Дезорієнтація, страх, радикалізація	Фільтрація контенту, медіаосвіта, VPN-захист
2	Втрата доступу до освіти	Зруйнована інфраструктура, нестабільний інтернет	Освітня ізоляція, зниження навичок цифрової грамотності	Онлайн-платформи, мобільні освітні класи
3	Зниження рівня батьківського нагляду	Вимушене переміщення, втрата одного чи обох батьків	Самоізоляція, необмежений доступ до небезпечного контенту	Просвітництво опікунів, цифрові батьківські контролю
4	Відсутність стійкої ІТ-інфраструктури	Атаки на енергосистему, хостинги, сервіси безпеки	Неможливість реагування на інциденти	Резервні дата-центри, автономні сервіси
5	Низький рівень довіри до інституцій	Дитина не повідомляє про кібернасилля або шантаж	Посилення психологічних травм	Онлайн-платформи анонімного звернення, чат-боти
6	Погіршення психоемоційного стану	Війна, втрати, депресія, кібербулінг	Замкненість, підвищений ризик самогубств	Онлайн-психолог, кризові центри, реєр-to-реєр підтримка
7	Недосконалість законодавства в умовах кризи	Повільне оновлення нормативно-правових актів	Прогалини у відповідальності, ускладнення притягнення до відповідальності	Адаптація законодавства, воєнні цифрові протоколи

Джерело: систематизовано автором

У механізмах реагування на такі інциденти в Україні залучено декілька ключових інституцій:

1. Кіберполіція Національної поліції України – спеціалізований підрозділ, що займається розслідуванням кіберзлочинів. Приймає звернення громадян, реагує на повідомлення про онлайн-злочини проти дітей через гарячу лінію, сайт або мобільний додаток [11].

2. Уповноважений Верховної Ради з прав людини – здійснює моніторинг дотримання прав дитини, зокрема й у цифровому просторі, має повноваження реагувати на скарги громадян та направляти подання до компетентних органів [10], [16].

3. Міністерство цифрової трансформації України – координує політику цифрової грамотності та реагування на інциденти через Національний центр оперативного реагування на комп'ютерні інциденти (CERT-UA).

4. Освітні заклади та педагогічні працівники – є першою лінією ідентифікації кіберінцидентів серед школярів, однак часто не мають достатніх повноважень або компетенцій для кваліфікованої реакції [34].

5. Служби у справах дітей, центри соціальних служб, психологічні служби – надають допомогу після виявлення інциденту, однак мають обмежений технічний та оперативний інструментарій.

6. Громадські організації та міжнародні партнери – реалізують власні системи фіксації, моніторингу та перенаправлення звернень до офіційних органів (наприклад, ECPAT, La Strada-Україна, StopSexting).

Хоча формально існують механізми міжінституційної взаємодії (наприклад, через Національну дитячу гарячу лінію, що координується кількома структурами одночасно), на практиці вони часто демонструють: відсутність єдиного інформаційного хабу щодо реєстрації кіберзагроз; подвійне або неповне реагування (коли звернення губляться між відомствами або не проходять належного опрацювання); вузький функціонал окремих служб, які не мають технічних ресурсів для ідентифікації джерел загроз; тривалість процедур, які не відповідають динаміці кіберзлочинів.

На думку дослідниці О. І. Димитрієвої, критичним викликом є саме фрагментарність управлінської структури реагування на цифрові загрози для

дітей, відсутність постійно діючих міжвідомчих координаційних центрів [35], [37].

Згідно з даними Кіберполіції за 2023 рік: біля 2 500 звернень стосувалися дітей як жертв онлайн-злочинів; 42% випадків були пов'язані з кібербулінгом; 19% – із спробами онлайн-грумінгу або вимагання інтимних фото; 14% – із втягненням дітей у «групи смерті» або радикальні онлайн-спільноти [11].

Однак офіційна статистика не завжди відображає реальні масштаби проблеми, оскільки більшість інцидентів залишаються нерозголошеними або не розслідуються через відсутність доказів, небажання батьків подавати заяви, страх дітей перед викриттям.

Для порівняння, в Естонії та Південній Кореї діють централізовані цифрові хаби з функцією автоматизованого виявлення загроз та міжвідомчого перенаправлення інцидентів протягом перших 24 годин після звернення. Польща впровадила систему «Dyzurnet», яка дозволяє повідомляти про порушення анонімно, а також інтегрувати базу даних з Європейським центром боротьби з кіберзлочинністю (EC3) [11].

Сучасна система реагування на кіберінциденти щодо дітей в Україні потребує структурного оновлення, централізації, технічного переоснащення та професійної підготовки кадрів. Без оперативної взаємодії між інституціями, автоматизованих механізмів обміну даними та правового захисту дитини як жертви кіберзлочину – національна система не зможе ефективно відповідати на сучасні цифрові виклики.

Необхідним є створення єдиного національного центру реагування на цифрові інциденти з дітьми, підключеного до міжнародних платформ, забезпеченого правовими інструментами, оперативною командою, психологічною та технічною підтримкою. Це стане не лише кроком до підвищення цифрової безпеки дітей, а й критичною складовою сучасної гуманітарної політики держави.

У сучасних умовах школа посідає центральне місце у системі захисту дитини в цифровому середовищі, виконуючи роль не лише освітнього закладу, а й осередку соціалізації, формування цифрової грамотності та первинної

профілактики кіберзагроз. Саме в шкільному середовищі дитина вперше стикається з системним користуванням інтернетом, спілкуванням у цифрових мережах, застосуванням освітніх платформ, а отже – й з першими ризиками. У цьому контексті школа перетворюється на ключовий простір реалізації державної політики безпеки у цифровому просторі.

Згідно з положеннями Національної стратегії захисту дітей у кіберпросторі на 2021-2026 роки [80], школи розглядаються як одна з пріоритетних ланок у впровадженні заходів цифрової безпеки. Відповідно до Стратегії, саме через заклади освіти мають здійснюватися: інтеграція цифрової грамотності в освітні програми; впровадження спеціалізованих курсів із кібербезпеки; професійна підготовка педагогів до викладання питань цифрової етики; створення безпечної цифрової інфраструктури в межах школи; психологічний супровід дітей, які зазнали кіберзагроз.

У цьому контексті школа виступає інституційним провідником як державної освітньої політики, так і соціальної місії із захисту вразливої категорії дітей. Одним з інструментів формування цифрової безпеки є освітній компонент. В Україні за останні роки відзначено низку позитивних зрушень, зокрема: включення до шкільної програми тем із цифрової етики, захисту персональних даних, безпечного спілкування в мережі; запуск проєктів типу «Онлайн-самостійність», «Безпека дітей в інтернеті», які реалізуються МОН у партнерстві з громадськими організаціями [32], [83]; участь шкіл у Всеукраїнському тижні безпечного інтернету у співпраці з Google, UNICEF, StopSexting тощо.

Втім, багато освітніх закладів все ще обмежуються формальними заходами, такими як разові лекції, перегляд відеороликів чи написання рефератів. Не вистачає системної інтеграції цифрової безпеки у навчальні плани, з урахуванням вікових особливостей дітей та динаміки кіберзагроз.

Однією з критичних проблем є низький рівень підготовки вчителів до реагування на інциденти у кіберпросторі. Дослідження [33], [34] свідчать, що понад 65% педагогів не мають чіткого уявлення про механізми ідентифікації

кібербулінгу, погроз, шкідливих онлайн-ігор. Водночас діти часто звертаються саме до вчителя як до авторитетної особи у випадках інцидентів.

Необхідність підвищення кваліфікації вчителів визнана на державному рівні, зокрема через відповідні модулі у межах підготовки за програмою НУШ (Нова українська школа). Проте такі курси мають бути масштабованими, інтерактивними, технічно обґрунтованими та супроводжуватись постійною методичною підтримкою [15], [34].

Інформаційна безпека також неможлива без належної цифрової інфраструктури. Багато українських шкіл досі: не мають фільтрації контенту в шкільних мережах; не застосовують захищені канали передачі даних; не впроваджують контроль доступу до онлайн-ресурсів для учнів молодших класів; зберігають персональні дані дітей без шифрування чи належного правового регулювання [43], [91].

У цьому контексті важливою є модернізація технічної бази, у тому числі – із залученням коштів ДФРР, місцевих бюджетів та партнерських ініціатив з приватним сектором [30], [123].

Школа також має забезпечувати психологічний супровід постраждалих від кібербулінгу, шантажу чи секстингу. Проте, за даними на 2023 рік, тільки 23% шкіл в Україні мають постійного практичного психолога. У багатьох випадках саме відсутність професійної допомоги посилює наслідки кіберінцидентів, особливо в умовах стресових ситуацій або замовчування проблеми.

Ключовим є усвідомлення того, що школа – це не просто навчальний заклад, а середовище раннього виявлення, реагування і профілактики цифрових загроз. За умови належної інтеграції заходів цифрової безпеки школа може: розпізнати перші ознаки кіберзагрози; організувати взаємодію з батьками та правоохоронними органами; виступати як платформа для формування критичного мислення та медіаграмотності.

Школа повинна трансформуватися з пасивного спостерігача на активного суб'єкта політики захисту дітей у кіберпросторі. Це вимагає оновлення програм, професійного розвитку педагогів, інвестицій у цифрову

інфраструктуру та розвитку партнерських зв'язків із правоохоронними, громадськими та міжнародними структурами. Успішна реалізація такого підходу дозволить забезпечити не лише знання, а й цифрову стійкість дитини – як на рівні школи, так і у всьому суспільстві.

У сучасному інформаційному суспільстві технологічне забезпечення виступає не лише інструментом навчання чи доступу до інформації, але й критично важливим елементом системи захисту дітей у кіберпросторі. Цифрова інфраструктура, засоби кіберзахисту, системи моніторингу загроз, а також безпечні середовища взаємодії (освітні платформи, соціальні мережі, онлайн-сервіси) – усе це формує середовище, у якому дитина може або реалізувати свої права безпечно, або стати вразливою до кіберзагроз.

У національному контексті питання технологічного забезпечення політики безпеки дітей у кіберпросторі є надзвичайно актуальним, враховуючи: масштабне поширення цифрових пристроїв серед дітей (відповідно до статистики Мінцифри, станом на 2023 рік понад 86% дітей віком 10–17 років мають особисті смартфони з виходом в інтернет); масовий перехід на дистанційне або гібридне навчання в умовах війни; зростаючу кількість шкідливого контенту, фішингових атак, маніпуляцій та пропагандистських впливів, спрямованих на дитячу аудиторію [10], [11], [32].

Елементи технологічного забезпечення представляють собою сукупність заходів.

1. Фільтрація контенту та безпечний інтернет-доступ. Сучасні системи контент-фільтрації дозволяють блокувати небажаний або шкідливий контент (наси́льство, порнографія, наркотики, ігри смерті тощо). Однак на практиці, за результатами опитувань, лише 29% українських шкіл користуються подібними системами регулярно. У домогосподарствах цей відсоток ще нижчий, адже батьки часто не мають технічних навичок або часу налаштовувати такі механізми.

Серед доступних рішень – OpenDNS, Kaspersky Safe Kids, Google SafeSearch, а також вбудовані функції батьківського контролю у Windows, Android, iOS. Масштабне поширення таких інструментів потребує державної

підтримки, інструкцій для закладів освіти і батьків, а також пілотного впровадження відповідних програм.

2. Цифрова ідентифікація та захист персональних даних. Захист персональних даних дітей набув нової актуальності з поширенням е-журналів, платформ онлайн-навчання, систем відеонагляду у школах. Згідно із Законом України «Про захист персональних даних» [91] та Законом України «Про охорону дитинства» [95], збирання, обробка й зберігання інформації про дитину повинні здійснюватися з дотриманням принципів мінімізації, обмеження доступу та інформованої згоди.

Проте аудит інформаційної безпеки в освітніх закладах показує, що понад 40% систем зберігання даних учнів не мають елементарного шифрування чи резервного копіювання [53].

3. Інструменти раннього виявлення та реагування. Застосування аналітичних платформ із елементами ШІ (наприклад, SafeToNet, Bark, Net Nanny) дозволяє виявляти ризиковані шаблони поведінки дитини в мережі: тривожні пошукові запити, ознаки кібербулінгу, комунікацію з невідомими дорослими, самогубні настрої тощо.

Такі системи особливо ефективні при застосуванні в контексті партнерства шкіл із батьками та ІТ-компаніями. Однак їх використання в Україні є фрагментарним і, здебільшого, обмеженим до кількох пілотних проєктів.

4. Захист каналів зв'язку та цифрової інфраструктури. На фоні гібридної війни та зростання загроз з боку іноземних ІТ-центрів, важливим стає питання кіберзахисту самих освітніх платформ. Йдеться про: шифрування даних (SSL/TLS); захист від DDOS-атак; багатофакторну автентифікацію; регулярні оновлення та аудит безпеки.

Такі заходи мають бути закладені в усі національні освітні ІТ-системи (E-schools, «Єдина школа», Національна електронна платформа тощо). Згідно з Національною стратегією кібербезпеки України [93] та Концепцією цифрової трансформації освіти, держава покликана не лише створювати правові умови, а й сприяти розвитку ІТ-інфраструктури на всіх рівнях. Реалізовано проєкти:

«Ноутбук кожному вчителю»; «Шкільний Wi-Fi»; платформа «Всеукраїнська школа онлайн»; підтримка грантів на цифрову модернізацію від Мінцифри.

Окремі громади впроваджують власні програми кібербезпеки – наприклад, у Львівській, Полтавській та Київській областях реалізуються ІТ-платформи для моніторингу шкільного контенту та кіберзагроз.

Компанії типу Microsoft, Google, Київстар, Ajax Systems надають технічну підтримку, хмарні рішення, освітні продукти із вбудованими протоколами безпеки для шкіл і навчальних платформ.

Таким чином, технологічне забезпечення та цифрова інфраструктура є фундаментальним фактором ефективності політики захисту дітей у кіберпросторі. Проте його реалізація потребує системного підходу: стратегічного планування, багаторівневої координації, технічної підтримки, фінансування та просвітницької роботи серед освітян, батьків і дітей.

Впровадження інтелектуальних інструментів захисту, автоматизованого моніторингу, кібергігієнічних протоколів у школах і домашньому середовищі має стати не опцією, а обов'язковою нормою в українських реаліях. Тільки в такому випадку можна гарантувати не лише формальну, а й реальну безпеку кожної дитини у цифровому просторі.

Однією з ключових проблем, що системно ускладнює реалізацію політики захисту дітей у кіберпросторі України, є відсутність цілісної системи моніторингу, оцінювання ефективності та прогнозування результатів. Цей структурний недолік не дозволяє вчасно виявляти нові кіберзагрози, коригувати заходи політики, адаптувати інституційні та правові механізми до мінливих цифрових реалій, а також – приймати обґрунтовані управлінські рішення на основі об'єктивних даних [3], [38].

На сьогодні відсутня єдина державна система збору, обробки та аналізу даних щодо інцидентів, пов'язаних із цифровою безпекою дітей. Інформація про кіберзагрози або поширюється епізодично через ЗМІ, або збирається фрагментарно різними органами – МВС, кіберполіцією, Офісом Уповноваженого з прав дитини, органами освіти, неурядовими організаціями – без міжвідомчого обміну чи стандартизації форматів даних.

Наприклад, відсутні уніфіковані статистичні звіти щодо: кількості випадків кібербулінгу, секстингу, онлайн-грумінгу серед дітей; типів загроз, найпоширеніших у регіонах; ефективності вжитих заходів реагування; рівня цифрової обізнаності та навичок кібергігієни серед дітей і вчителів; впроваджених технічних рішень у навчальних закладах (фільтрація, моніторинг, навчання).

Наразі жоден орган не здійснює регулярного щорічного моніторингу динаміки ризиків у кіберпросторі саме для дітей, як це робиться у сфері охорони здоров'я чи соціального захисту. Неможливість оцінити реальний масштаб проблеми. Фактична кількість постраждалих дітей залишається невідомою. Створюється ілюзія контрольованої ситуації, в той час як загрози можуть мати масовий, латентний характер. Відсутність об'єктивних показників для оцінки ефективності політики. Без системних індикаторів неможливо оцінити, які заходи діють, а які – є неефективними або застарілими. Ризик дублювання функцій і нераціонального використання ресурсів. У відсутності координації інституції можуть паралельно розробляти схожі програми, замість синергії, обміну даними й інтеграції зусиль. Нездатність до оперативного реагування на нові цифрові загрози. Кіберсередовище динамічне – нові виклики (наприклад, використання нейромереж у фейкових відео або злочини у метавсесвітах) виникають швидше, ніж до них встигає адаптуватись державна політика.

Недовіра суспільства та міжнародних партнерів. Відсутність відкритих, підтверджених показників і звітності заважає співпраці з міжнародними організаціями та обмежує інституційну спроможність залучати технічну чи фінансову допомогу (табл. 2.7).

Відсутність системного моніторингу та оцінювання цифрових загроз для дітей є не просто організаційною проблемою, а сутнісним бар'єром на шляху до ефективної, превентивної і прозорої державної політики. Наявність такої системи дозволила б перейти від реактивних до проактивних дій, базувати рішення на доказах, адаптуватися до змін і, зрештою, ефективно захищати найуразливішу частину суспільства – дитину – в цифровому світі.

Ключові показники цифрової вразливості дітей в умовах війни

Показник	Значення / тренд	Коментар до впливу
Частка дітей до 15 років, які мають доступ до інтернету в Україні	~ 50,2% (станом на 2019 р.) ЮНІСЕФ	Базова цифрова присутність – діти онлайн, отже під ризиком цифрових загроз
Частка молоді (15-24 роки), яка стикалася з онлайн-шахрайством, фішингом або зламами	~ 1 з 3 опитаних ЮНІСЕФ	Вказує на активне проявлення кіберризиків серед молоді в Україні
Кількість кіберінцидентів – Україна (усього за 2024 р.)	~ 3 млн оброблених подій, >1 000 підтверджених інцидентів Syble	Висока активність кіберзагроз у воєнний час – підсилює ризики для дітей
Зростання кількості кібератак в Україні за рік	+70% (за повідомленнями на початок 2025 р.) Українська правда	Демонструє динаміку загострення кіберзагроз – діти більш піддані ризикам
Частка дітей та підлітків, які не звертаються по допомогу після кібербулінгу	~ 1 з 5 опитаних ЮНІСЕФ	Показник соціальної вразливості: неготовність або страх звертатися за захистом

Джерело: [67]

Повномасштабна війна, що триває на території України з 2022 року, радикально трансформувала суспільні процеси, зокрема й у сфері забезпечення цифрової безпеки дітей. У контексті воєнного конфлікту зростає не лише кількість зовнішніх кіберзагроз, а й ускладнюється реалізація базових функцій держави щодо захисту дітей у кіберпросторі, що створює серйозні виклики як для органів влади, так і для освітніх і соціальних інституцій [7], [27], [30].

В умовах війни діти, особливо ті, що проживають на тимчасово окупованих територіях, у зоні бойових дій або в евакуації, опиняються в середовищі, де цифрові технології часто є єдиним інструментом комунікації, освіти, соціалізації та психологічної підтримки. Однак такий цифровий простір не є безпечним. Воєнний контекст породжує:

1. Посилення інформаційно-психологічного впливу, включаючи пропаганду, фейки, маніпуляції, дезінформацію, спрямовану на формування викривленої картини світу у дітей, особливо через соціальні мережі.

2. Активізацію кіберзлочинних груп, які використовують війну як привід для виманювання персональних даних, шантажу, вербування чи поширення шкідливого контенту.

3. Підвищену залежність дітей від онлайн-середовища, що призводить до надмірного екранного часу, розмиття реальності, депресивних або суїцидальних станів [10], [79].

Особливо небезпечною є інформаційна обробка дітей російською пропагандистською машиною, яка через TikTok, Telegram-канали, YouTube поширює наративи про «звільнення», дискредитує державні інституції, насаджує культуру агресії та ненависті. Діти з окупованих регіонів – Харківщини, Луганщини, Донеччини, Запоріжжя – перебувають під постійним впливом таких меседжів.

