УДК 351:004.738.5-053.2(477)
DOI https://doi.org/10.32782/pdu.2021.4.29

О. І. Димитрієва
здобувач наукового ступеня кандидата наук
Національного університету цивільного захисту України

ОРГАНІЗАЦІЙНО-ФУНКЦІОНАЛЬНА МОДЕЛ ДЕРЖАВНОГО УПРАВЛІННЯ КІБЕРБЕЗПЕКОЮ ДІТЕЙ

У статті здійснено ґрунтовне наукове осмислення проблеми формування та впровадження організаційно-функціональної моделі державного управління кібербезпекою дітей в умовах глобальної цифровізації. Актуальність дослідження зумовлена різким зростанням частки дитячої аудиторії в мережі Інтернет, яка наражається на постійні ризики дезінформації, кібербулінгу, онлайн-шахрайства, сексуалізованого контенту та інших видів шкідливого впливу цифрового середовища. У роботі доведено, що для ефективного управління в цій сфері потрібна цілісна модель, що забезпечує координацію діяльності органів виконавчої влади, освітніх інституцій, правоохоронних структур, суб'єктів приватного сектору та громадських організацій. Розкрито концептуальні засади моделі, яка базується на поєднанні чотирьох функціональних блоків: превентивного (розвиток цифрової грамотності дітей, впровадження освітніх програм і курсів кібергігієни), моніторингового (створення центрів кібернагляду та впровадження інтелектуальних систем виявлення загроз), реагуючого (організація гарячих ліній, оперативне блокування небезпечних ресурсів, правова підтримка постраждалих) та аналітично-координаційного (збір та аналіз статистичних даних, прогнозування ризиків, розробка національних стратегій та програм). У статті акцентується на необхідності формування національного координаційного центру з питань кібербезпеки дітей, здатного забезпечити міжвідомчу взаємодію та контроль за виконанням завдань у цій сфері. Особливе місце відведено аналізу міжнародного досвіду, зокрема прикладів реалізації публічно-приватних партнерств, які дозволяють залучати провідні ІТ-компанії до проєктів з кіберзахисту дітей, розробляти та впроваджувати спеціалізовані програмні рішення, створювати інформаційно-аналітичні платформи. У роботі підкреслюється, що впровадження запропонованої моделі сприятиме підвищенню ефективності державної політики з кібербезпеки дітей, створенню безпечного інформаційного середовища, формуванню культури відповідального користування цифровими ресурсами серед молоді, а також адаптації світових стандартів кіберзахисту до національних умов. Представлені наукові положення та практичні рекомендації мають потенціал для використання у процесі розробки нормативно-правових актів, освітніх стандартів, а також у діяльності органів державної влади та громадських інституцій, що опікуються питаннями захисту дітей у цифровому просторі.

Ключові слова: *кібербезпека дітей, державне управління, організаційно-функціональна модель, кіберзагрози, моніторинг цифрового середовища, публічно-приватне партнерство, цифрова трансформація, національна стратегія, кібергігієна, інформаційна безпека.*

Постановка проблеми. Стрімкий розвиток інформаційних технологій та глобальна цифровізація суспільства створили нові можливості для розвитку освіти, комунікації та дозвілля дітей, але водночас породили цілу низку загроз, які раніше не були настільки актуальними й масштабними. Сьогодні діти є активними користувачами мережі Інтернет, соціальних медіа, онлайн-ігор та освітніх платформ, проте їхня вразливість у цифровому середовищі суттєво зростає через брак досвіду, обмежені навички критичного мислення та відсутність достатньої обізнаності щодо ризиків. Поширення кібербулінгу, онлайн-шахрайства, сексу-