Війна суттєво послабила інституційну спроможність держави захищати дітей у цифровому просторі. До ключових проблем належать: руйнування інфраструктури освіти і соціального захисту, внаслідок чого тисячі дітей втратили доступ до офлайн-закладів, консультацій, превентивної підтримки; вимушене переміщення мільйонів дітей, що ускладнило їх облік, контроль за умовами доступу до Інтернету, фіксацію випадків кіберзлочинів; переформатування пріоритетів політики, коли більшість ресурсів зосереджуються на воєнних цілях, а цифрова безпека дітей сприймається як другорядне завдання; погіршення координації між органами влади, зокрема через часті зміни в структурі органів, дефіцит кадрів, відтік спеціалістів у сфері кіберзахисту.

Цифровізація освіти під час війни набула стрімкого, але хаотичного характеру. Попри те, що дистанційне навчання стало єдиною можливою формою навчання для мільйонів дітей, школи не завжди мали технічну, методичну та кадрову готовність до ефективного впровадження цифрових інструментів: Не всі заклади забезпечені фільтрацією трафіку, антивірусним захистом, кіберпедагогами. Частина педагогів не має належних навичок для розпізнавання кіберризиків. Контент, який споживають діти під виглядом «навчального», часто не модерується. Відсутня централізована підтримка для вразливих дітей (діти з інвалідністю, сироти, ВПО).

Чинне українське законодавство, хоч і має певні механізми забезпечення кібербезпеки (Закони України «Про основні засади забезпечення кібербезпеки»

[93], «Про охорону дитинства» [95], «Про захист персональних даних» [91]), однак не враховує реалії воєнного стану – масової цифрової міграції, онлайн-освіти, кіберзагроз в умовах окупації, гібридної війни.

Наприклад, не визначено, які органи відповідають за моніторинг цифрової безпеки дітей на тимчасово окупованих територіях або в евакуаційних центрах. Відсутні також положення про захист дітей у кіберпросторі в умовах надзвичайного або воєнного стану, що створює правовий вакуум і невизначеність. Використання дітей у кібератаках або для розповсюдження контенту, включно з публікаціями проросійського змісту, фейками, DDoS-атаками на освітні ресурси. Поширення «військового контенту» серед неповнолітніх, що пропагує насильство, нормалізує зброю, формує хибну картину про воєнні дії як героїчну гру. Вразливість дітей до маніпуляцій, пов'язаних з втратою близьких, переселенням, що робить їх легкою мішенню для експлуататорів і злочинців.

Війна не лише загострила існуючі виклики у сфері цифрової безпеки дітей, а й створила нові, системні загрози, що потребують негайної адаптації політики, правових механізмів, інституційної моделі та цифрової інфраструктури. У нинішніх умовах неможливо забезпечити ефективний захист дітей у кіберпросторі без урахування реалій війни, зокрема специфіки інформаційного середовища, зміни освітніх форматів, міграції населення, правового статусу територій.

Україна повинна розглядати цифровий захист дітей як складову гуманітарної та національної безпеки, адаптувати відповідну стратегію, створити кризові протоколи реагування, механізми інформування та підтримки для сімей з дітьми у воєнних умовах, а також забезпечити доступ до правдивої, безпечної, дитячої цифрової екосистеми.

Висновки до розділу 2

У результаті всебічного аналізу було 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.

Класифікація загроз, проведена у розділі, засвідчила, що їх природа є багат шаровою: 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.

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 переважно декларативним, а діти часто залишаються сам на сам із загрозами, не маючи ані необхідних знань, ані ефективної підтримки.

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.

РОЗДІЛ 3. ШЛЯХИ ВДОСКОНАЛЕННЯ ДЕРЖАВНОЇ ПОЛІТИКИ ЗАХИСТУ ДІТЕЙ У КІБЕРПРОСТОРІ В КОНТЕКСТІ ГУМАНІТАРНОЇ БЕЗПЕКИ

3.1. Стратегічні пріоритети державної політики захисту дітей у кіберпросторі

Цифровізація усіх сфер суспільного життя, зокрема освіти, культури, дозвілля, комунікації та державного управління, зумовила не лише нові можливості, але й нову архітектуру ризиків, пов'язаних із безпекою дитини у кіберпросторі. Особливої актуальності це питання набуло для України в умовах воєнного часу, коли інформаційні впливи та цифрові атаки мають не лише технологічну, але й гуманітарну складову, спрямовану на підриг ментальної стійкості молодого покоління [35], [7], [81].

Водночас на тлі динамічного розвитку цифрових технологій та інтернет-середовища, нормативне, інституційне та освітнє реагування держави виявляється переважно фрагментарним і реактивним [36], [37]. Попри наявність окремих документів стратегічного рівня – таких як Національна стратегія захисту дітей у кіберпросторі на 2021–2026 роки [80] – система державної політики захисту дітей у кіберпросторі ще не має чітко виокремлених пріоритетів, інтегрованих у загальнонаціональні плани цифрового розвитку, кібербезпеки та гуманітарної безпеки [92], [93].

Крім того, стратегічне планування у сфері захисту дитини в цифровому просторі потребує врахування таких глобальних викликів, як: масове поширення цифрових залежностей серед підлітків; зростання обсягів шкідливого контенту; комерціалізація дитячих даних; використання алгоритмів для впливу на емоційний стан дітей [128], [142]; кібербулінг, грумінг, онлайн-експлуатація [79], [10].

Державна політика має не лише реагувати на існуючі ризики, а й системно запобігати їх виникненню, формуючи культуру цифрової безпеки в суспільстві. Для цього потрібні чітко окреслені стратегічні пріоритети, які

визначатимуть: цілісне бачення проблеми, механізми координації між секторами, технологічну інфраструктуру, нормативно-правову базу, і найголовніше – орієнтацію на права, потреби та інтереси дитини [52], [84].

З огляду на це, стратегічні пріоритети політики захисту дітей у кіберпросторі мають включати: розвиток цифрової грамотності дітей і дорослих; інституційне укріплення системи захисту; впровадження інноваційних технологій безпеки; гармонізацію з міжнародними стандартами; моніторинг, аналітику та участь дітей у формуванні безпечного цифрового простору [33], [38], [128].

Метою цього підрозділу є комплексний аналіз ключових стратегічних напрямів формування та реалізації державної політики у сфері захисту дітей у кіберпросторі, що дозволить забезпечити не лише фізичну та інформаційну безпеку, а й ментальне, психологічне та соціальне благополуччя дитини в цифрову епоху (табл. 3.1).

Запобігання загрозам у кіберпросторі є одним із ключових елементів забезпечення національної, гуманітарної та інформаційної безпеки держави, що набуває особливої актуальності у контексті захисту прав і свобод дитини. У сучасному кіберпросторі дитина стикається з багатовимірною системою ризиків – від доступу до шкідливого контенту та цифрового насильства до маніпулятивних алгоритмів та експлуатації персональних даних [10], [43], [128].

Фундаментальною умовою для мінімізації таких ризиків є підвищення рівня цифрової грамотності всіх учасників освітнього та соціального процесу – не лише дітей, а й батьків, педагогів, соціальних працівників, правоохоронців і самих держслужбовців, відповідальних за розробку та реалізацію політики. Цифрова грамотність у цьому контексті має розумітися не лише як здатність користуватись цифровими пристроями, але як комплекс компетентностей, що включають критичне мислення, навички онлайн-комунікації, безпечну поведінку в мережі, базові правові знання щодо захисту особистих даних та відповідальності за порушення норм цифрової етики [15], [50], [51].

Стратегічні пріоритети державної політики захисту дітей у кіберпросторі України

№	Напрямок	Стратегічна ціль	Інструменти та механізми реалізації	Очікувані результати
1	Цифрова грамотність та освіта	Формування компетенцій безпечного користування Інтернетом у дітей	Впровадження курсів у школах, онлайн-навчання, тренінги для педагогів, інтерактивні платформи	Зменшення кількості кіберінцидентів за участі дітей; підвищення цифрової стійкості
2	Інституційна координація	Забезпечення ефективної взаємодії державних структур і громадського сектору	Координаційні ради, спільні протоколи реагування, міжвідомчі платформи	Швидке реагування на інциденти, уніфікована політика
3	Технологічне забезпечення	Побудова інфраструктури захисту дітей у кіберпросторі	Фільтрація контенту, системи моніторингу, AI-аналіз ризиків, національні сервіси скарг	Виявлення та запобігання загроз у режимі реального часу
4	Міжнародна інтеграція та стандарти	Адаптація української політики до міжнародних стандартів захисту дітей	Імплементация Конвенції про кіберзлочинність, дотримання GDPR, участь у програмах ЄС, НАТО	Гармонізація політики, покращення репутації України
5	Юридичне та нормативне вдосконалення	Оновлення законодавства відповідно до цифрових викликів	Внесення змін до законів про захист дітей, персональні дані, цифрову освіту	Своєчасна правова відповідь на новітні загрози
6	Моніторинг та наукове супроводження	Створення системи оцінки ризиків, ефективності політик	Центри аналітики, співпраця з ВНЗ, пілотні проекти, державна статистика	Прийняття рішень на основі даних; адаптивне управління
7	Підвищення кваліфікації фахівців	Розвиток кадрового потенціалу у сфері захисту дітей в цифровому середовищі	Підвищення кваліфікації педагогів, соцпрацівників, кіберполіції	Покращення якості реагування та профілактики
8	Участь дітей та молоді	Забезпечення залучення дітей до формування безпечного цифрового середовища	Молодіжні форуми, дитячі ради, платформи для ініціатив	Більша ефективність політик завдяки зворотному зв'язку
9	Виклики воєнного часу	Адаптація безпекової політики до умов гібридної війни	Кіберзахист шкільної інфраструктури, підтримка дітей ВПО, протидія дезінформації	Стійкість освітнього процесу; менше інцидентів, пов'язаних з воєнними кіберзагрозами

Джерело: систематизовано автором

З огляду на європейську парадигму розвитку політик цифрової безпеки, ефективно запобігання загрозам передбачає перехід від реактивних до проактивних моделей. Це означає, що державна політика має орієнтуватися не лише на реагування на вже скоєні правопорушення у кіберсфері, а передусім – на створення запобіжних бар'єрів, формування культури відповідального використання цифрових ресурсів та просування цінностей інформаційної етики.

У 2021 році Україна вперше прийняла Національну стратегію захисту дітей у кіберпросторі[80], яка визначила пріоритетність цифрової грамотності як системного напрямку державної політики. У цьому документі наголошено, що формування цифрової компетентності дітей є основною запорукою їхнього безпечного перебування в онлайн-просторі, з урахуванням принципу «благополуччя дитини насамперед» (best interests of the child first) [47], [84].

Ключові аспекти цифрової грамотності як елемента безпеки передбачають наступне:

1. Критичне мислення у кіберпросторі. Формування в дітей здатності аналізувати, перевіряти достовірність джерел, розпізнавати фейки, маніпуляції, пропаганду. Цей компонент є надзвичайно важливим в умовах воєнної агресії РФ, коли діти нерідко стають мішенню психологічних операцій через TikTok, YouTube, Telegram тощо [128], [35].

2. Цифрова гігієна. Навички щодо управління пароллями, персональними даними, поведінкою у соцмережах, уникнення випадкових кліків на небезпечні посилання, захисту пристроїв. Практика низки країн (Естонія, Польща) свідчить, що інтеграція елементів цифрової гігієни у шкільну програму значно знижує вразливість учнів до кіберзагроз [138].

3. Розуміння правових аспектів цифрової поведінки. Діти мають знати свої права у кіберпросторі, зокрема право на приватність, захист персональних даних, заборону на кібербулінг і грумінг, а також можливість звернення до відповідних органів – Кіберполіції, Уповноваженого з прав дитини, суду [11], [112].

4. Емоційна саморегуляція та психологічна стійкість. Цифрова безпека тісно пов'язана з емоційним здоров'ям дитини. Вплив алгоритмів соціальних

мереж на самооцінку, залежність від лайків, експозиція до шкідливого контенту (самопошкодження, насильство) можуть викликати стрес, тривожність, депресивні стани [10], [142]. Тому важливо навчати дітей розпізнавати власні емоції в цифровому середовищі.

5. Медіаграмотність як частина шкільної освіти. В Україні впроваджується курс «Культура добросусідства» з елементами критичного мислення, проте загальний обсяг уроків цифрової грамотності залишається вкрай обмеженим. Для ефективного впровадження необхідна інтеграція цифрових модулів в обов'язкові дисципліни або створення окремого міждисциплінарного курсу [33], [36].

6. Цифрова просвіта батьків і педагогів. Як свідчать дані Міністерства цифрової трансформації, понад 70% батьків в Україні не знають, як контролювати онлайн-активність дитини або реагувати на кіберінциденти [10]. Це вимагає системного просвітницького компоненту через онлайн-курси (наприклад, «Дія.Цифрова освіта»), методичні посібники, тренінги для батьків, вчителів, соціальних педагогів [15].

Практичні напрямки реалізації пріоритету: Запровадження обов'язкового курсу «Цифрова безпека» для учнів 5–11 класів. Сертифікація цифрових компетентностей учителів за моделлю DigCompEdu. Розвиток національних кампаній цифрової просвіти (типу «StopFake», «КіберОсвітник»). Створення інтерактивних навчальних платформ для дітей з віковими адаптаціями (із залученням гейміфікації). Співпраця з соціальними мережами з метою маркування шкідливого контенту, блокування грумінгу та кібербулінгу.

Цифрова грамотність є ключовим щитом, що захищає дитину в умовах всеохоплюючого цифрового середовища. Без її розвитку неможливо реалізувати інші пріоритети державної політики захисту дітей – ні технологічні, ні правові, ні інституційні. Це не лише освітня, але й гуманітарна та безпекова інвестиція у майбутнє покоління українців. Формування комплексної цифрової компетентності дітей, батьків і освітян повинно стати одним із базових орієнтирів державного розвитку у сфері безпеки та прав людини (табл. 3.2).

Ефективна реалізація державної політики захисту дітей у кіберпросторі вимагає не лише наявності нормативної бази та освітніх ініціатив, а й скоординованої взаємодії між державними органами, громадським сектором, освітніми установами, ІТ-галуззю та міжнародними партнерами. У сучасних умовах, коли цифрові загрози носять багатовимірний характер – від кібербулінгу до цифрової експлуатації, від втрати персональних даних до впливу на психоемоційний стан – ізольоване реагування окремих інституцій є неефективним.

Таблиця 3.2

Ключові компоненти цифрової грамотності дітей у контексті запобігання кіберзагрозам

№	Компонент цифрової грамотності	Зміст та призначення	Вікова адаптація	Потенційна загроза, яку нейтралізує
1	Критичне мислення	Уміння аналізувати інформацію, виявляти фейки, дезінформацію, пропаганду	10+ років	Фейкові новини, пропаганда, психологічні операції
2	Цифрова гігієна	Захист паролів, обмеження доступу до персональних даних, використання антивірусу	7+ років	Витік даних, хакінг, шкідливе ПЗ
3	Медіаграмотність	Розпізнавання джерел інформації, робота з відео/зображеннями, захист від маніпуляцій	12+ років	Алгоритмічні маніпуляції, деструктивний контент
4	Правова грамотність	Знання прав у цифровому просторі, механізмів скарг та звернень	10+ років	Грумінг, кібербулінг, експлуатація
5	Емоційна саморегуляція	Управління емоціями, стресостійкість, реагування на онлайн-насильство	9+ років	Емоційне вигорання, залежність, кібернасильство
6	Навички безпечної комунікації	Уміння взаємодіяти з однолітками й незнайомцями в соцмережах, уникати провокацій	8+ років	Грумінг, секстинг, тролінг, шантаж
7	Управління часом у кіберпросторі	Навички обмеження часу онлайн, баланс між офлайн- та онлайн-життям	6+ років	Залежність від гаджетів, порушення сну, когнітивні ризики
8	Участь батьків / супровід дорослих	Вміння залучати дорослих до вирішення проблем, звертатися за підтримкою	Усі вікові категорії	Самотність в ситуації ризику, відсутність допомоги

Джерело: систематизовано автором

Україна вже має інституційний фундамент для реалізації політики захисту дітей у цифровому просторі. До ключових суб'єктів належать: Міністерство

цифрової трансформації України, що відповідає за цифрову інфраструктуру, стратегії цифровізації та реалізацію Національної стратегії захисту дітей у кіберпросторі на 2021–2026 роки [80]; Міністерство освіти і науки України, яке координує впровадження цифрової грамотності у шкільну програму та виховні ініціативи [33]; Кіберполіція Національної поліції України, яка розслідує злочини проти дітей у кіберпросторі та веде профілактичну діяльність [11]; Служба у справах дітей, яка має повноваження у сфері соціального захисту та реагування на випадки жорстокого поводження, в тому числі й у цифровій формі [46]; Уповноважений Верховної Ради України з прав людини (омбудсман), що забезпечує дотримання прав дитини та координує механізми реагування на скарги у цифровій сфері [16], [42]; Громадські організації та експертні аналітичні центри (наприклад, Stop Sexting, Ла Страда-Україна), які реалізують тренінги, гарячі лінії, аналітичні дослідження й моніторинг.

Однак системність у діях цих інституцій часто відсутня. Проблемою є недостатній рівень міжвідомчої взаємодії, що проявляється у дублюванні функцій, слабкій обізнаності про повноваження партнерських органів, відсутності спільних цифрових платформ обміну даними, а також у фрагментарності профілактичних заходів. Така ситуація особливо загострюється в умовах війни, коли велика кількість дітей переміщена або втратила доступ до звичних освітніх та соціальних сервісів [35].

Ключовим елементом ефективної координації має стати створення єдиної міжвідомчої платформи, яка забезпечуватиме: синхронізацію політик на рівні міністерств та регіональних органів; обмін інформацією про кіберінциденти; моніторинг виконання стратегічних документів; включення ІТ-сектору до розробки та реалізації цифрових рішень захисту; стандартизацію реагування на інциденти, пов'язані з цифровими загрозами.

Значну роль у цьому процесі має відігравати Національний центр кібербезпеки при РНБО України, який повинен координувати діяльність усіх суб'єктів у сфері кіберзахисту, включаючи дитячу безпеку як пріоритетний напрям [93]. Також необхідним є створення національного хабу взаємодії з

громадянським суспільством, що дозволить посилити практичний вплив недержавних ініціатив на формування політик та реакцію на нові типи загроз.

Варто зазначити, що низка європейських країн – зокрема Естонія, Німеччина, Польща – вже впровадили інтегровані моделі міжвідомчої взаємодії, де участь батьків, освітян, кіберполіції, провайдерів інтернету та ІТ-компаній формалізована через протоколи співпраці, а не є виключно волонтерською практикою [138], [134].

Таким чином, посилення міжвідомчої координації в Україні є необхідною умовою для ефективного захисту дітей у кіберпросторі. Це потребує не тільки реформування існуючих інституційних механізмів, але й інституалізації співпраці, чіткої нормативної бази для обміну інформацією, формування спільної системи моніторингу, а також державного фінансування спільних ініціатив.

У сучасних умовах швидкої цифровізації всіх сфер суспільного життя, технологічна складова набула ключового значення для забезпечення безпеки дітей у кіберпросторі. Від ефективності цифрових інструментів, безпечної інфраструктури та інноваційних рішень безпосередньо залежить спроможність держави, освітніх закладів та сім'ї вчасно і якісно реагувати на кіберзагрози, попереджати їх та мінімізувати наслідки. У зв'язку з цим розвиток безпечної цифрової інфраструктури має бути інтегрованим стратегічним пріоритетом державної політики захисту дітей.

Станом на сьогодні в Україні вже запроваджено низку технологічних рішень, зокрема: системи батьківського контролю на рівні мобільних операторів та провайдерів інтернету; інтеграція фільтрів контенту у шкільні локальні мережі; сервіси повідомлень про шкідливий контент або протиправні дії (наприклад, бот кіберполіції «Stop Sexting» або платформи типу StopBullying); національні освітні платформи, що пропонують курси з цифрової грамотності та кібергігієни, наприклад, «Дія.Цифрова освіта» [80].

Однак ці рішення є фрагментованими, переважно орієнтованими на дорослу аудиторію або не мають повноцінного функціоналу інтеграції між собою. Більшість шкіл, особливо в сільській місцевості, не мають технічної

спроможності впроваджувати сучасні цифрові системи захисту, що ускладнює реалізацію політики безпеки в освітньому процесі [34], [33].

Значну роль у зміцненні технологічного фронту повинна відігравати державна цифрова інфраструктура. Сюди входять: захищені канали зв'язку та зберігання даних у навчальних закладах; впровадження єдиної освітньої хмарної платформи, яка б унеможлиблювала витоки персональних даних; системи виявлення ризикованої поведінки дітей у мережі на основі штучного інтелекту; механізми авторизації та автентифікації, що забезпечують перевірку віку та обмеження доступу до потенційно шкідливого контенту.

Крім того, важливим аспектом є цифрова доступність: у контексті війни багато дітей вимушено перемістилися або втратили зв'язок з базовими освітніми сервісами. Це зумовлює необхідність розгортання резервних освітніх платформ, забезпечення доступу до Інтернету через супутникові або мобільні рішення (наприклад, використання Starlink у віддалених громадах), а також розвиток офлайн-додатків, що дозволяють навчатись основам кібергігієни навіть без стабільного підключення.

Іншою важливою технологічною складовою є державно-приватне партнерство у сфері кіберзахисту. Найуспішніші кейси у світі (наприклад, співпраця уряду Великобританії з Google, TikTok та Meta у межах ініціативи «Project Protect») доводять ефективність спільного реагування на виклики цифрової безпеки. В Україні така взаємодія лише формується, хоча окремі ініціативи, як-от співпраця кіберполіції з соціальними мережами для видалення шкідливого контенту, вже дають позитивні результати [11].

У рамках Національної стратегії захисту дітей у кіберпросторі[80] закладено перспективу розробки: Національної платформи моніторингу загроз для дітей у мережі; інструментів попереднього аналізу контенту; технологій верифікації особи та віку користувачів; інноваційних освітніх ігор та симуляторів, які навчають безпеці у форматі, доступному для дітей.

Для реалізації цих завдань потрібне не лише фінансування, а й професійне кадрове забезпечення: фахівці з кібербезпеки, програмісти, аналітики, педагоги цифрової грамотності. Також слід забезпечити відкрите

ліцензування та адаптацію програмного забезпечення, яке використовуватиметься у школах, соціальних службах, психологічній підтримці.

Таким чином, інноваційна цифрова інфраструктура є основою стійкої системи захисту дітей у кіберпросторі, і без належного рівня технологічного забезпечення будь-яка стратегія залишатиметься лише декларативною. Виклики часу, зокрема повномасштабна війна та гібридні загрози, зобов'язують державу до швидкої модернізації технологічного середовища з урахуванням інтересів найвразливіших – дітей.

У світлі зростання цифрових загроз, що не знають державних кордонів, міжнародна інтеграція та дотримання міжнародних стандартів є не просто важливим аспектом державної політики, а її системоутворювальною основою. Глобалізований характер інтернету потребує узгоджених дій держав щодо захисту найуразливіших категорій користувачів – передусім дітей, для яких цифровий простір є не лише джерелом знань і соціалізації, а й зоною підвищених ризиків.

Відповідно до взятих на себе міжнародних зобов'язань, Україна є стороною низки ключових документів, які регулюють питання прав дитини та захисту її у кіберпросторі. Зокрема, це: Конвенція про права дитини (1989), яка визначає право дитини на захист від усіх форм насильства, включно з психологічним та інформаційним тиском [47]; Європейська конвенція про здійснення прав дітей (1996) [97]; Конвенція про кіберзлочинність Ради Європи (Будапештська конвенція, 2001) – перший міжнародний договір, що встановлює стандарти боротьби з кіберзлочинами, включаючи злочини проти неповнолітніх [48].

Особливе значення має дотримання принципів Загальної декларації прав людини [41] та Міжнародного пакту про громадянські і політичні права [78], які, хоча й не мають специфічно дитячої орієнтації, містять важливі положення щодо захисту від свавільного втручання в особисте життя, право на доступ до інформації, а також свободу вираження поглядів – що є критично важливими у цифрову епоху.

Україна також бере участь у ініціативах Європейського Союзу, зокрема у межах платформи EU Kids Online та співпраці з ENISA (Європейське агентство з кібербезпеки). Національна стратегія захисту дітей у кіберпросторі(2021–2026) була розроблена з урахуванням Глобального індексу цифрової грамотності дітей (DQ Global Standards), який є результатом міжнародної консолідації знань і практик [80], [134].

Проте міжнародна інтеграція передбачає не лише формальне визнання документів, а й реальне впровадження стандартів через державну політику, нормативно-правові акти, інституційну координацію, підготовку кадрів та інноваційні рішення. На цьому етапі Україна стикається з низкою викликів: недостатня адаптація європейських стандартів до національного законодавства; повільне імплементаційне наповнення міжнародних зобов'язань, особливо у частині протидії онлайн-експлуатації дітей; відсутність систематичного моніторингу впровадження стандартів у практику діяльності закладів освіти, органів поліції, ювенальних структур; фрагментарність співпраці з міжнародними ІТ-компаніями, що стримує швидке блокування шкідливого контенту чи ідентифікацію кіберзлочинців.

З огляду на це, стратегічним завданням має стати посилення інтеграції з міжнародними ініціативами, такими як: INHOPE (міжнародна мережа гарячих ліній для боротьби з матеріалами сексуального насильства над дітьми); WeProtect Global Alliance, що розробляє глобальні стратегії запобігання сексуальному насильству в інтернеті; OECD Recommendation on Children in the Digital Environment (2021) – рекомендації щодо дотримання цифрових прав дітей у політиці держав.

Також Україна потребує активної участі в розробці нових міжнародних підходів до регулювання соціальних платформ, шифрування повідомлень, використання штучного інтелекту для захисту дітей – з одночасним забезпеченням правової визначеності й запобіганням надмірному втручання в приватне життя.

У контексті війни питання міжнародної інтеграції набуло ще більшої ваги, оскільки національні ресурси вичерпуються, а міжнародна підтримка

(інституційна, технічна, правова) є ключем до збереження цифрового суверенітету держави та безпеки її найвразливіших громадян – дітей.

Отже, дотримання міжнародних стандартів у сфері цифрової безпеки дітей не є опцією, а зобов'язанням, від якого залежить не лише відповідність правової системи сучасним вимогам, але й довіра до держави як гаранта гуманітарної безпеки у цифровому столітті.

У контексті зростання кіберзагроз для дітей та комплексного характеру цифрового середовища, яке постійно змінюється, критичною умовою результативної реалізації державної політики є ефективна система моніторингу, аналітики та наукового супроводження. Вона повинна забезпечувати постійне спостереження за ризиками, виявлення новітніх форм цифрової небезпеки, прогнозування їх впливу на дітей та обґрунтування управлінських рішень на основі об'єктивних даних.

На жаль, в Україні наразі відсутня єдина системна інфраструктура моніторингу кіберзагроз для дітей, яка б функціонувала на національному рівні. Наявні ініціативи здебільшого мають фрагментарний характер – це або окремі звіти неурядових організацій, або статистика МВС щодо кіберзлочинів. Водночас, державна система аналітичного супроводження ризиків у сфері цифрової безпеки дітей лише починає формуватися, що істотно обмежує спроможність держави адекватно реагувати на виклики сучасності [34], [35], [37].

Проведення регулярного, стандартизованого моніторингу поведінкових моделей дітей у кіберпросторі, доступу до небажаного контенту, випадків кібербулінгу чи грумінгу дозволяє: визначити географію ризиків та їхню інтенсивність; виявити тренди в змінах кіберзагроз; обґрунтувати пріоритети політики у сфері цифрового захисту; формувати науково обґрунтовані методичні рекомендації для шкіл, батьків, державних структур.

Інтеграція в управлінський процес інструментів цифрової аналітики, зокрема з використанням великих даних (Big Data), штучного інтелекту (AI) та алгоритмів машинного навчання, відкриває нові горизонти для виявлення

аномалій у поведінці дітей, онлайн-маніпуляцій, шкідливих патернів інформаційного споживання тощо [66], [148].

Крім цього, важливу роль відіграє наукове супроводження політики у сфері кіберзахисту. Воно забезпечує глибоке осмислення причин, наслідків та механізмів впливу цифрового середовища на психоемоційний стан, соціальну поведінку, правову свідомість дітей. Наукова спільнота, у партнерстві з державою та міжнародними структурами, повинна формувати індикатори оцінки ефективності політики, розробляти прогностичні моделі, здійснювати експертний аудит правових інструментів захисту [38], [7], [37].

Суттєвим викликом залишається відсутність постійно оновлюваної національної бази даних щодо інцидентів, що стосуються цифрової безпеки дітей. Наявна статистика носить описовий характер, не дозволяє виявити причинно-наслідкові зв'язки, а також недостатньо деталізована за типами загроз (булінг, грумінг, секстинг, фішинг, порнографія тощо). Це ускладнює розробку диференційованої державної політики для різних вікових, соціальних та регіональних груп.

Крім того, відсутня сталість у фінансуванні наукових досліджень у цій сфері, що веде до фрагментарності знань та відсутності довгострокових стратегій. Такий стан справ є несумісним з масштабами та динамікою цифрових викликів, які щоденно постають перед українськими дітьми, особливо в умовах війни.

З огляду на викладене, державна політика у сфері захисту дітей у кіберпросторі повинна передбачати: створення Національного центру моніторингу цифрової безпеки дітей; забезпечення міжвідомчої бази даних щодо випадків кіберінцидентів; запровадження цифрових дашбордів для онлайн-відслідковування ситуації у школах, громадах; налагодження системного фінансування досліджень, зокрема в рамках Державного фонду досліджень; залучення провайдерів, платформ, ІТ-компаній до спільного збору, аналізу та обміну даними.

Таким чином, моніторинг, аналітика та наукове супроводження повинні розглядатися не як допоміжні, а як базові елементи ефективної моделі захисту

дітей у кіберпросторі— ті, що дозволяють діяти на випередження, знижувати ризики та забезпечувати стійкість державної політики в умовах турбулентності.

Одним із критично важливих стратегічних напрямів державної політики у сфері забезпечення цифрової безпеки дітей є юридичне та нормативне вдосконалення. У сучасних умовах, коли цифрове середовище стрімко трансформується, а кіберзагрози набувають нових, гібридних форм, правова система України має реагувати на виклики не лише постфактум, а й на випередження — шляхом формування гнучкої, актуальної, комплексної та адаптивної нормативно-правової бази [36], [37], [55].

Станом на сьогодні законодавче регулювання захисту дітей у кіберпросторі України здійснюється фрагментарно. В основі цієї регуляції лежить низка базових законодавчих актів, зокрема: Закон України «Про охорону дитинства» [95], Закон України «Про основні засади забезпечення кібербезпеки України» [93], Закон України «Про захист персональних даних» [91], Конституція України [49], Кримінальний та Цивільний кодекси України [109].

Однак жоден із цих документів не містить системної концепції захисту дітей від цифрових загроз. Зокрема, поняття «цифрова безпека дитини», «кібербулінг», «грумінг», «сексуальна експлуатація в мережі», «дитяча цифрова ідентичність» не мають чіткого правового визначення. Це ускладнює як судову практику, так і діяльність правоохоронних, освітніх та соціальних інституцій [12], [46], [107].

Крім того, чинна система адміністративної та кримінальної відповідальності за вчинення кіберзлочинів проти дітей часто не відповідає сучасним викликам. Наприклад, такі дії як сексуальне домагання в Інтернеті, секстинг, шантаж через мережу досі залишаються або не повністю врегульованими, або потребують актуалізації санкційного блоку. Не менш важливо й те, що провайдери контенту, хостинг-платформи та мобільні оператори не мають достатньої правової мотивації або зобов'язань щодо превентивного моніторингу контенту, який може загрожувати дитячій безпеці [43], [112].

Особливої актуальності набуває питання гармонізації українського законодавства з міжнародними стандартами, зокрема: Конвенцією ООН про права дитини, Європейською конвенцією з прав людини [47], Конвенцією про кіберзлочинність (Будапештська конвенція) [48], GDPR (General Data Protection Regulation) [145], міжнародними стандартами ITU, DQ Institute, UNICEF.

Ці документи передбачають не лише високі стандарти захисту персональних даних та приватності дитини, але й акцентують на інтересах дитини як пріоритеті в усьому життєвому циклі цифрових послуг.

На цьому тлі, пріоритетними завданнями юридичного вдосконалення є:

1. Розробка та прийняття окремого Закону України «Про захист дітей у кіберпросторі», який має закріпити поняття, принципи, інституційну модель, обов'язки всіх суб'єктів – від держави до приватного сектору.
2. Внесення змін до КК України щодо криміналізації нових видів цифрового насильства (кіберсталкінг, сексторшн, інтернет-грумінг).
3. Затвердження єдиних національних стандартів цифрової безпеки дітей у школах, в т.ч. через нормативи МОН.
4. Обов'язкове впровадження механізмів батьківського контролю, звітності платформ та захисту цифрової ідентичності дитини (анонімізація, згода на обробку персональних даних).
5. Розробка типових міжвідомчих алгоритмів реагування на кіберінциденти, що стосуються дітей.

Ключовою умовою ефективності такого юридичного реформування має стати міжвідомча координація, залучення експертної та громадської спільноти, активна участь міжнародних партнерів. Усі зміни повинні ґрунтуватися на підході «best interest of the child» (найкращі інтереси дитини) як визначальному принципі політики і права [84], [52].

Отже, юридичне та нормативне вдосконалення є необхідною базою для реалізації ефективної, превентивної та гуманістично орієнтованої політики у сфері цифрового захисту дітей. Воно повинно відповідати викликам цифрової трансформації, сприяти формуванню цифрово-захищеного середовища та бути

інструментом не лише покарання, а й профілактики, просвітництва та соціальної підтримки.

В умовах стрімкого розвитку цифрових технологій та еволюції загроз у кіберпросторі захист дітей вимагає не лише належного нормативно-правового та технологічного забезпечення, але й високого рівня професійної підготовки фахівців, які безпосередньо здійснюють реалізацію політики у цій сфері. Йдеться не лише про спеціалістів правоохоронних органів, а й про вчителів, соціальних працівників, психологів, суддів, медіаторів, працівників органів опіки, фахівців з інформаційної безпеки та державних службовців, які відповідають за діджитал-політику на національному та регіональному рівнях [34], [35], [37].

На сьогодні українська система підготовки та підвищення кваліфікації фахівців не повною мірою охоплює специфіку цифрового дитинства. Здебільшого питання кіберзагроз для дітей інтегруються у загальні курси інформаційної безпеки або залишаються поза увагою, особливо у секторах освіти та соціального захисту. Як наслідок, фахівці не завжди здатні ідентифікувати загрози, розпізнавати симптоматику цифрового насильства, належно реагувати на інциденти та комунікувати з дитиною вразливого стану.

Водночас міжнародна практика демонструє успішні моделі системного навчання персоналу: у Південній Кореї та Естонії діють національні освітні програми для вчителів і поліції щодо цифрової безпеки, а в Польщі інтегровані підходи до підготовки суддів і прокурорів з питань цифрових злочинів проти неповнолітніх [138], [134].

У цьому контексті для України стратегічно важливо забезпечити:

1. Розробку спеціалізованих навчальних програм підвищення кваліфікації за напрямом "Цифрова безпека дітей" для всіх професійних груп, які мають справу з дітьми в офлайн- або онлайн-середовищі.

2. Інтеграцію тематики цифрових ризиків до системи підготовки педагогів – як у закладах вищої педагогічної освіти, так і в межах післядипломної освіти.

3. Підготовку мультидисциплінарних команд швидкого реагування на кіберінциденти за участі юристів, айтишників, психологів та соціальних працівників.

4. Співпрацю з міжнародними партнерами для запозичення найкращих практик навчання та тренінгових програм – зокрема від ЮНІСЕФ, ITU, Europol, INTERPOL та ECPAT [134].

5. Запровадження системи сертифікації фахівців, що мають справу із захистом дітей у кіберпросторі– для гарантії компетентності та етичної відповідальності.

Особливу увагу слід приділити інституціям первинної допомоги – школам, ЦСССДМ, поліції. Для педагогів важливо вміти не лише користуватись технічними засобами захисту, але й розпізнавати ознаки кібербулінгу, деструктивної онлайн-поведінки або вербування. Поліцейські ж повинні володіти як технічними навичками розслідування цифрових злочинів, так і психологічною чутливістю до дитячих травм [79], [107].

Таким чином, інвестування у людський капітал – підготовку та розвиток кадрів – є одним із найефективніших інструментів попередження цифрових ризиків для дітей. Без підготовлених фахівців – жодна стратегія, жодна технологія чи закон не будуть ефективними.

Сучасна парадигма державної політики у сфері цифрової безпеки дітей дедалі більше визнає важливість залучення самих дітей та молоді як суб'єктів – не лише як отримувачів захисту, але і як активних учасників формування безпечного цифрового середовища. Такий підхід базується на принципах Конвенції ООН про права дитини (1989) [47], яка передбачає право кожної дитини на участь у прийнятті рішень, що стосуються її життя, з урахуванням віку та зрілості.

Участь дітей у виробленні політик, програм, кампаній і освітніх заходів є ключовою складовою інклюзивного та стійкого підходу до цифрової безпеки, оскільки діти самі є безпосередніми користувачами цифрових платформ і найкраще розуміють, які саме ризики є для них актуальними. Особливо цінною

є перспектива підлітків, які мають високий рівень цифрової грамотності, критичного мислення, а також здатність до креативних рішень.

У розвинених країнах така участь уже давно є практикою. Наприклад, в Естонії існують молодіжні цифрові ради, які беруть участь у формуванні стандартів безпеки на національному рівні. У Південній Кореї молоді користувачі консультують урядові органи щодо ризиків у соцмережах та тестують нові освітні програми [138], [134]. Польща реалізує принцип «peer-to-peer education» – навчання молоддю однолітків на теми цифрової етики, кібербулінгу, захисту персональних даних.

В Україні такі практики лише починають впроваджуватись. Прикладом є ініціативи Національної дитячої ради, окремі шкільні проєкти, підтримані ЮНІСЕФ, участь молоді в обговоренні Національної стратегії захисту дітей в цифровому середовищі на 2021–2026 роки [80]. Проте системність у цьому процесі поки що відсутня.

Для посилення участі дітей доцільно впровадити такі стратегічні кроки:

1. Створення молодіжних рад або консультативних органів при державних структурах, які відповідають за цифрову трансформацію та безпеку.
2. Інституалізація механізмів зворотного зв'язку у шкільному середовищі щодо роботи з цифровими інструментами, системами моніторингу, освітніми платформами.
3. Підтримка ініціатив «діти для дітей»: проєкти, хакатони, блоги, подкасти, соціальні кампанії, які ініціюються самими дітьми і спрямовані на формування безпечного онлайн-середовища.
4. Створення платформ електронної участі для молоді у прийнятті цифрових рішень: опитування, консультації, громадські обговорення з адаптованими інтерфейсами.
5. Інтеграція принципів цифрового громадянства у шкільну програму з акцентом на активну участь у цифровому суспільстві.

Залучення дітей не лише підвищує ефективність державної політики, а й сприяє розвитку громадянської свідомості, самоповаги, критичного мислення і відповідальності за дії в цифровому середовищі. Це дозволяє не лише захистити

дитину, а й сформувати покоління відповідальних цифрових громадян, здатних у майбутньому самостійно відстоювати свої права у цифровому просторі.

Таким чином, інституційне та культурне визнання дітей як партнерів у забезпеченні цифрової безпеки є не лише етичним, але й стратегічно ефективним кроком, що відповідає міжнародним стандартам прав дитини та викликам сучасного цифрового світу.

Аналіз стратегічних пріоритетів державної політики захисту дітей у кіберпросторі засвідчує, що в умовах стрімкої цифровізації українського суспільства та ускладнення загроз кіберпростору особливої актуальності набуває формування комплексного, багаторівневого та скоординованого підходу до убезпечення найуразливіших категорій – дітей та молоді. Визначені у межах Національної стратегії захисту дітей у кіберпросторі (2021–2026) вектори дій охоплюють такі пріоритетні напрями, як цифрова грамотність, інституційна взаємодія, технологічна модернізація, міжнародне партнерство, правове вдосконалення та залучення самих дітей до розробки безпечного цифрового простору [80], [36], [35].

Особливо важливим стратегічним вектором є формування цифрової грамотності, що має спиратися на міжвідомчі ініціативи, шкільну освіту та неформальне навчання, з урахуванням вікових, соціальних та регіональних особливостей. Ефективна профілактика загроз потребує розвитку критичного мислення, медіаосвіти, навичок цифрової гігієни вже з молодшого шкільного віку [32], [10].

Інституційна координація залишається ключовим чинником результативності державної політики: лише за умови тісної взаємодії між освітніми, соціальними, правоохоронними органами та інституціями з кібербезпеки можливе створення дієвого захисного середовища для дитини [33], [34]. Особливе значення мають технологічні рішення – від фільтраційного програмного забезпечення до систем раннього попередження та національних платформ звітності про інциденти [51], [30].

Водночас стратегічний контекст вимагає і міжнародної інтеграції, включаючи гармонізацію законодавства з Конвенцією про кіберзлочинність

[48], впровадження принципів GDPR щодо обробки персональних даних дітей [145], а також адаптацію найкращих практик країн ЄС, Азії та НАТО у сфері цифрового захисту.

Поряд з цим, політика повинна передбачати наукове супроводження, моніторинг, аналітику та регулярне оновлення стратегічних документів з урахуванням динаміки ризиків та технологічних змін. Юридичне та нормативне середовище має бути адаптивним і відкритим до перегляду в частині захисту прав дитини у кіберпросторі[46], [36].

Окремим досягненням має стати залучення дітей та молоді до формування політик цифрової безпеки, що відповідає принципам демократичного врядування, підходам ЮНІСЕФ і практикам розвинених країн [138], [134]. Це дозволяє не лише ефективніше реагувати на нові загрози, а й формувати відповідальне цифрове покоління.

Таким чином, державна політика у сфері цифрової безпеки дітей повинна спиратися на інтегрований, інноваційний та права-орієнтований підхід. Її стратегічні пріоритети мають постійно переглядатися, поглиблюватися й адаптуватися до нових реалій – зокрема, до воєнного часу, гібридних загроз, зміни цифрових звичок та поведінкових моделей дітей. Без належного стратегічного управління і постійної міжвідомчої координації держава ризикує не тільки не захистити дитину, а й залишити її сам на сам із цифровими загрозами майбутнього.

3.2. Запровадження ефективних механізмів попередження та реагування на кіберзагрози

У сучасному кіберпросторі діти виступають не лише активними користувачами інформаційних технологій, а й однією з найбільш вразливих категорій до кіберзагроз. Масове використання соціальних мереж, онлайн-ігор, освітніх платформ і месенджерів підвищує ризики контакту неповнолітніх із шкідливим контентом, маніпуляціями, кібербулінгом, грумінгом та іншими формами цифрового насильства. На тлі гібридної агресії проти України та

посилення інформаційної війни в кіберпросторі, рівень загроз значно підвищився, що потребує впровадження чітко скоординованих механізмів попередження, реагування й відновлення.

Попри наявність нормативно-правової бази та інституційних структур, в Україні досі відсутня ефективна, проактивна та інтегрована модель реагування на інциденти, що стосуються цифрової безпеки дітей. Практика показує, що більшість випадків залишаються поза офіційною статистикою, а інформування, технічне реагування та підтримка жертв не відповідають сучасним стандартам [10], [11], [30], [35]. Потреба в оновленні механізмів управління в цій сфері є надзвичайно актуальною, оскільки без системного підходу до профілактики, виявлення та реагування будь-яка стратегія залишатиметься декларативною.

Даний підрозділ спрямований на комплексний розгляд елементів ефективного механізму протидії кіберзагрозам у контексті захисту дітей: інституційної структури, технологічних рішень, стандартів реагування, кризового менеджменту та постінцидентного супроводу. Особливу увагу приділено адаптації найкращих міжнародних практик до українського контексту, з урахуванням воєнних викликів та ресурсних обмежень.

Ефективне попередження кіберзагроз для дітей у кіберпросторі потребує розбудови комплексної системи раннього попередження, яка має на меті не лише виявлення потенційних інцидентів, а й своєчасне інформування відповідних інституцій, користувачів, батьків, а також самих дітей про можливі ризики та механізми їх нейтралізації. В основі цієї системи повинна лежати мультикомпонентна структура, яка поєднує інструменти технологічного моніторингу, алгоритмічного аналізу, освітньої профілактики та міжвідомчої координації.

Важливою передумовою створення такої системи є функціонування національного кібермоніторингу, орієнтованого не лише на критичну інфраструктуру, а й на соціально вразливі групи населення, зокрема дітей. У цьому контексті доцільним є розроблення спеціалізованих модулів в рамках систем CERT/CSIRT, адаптованих до моніторингу дитячого цифрового простору [30], [34], [55]. Подібні рішення застосовуються у практиці деяких країн

Європейського Союзу, зокрема в Естонії та Нідерландах, де інтегровані платформи дозволяють відстежувати прояви онлайн-грумінгу, сексуальної експлуатації та кібербулінгу у відкритих мережах.

Окремий акцент має бути зроблений на впровадженні механізмів «поведінкової аналітики» з використанням штучного інтелекту (AI) та машинного навчання. Такі алгоритми здатні фіксувати нетипові дії користувачів (зокрема неповнолітніх), а також ідентифікувати патерни поведінки, що потенційно свідчать про втягнення дитини у ризиковану онлайн-активність [66], [28]. Використання цих технологій потребує дотримання суворих вимог щодо захисту персональних даних, тому актуальним є паралельне впровадження механізмів правового контролю відповідно до Закону України «Про захист персональних даних» [91] та Регламенту GDPR [145].

Не менш значущим компонентом системи раннього попередження є створення інтерактивної бази інцидентів, куди батьки, освітяни, самі діти та правоохоронні органи можуть оперативно передавати інформацію про потенційно небезпечні ситуації. У Польщі, наприклад, функціонує державна система *Dyżurnet.pl*, яка дозволяє громадянам анонімно повідомляти про підозрілий онлайн-контент, що порушує права дитини. Подібна модель можлива й в Україні, з урахуванням практики впровадження державних сервісів е-інформування [57], [45].

Важливим також є розбудова аналітичного сегменту системи раннього попередження, який має здійснювати прогнозування можливих сплесків кіберзагроз на основі даних з освітніх, соціальних, правоохоронних платформ. У цьому контексті корисним є залучення університетських дослідницьких центрів, що спеціалізуються на питаннях кібербезпеки, соціології та дитячої психології. Наукове супроводження таких процесів дозволяє забезпечити системність і валідність прийнятих управлінських рішень [38], [66].

Не можна залишити поза увагою й освітній компонент, який є профілактичною складовою системи раннього попередження. Масові інформаційні кампанії, інтерактивні уроки цифрової безпеки, поширення інформаційних брошур та гейміфікованих онлайн-платформ сприяють не лише

підвищенню цифрової грамотності, а й створенню умов, за яких дитина сама зможе розпізнати загрозу та повідомити про неї. У Національній стратегії захисту дітей у кіберпросторі(2021–2026) прямо вказується на необхідність впровадження «систем раннього реагування, які об'єднують технологічну, освітню та соціальну складові» [80].

Слід також зазначити, що побудова дієвої системи раннього попередження неможлива без сталого фінансування, нормативного врегулювання та міжвідомчої взаємодії. Особливе значення має централізована координація через відповідні урядові структури, зокрема МОН, МВС, Службу у справах дітей, Міністерство цифрової трансформації тощо [34], [37]. Успішна реалізація цієї політики значною мірою залежатиме від запровадження пілотних проєктів на регіональному рівні та активної участі громадських організацій.

Таким чином, система раннього попередження кіберзагроз для дітей повинна поєднувати технологічні, правові, освітні та управлінські компоненти в єдину адаптивну модель. Її ефективність залежить від швидкості виявлення, достовірності сигналів про загрози та наявності ефективних каналів комунікації між усіма суб'єктами системи безпеки в цифровому середовищі.

Своєчасне виявлення кіберінцидентів у сфері дитячої безпеки є лише початковою ланкою в загальному ланцюгу протидії цифровим загрозам. Не менш важливою складовою державної політики є ефективність механізмів повідомлення про інциденти та реагування на них. В умовах сучасного цифрового середовища, коли обсяг загроз постійно зростає, а форми зловживань еволюціонують, традиційні підходи до фіксації й реагування потребують істотної модернізації.

Одним із найважливіших викликів є створення доступної, швидкої та безпечної процедури повідомлення про кіберінциденти, що пов'язані з дітьми. На сьогодні в Україні діють кілька паралельних механізмів, серед яких найбільш поширеними є: платформи кіберполіції (наприклад, форма онлайн-звернення на офіційному сайті [11]); гарячі лінії національних омбудсменів та дитячих служб; анонімні платформи громадських організацій, зокрема ті, що співпрацюють з міжнародними ініціативами типу INHOPE.

Проте, за даними досліджень, більшість батьків і дітей не знають, куди і як повідомити про загрозу, або ж не довіряють органам влади через ризики стигматизації [10], [32], [83]. Це свідчить про потребу у створенні єдиного національного хабу кібербезпеки дітей – інтегрованої цифрової платформи з багаторівневим доступом для батьків, дітей, освітян, правоохоронців.

У цьому контексті варто вивчити досвід Польщі, де діє система Dużurnet.pl, а також Естонії, де функціонує інтегрована кіберплатформа для шкіл і батьків, яка дозволяє не лише повідомляти про інциденти, а й одразу отримувати правову й психологічну допомогу [138].

Після фіксації інциденту необхідним є швидке реагування, яке передбачає як технічні дії (блокування акаунтів, контенту, виявлення IP-джерела тощо), так і соціально-психологічні заходи – інформування батьків, надання консультацій дитині, залучення фахівців.

На практиці в Україні часто спостерігається фрагментація: реагування покладається або на кіберполіцію, або на адміністрацію шкіл, або зовсім перекладається на батьків. Через відсутність чіткого алгоритму міжвідомчої взаємодії процес втрачає оперативність і ефективність. Згідно з висновками Димитрієвої О.І., в Україні фактично відсутній закріплений механізм координації реагування між МВС, МОН, Службою у справах дітей та закладами освіти [34], [35], [37].

Для розв'язання цієї проблеми доцільним є запровадження моделі «Case management» – персоніфікованого супроводу випадків цифрового насильства чи кібербулінгу, що включає: фіксацію випадку; аналіз загроз; визначення відповідального координатора; зв'язок із психологами, соціальними службами, поліцією; контроль за результатами розв'язання ситуації.

В умовах воєнного часу, коли діти перебувають в інформаційно вразливому становищі (через втрату домівки, переміщення, смерть близьких), оперативність реагування стає питанням національної гуманітарної безпеки [7], [27], [80].

Окремо слід підкреслити значення психологічної підтримки постраждалих дітей. За даними Національної соціальної сервісної служби,

понад 40% звернень, пов'язаних із кібербулінгом, мають тривалі психоемоційні наслідки для дитини. Проте системна мережа психологів, які мають цифрову компетентність, на національному рівні не розбудована [33], [36]. Рекомендовано впровадити програми перепідготовки для шкільних психологів і соціальних педагогів на базі МОН та профільних інститутів післядипломної освіти.

Ефективні механізми повідомлення та реагування на кіберінциденти щодо дітей повинні базуватись на інтегрованості, швидкодії та конфіденційності. Наявна система в Україні фрагментована та недостатньо орієнтована на інтереси дитини. Впровадження національної платформи реагування, розробка єдиного протоколу дій, міжвідомча координація та розбудова психологічної допомоги є ключовими завданнями на найближчу перспективу. Без цього подолання цифрових загроз для дітей залишатиметься точковим, неефективним і реактивним.

У контексті забезпечення комплексного захисту дітей у кіберпросторі особливої уваги заслуговує роль громадянського суспільства та приватного ІТ-сектору. Їхня участь є не лише додатковим ресурсом для держави, але й стратегічним партнерством, що дозволяє швидко реагувати на динамічні цифрові виклики, формувати культуру відповідального користування інтернетом, а також впроваджувати інноваційні технологічні рішення.

Громадські організації, благодійні фонди, батьківські об'єднання, профільні професійні асоціації відіграють ключову роль у: просвітницькій діяльності: розробка інформаційних кампаній, освітніх програм, тренінгів для дітей, батьків і вчителів; адвокації змін у законодавстві та політиках державного рівня; моніторингу порушень прав дитини в цифровому просторі; психологічній та правовій допомозі постраждалим від кібербулінгу, онлайн-насильства, грумінгу тощо.

Яскравим прикладом є діяльність української ініціативи Stop Sexting, яка спільно з Міністерством цифрової трансформації України та ЮНІСЕФ реалізує програми для підлітків та освітян. Інші активні суб'єкти – ГО «Ла Страда-Україна», «Батьки за вакцинацію» (у контексті боротьби з дезінформацією)

тощо. Їхня сила полягає в гнучкості, мобільності та довірі аудиторії, чого часто бракує державним інституціям [33], [34], [35].

Проте участь громадського сектору наразі має епізодичний характер і залежить від грантового фінансування, що робить її нестабільною та непередбачуваною. Відсутність системної співпраці з МОН, Держспецзв'язку, Службою у справах дітей обмежує вплив громадянського суспільства на формування політики.

Сучасний цифровий світ керується не лише державними рішеннями, а й алгоритмами, розробленими приватними ІТ-компаніями. Тому зобов'язання технологічних компаній щодо захисту дітей стає ключовим елементом цифрової політики. У країнах ЄС вже діють зобов'язання, відповідно до яких великі платформи повинні: автоматично блокувати незаконний контент (CSAM – Child Sexual Abuse Material); модерувати вміст із використанням штучного інтелекту; впроваджувати батьківський контроль; забезпечувати верифікацію віку; співпрацювати з правоохоронцями в межах юридичних процедур.

В Україні ж законодавчі зобов'язання для платформ та провайдерів зв'язку мінімальні. Хоча деякі компанії (наприклад, «Київстар» або «Лайфселл») ініціюють освітні кампанії або блокують шкідливі ресурси на основі звернень, ця діяльність не є зобов'язанням, а лише соціальною відповідальністю бізнесу. З іншого боку, деякі українські ІТ-компанії активно долучаються до створення продуктів захисту – фільтри контенту, системи батьківського контролю, боти для виявлення ризикової поведінки дітей у соцмережах.

Для ефективного партнерства з ІТ-сектором необхідно: Закріпити юридичну відповідальність за сприяння поширенню шкідливого контенту, що становить небезпеку для дітей [91], [93]; Створити платформи координації між ІТ-бізнесом і державними органами, наприклад, у форматі публічно-приватного партнерства (як у моделі Німеччини чи Південної Кореї [114], [123]); Запровадити стимулюючі інструменти, включно з податковими преференціями або державними грантами на розробку технологій безпеки; Залучати українські

стартапи до міжнародних ініціатив із кібербезпеки, зокрема проєктів в рамках НАТО CCDCOE чи ENISA.

Успішна реалізація політики захисту дітей у кіберпросторі потребує реальної тристоронньої взаємодії – держава, громадянське суспільство та бізнес. Громадські організації забезпечують близькість до потреб громадян, ІТ-сектор – технологічні рішення, а держава – нормативну основу та гарантії. Без узгодженої співпраці цих секторів політика залишатиметься декларативною. Тому стратегічно важливо створити національну платформу цифрового партнерства, що акумулює ресурси, компетенції та інструменти для спільної дії в інтересах найвразливішої групи – дітей.

Формування та розвиток цифрової культури безпеки є одним з основоположних елементів стратегічної державної політики у сфері захисту дітей у кіберпросторі. У глобалізованому інформаційному суспільстві безпека вже не зводиться виключно до технічного захисту, а охоплює цілісний підхід до культури взаємодії з цифровим середовищем. У цьому контексті поняття «цифрова культура безпеки» розуміється як сукупність цінностей, знань, навичок, моделей поведінки та соціальних практик, що формують усвідомлене, відповідальне та безпечне користування цифровими технологіями всіма учасниками суспільства, зокрема дітьми та молоддю [15], [36].

Національна цифрова культура безпеки має багатовимірну структуру, що включає:

1. Інформаційну грамотність – здатність орієнтуватися в інформаційному потоці, перевіряти джерела, виявляти дезінформацію;
2. Кібергігієну – щоденні практики, спрямовані на зниження ризиків (використання складних паролів, оновлення ПЗ, уникавання підозрілих посилань);
3. Цифрову етику – дотримання норм поведінки у віртуальному середовищі, зокрема повага до приватності, недопущення кібербулінгу;
4. Безпекові навички – знання алгоритмів дій у разі кіберзагроз, вміння розпізнавати ризикову поведінку, користування інструментами захисту;

5. Цифрові права – усвідомлення прав дітей як користувачів, у тому числі права на конфіденційність, захист персональних даних, свободу вираження тощо [91], [112].

Ці компоненти мають бути інтегрованими в усі рівні соціалізації – від родини до шкільної освіти, від ЗМІ до державної політики, від професійного середовища до інформаційних кампаній.

Аналіз сучасного стану цифрової культури безпеки в Україні свідчить про фрагментарність і недостатність системного підходу. Більшість громадян, включно з дітьми, не мають достатнього рівня обізнаності про кіберзагрози та способи їх уникнення. За даними дослідження U-Report/ЮНІСЕФ (2023), понад 60% підлітків віком 14–17 років хоча б раз стикались із агресією чи шкідливим контентом в інтернеті, але лише кожен п'ятий знає, куди звернутися по допомогу [11], [32].

Також варто зазначити, що цифрова культура є нерівномірною за регіонами та соціальними групами. Діти в умовах збройного конфлікту, ВПО, або ті, що проживають у сільській місцевості, мають значно обмежені доступи до цифрових знань і технологій, що посилює їхню вразливість у кіберсередовищі [9], [35].

Для формування національної цифрової культури безпеки державна політика має бути орієнтована на такі стратегічні вектори.

1. Інтеграція цифрової безпеки в освіту: Включення тем з кібербезпеки, медіаграмотності та цифрової етики до навчальних програм усіх рівнів освіти (від початкової до вищої); Підготовка вчителів та викладачів за спеціалізованими модулями; Проведення національних тижнів цифрової грамотності.

2. Національні кампанії підвищення обізнаності: Соціальні медіа-кампанії, що охоплюють питання небезпек онлайн-грумінгу, кібербулінгу, шкідливого контенту; Використання відеоблогів, анімацій, чат-ботів, мобільних додатків, орієнтованих на дітей та підлітків.

3. Залучення лідерів думок та інфлюенсерів: Участь молодіжних амбасадорів, публічних осіб, освітян, блогерів у просуванні ідей цифрової безпеки; Поширення позитивних моделей поведінки у кіберпросторі.

4. Формування цифрових компетентностей у батьків: Онлайн-курси та тренінги для дорослих; Практичні інструкції щодо контролю за цифровими звичками дітей (встановлення фільтрів, налаштування приватності, використання parental control).

5. Міжвідомча координація та стандартизація: Розробка національних стандартів цифрової культури безпеки на рівні освітньої політики, кібербезпеки, юстиції та охорони здоров'я [37], [57].

6. Інституційне закріплення: Запровадження цифрової безпеки як окремого напрямку в діяльності Національної ради з питань телебачення і радіомовлення, Мінцифри, МОН тощо; Створення індикаторів вимірювання рівня цифрової культури на державному рівні.

Розвиток національної цифрової культури безпеки є довгостроковим, міжсекторальним і багатоаспектним процесом, який вимагає об'єднання зусиль уряду, громадянського суспільства, освітянської спільноти, ІТ-сектору та самих дітей. Лише через створення стійкого культурного фундаменту вдасться сформувати покоління свідомих, критично мислячих та відповідальних користувачів цифрового простору. Такий підхід не лише знижує рівень ризиків, а й перетворює безпеку на частину цифрової ідентичності сучасної дитини та суспільства загалом [15], [33], [38], [80].

У сучасних умовах стрімкого розвитку цифрових технологій та зростання ризиків, пов'язаних із онлайн-активністю неповнолітніх, необхідність формування ефективної системи національного моніторингу кіберзагроз для дітей набуває стратегічного значення. Така система має забезпечити своєчасне виявлення загроз, оцінку ризиків, формування сценаріїв реагування, а також розробку політик захисту на основі доказових даних. У національному вимірі йдеться не лише про технічне рішення, а про комплексну, міжвідомчу інституційну модель, яка має працювати на засадах системності, прозорості, оперативності та інклюзивності [38], [106].

На сьогодні Україна не має єдиної централізованої платформи, яка б дозволяла відстежувати, аналізувати та прогнозувати кіберзагрози для дітей у реальному часі. Існуючі ініціативи розпорошені між різними установами (освітні заклади, кіберполіція, соціальні служби), що створює фрагментарність, дублювання зусиль і унеможлиблює узгоджене прийняття рішень. У таких умовах вкрай актуальним є створення національного Центру моніторингу та аналітики цифрової безпеки дітей, інтегрованого із системами обліку інцидентів, освітніми платформами, аналітичними інструментами штучного інтелекту, а також із міжнародними базами даних [34], [57].

Концептуальні засади такої системи повинні ґрунтуватися на кількох ключових принципах. По-перше, регулярність та систематичність збору даних – ідеться як про автоматизований збір інформації з відкритих джерел (зокрема, соціальних мереж), так і про опрацювання звернень громадян, даних зі шкіл, лікарень, поліції. По-друге, інтегрованість – всі органи, дотичні до захисту прав дітей, мають бути об'єднані у єдиний інформаційний простір, що дозволить уникнути дублювання функцій та забезпечити повноту даних. По-третє, аналітичність – сучасна система повинна мати модулі прогнозування та оцінювання, що дозволить не лише реагувати на інциденти, а й виявляти їх на ранніх стадіях, за допомогою індикаторів ризику, моделей машинного навчання тощо. По-четверте, прозорість і захист персональних даних – важливою умовою функціонування системи є відповідність вимогам національного та міжнародного законодавства щодо конфіденційності, включно з GDPR та Законом України «Про захист персональних даних» [91], [112].

Серед функціональних блоків запропонованої системи мають бути: національний реєстр кіберінцидентів щодо дітей; інтегрована аналітична платформа оцінки ризиків; система раннього попередження на основі патернів та тригерів; модулі публічної звітності та освітньої комунікації. Така система дозволить формувати візуалізацію динаміки загроз, здійснювати порівняльний аналіз за регіонами, віковими категоріями, джерелами загроз, а також генерувати адаптовані рекомендації для батьків, педагогів, органів влади та громадських організацій.

Досвід низки країн (Південна Корея, Естонія, Польща) демонструє ефективність подібних підходів. Зокрема, у Південній Кореї діє державна платформа Smart Safety Net, що у реальному часі виявляє небезпечну поведінку в інтернеті та передає сигнали тривоги батькам. В Естонії діє система e-Governance із включеним модулем цифрової безпеки в школах, а Польща здійснює постійний моніторинг онлайн-загроз через національну платформу «Dziecko w Sieci» за участю поліції, освітян і громадських організацій [138].

Попри очевидну важливість створення такої системи в Україні, на шляху до її реалізації існує низка викликів. Передусім – відсутність чіткого розподілу повноважень між інституціями, які мають бути дотичні до цього процесу. Також проблемою є кадровий дефіцит, особливо у сфері кіберосвіти, аналітики даних, цифрового права. Крім того, існують законодавчі бар'єри щодо обробки персональних даних дітей, а також недостатній рівень цифрової культури в суспільстві, що ускладнює ефективну комунікацію між державою, школами, батьками та дітьми [30], [53].

Таким чином, створення системи національного моніторингу кіберзагроз для дітей є не лише технічним, а й комплексним управлінським викликом, що потребує політичної волі, фінансового забезпечення, нормативного удосконалення та широкого суспільного консенсусу. Лише за умови функціонування такої системи можливо перейти від реактивної моделі до превентивного, прогностного та орієнтованого на результат підходу у захисті прав дитини в цифровому середовищі.

Ефективність державної політики неможливо гарантувати без постійного аналізу її результативності, динаміки та впливу на цільову аудиторію. У сфері захисту дітей у кіберпросторі потреба є особливо актуальною, адже ідеться про швидкоплинний технологічний контекст, мінливу природу загроз, а також про особливу вразливість суб'єкта – дитини. Тому система оцінювання ефективності має бути не лише формальною, а орієнтованою на глибоку аналітику, порівняльні показники, зворотній зв'язок із дітьми, батьками, вчителями та експертним середовищем.

На сьогодні в Україні немає сталої методики, яка б дозволяла оцінити результативність заходів державної політики щодо захисту дітей в інтернеті. Наявні показники, як правило, носять фрагментарний характер і стосуються переважно кількісних параметрів – кількості звернень, скарг, інцидентів, проведених тренінгів тощо. Водночас важливими є якісні індикатори, як-от рівень обізнаності дітей, відчуття безпеки в цифровому просторі, довіра до державних інституцій, швидкість реагування на загрозу, профілактичний ефект реалізованих програм [38].

Науковці (зокрема, Димитрієва О. І.) запропонували низку методичних підходів до оцінки ефективності державної політики у сфері цифрової безпеки дітей, які базуються на принципах цільової відповідності, гнучкості та багаторівневої координації [38]. Основу такої системи можуть становити такі елементи:

1. Індикатори досягнення політичних цілей, які оцінюють ступінь реалізації ключових завдань Стратегії (наприклад, збільшення охоплення цифровою грамотністю дітей на певну кількість відсотків щорічно);
2. Оцінка впливу (impact assessment) – аналіз змін у середовищі або поведінці цільової групи після реалізації політики (наприклад, зниження рівня кібербулінгу або саморепортованих випадків насильства в мережі серед підлітків);
3. Механізм незалежного аудиту – залучення громадських організацій, академічних інститутів, правозахисників до зовнішнього оцінювання ефективності програм і кампаній [53];
4. Соціологічні опитування та інтерв'ювання дітей і підлітків щодо їх досвіду, обізнаності та сприйняття цифрової безпеки [138];
5. Регулярна аналітика та візуалізація даних – побудова інтерактивних дашбордів, публічних звітів на основі відкритих даних, що доступні для батьків, журналістів, науковців [82].

Окрему роль відіграє державний аудит політик – як формальний механізм контролю за ефективністю витрачання бюджетних коштів, реалізацією нормативних актів та досягненням стратегічних пріоритетів. Такий аудит має

бути інтегрований у систему управління результатами (Results-Based Management), рекомендовану ООН як еталонну модель для оцінки державної ефективності.

Серед основних викликів в імплементації ефективного моніторингу варто виділити: недостатню інституційну спроможність органів влади до збору та обробки релевантних даних; відсутність єдиної системи показників та їх стандартизації на національному рівні; невизначеність відповідальних органів, які здійснюють методичне забезпечення оцінювання; низький рівень обізнаності персоналу, зокрема в органах освіти, соціального захисту та правоохоронних структурах, щодо механізмів збору даних і оцінки [30], [106].

Для подолання зазначених бар'єрів необхідно, щоб розробка системи оцінки ефективності здійснювалася одночасно із формуванням цифрових політик, була інтегрованою з системами збору даних, а також враховувала міжнародні підходи (зокрема, UNICEF Child Protection Monitoring Framework).

Таким чином, механізм оцінювання ефективності політики захисту дітей у кіберпросторі має стати не додатком, а інтегрованим компонентом усієї архітектури цифрової безпеки, надаючи державі об'єктивні дані для ухвалення рішень, а суспільству – прозорість і підзвітність у цій стратегічній сфері (табл.3.3).

Ефективна протидія кіберзагрозам для дітей вимагає міжсекторальної синергії, що забезпечується через системну взаємодію ключових суб'єктів: закладів освіти, органів правопорядку, соціальних служб, батьківських об'єднань та громадянського суспільства. Кожен з учасників виконує унікальну функцію в механізмі захисту, але лише комплексна координація дій може забезпечити повноцінну превенцію, своєчасне виявлення ризиків та реагування на цифрові загрози.

Заклади освіти, відповідно до Стратегії захисту дітей у кіберпросторі[80], повинні не лише здійснювати навчання з основ цифрової безпеки, а й виступати першою лінією виявлення ознак ризикової поведінки дитини, зокрема в результаті кібербулінгу, сексторшену, грумінгу чи впливу деструктивних інтернет-спільнот. Для цього педагогічні працівники мають бути фахово

підготовленими до розпізнавання ознак віртуального насильства та знати алгоритми подальших дій у межах правового поля [33], [36].

Таблиця 3.3

Модель ефективності політики захисту дітей у кіберпросторі

Компонент моделі	Опис елементу	Індикатори оцінювання
1. Цільова результативність	Досягнення стратегічних завдань, закладених у національній політики та стратегії	- Рівень реалізації положень Нац. стратегії (2021–2026) [80]
		- Частка реалізованих цільових програм
2. Оцінка впливу (impact assessment)	Аналіз фактичних змін у поведінці, знаннях, безпеці дітей після впровадження заходів	- % зниження випадків кібербулінгу [79]
		- Рівень цифрової тривожності серед дітей до/після кампаній
3. Інституційна спроможність	Оцінка здатності органів влади, закладів освіти та політики здійснювати якісну реалізацію програм	- Кількість підготовлених фахівців
		- Наявність внутрішніх регламентів, інструкцій, локальних політик
4. Взаємодія та координація	Налагодженість міжвідомчої та міжсекторної взаємодії (уряд – громада – ІТ-сектор – НГО)	- Кількість спільних ініціатив/проектів [35]
		- Кількість укладених Меморандумів про співпрацю
5. Аналітична підтримка та зворотний зв'язок	Збір, аналіз, використання даних для прийняття рішень, моніторинг, відкритість результатів	- Частота публікацій звітів та даних
		- Охоплення онлайн-опитуваннями дітей/батьків/вчителів [38], [82]

Правоохоронні органи, в першу чергу кіберполіція, здійснюють оперативне реагування на повідомлення про кіберінциденти, проводять превентивні заходи, співпрацюють з ІТ-компаніями щодо блокування шкідливого контенту. У межах міжвідомчої взаємодії саме поліція забезпечує контакт з міжнародними структурами, такими як INTERPOL, Europol, INHOPE, для виявлення випадків транснаціональної кіберзлочинності, що зачіпає інтереси українських дітей [11], [30].

Соціальні служби відіграють ключову роль у супроводі постраждалих осіб, реабілітації та поверненні до безпечного соціального середовища. У випадках, коли виявляється загроза психоемоційному стану дитини, соціальні працівники зобов'язані вжити заходів із залучення психологів, медичних фахівців, іноді – ювенальної юстиції [7], [64].

Батьки ж, будучи першими вихователями дитини, несуть основну відповідальність за її цифрову безпеку в умовах домашнього середовища. За статистикою, понад 60% випадків шкідливого онлайн-контенту споживаються дітьми саме з домашніх пристроїв [32], [83]. Відтак, підвищення цифрової грамотності батьків, забезпечення регулярної комунікації з дитиною про правила онлайн-поведінки є необхідною складовою профілактики.

Успішна реалізація політики можлива лише за умов функціонування єдиного національного протоколу взаємодії, цифрової платформи для повідомлень, інтегрованих інформаційних систем та узгоджених механізмів міжінституційного реагування.

У сучасних умовах, коли швидкість поширення деструктивного контенту перевищує можливості людського реагування, особливої актуальності набуває використання інноваційних технологій – зокрема, інструментів штучного інтелекту, автоматизованого моніторингу та фільтрації загроз. Вони слугують не лише інструментом превенції, але й критичною ланкою у системі реагування на інциденти, пов'язані з дітьми.

AI-моніторинг (на основі NLP та комп'ютерного зору) дозволяє здійснювати контент-аналіз платформ, чатів, відео-стрімінгів з метою виявлення порушень, що становлять загрозу для неповнолітніх – від сексуалізованого контенту до самогубчих наративів чи радикалізації. Такі системи вже використовуються на платформах YouTube, Meta, TikTok, але потребують адаптації до національних особливостей та мови [128], [134].

Кіберпатруль – форма активного моніторингу цифрового простору з боку держави або уповноважених структур, що дозволяє виявляти порушення в реальному часі. В Україні така практика реалізується у співпраці кіберполіції з громадськими організаціями через функцію електронних звернень щодо шкідливого контенту [11].

Інтеграція чат-ботів (на прикладі «Кіберпес» чи «STOP_SEXтинг») дозволяє дітям анонімно повідомляти про загрози або отримати консультацію. Ефективність таких ботів особливо висока серед підлітків, які часто уникають звернення до дорослих у критичних ситуаціях [32].

Системи фільтрації контенту, інтегровані на рівні освітніх платформ, шкільного Wi-Fi або домашніх маршрутизаторів, виконують роль технічної профілактики. Проте, як зазначено в дослідженнях, пасивна фільтрація не є достатньою без паралельної інформаційно-просвітницької роботи та формування критичного мислення [15], [66].

Застосування технологій має супроводжуватись етичними нормами, захистом приватності та недопущенням надмірного контролю. Баланс між безпекою й правами дитини – ключова умова легітимності таких рішень у демократичному суспільстві [36], [112].

У сучасному інформаційно-комунікаційному суспільстві формування та реалізація комплексної політики захисту дітей у кіберпросторі потребує системного залучення всіх основних суб'єктів – як державних, так і недержавних. З огляду на це, особливого значення набуває аналіз взаємодії між ключовими стейкхолдерами: освітніми установами, правоохоронними органами, соціальними службами, батьками, ІТ-сектором і громадськими організаціями. Їхня координація є вирішальним чинником у створенні ефективної моделі запобігання, виявлення та реагування на кіберзагрози, орієнтованої на потреби дитини [33], [34], [35].

Крім того, сучасна цифрова реальність вимагає впровадження інноваційних технологій, таких як системи штучного інтелекту для моніторингу ризиків, автоматизовані боти для інформування про загрози, кіберпатрулювання онлайн-простору, інтеграція фільтраційного програмного забезпечення. Технології мають стати не лише інструментами, а й системоутворюючими компонентами державної політики, що дозволяють здійснювати проактивний захист дітей в онлайн-просторі [66], [44], [28] (табл. 3.4-3.5).

Представлені таблиці систематизують роль кожного суб'єкта у контексті наявних механізмів та напрямів взаємодії, а також візуалізують можливості застосування технологій у сфері безпеки дітей. Такий підхід дозволяє не лише узагальнити поточний стан, а й окреслити вектори подальшого вдосконалення державної політики у цій сфері.

Інноваційні технології у сфері захисту дітей у кіберпросторі

Технологія	Функція	Приклад застосування	Потенціал для України
АІ-моніторинг	Аналіз контенту, виявлення шкідливої інформації в режимі реального часу	YouTube AI для виявлення неприйнятного відео; Trust & Safety AI (Meta)	Створення національного АІ-хабу для моніторингу українськомовного контенту [128], [66]
Кіберпатруль	Активне сканування онлайн-середовища, моніторинг чатів, форумів, груп	Кіберполіція України, INTERPOL Cyber Patrol	Розширення повноважень Кіберполіції, залучення волонтерських структур [11], [30]
Чат-боти підтримки	Надання консультацій, прийом повідомлень, виявлення загроз	Бот «Кіберпес», «STOP_SEXтинг»	Масштабування на всі регіони, інтеграція в освітні платформи [32], [34]
Системи фільтрації	Блокування шкідливих ресурсів, попередження перегляду небажаного контенту	Norton Family, SafeDNS, OpenDNS	Інтеграція на рівні шкіл та сімей, субсидування провайдерів на безкоштовні фільтри [15]
Цифрові платформи моніторингу	Збір даних про інциденти, формування статистики, підтримка рішень	INHOPE, NetClean Analyze, Google Transparency Report	Створення українського аналога на базі НАЗК/Мінцифри [38], [80]
Аналітичні панелі (dashboard)	Візуалізація ризиків, динаміки загроз, підтримка публічної звітності	Панелі в США, Великобританії	Впровадження в межах системи EduNet або Diia.Освіта [34], [80]

Аналіз взаємодії між основними суб'єктами цифрового захисту дітей та огляд технологічних інструментів свідчить про наявність потенціалу для створення інтегрованої, мультиагентної системи реагування на загрози в інтернеті. Водночас ефективність такої системи залежить від рівня координації, нормативного регулювання та доступу до технологічної інфраструктури на всіх рівнях – від національного до муніципального.

Зокрема, спостерігається тенденція до зростання ролі освітніх установ як первинної ланки виявлення інцидентів та формування цифрової компетентності, тоді як правоохоронні органи потребують посилення аналітичних можливостей через впровадження АІ-інструментів та автоматизованих систем обробки сигналів. Недостатня інтеграція даних між суб'єктами, фрагментарність заходів, обмежене охоплення просвітницьких кампаній свідчать про необхідність уніфікованої платформи координації, яка б забезпечувала системний обмін інформацією, стандартизовані протоколи реагування та постійний моніторинг ефективності дій.

Отже, представлений аналіз не лише деталізує поточну конфігурацію захисного поля, а й демонструє шляхи до його посилення через технологічні рішення, правове оновлення та глибоку міжвідомчу синергію відповідно до кращих міжнародних практик [138], [80], [44].

Таблиця 3.5

Взаємодія між суб'єктами захисту дітей у цифровому просторі

Суб'єкт	Основна роль	Напрями взаємодії	Приклади взаємодії/результати
Освітні установи	Формування цифрової культури, первинне виявлення проблем	Співпраця з кіберполіцією, тренінги, використання фільтраційних систем	Впровадження уроків цифрової безпеки, впровадження EduNet [32], [15]
Кіберполіція та МВС	Виявлення кіберзлочинів, технічний аудит інцидентів	Прямі канали зв'язку зі школами, батьками, платформами соцмереж	Платформа для повідомлень про кібербулінг [11], лінії довіри
Служби у справах дітей	Психосоціальний супровід, реагування на складні випадки	Робота з жертвами кібернасильства, захист прав, соціальна реабілітація	Виявлення та супровід дітей, які стали жертвами онлайн-грумінгу [16]
Батьки/опікуни	Контроль цифрової поведінки вдома, виховання	Використання систем фільтрації, участь у програмах цифрового виховання	Впровадження “батьківського контролю”, участь у кампаніях STOP_SEXтинг
ІТ-сектор та медіаплатформи	Технологічне забезпечення, фільтрація, саморегуляція	Угоди з державою, дотримання правил, видалення небезпечного контенту	Участь у кампаніях з захисту, впровадження алгоритмів автоаналізу
Громадські організації	Адвокація, освітні кампанії, інноваційні практики	Просвітницька діяльність, проекти підтримки, незалежний моніторинг	Проекти як “Ла Страда”, “Батьки за безпечний інтернет” [32], [33]

Проведений аналіз свідчить, що ефективна реалізація державної політики у сфері захисту дітей у кіберпросторі можлива лише за умови багаторівневої, скоординованої та технологічно підкріпленої системи реагування. Основні вектори – від створення системи раннього попередження та каналів повідомлення про інциденти до залучення громадянського суспільства та

розвитку цифрової культури – повинні діяти не ізольовано, а в єдиному логічному та інституційному контексті.

Ключову роль у цьому процесі відіграє системна взаємодія між суб'єктами: освітою, правоохоронними органами, соціальними службами, батьками, а також цифровим бізнесом. Лише через об'єднання зусиль та ресурсів можна досягти належної превенції, оперативного реагування та відновлення безпеки дитини після інцидентів у цифровому просторі.

Окремо слід підкреслити потенціал новітніх технологій – AI-моніторингу, чат-ботів, систем автоматичного фільтрування контенту, а також кіберпатрулювання. Їх впровадження потребує правового регулювання, технічної адаптації до національного середовища та високого рівня цифрової компетентності всіх учасників процесу.

Критично важливим залишається створення системи національного моніторингу кіберзагроз для дітей – як елемента аналітичного супроводу політики. Така система повинна виконувати функції раннього виявлення тенденцій, оцінки ефективності впроваджених заходів та формування адаптивної державної стратегії.

Загалом, ефективність механізмів реалізації державної політики у сфері цифрової безпеки дітей має визначатися не лише формальними показниками, а й рівнем довіри, включеності та усвідомленої участі дітей, батьків і педагогів у формуванні безпечного онлайн-середовища. Саме такий підхід – гуманітарно-центричний, технологічно обґрунтований та інституційно скоординований – може стати основою стійкої моделі цифрового захисту дітей в Україні в умовах сучасних викликів.

3.3. Цифрова трансформація державної політики у сфері захисту дітей

Сучасне інформаційне суспільство перебуває в етапі глибокої цифрової еволюції, що зумовлює зміну парадигм функціонування всіх сфер державного управління, зокрема й у чутливій галузі захисту прав дитини. З огляду на зростання цифрової присутності дітей, а також зростаючі ризики кіберзагроз,

виникає об'єктивна потреба не лише в адаптації існуючих управлінських моделей, а й у глибокій трансформації державної політики – як за змістом, так і за інструментами її реалізації [80], [36].

Цифрова трансформація у сфері захисту дітей у кіберпросторі – це не суто технічне оновлення державних сервісів, а системна зміна логіки управлінських рішень, способів комунікації, координації між суб'єктами, а також залучення інноваційних технологій для превенції, реагування та моніторингу цифрових ризиків. Цей процес вимагає переходу від фрагментарних заходів до цілісної цифрової екосистеми безпеки дитини, яка включає інтеграцію інституцій, впровадження сучасних ІТ-рішень, формування цифрової культури та активне залучення громадянського суспільства [34], [35], [37].

Значну роль у цьому процесі відіграє створення державних цифрових платформ, використання штучного інтелекту, розбудова національної аналітичної інфраструктури, а також посилення нормативно-правового регулювання з урахуванням цифрової специфіки дитячих прав. Такий підхід має бути не лише реактивним, спрямованим на усунення наслідків, а насамперед – проактивним і превентивним.

В умовах гібридних загроз, повномасштабної війни та гуманітарних викликів, Україна має унікальний історичний шанс закласти інноваційний фундамент цифрового управління захистом дітей, спираючись як на власний досвід, так і на найкращі міжнародні практики (наприклад, моделі Польщі, Естонії, Південної Кореї) [138], [140].

У цьому підрозділі досліджуються стратегічні напрямки та практичні кроки цифрової трансформації державної політики у сфері захисту дітей. Зокрема, розглядаються інституційні, технологічні, правові та організаційні аспекти цієї трансформації, визначаються ключові пріоритети державної політики, а також запропоновано низку інструментів, здатних забезпечити системну і сталу протидію цифровим загрозам для дітей.

Таким чином, цифрова трансформація постає не лише як вимога часу, але як основа модернізованої системи публічного управління, яка має відповідати

викликам цифрового сьогодення та гарантувати безпечне, етичне й сприятливе середовище для розвитку дитини у цифрову епоху.

Формування концептуальних основ цифрової трансформації державної політики у сфері захисту дітей є ключовим етапом переходу від традиційної моделі управління до гнучкої, технологічно адаптованої та орієнтованої на потреби дитини системи. Така трансформація передбачає не лише впровадження цифрових інструментів, але й переосмислення стратегічних підходів, ролі інституцій, нормативно-правового підґрунтя, принципів взаємодії з суспільством, а також участі самих дітей у формуванні політик безпеки [37], [38], [80].

Концептуальне ядро цифрової трансформації має будуватись на ціннісному підході, згідно з яким дитина визнається повноцінним суб'єктом цифрового суспільства, права і безпека якого мають бути захищені як у фізичному, так і у віртуальному середовищі. Це відповідає загальноєвропейському принципу «best interests of the child» (найкращі інтереси дитини), закріпленому в Конвенції ООН про права дитини [47], [97].

Ключовими концептуальними засадами цифрової трансформації виступають:

1. Дитиноцентричність цифрової політики. Це означає, що всі управлінські рішення, цифрові сервіси та протоколи безпеки мають враховувати вікові особливості дітей, їхні потреби, права на приватність, самовираження, захист від шкідливого контенту тощо [10], [36].

2. Принцип «безпеки за замовчуванням» (safety by design). Цифрове середовище, включаючи державні портали, навчальні платформи, кіберсервіси, має бути заздалегідь налаштованим на забезпечення безпечного досвіду для дітей, включаючи обмеження доступу до ризикованого контенту, анонімізацію персональних даних, відстеження ознак кібербулінгу тощо [11], [112].

3. Інтероперабельність та інтегрованість цифрових рішень. Ефективна цифрова трансформація потребує уніфікації даних, платформ і сервісів, які використовують різні державні структури (освітні, соціальні, правоохоронні

тощо), з метою забезпечення швидкої реакції на інциденти, координації дій та мінімізації дублювання функцій [28], [55].

4. Прозорість, підзвітність та етичність управління даними. Цифрове управління захистом дітей повинно бути підпорядковане чітким етичним стандартам, включаючи захист персональних даних, інформовану згоду батьків, право дитини на інформацію про себе та механізми контролю за використанням даних [91], [112], [145].

5. Участь дитини у формуванні політик. Концептуальна модель цифрового захисту дітей має враховувати позицію дітей як активних учасників цифрового середовища, залучаючи їх до консультацій, опитувань, створення освітнього контенту, тестування цифрових сервісів тощо [80], [84].

6. Стійкість до криз і гнучкість управлінської системи. В умовах війни, кібератак та соціальної нестабільності, цифрова трансформація повинна включати елементи адаптивності, сценарного моделювання, децентралізованого реагування та кіберрезервів для підтримання базових функцій безпеки [27], [30], [106].

Таким чином, формування концептуальних основ цифрової трансформації у сфері захисту дітей – це багатоаспектний процес, який об'єднує ціннісні орієнтири, управлінську логіку, правову рамку, технологічні інновації та соціальну взаємодію. Без чіткого концептуального підґрунтя цифрова трансформація ризикує залишитися сукупністю розрізнених ІТ-проектів без системної координації, що не здатні адекватно захистити дитину в умовах зростаючих кіберзагроз. Саме тому на цьому етапі необхідно сформулювати стратегічне бачення майбутньої цифрової екосистеми захисту дітей, яка буде адаптивною, інноваційною, етичною та інклюзивною.

Ефективна цифрова трансформація державної політики у сфері захисту дітей неможлива без комплексної інституційної цифрової інтеграції та вдосконалення чинної нормативно-правової бази. На сучасному етапі цифрового розвитку України особливого значення набуває створення єдиного інтегрованого простору взаємодії між усіма зацікавленими суб'єктами – органами державної влади, правоохоронними структурами, освітніми

зкладами, службами у справах дітей, громадянським суспільством та ІТ-сектором. Така інтеграція дозволяє забезпечити оперативний обмін інформацією, ефективне реагування на кіберінциденти та впровадження інноваційних моделей захисту.

Інституційна цифрова інтеграція передбачає:

1. Створення єдиної національної платформи (або екосистеми) для моніторингу, аналізу та реагування на кіберзагрози щодо дітей. Така система повинна включати елементи big data, штучного інтелекту (AI), автоматичної ідентифікації загроз, механізми зворотного зв'язку з батьками, школами та службами. Подібна модель вже реалізується в деяких країнах ЄС, зокрема, в Естонії, де державні та приватні органи діють у рамках об'єднаної цифрової архітектури [138].

2. Інтероперабельність між системами та реєстрами. Наразі в Україні існує фрагментарність у роботі між МОН, МВС, Мінцифри, Мінсоцполітики та іншими структурами, що ускладнює координацію дій. Необхідно забезпечити технічну та адміністративну можливість автоматичного обміну релевантними даними у межах правового поля [36], [37].

3. Цифровізація механізмів роботи з інцидентами. Наприклад, алгоритм повідомлення про випадки кібербулінгу або онлайн-експлуатації має бути максимально спрощений і цифрово доступний – через чат-боти, мобільні застосунки або спеціалізовані гарячі лінії, інтегровані з системами правоохоронних органів [11], [80].

4. Запровадження інституційно-цифрової відповідальності. Кожна установа, що працює з дітьми у кіберпросторі, повинна мати затверджені внутрішні політики з цифрової безпеки, призначену відповідальну особу (наприклад, цифрового координатора), а також звітувати про виконання державних стратегічних цілей у цій сфері [35], [36].

Паралельно з цим, важливо системно вдосконалювати нормативно-правову базу, яка часто не встигає за динамікою цифрових загроз. Попри наявність низки важливих документів – зокрема, Закону України «Про основні засади забезпечення кібербезпеки України» [93], Закону «Про охорону

дитинства» [95], «Національної стратегії захисту дітей в цифровому середовищі на 2021–2026 роки» [80] – нормативна сфера залишається розпорошеною, із численними прогалинами, особливо у сфері профілактики цифрового насильства, обробки персональних даних дітей, алгоритмічної прозорості та цифрової етики.

Ключові напрямки вдосконалення законодавства мають включати: Уніфікацію цифрових понять і термінів у законах, що стосуються дітей, кібербезпеки, освіти, соціального захисту – для уникнення колізій; Розширення правових механізмів захисту дітей від новітніх цифрових загроз – таких як грумінг, сексторшен, залучення в онлайн-секти або ризиковані ігри (наприклад, «Синій кит»); Ратифікацію та гармонізацію міжнародних угод, зокрема протоколів Конвенції Ради Європи про кіберзлочинність (Будапештська конвенція) [48], Декларацій ООН, стандартів GDPR щодо персональних даних дітей [145], [112]; Запровадження адміністративної відповідальності за недотримання вимог цифрової безпеки у закладах освіти, сервісах, застосунках, платформах; Розробку механізмів цифрової відповідальності платформ та провайдерів контенту, включаючи обов’язок швидкого реагування на звернення щодо порушень прав дітей.

У цьому контексті варто зазначити важливість науково-методичного забезпечення правотворчого процесу, зокрема проведення регулярної оцінки ефективності чинної політики та моніторингу реального цифрового досвіду дітей в Україні, що дозволить адаптувати регулювання до нових викликів [38], [34].

Таким чином, інституційна цифрова інтеграція та нормативно-правове оновлення – це не просто умова ефективної цифрової трансформації, а необхідна основа сталого захисту дітей в цифровому світі. Лише за умов синергії інституцій, технологій і сучасного законодавства держава зможе гарантувати дитиноцентричну, прозору, адаптивну і ефективну політику у сфері цифрової безпеки.

Реалізація стратегії цифрової трансформації державної політики у сфері захисту дітей в цифровому середовищі повинна ґрунтуватися на чітко

визначених очікуваних результатах, які водночас слугуватимуть індикаторами ефективності впровадженої політики. У науковому дискурсі цифрова трансформація трактується не як суто технологічне оновлення інституційних процесів, а як комплексна зміна парадигми управління, що поєднує інноваційні цифрові рішення з ціннісно орієнтованим підходом до прав людини, зокрема прав дитини [28], [38], [55].

По-перше, системне підвищення рівня цифрової безпеки дітей виявиться у скороченні кількості інцидентів кіберзлочинності проти дітей, зокрема таких форм, як грумінг, кібербулінг, онлайн-експлуатація та поширення шкідливого контенту. Це стане можливим завдяки впровадженню ефективних механізмів раннього попередження, автоматизованого виявлення загроз, кіберпатрулювання та функціонування єдиної національної системи моніторингу [30], [36].

По-друге, зміцнення міжвідомчої та міжсекторальної взаємодії передбачає створення дієвої цифрової екосистеми, де суб'єкти державної політики (МОН, Мінцифри, МВС, ОВА), освітні установи, правоохоронні органи, соціальні служби та громадські організації об'єднані спільною цифровою інфраструктурою, базами даних, протоколами реагування та обміну інформацією. Це дасть змогу оперативно реагувати на виклики, запобігати їх ескалації та здійснювати ефективну профілактику [33], [34].

По-третє, розширення цифрової компетентності суб'єктів освітнього процесу, батьків та дітей. Очікується, що завдяки інтеграції цифрової грамотності у навчальні програми, реалізації просвітницьких кампаній, запуску платформ самоосвіти та сертифікаційних програм для педагогів і фахівців соціальної сфери, зросте загальний рівень цифрової культури, обізнаності про ризики та здатності до самозахисту у кіберпросторі [32], [105].

По-четверте, модернізація правового поля відповідно до міжнародних стандартів захисту дітей (GDPR, Конвенція Ради Європи про кіберзлочинність, Конвенція ООН про права дитини), що уможливить зменшення правових прогалин та збільшення правових гарантій. Цей результат виявлятиметься у прийнятті нових підзаконних актів, адаптації освітнього законодавства до

цифрового середовища, а також у забезпеченні правової відповідальності цифрових платформ, провайдерів та адміністраторів контенту [47], [48], [91], [145].

По-п'яте, розвиток національної моделі цифрової етики та дитиноцентричного дизайну цифрових сервісів, що передбачає забезпечення конфіденційності, мінімізації даних, прозорості алгоритмів і доступності платформ для дітей з особливими освітніми потребами. Результатом стане вищий рівень довіри дітей та батьків до державних і освітніх онлайн-інструментів, а також до цифрового середовища загалом.

По-шосте, науково обґрунтована система оцінювання ефективності цифрової трансформації у сфері захисту дітей. Вона має включати регулярний моніторинг впроваджених інновацій, аналітичну оцінку рівня загроз, формування відкритих звітів та індикаторів результативності. Очікується, що такі підходи сприятимуть прозорості державної політики, її адаптивності та ефективному коригуванню у разі виникнення нових викликів [38], [56].

У підсумку, реалізація цифрової трансформації не лише дозволить підвищити ефективність захисту дітей у кіберпросторі, але й забезпечить створення сучасної інституційно-технологічної моделі державного управління, що базується на принципах відкритості, взаємодії, превентивності та захисту прав дитини як фундаментальної складової національної безпеки [7], [23], [93].

Таким чином, очікувані результати цифрової трансформації є багатоаспектними та взаємопов'язаними – вони формують цілісну стратегічну мету: створення безпечного, дитиноцентричного, етичного та прозорого цифрового середовища, де кожна дитина має захищене право на розвиток, безпеку та приватність.

У контексті сучасної кіберреальності, яка дедалі інтенсивніше інтегрується у повсякденне життя дітей, формування та розгортання національної цифрової інфраструктури для захисту дітей постає не лише як технологічне, але й соціально-політичне та гуманітарне завдання державної ваги. Така інфраструктура є основою функціонування всієї системи превенції, моніторингу, реагування та просвіти у сфері кібербезпеки неповнолітніх, що

прямо пов'язана з реалізацією конституційного обов'язку держави щодо охорони прав та свобод дитини [49], [95].

1. Структурні компоненти цифрової інфраструктури. Розгортання національної цифрової інфраструктури повинне включати:

1.1. Єдину національну платформу кіберзахисту дітей – хмарно орієнтовану систему, яка об'єднує дані з кіберполіції, освітніх установ, соціальних служб, провайдерів, батьківських організацій та міжнародних партнерів. Ця платформа має виконувати функції виявлення кіберінцидентів, формування ризик-профілів, попередження та реагування.

1.2. Систему автоматизованого моніторингу на основі штучного інтелекту, здатну аналізувати відкриті джерела, соціальні мережі, форуми, месенджери для виявлення небезпечного контенту, грумінгу, агресивної поведінки або ознак суїцидального ризику серед дітей [28], [66].

1.3. Багаторівнева система фільтрації контенту з адаптивними алгоритмами, що враховують вік дитини, особливості психоемоційного розвитку, контекст споживання інформації. Технічна реалізація такої фільтрації можлива через партнерство з провайдерами інтернет-послуг та операторами мобільного зв'язку [11], [44].

1.4. Національний кіберпатруль – підрозділ кіберполіції з розширеними функціями цифрової профілактики, онлайн-нагляду за цифровим середовищем, а також взаємодії з громадянами через чат-боти, гарячі лінії, мобільні додатки тощо.

1.5. Єдиний електронний реєстр інцидентів кібернасильства над дітьми, який повинен функціонувати в закритому форматі для зареєстрованих суб'єктів реагування, забезпечуючи міжвідомчу координацію, правову доказовість і захист персональних даних відповідно до GDPR [112], [145].

2. Інфраструктурні вимоги. Для забезпечення функціонування вказаних компонентів цифрової інфраструктури необхідні:

2.1. Широкосмугове покриття та цифрова інклюзивність у всіх регіонах України, включаючи сільську місцевість, тимчасово окуповані та деокуповані території;

2.2. Захищені дата-центри для зберігання, обробки та шифрування персональних даних дітей, з урахуванням стандартів ISO/IEC 27001 та рекомендацій ENISA;

2.3. Інтероперабельність систем між відомствами, уніфіковані формати даних, API-доступ та стандарти кібервзаємодії;

2.4. Резервні центри обробки даних та кризові плани відновлення у випадках кіберкатастроф або фізичного знищення ІТ-інфраструктури, що є особливо актуальним в умовах воєнного стану [6], [106].

3. Виклики та ризики. Водночас реалізація такої інфраструктури стикається з низкою ризиків: Низький рівень цифрової компетентності на місцях; Недостатнє фінансування ІТ-сектору у гуманітарній сфері; Ймовірність несанкціонованого доступу до конфіденційної інформації; Відсутність правової уніфікації понять «кіберінцидент», «шкідливий контент», «загроза для дитини в мережі» [12], [36].

4. Перспективи розвитку. Розгортання цифрової інфраструктури для захисту дітей повинне супроводжуватися:

4.1. Ухваленням національного плану цифрової безпеки дітей з чітко прописаними етапами, ресурсами та відповідальними виконавцями;

4.2. Інституалізацією центру цифрового захисту дітей – постійно діючого аналітичного та координаційного органу;

4.3. Партнерством із BigTech-компаніями (Meta, Google, TikTok) щодо локалізації алгоритмів фільтрації, українськомовної модерації та прозорості звітності;

4.4. Масовим впровадженням EdTech-рішень у школах та позашкільній освіті, спрямованих на безпеку у кіберпросторі (симулятори загроз, кібернавчання, інтерактивні курси з безпеки).

Отже, національна цифрова інфраструктура – це не лише технологічний, а й стратегічний ресурс, що дозволяє державі діяти проактивно, інтегровано та ефективно в умовах постійно еволюціонуючих кіберзагроз. Її розгортання є передумовою не лише для захисту конкретної дитини, а й для формування стійкого цифрового майбутнього України.

У сучасних умовах цифрової епохи, що характеризується стрімким розвитком інформаційних технологій, національна цифрова інфраструктура стає фундаментальним чинником забезпечення кібербезпеки дітей. Саме її ефективна побудова та функціонування дозволяють не лише оперативно виявляти й реагувати на загрози, а й запобігати їм шляхом впровадження проактивних механізмів. Запропонована у таблиці модель охоплює ключові компоненти такої інфраструктури з урахуванням поточних потреб України, міжнародного досвіду (Польщі, Естонії, Південної Кореї) [138], а також стратегічних напрямів, закладених у Національній стратегії захисту дітей у кіберпросторі[80].

Кожен із компонентів, включених у таблицю 3.7, виконує чітко визначену функцію в системі: від аналітичного спостереження та моніторингу (AI-системи), до реагування (чат-боти, кіберпатрулі), запобігання (фільтраційні механізми), збереження доказової бази (реєстри кіберінцидентів), і до загальної координації через єдину платформу. Такий підхід дозволяє реалізовувати принципи інтегрованого, міжвідомчого, технологічно-орієнтованого управління в умовах цифрового суспільства [2], [18], [30].

Окрему увагу у таблиці приділено індикаторам ефективності, які відіграють ключову роль у системі управлінського моніторингу та дозволяють здійснювати регулярну оцінку результативності запроваджених рішень [1], [14], [38]. Це дає змогу державі гнучко адаптувати політику відповідно до нових викликів.

Запропонована модель цифрової інфраструктури засвідчує необхідність системного підходу до організації захисту дітей у цифровому просторі, де кожен елемент не є ізольованим, а взаємопов'язаний із загальною архітектурою кібербезпеки. Її реалізація сприятиме:

- зміцненню міжвідомчої взаємодії між державними структурами, освітніми установами, ІТ-сектором та громадським суспільством;
- зниженню ризиків деструктивного впливу цифрового середовища на дітей;

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

- зростанню рівня довіри до державної політики кіберзахисту серед батьків, педагогів та самих дітей;

- підвищенню рівня готовності країни до реагування на інциденти в реальному часі;
- формуванню сталого цифрового середовища, що базується на етичних, безпечних і правових нормах [10], [12], [33], [35].

Таким чином, впровадження комплексної цифрової інфраструктури має розглядатися не як окремий напрям державної політики, а як невід’ємна складова національної системи безпеки та розвитку дитини в умовах цифрового майбутнього.

Висновки до розділу 3

У межах проведеного дослідження 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. Ці загрози включають кібербулінг, сексуальну експлуатацію, деструктивний контент, втручання в приватність, ігрову залежність, а також використання персональних даних дітей у зловмисних цілях. Такий комплексний підхід дав змогу розробити класифікацію загроз з урахуванням вікових, поведінкових та соціокультурних особливостей дітей, а також визначити ключові наслідки кожного з типів впливу.

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. 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.

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). 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 ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Андріяш В., Громадська Н., Малікіна О. Оцінювання державних управлінських рішень: моделі та критерії. 2021. № 9. URL: <http://www.dy.nayka.com.ua/?op=1&z=2201>.
2. Бакуменко В. Державні та управлінські рішення: Навч. Київ: ВПЦ АМУ, 2012. 344 с.
3. Бакуменко В. Формування державно-управлінських рішень: проблеми теорії, методології, практики : монографія. Київ: Видавництво УАДУ, 2000. 328 с.
4. Бакуменко В., Усаченко Л. Бакуменко В., Усаченко Л., Червякова О. Теоретичні засади державного управління: навч. посіб. / за заг. ред. Л. М. Усаченко. Київ : ТОВ «НВП «Інтерсервіс», 2013. 174 с.
5. Барило О. Інформація як складова системи державної політики в надзвичайних ситуаціях. Інвестиції: практика та досвід. 2011. № 2. С. 76–78.
6. Баштанник В. В. Трансформація державної політики в контексті європейських інтеграційних процесів: монографія. Дніпропетровськ: ДРІДУ НАДУ, 2010. 390 с.
7. Баяк М. І. Гуманітарна складова політики державної безпеки: поняття, принципи. Університетські наукові записки. 2018. № 1. С. 186–199.
8. Безверхнюк Т. Партнерська мережа як інституціональна форма державного механізму проектного управління регіональним розвитком. Держава та регіони. Серія Державне управління. 2016. № 1 (53). С. 163–173.
9. Безпаленко О. В. Вектори соціальної політики для України в умовах викликів війни. Проблеми сучасних трансформацій. 2022. № 4. С. 1–8.
10. Безпека дитини у кіберпросторі: як попередити негативний вплив Інтернету. URL: https://www.ombudsman.gov.ua/news_details/bezpeka-ditini-u-kiberprostori-yak-poperediti-negativnij-vpliv-internetu
11. Безпека дітей в інтернеті: поради кіберполіції. URL: <https://cyberpolice.gov.ua/article/bezpeka-ditej-v-interneti-porady-kiberpolicziyi-3851/>

12. Бухарєв В. В. Адміністративно-правові засади забезпечення кібербезпеки України : автореф. дис. ... канд. юрид. наук: 12.00.07 / Бухарєв Владислав Вікторович ; Сум. держ. ун-т. - Суми, 2018. 20 с.
13. Вагапов В., Лисицин Е. Поняття національної безпеки в контексті національних інтересів України. Наука і оборона. 2002. №1. С. 18-24.
14. Василенко В. Теорія і практика розробки управлінських рішень: навчальний посібник. К., 2015. 256 с.
15. Використання інформаційних та комунікаційних технологій в сучасному цифровому суспільстві : колективна монографія. Херсон: Вишемирський В. С., 2020. 148 с.
16. Волкова Н. В. Захист прав та інтересів дитини Уповноваженим Президента України з прав дитини: окремі аспекти. Правові та інституційні механізми забезпечення розвитку України в умовах європейської інтеграції : матеріали Міжнар. наук.-практ. конф. (Одеса, 18 травня 2018 р.) У 2-хт. Т. 2. Одеса : Видавничий дім «Гельветика», 2018. С. 586–589.
17. Волкова Н. В. Міжнародно-правовий захист сімейних прав та інтересів дитини Європейським судом з прав людини. Jurnalul Juridic National: teorie si practica. 2018. № 1 (29). С. 84-87.
18. Гончар С. Ф. Оцінювання ризиків кібербезпеки інформаційних систем об'єктів критичної інфраструктури: монографія / С. Ф. Гончар; НАН України, Ін-т проблем моделювання в енергетиці ім. Г. Є. Пухова. Київ: Альфа Реклама, 2019. 175 с.
19. Гончаренко О., Лисицин Е. Методологічні засади розробки нової редакції Концепції національної безпеки України. Національна безпека. 2001. Вип. 4. С. 6-7.
20. Гонюкова Л., Рак Ю. Конфліктна взаємодія органів публічної влади і громадянського суспільства як об'єкт наукових досліджень. «Актуальні питання у сучасній науці. Серія «Державне управління». Київ, 2023. № 1(7). С. 147–158.
21. Горбулін В., Качинський А. Стратегічне планування: вирішення проблем національної безпеки: монографія. Київ: НІСД, 2010. 288 с.

22. Горбулін В., Качинський. А. Стратегічне планування: вирішення проблем національної безпеки. К.: НІСД, 2010. 288 с. URL: https://niss.gov.ua/sites/default/files/2011-07/Gorbulin_Kachynsky-e2dd0.pdf
23. Горбулін В., Литвиненко О. Національна безпека: український вимір. Київ : ПП «Інтертехнологія», 2008. 104 с.
24. Гордєєв О. Концептуальні підходи до сутності інституційного механізму. Управління. 2016 р. № 3. URL: <http://kbuara.kharkov.ua/e-book/putp/2012-3/doc/1/07.pdf>
25. Гришко В. Квадрат ефективності публічного управління. Інвестиції: практика та досвід. 2020. № 17–18. С. 81–84.
26. Губаль Ю. Поняття та види гарантій захисту прав і свобод дитини відповідно до законодавства України та Угорщини. Науковий вісник Ужгородського національного університету. Серія: Право. 2015. Вип. 34 (1). С. 66–68.
27. Гута С. Поняття «кризова ситуація, зумовлена воєнно-політичними факторами», «воєнно-політична криза» в теорії державного управління. Інвестиції: практика та досвід. 2017. № 7. С. 116–120.
28. Даник Ю. Г. Основи кібербезпеки та кібероборони: підручник / Ю. Г. Даник, П. П. Воробієнко. Одеса: ОНАЗ, 2019. 320 с.
29. Даниленко С. А. Відкритість та прозорість влади: механізм регулювання взаємодії зі ЗМІ на регіональному рівні : автореф. дис. ... канд. наук з держ. упр.: 25.00.02 / Даниленко Сергій Анатолійович; Нац. акад. держ. упр. при Президентові України, Одес. регіон. ін-т держ. упр. Одеса, 2018. 20 с.
30. Державно-приватне партнерство у сфері кібербезпеки: міжнародний досвід та можливості для України: аналіт. доп. / [Д. В. Дубов та ін. ; за заг. ред. Д. Дубова]; Нац. ін-т стратег. дослідж. Київ : НІСД, 2018. 81 с.
31. Дзьобань О. П. Інформаційна безпека у проблемному полі соціокультурної реальності / О. П. Дзьобань . Харків: Майдан, 2010. 259 с.
32. Діти в інтернеті: як навчити безпеці у віртуальному світі. URL: https://urlicey.dp.ua/uploads/file/A5_Ukrainian.pdf?utm_source=chatgpt.com

33. Димитрієва О.І. Комунікаційні стратегії держави у сфері захисту дітей від цифрових загроз. Держава та регіони. 2022. №2(76). С.162-166.
34. Димитрієва О.І. Застосування технологічних інструментів у державному управлінні кібербезпекою дітей. Держава та регіони. 2023. №1(79). С. 180-185.
35. Димитрієва О.І. Механізми запобігання кіберзагрозам для дітей у системі гуманітарної безпеки України. Право та державне управління. 2023. №1. С. 426-431.
36. Димитрієва О.І. Нормативно-правове забезпечення кіберзахисту дітей в Україні. Право та державне управління. 2021. №2. С. 353-358.
37. Димитрієва О.І. Організаційно-функціональна модель державної політики кібербезпекою дітей. Право та державне управління. 2021. №4. С. 207-302.
38. Димитрієва О.І. Методичні підходи до оцінки ефективності державної політики щодо захисту дітей у кіберпросторі. Вчені записки Таврійського національного університету імені В.І. Вернадського. 2023. Том 34 (73) №2. С.164-172.
39. Дрозд О., Хуторянська Т. Міжнародні стандарти забезпечення прав і законних інтересів дитини та їх імплементація в законодавство України. Актуальні проблеми держави і права. 2015. Вип. 75. С. 255–261.
40. Євсюков О. Науково-теоретичні визначення сутності та змісту безпеки держави. Вісник Національного університету цивільного захисту України. Серія: «Державне управління». 2017. Вип. 2(7). С. 22-28.
41. Загальна декларація прав людини. URL: <https://www.coe.int/uk/web/compass/theuniversal-declaration-of-human-rights-fullversion->.
42. Закриницька В. Омбудсмен з прав дитини в механізмі державного захисту прав, свобод і законних інтересів дітей: зарубіжний досвід. Вісник академії правових наук. 2012. № 4. С. 346–356.

43. Захист персональних даних дитини: на що треба звернути увагу батькам? URL: <https://www.radiosvoboda.org/a/zahystpersonalnyh-danyh-dytyny/31603271.html>.

44. Кібербезпека мереж наступного покоління: навч. посіб. у галузі знань 1701 "Інформаційна безпека" за спец. 8.17010201 - Системи технічного захисту інформації, автоматизація її обробки / О. О. Вараксін [та ін.] ; за ред. чл.-кор. МАЗ В. Г. Кононовича; Одес. нац. акад. зв'язку ім. О. С. Попова, Каф. інформ. безпеки та передачі даних. О.: ОНАЗ ім. О. С. Попова, 2013. 238 с.

45. Клименко І. В. Складові ефективності електронного врядування. Інвестиції: практика та досвід. 2010. № 16. С. 92–94.

46. Коломоєць Н. В. Адміністративно-правовий захист прав дитини в Україні : монографія. Харків : Панов, 2019. 352 с.

47. Конвенція про захист прав людини і основоположних свобод (з протоколами) (Європейська конвенція з прав людини) (1950). URL: https://zakon.rada.gov.ua/laws/show/995_004#Text.

48. Конвенція про кіберзлочинність. Офіційний переклад URL: http://zakon4.rada.gov.ua/laws/show/994_575.

49. Конституція України: закон України від 28 червня 1996 р. № 254к/96-ВР / Верховна Рада України. Відомості Верховної Ради України. 1996. № 30. Ст. 41. URL: <http://zakon5.rada.gov.ua/laws/show/254%D0%B>.

50. Кормич Б. А. Інформаційна безпека: організаційно-правові основи : навчальний посібник для вузів / Б. А. Кормич . Київ: Кондор, 2008. 382 с.

51. Корнієнко Б. Я. Безпека інформаційно-комунікаційних систем та мереж: навч. посіб. для студентів спец. 125 "Кібербезпека" / Б. Я. Корнієнко; Нац. авіац. ун-т. Київ : НАУ, 2018. 225 с.

52. Корнієнко М. Принцип дотримання найкращих інтересів дитини та його застосування у цивільному судочинстві України. Юридичний вісник. 2020. № 1. С. 398–404.

53. Котух Є.В. Аудит інформаційної безпеки як необхідна складова управління в державних установах. Державне будівництво. 2021. № 1. URL: <https://db.kh.ua/index.php/db/article/view/117/110>.

54. Котух Є.В. Електронний уряд і кібербезпека у соціальних мережах: особливості реалізації. Вісник НУЦЗ України. Серія: Державне управління. 2020. № 2. С. 564-572.
55. Котух Є.В. Кібербезпека у публічному секторі : монографія / Є.В. Котух. Харків: Колегіум, 2021. 272 с.
56. Котух Є.В. Кібербезпека як один з пріоритетів національної політики. Державне будівництво. 2020. № 2. URL: <http://db.journal.kharkiv.ua/index.php/db/article/download/90/85>.
57. Котух Є.В. Національні стратегії кібербезпеки: порівняльний аналіз. Актуальні проблеми державного управління. 2021. № 1. С. 48-57.
58. Котух Є.В. Основні виклики врядування у сфері кібербезпеки. Теорія та практика державного управління. 2020. № 4 (71). С. 38-46.
59. Крестовська Н. М. Сучасне розуміння прав дитини. Форум права. 2011. № 3. С. 409–413.
60. Крук С. І. Методологія побудови інституційних механізмів державної політики у сфері національної безпеки. Вчені зап. Тавр. нац. ун-ту ім. В. І. Вернадського. Серія: Держ. упр. 2018. Т. 29(68), №6. С. 8-11.
61. Крук С. І. Організаційний механізм державної політики у сфері забезпечення національної безпеки України. Держава та регіони. Серія: Державне управління. 2018. №3(63). С. 105-108.
62. Крук С. І. Планування у сфері національної безпеки. Теорія та практика державної політики і місцевого самоврядування. 2019. №1. URL: http://nbuv.gov.ua/UJRN/Ttpdu_2019_1_24
63. Кулачок-Тітова Л. В., Кім К. В. До питання врегулювання трудових конфліктів державних службовців позасудовими способами. Вісник Харківського національного університету імені В. Н. Каразіна. Серія «Право». Харків, 2015. № 20. С. 109–113.
64. Кулик Т. О. Зима Н. Ф. Механізм забезпечення прав дітей в Україні: проблеми суб'єктного складу. Науковий вісник Національної академії внутрішніх справ. 2020. № 2 (115). С. 94–102.

65. Кушнір С. П. Професійна компетентність державного службовця: сутнісно-понятійна характеристика та правове регулювання: дис.... канд. юрид. наук: 12.00.07. Одеса, 2021. 211 с

66. Ланде Д. В. Основи теорії і практики інтелектуального аналізу даних у сфері кібербезпеки: навч. посіб. / Д. В. Ланде, І. Ю. Субач, Ю. Є. Бояринова ; Ін-т спец. зв'язку та захисту інформації Нац. техн. ун-ту України "Київ. політехн. ін-т ім. Ігоря Сікорського". Київ : ІСЗЗІ КПІ ім. Ігоря Сікорського, 2018. 300 с.

67. Ларін С. В. Активізація взаємодії держави і суспільства щодо захисту національних цінностей у сфері національної безпеки. Держава та регіони. Серія: Державне управління. 2017. Вип. 3. С. 16-20.

68. Левківський Б. К. Захист прав дитини: окремі проблеми здійснення батьками права на самозахист дитини. Порівняльне аналітичне право. 2013. № 3–2. С. 136–139.

69. Лесечко М. Д., Чемерис А.О., Рудницька Р.М. Психологія управлінських рішень і створення ефективних команд: навч. посібник. Львів: ЛРІДУ УАДУ, 2003. 100 с.

70. Ложкін Г. В., Волянчук Н. Ю. Психологія конфліктної взаємодії у військовому колективі. Вісник Національної академії оборони України. Київ, 2008. Вип. 3 (7). С. 64–68.

71. Ложкін Г. В., Пов'якель Н. І. Психологія конфлікту: теорія і сучасна практика : навч. посіб. Київ: ВД Професіонал, 2006. 416 с.

72. Лозова Г. М., Шорубалко Б. В. Інтелектуальна безпека держави в системі конкурентоспроможності національної економіки. Науковий вісник Ужгородського національного університету. Серія: Міжнародні економічні відносини та світове господарство. 2018. Вип. 20 (2). С. 102-106.

73. Мазур В. Г. Комунікації як механізм взаємодії державних органів влади та громадськості на регіональному рівні. Державне управління: удосконалення та розвиток. 2011. № 8. URL: <http://www.dy.nayka.com.ua/?op=1&z=313>.

74. Макаренко М. М. Поняття та особливості управлінських рішень в органах Державної податкової служби України. Актуальні проблеми права: теорія і практика. 2010. № 18. С. 397-404.

75. Максимець В. Є. Парадигма європейської безпеки у вимірах встановлення нової системи «Балансу сил» у Центрально-Східній Європі. Прикарпатський вісник НТШ. Думка. 2017. №5-6. С. 137-147. URL: http://nbuv.gov.ua/UJRN/Pvntsh_2017_5-6_16

76. Мала Н.Т., Проник І.С. Мистецтво прийняття управлінського рішення. Вісник Національного університету «Львівська політехніка». Львів: Вид-во НУ «Львівська політехніка», 2010. С. 345-351.

77. Манокін Є. В. Модель прийняття управлінських рішень щодо забезпечення інформаційної безпеки в органах управління Державної прикордонної служби України. Інвестиції: практика та досвід. 2015. № 1. С. 130- 135

78. Міжнародний пакт про громадянські і політичні права (1966). URL: https://zakon.rada.gov.ua/laws/show/995_043#Text.

79. Найдьорова Л.А. Кібербулінг або агресія в інтернеті: способи розпізнання і захист дитини / Л.А.Найдьорова // Методичні рекомендації – К., 2014. – 80 с.

80. Національна стратегія захисту дітей в цифровому середовищі на 2021 – 2026 роки. URL: https://thedigital.gov.ua/storage/uploads/files/normative_document/2020/1/%D0%9D%D0%B0%D1%86%D1%96%D0%BE%D0%BD%D0%B0%D0%BB%D1%8C%D0%BD%D0%B0%20%D1%81%D1%82%D1%80%D0%B0%D1%82%D0%B5%D0%B3%D1%96%D1%8F%20v1_1.pdf

81. Основи кіберпростору, кібербезпеки та кіберзахисту: навч. посіб. Київ: Ліра-К, 2020. 554 с.

82. Оцінка електронної готовності України Державним агентством з питань електронного урядування URL: http://www.dknii.gov.ua/sites/default/files/dodatok_5.pdf.

83. 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>
84. Петрочко Ж. В. Найкращі інтереси дитини: сутність і шляхи забезпечення. Наукові записки Ніжинського державного університету ім. М. Гоголя. Психолого-педагогічні науки. 2014. № 3. С. 70–74.
85. Про доступ до публічної інформації: Закон України від 13.01.2011 р. № 2939-VI URL: <http://zakon4.rada.gov.ua/laws/show/2939-17>.
86. Про електронний цифровий підпис: Закон України від 22.05.2003 р. № 852-IV. URL: <http://zakon4.rada.gov.ua/laws/show/852-15>.
87. Про електронні документи та електронний документообіг : Закон України від 22.05.2003 р. № 851-IV URL: <http://zakon4.rada.gov.ua/laws/show/851-15>.
88. Про запровадження електронного сервісу для платників податків – юридичних осіб: Наказ Державної податкової адміністрації України від 11.02.2011 р. № 85 URL: <http://www.tax.gov.ua/elektronna-zvitnist/platnikam-podatkov-pro/povidomlennya-platnikam-pod/58694.html>.
89. Про запровадження Національної системи індикаторів розвитку інформаційного суспільства: постанова Кабінету Міністрів України від 28.11.2012 № 1134 URL: <http://zakon4.rada.gov.ua/laws/show/1134-2012-%D0%BF>.
90. Про затвердження Методики формування індикаторів розвитку інформаційного суспільства: Наказ МОН України від 06.09.2013 р. № 1271 URL: <http://zakon4.rada.gov.ua/laws/show/z1664-13>.
91. Про захист персональних даних: закон України від 1 червня 2010 року № 2297- VI. Відомості Верховної Ради України (ВВР). 2010. № 34, ст. 481. URL: <https://zakon.rada.gov.ua/laws/show/2297-17#Text>.
92. Про основи національної безпеки України : Закон України від 19.06.2003 р. № 964-IV URL: <http://zakon4.rada.gov.ua/laws/show/964-15>.

93. Про основні засади забезпечення кібербезпеки України : Закон України від 5 жовтня 2017 року № 2163-VIII // ВВР України. 2017. № 45. Ст. 403.

94. Про Основні засади розвитку інформаційного суспільства в Україні на 2007 – 2015 роки : Закон України від 09.01.2007 р. № 537-V URL: <http://zakon4.rada.gov.ua/laws/show/537-16>.

95. Про охорону дитинства : Закон України від 26.04.2001 р. № 2402-III. База даних «Законодавство України». ВР України. URL: <http://zakon5.rada.gov.ua/laws/show/2402-14>

96. Про платіжні системи та переказ коштів в Україні: Закон України від 05.04.2001 р. № 2346-III URL: <http://zakon4.rada.gov.ua/laws/show/2346-14>.

97. Про ратифікацію Європейської конвенції про здійснення прав дітей: Закон України від 03.08.2006 р. № 69-V. База даних «Законодавство України». ВР України. URL : <https://zakon.rada.gov.ua/laws/show/69-16#Text>

98. Про схвалення Концепції розвитку електронного урядування в Україні: розпорядження Кабінету Міністрів України від 13 грудня 2010 р. № 2250-р URL: <http://zakon4.rada.gov.ua/laws/show/2250-2010-%D1%80>.

99. Про схвалення Концепції розвитку цифрової економіки та суспільства України на 2018-2020 роки та затвердження плану заходів щодо її реалізації: Розпорядження Кабінету Міністрів України від 17 січня 2018 р. № 67-р URL. : <https://zakon.rada.gov.ua/laws/show/67-2018-%D1%80#Text>.

100. Про схвалення Стратегії розвитку інформаційного суспільства в Україні : розпорядження Кабінету Міністрів України від 15.05.2013 р. № 386- р URL: <http://zakon4.rada.gov.ua/laws/show/386-2013-%D1%80>.

101. Резвова О. В. Генезис законодавства України щодо прав та обов'язків батьків з виховання дитини. Логос. Мистецтво наукової думки. 2020. Вип. 9. С. 101–106.

102. Резвова О. В. Права та обов'язки батьків щодо виховання дитини в сімейному праві України : дис. ... д-ра філософії : 081 – Право. Київ, 2021. 214 с.

103. Саблук С. А. Історичні передумови формування правового статусу дитини в Україні. Університетські наукові записки. 2006. № 3-4. С. 253–260.

104. Семигіна Т. В. Конвенція про права дитини як основа державної політики захисту дітей: оцінка ефективності впровадження в Україні Національного плану дій. Вісник Академії праці і соціальних відносин Федерації профспілок України. Серія «Право та державне управління». 2015. Вип. 1-2. С. 83–90

105. Сокол І.М. Коли необхідно вчитись «безпечному» інтернету? URL: http://nbuv.gov.ua/UJRN/komp_2012_8_9.

106. Станіславський Т. В. Механізми публічного управління забезпечення кібербезпеки в сучасних умовах : автореф. дис. ... канд. наук з держ. упр.: 25.00.02 / Станіславський Тарас Володимирович; Ін-т підгот. кадрів держ. служби зайнятості України. Київ, 2020. 20 с.

107. Стешенко В. М. Правовий захист прав дітей та підлітків і безпечний інформаційний простір : навч. посіб. Харків : Лисенко І. Б., 2019. 386 с.

108. Фоменко В. Особливості розгляду справ про надання дитині дозволу на виїзд за межі України. Юридична газета. URL: <https://yurgazeta.com/publications/practice/simeynepravo/osoblivosti-rozglyadu-sprav-pronadannya-ditini-dozvolu-na-viyizd-za-mezhi-ukrayini.html>

109. Цивільний кодекс України від 16 січня 2003 року № 435-IV. Відомості Верховної Ради України (ВВР). 2003. №№ 40–44, ст. 356.

110. Шипілова Л. Порівняльний аналіз ключових понять і категорій основ національної безпеки України: автореф. дис. к. політ. н.: 21.01.01. Київ, 2007. 20 с.

111. Ширшикова Р. До питання про ознаки управлінського рішення, що приймаються центральними органами державної влади: общественнополитическая література. Держава і право: зб. наук. пр. 2007. Вип. 36: Юридичні і політичні науки. С. 271-277.

112. Явор О.А, Піддубна В.Ф., Рубан О.О. Правові проблеми захисту персональних даних неповнолітніх осіб відповідно до вимог вітчизняного

законодавства та вимог GDPR. Journal «ScienceRise: Juridical Science». 2023. № 3 (25). С. 23–34.

113. Blakemore, M., and Lloyd, P. (2007). “Trust and transparency: Prerequisites for effective eGovernment,” Citizen-Centric eGovernment Think Paper, 2007: 10.

114. BMI (2011b) Cyber Security Strategy for Germany, Federal Ministry of the Interior (Bundesministerium des Innern), Berlin, Germany, available at http://www.cio.bund.de/SharedDocs/Publikationen/DE/ITSicherheit/css_engl_download.pdf?__blob=publicationFile.

115. Booz Allen Hamilton. (2009). “Cyber IN-Security: Strengthening the Federal Cybersecurity Workforce,” Partnership for Public Service, July 2009: <http://www.ourpublicservice.org>.

116. Borg S (2005) Economically complex cyberattacks. Secur Priv 3(6):64-67.

117. Bovaird, T and Loffler, E. 2003. Public Management and Governance. London: Routledge.

118. Bovens, M., and Loos, E. (2002). “The digital constitutional state: Democracy and law in the information society,” Information Policy, Vol. 7, №4, 2002, pp. 16, 185-197.

119. Brechbuhl, Hans, Robert Bruce, Scott Dynes, and M. Eric Johnson (2010), ‘Protecting Critical Information Infrastructure: Developing Cybersecurity Policy’, Information Technology for Development, Vol.16, No.1, pp.83-91.

120. Broad, W. J. et al. (2011). “Israeli Test on Worm Called Crucial in Iran Nuclear Delay.” New York Times (January 15), p. 1A.

121. Brown, David (2005), “Electronic government and public administration”. International Review of Administrative Sciences. Vol. 71 (2): 241-254, London, Thousand Oaks, CA and New Delhi: Sage Publications

122. Carr, Jeffrey (2018): Inside Cyber Warfare, Sebastopol, CA: O’Reilly.

123. Carr, M. (2016). Public Private Partnerships in National Security Strategies. International Affairs, 43-62.

124. CCDCOE (Cooperative Cyber Defence Centre of Excellence). 2018. "Cyber Definitions." Resources 2017. Accessed February 1. <https://ccdcoe.org/cyber-definitions.html>.
125. Chabinsky, Steven R. (2010), 'Cybersecurity Strategy: A Primer for Policy Makers and Those on the Front Line', Journal of National Security Law & Policy, Vol.4, No.1, pp.27-39.
126. Chadwick, A. 2006. Internet politics: States, citizens and new communication technologies. Oxford: Oxford University Press
127. CIO Council's Guidelines for Secure Use of Social Media by Federal Departments and Agencies: http://www.cio.gov/documents_details.cfm/uid/1F4378B4-2170-9AD7-F2A2B098D3F954EE/structure/Information%20Technology/category/IT%20Security-Privacy
128. Cybersecurity awareness for children: A systematic literature review. URL: https://www.sciencedirect.com/science/article/pii/S2212868921000581?utm_source=chatgpt.com
129. Deane, Arsala (2003), "Increasing Voice and Transparency Using ICT Tools: (E-Government, E-Governance)". World Bank. March 2003.
130. Deibert, R. J. (2002). Dark guests and great firewalls: The Internet and Chinese security policy. Journal of Social Issues, 58, 143-159.
131. Deibert, R., & Crete-Nishihata, M. (2011). Blurred boundaries: Probing the ethics of cyberspace research. Review of Policy Research, 28, 531-537.
132. Deibert, Ronald J., and Rafal Rohozinski (2010), 'Risking Security: Policies and Paradoxes of Cyberspace Security', International Political Sociology, Vol.4, No.1, pp.15-32.
133. Demchak, Chris, and Peter Dombrowski. "Rise of a Cybered Westphalian Age." Strategic Studies Quarterly, March 2011. Accessed January 28, 2013

- a. Derrick, L. (2011) Available at <http://lafiga.firedoglake.com/2011/06/03/finally-an-intelligent-use-for-cupcakeshacking-terrorist-sites>.
134. ECPAT International, Sexual Exploitation Of Children In The Middle East And North Africa, DQ Institute, 2020 Child Online Safety Report, 2020
135. Eriksson, Johan, and Giampiero Giacomello. International Relations and Security in the Digital Age. London: Routledge, 2007.
136. Eriksson, Johan. Threat Politics: New Perspectives on Security, Risk, and Crisis Management. Aldershot, Hants, England: Ashgate, 2001.
137. Etzioni, A. (2014). The private sector: A reluctant partner in cybersecurity. Georgetown Journal of International Affairs, 69-78. Retrieved from <https://search.proquest.com/docview/1832800641?accountid=28902>.
138. EU Kids Online, EU Kids Online 2020: Survey results from 19 countries, 2020
139. European Transparency Initiative, IDABC European eGovernment News Roundup. November 2, 2005, № 116.
140. European Union (2012), “Neelie Kroes. A European Strategy for Internet Security. High Level Public-Private Security Roundtable. Brussels, 21st March 2012”. Available at <http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/12/204>
141. Fitzgerald, Ben. "The Theory Of Intersectionality Can Make Cybersecurity Collaboration Real." TechCrunch. May 17, 2015. <http://techcrunch.com/2015/02/17/the-theory-of-intersectionality-can-makecybersecurity-collaboration-real/>. Accessed January 10, 2016
142. Floridi, L. (2014). The fourth revolution, how the infosphere is reshaping human reality. Oxford: Oxford University Press.
143. Floridi, L. (2016). Mature information societies—a matter of expectations. Philosophy & Technology, 29(1), 1-4.
144. Friedman, N. (2010). “Virus Season.” Proceedings: United States Naval Institute (November), 136:11, 88-89.
145. General Data Protection Regulation. URL: <https://gdpr.eu/tag/gdpr/>.

146. Human Capital Institute and Saba, "Social Networking in Government: Opportunities and Challenges," January 2010.
147. ICS-CERT. (2013, Jun.) ICS-CERT monitor report between April-June 2013 of department of homeland security. [Online]. Available: http://icscert.uscert.gov/sites/default/files/ICCERT_Monitor_AprilJune2013_3.pdf
148. Klimburg A., Ed., National cyber security framework manual. NATO CCD COE Publications, 2012.
149. Klimburg, A. and Healey, J. (2012) "Strategic Goals & Stakeholders" in Alexander Klimburg (Ed.), National Cyber Security Framework Manual, NATO CCD COE Publication, Talinn.
150. Klimburg, A., ed. 2012. National Cyber Security Framework Manual. Tallin: NATO Cooperative Cyber Defence Centre of Excellence.
151. Kotukh Y.V. State Information Security Policy (Comparative Legal Aspect) / Y. V. Kotukh, V. B. Dziundziuk, O. M. Krutii, V. P. Solovykh, O. A. Kotukov // Cuestiones Políticas. 2021. 39(71). Pp. 166-186.
152. Kotukh Ye.V. Spread of virtual communities as a potential threat to national security / Viacheslav B. Dziundziuk, Oleksandr A. Kotukov, Dmytro V. Hryn, Eugene V. Kotukh // Rivista Di Studi Sulla Sostenibilita (Scopus). 2020. Issue 2. Pp. 7-18.
153. Kotukh, Y. V. Cybercrime and subculture of cybercriminals. Linguistics and Culture Review. 2021. 5(S4). Pp. 858-869.
154. Lawson, Sean (2010), 'General Alexander's Confirmation and the Failure of Cyberwar Transparency', The Firewall, 13 May 2010 [online]; available at <http://blogs.forbes.com/firewall/2010/05/13/general-alexanders-confirmationand-the-failure-of-cyberwar-transparency/>.
155. Lobato, C. L., & Kenkel K. M. (2015). Discourses of cyberspace securitization in Brazil and in the United States. *Revista Brasileira de Politica International*, 58(2), 23-43. Available at [http:// www.scielo.br/pdf/rbpi/v58n2/0034-7329-rbpi-58-02-00023.pdf](http://www.scielo.br/pdf/rbpi/v58n2/0034-7329-rbpi-58-02-00023.pdf).

156. Lord, Kristin M. Sharp, Travis (2018): America's Cyber Future: Security and Prosperity in the Information Age: Volume I, Washington, DC: Center for a New American Security.
157. Luijff, H.A.M. (2008) 'Cyberterrorisme', in Muller, E.R., Rosenthal, U. and De Wijk, R., (Eds.): Terrorisme: Studies Over Terrorisme en Terrorismebestrijding, Kluwer, Deventer, Netherlands, pp.149-168.
158. Luijff, E. and Healey, J. (2012) "Organizational Structures & Considerations" in Alexander Klimburg (Ed.), National Cyber Security Framework Manual, Talinn, NATO CCD COE Publication.
159. Ponemon Institute LLC. (2019). 'Cybersecurity in Operational Technology: 7 Insights You Need to Know, March 2019'. Ponemon Institute LLC. <https://lookbook.tenable.com/ee2b2c72-e552-43f6-843e-3a63a29d895c>.
160. Ponemon Institute. 2016. Cyber Security Mega Trends: Study of IT leaders in the U.S. federal government.
161. Zetter, Kim. "Legal Experts: Stuxnet Attack on Iran Was Illegal 'Act of Force.'" PC, March 25, 2013.Wired. March 25th, 2013: <http://www.wired.com/2013/03/stuxnet-act-of-force/> Accessed October 4, 2014.

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.).



ЧЕРНІГІВСЬКИЙ ІНСТИТУТ ІНФОРМАЦІЇ, БІЗНЕСУ І ПРАВА
ЗВО „МІЖНАРОДНИЙ НАУКОВО-ТЕХНІЧНИЙ УНІВЕРСИТЕТ
ІМЕНІ АКАДЕМІКА ЮРІЯ БУГАЯ”

Вул. Гонча, 37, м. Чернігів, 14000, e-mail: chiibip.mnty@gmail.com, код ЄДРПОУ 25623216

Вихідна № 186/24

«09» 07 2024р.

ДОВІДКА

про використання результатів дослідження

ДИМИТРІЄВОЇ ОКСАНИ ІГОРІВНИ НА ТЕМУ

“Державна політика захисту дітей у кіберпросторі як пріоритет гуманітарної безпеки України” у науково-дослідній роботі Чернігівського інституту інформації, бізнесу і права Міжнародного науково-технічного університету імені академіка Юрія Бугая за темою:

«Соціально-економічні детермінанти формування та реалізації публічної політики України в умовах цифровізації» (ДР № 0122U001115) в межах якої автором запропоновано інструменти державної політики щодо розвитку інформаційної сфери в Україні.

Довідка видана для подання за місцем захисту дисертації.

З повагою,
проректор з навчальної роботи



Олена СЕМЧЕНКО



**Громадська
організація
«Освітній компас»**

14000, м. Чернігів вул. Ремісничка, 28

ЄДРПОУ 45243912
Тел. +380634023737

Вих. №05/24 від 25.12.2024 р.

ДОВІДКА

про впровадження науково-практичних результатів дисертаційної роботи

ДИМИТРІЄВОЇ ОКСАНИ ІГОРІВНИ

**НА ТЕМУ: “ДЕРЖАВНА ПОЛІТИКА ЗАХИСТУ ДІТЕЙ У
КІБЕРПРОСТОРІ ЯК ПРІОРИТЕТ ГУМАНІТАРНОЇ БЕЗПЕКИ УКРАЇНИ ”**

Громадською організацією «Освітній компас» при розробці заходів щодо розвитку інформаційної сфери в Україні були розглянуті та використані пропозиції з матеріалів дослідження **Димитрієвої Оксани Ігорівни**.

Заслужовують на увагу стратегічні напрями вдосконалення механізмів кіберзахисту дітей, які передбачають створення незалежних центрів кібермедіації для вирішення інцидентів у цифровому середовищі, запровадження єдиних стандартів цифрової грамотності для дітей, батьків та педагогів, а також посилення відповідальності цифрових платформ за безпеку дитячого контенту, що дозволить забезпечити ефективне державне управління у сфері цифрової безпеки дітей.

З повагою,

Голова ГО «Освітній компас»



Тетяна ШЕСТАКОВСЬКА

Довідка
про впровадження результатів дисертаційної роботи
Димитрієвої Оксани Ігорівни на тему “Державна політика захисту дітей
у кіберпросторі як пріоритет гуманітарної безпеки України”

Отримані результати дослідження Димитрієвої Оксани Ігорівни мають практичну цінність у частині вдосконалення механізмів кіберзахисту дітей, які передбачають створення незалежних центрів кібермедіації для вирішення інцидентів у цифровому середовищі, запровадження єдиних стандартів цифрової грамотності для дітей, батьків та педагогів, а також посилення відповідальності цифрових платформ за безпеку дитячого контенту, що дозволить забезпечити ефективне державне управління у сфері цифрової безпеки дітей.

Заслужують на увагу новітні підходи до налагодження ефективної взаємодії між державою та суспільством через цифрові платформи, що дозволяють оперативно реагувати на кіберінциденти та поширювати інформацію про загрози; соціальні мережі, які можуть використовуватися як інструмент для навчання дітей основам цифрової безпеки; краудсорсингові ініціативи, що залучають громадянське суспільство до моніторингу цифрового середовища та виявлення потенційних загроз для дітей.

**Заступник директора
 департаменту стратегічних
 комунікацій та промоції
 української культури -
 начальник відділу з питань
 інформаційної безпеки
 Міністерства культури та
 стратегічної комунікації України**

Олександр Макобрій



Григорій Захарченко

Відп. № 20/14.25/16/19 03.02.2025



НАРОДНИЙ ДЕПУТАТ УКРАЇНИ

вул. М. Грушевського, 5, м. Київ, 01008, www.rada.gov.ua

Довідка

про впровадження результатів дисертаційного дослідження

Розробки та результати дисертаційної роботи Димитрієвої Оксани Ігорівни на тему “Державна політика захисту дітей у кіберпросторі як пріоритет гуманітарної безпеки України” були застосовані в своїй діяльності народним депутатом України.

Застосування на практиці запропонованих Димитрієвою О.І. розробок щодо інструментів державної політики запобігання кіберзагрозам з урахуванням європейських практик (зокрема, адаптацію стандартів GDPR для захисту персональних даних дітей), цифрові інструменти для моніторингу загроз у кіберпросторі (автоматизовані системи аналізу контенту та поведінки користувачів на онлайн-платформах), механізми відкритого уряду, що сприяють підвищенню рівня підзвітності державних органів у сфері кіберзахисту дітей. Відмінністю запропонованої методології є її комплексний характер, що охоплює не лише правові механізми, а й технологічні аспекти захисту даних, забезпечення кібербезпеки, удосконалення механізмів державного контролю за інформаційним простором.

**З повагою,
народний депутат України**

**Сергій ГРИВКО
(посв. №110)**



ЄАС ВЕРХОВНОЇ РАДИ УКРАЇНИ
Підписувач: Гривко Сергій Дмитрович
Сертифікат: 3FAA9288358EC00304000000C00C310056D9E600
Дійсний до: 28.07.2027 0:00:00

Апарат Верховної Ради України
110д9/10-2025/196113 від 25.08.2025



1983815



Прокуратура України
ОФІС ГЕНЕРАЛЬНОГО ПРОКУРОРА

вул. Різницька, 13/15, Київ, 01011, факс: (044) 280-26-03

e-mail: office@gp.gov.ua, web: www.gp.gov.ua

Код ЄДРПОУ 000334051

03.09.2025 № 24/1/1-691ВІХ-25

На № _____ від _____

ДОВІДКА

щодо використання результатів дисертаційної роботи
Димитрієвої Оксани Ігорівни на тему «Державна політика захисту дітей
у кіберпросторі як пріоритет гуманітарної безпеки України»

Заслужують на увагу механізми запобігання загрозам у кіберпросторі для дітей, які, на відміну від існуючих, передбачають інтеграцію системи раннього виявлення кіберризиків через аналітичні платформи для моніторингу кіберзагроз, що базуються на технологіях великих даних (Big Data) та алгоритмах машинного навчання; алгоритми прогнозування ризиків, які здійснюють оцінку поведінкових моделей дітей у цифровому середовищі та дозволяють виявити групи підвищеної вразливості; адаптивні комунікаційні стратегії, що включають проактивне інформування дітей, батьків і вчителів про можливі загрози через цифрові платформи та персоналізовані механізми реагування, спрямовані на зниження рівня ризику.

Взято до уваги удосконалений методичний підхід до оцінки ефективності механізмів захисту дітей у кіберпросторі, який, на відміну від існуючих, поєднує якісні та кількісні методи аналізу, що дозволяє об'єктивно визначити ступінь впливу заходів безпеки на гуманітарну безпеку держави. Запропонований підхід включає SWOT-аналіз рівня захищеності дітей у кіберпросторі, метод експертних оцінок для ідентифікації найбільш критичних загроз, а також кореляційно-регресійний аналіз, який дозволяє визначити залежність між рівнем кіберзагроз та ефективністю державної політики у сфері захисту дітей у цифровому середовищі.

Начальник Департаменту
захисту інтересів дітей та
протидії домашньому насильству



Максим ЧЕРВОНІЙ

Офіс Генерального прокурора
03.09.2025 №24/1/1-691ВІХ-25