альної експлуатації, дезінформації, залучення до небезпечних спільнот, а також доступ до контенту, що шкодить психічному та фізичному здоров'ю, вимагають негайної реакції з боку державних структур. Традиційні підходи до захисту дітей, які переважно ґрунтувалися на контролі з боку батьків або закладів освіти, вже не відповідають викликам сучасного кіберпростору, де загрози є динамічними, прихованими й часто транснаціональними [1; 3]. Складність проблеми полягає у фрагментарності існуючих механізмів захисту та відсутності чіткої системної моделі державного управління у цій сфері. Наявні державні програми та нормативно-правові акти здебільшого спрямовані на загальне забезпечення кібербезпеки, проте не враховують специфіку дітей як особливої групи, що потребує спеціального правового, організаційного та технічного захисту. Крім того, спостерігається недостатня координація між органами влади, освітніми установами, правоохоронними органами та приватним сектором, що призводить до дублювання функцій або, навпаки, прогалин у захисті [2; 4; 5]. Ще однією проблемою є недостатнє використання потенціалу публічно-приватного партнерства, коли держава могла б залучати IT-компанії, провайдерів послуг і громадські організації до спільних програм, спрямованих на моніторинг і блокування небезпечного контенту, а також на розробку навчальних платформ для дітей і батьків [7]. У результаті відсутність узгодженого, комплексного підходу до управління кібербезпекою дітей ставить під загрозу не лише безпеку кожної окремої дитини, але й інформаційний суверенітет держави та стійкість суспільства до цифрових загроз [6; 8]. Отже, проблема полягає у необхідності формування ефективної організаційно-функціональної моделі державного управління кібербезпекою дітей, яка б інтегрувала правові, інституційні, освітні та технологічні інструменти, забезпечувала координацію дій усіх суб'єктів та відповідала сучасним міжнародним стандартам захисту дітей у цифровому середовищі.

Аналіз останніх досліджень і публікацій. Проблематика державного управління у сфері кібербезпеки, зокрема захисту дітей у цифровому середовищі, знаходить відображення у низці сучасних наукових праць, проте здебільшого розглядається фрагментарно. У дослідженні Станіславського Т.В. акцент зроблено на механізмах публічного управління кібербезпекою та необхідності їх адаптації до сучасних умов інформаційної взаємодії [1]. Бухарєв В.В. розглядає адміністративно-правові засади забезпечення кібербезпеки, наголошуючи на потребі розробки спеціалізованих нормативних актів для захисту вразливих груп, зокрема дітей [2]. У монографії Котуха Є.В. представлено системний аналіз кібербезпеки у публічному секторі та окреслено важливість інтеграції освітніх, технічних і правових механізмів [3], а в його статті проведено порівняльний аналіз національних стратегій кібербезпеки, що демонструє досвід інших країн у створенні комплексних моделей захисту [4]. Даник Ю.Г. та Воробієнко П.П. у підручнику з основ кібербезпеки й кібероборони розкривають загальні принципи протидії кіберзагрозам і підкреслюють роль превентивних заходів у роботі з молоддю [5]. Важливим доповненням є дослідження Ланде Д.В. та співавторів щодо інтелектуального аналізу даних, що відкриває нові можливості для моніторингу та прогнозування загроз у цифровому середовищі [6]. Також варто виділити аналітичну доповідь під редакцією Дубова Д., яка розкриває міжнародний досвід державного і приватного секторів у сфері кібербезпеки та наголошує на перевагах публічно-приватного партнерства [7]. Гончар С.Ф. у своїй монографії акцентує увагу на методиках оцінювання ризиків для об'єктів критичної інфраструктури, що є важливим для побудови превентивної системи захисту дітей [8]. Отже, наявні наукові розробки створюють ґрунт для подальшого формування цілісної організаційно-функціональної моделі, проте потребують інтеграції та адаптації до специфіки забезпечення кібербезпеки дітей.

Метою статті є наукове обґрунтування та розроблення організаційно-функціональної моделі державного управління кібербезпекою дітей, яка забезпечує комп-

лексний, системний та узгоджений підхід до захисту дітей у цифровому середовищі.

Виклад основного матеріалу. Побудова організаційно-функціональної моделі державного управління кібербезпекою дітей ґрунтується на міждисциплінарному підході, який поєднує теорію державного управління, правові механізми забезпечення інформаційної безпеки та сучасні технологічні рішення, спрямовані на мінімізацію ризиків у цифровому середовищі. У наукових працях із публічного управління та кібербезпеки наголошується, що ефективне управління у цій сфері можливе лише за умови чіткого розмежування функцій між центральними органами виконавчої влади та регіональними структурами, а також за умови активного залучення громадянського суспільства й приватного сектору [1; 3]. Відповідно до досліджень сучасних механізмів публічного управління кібербезпекою, модель повинна враховувати принципи системності, ієрархічності та функціональної взаємодоповнюваності органів влади [1].

Теоретично модель базується на концепції багаторівневого управління, яка передбачає інтеграцію локальних, національних і міжнародних механізмів регулювання цифрового середовища. У цьому контексті важливим є положення, викладене у працях щодо адміністративно-правових засад кібербезпеки, де підкреслюється значення нормативно-правової бази, що визначає компетенції органів та процедурні механізми реалізації політики безпеки [2]. В основі моделі лежить також принцип субсидіарності, коли конкретні завдання, пов'язані із захистом дітей у кіберпросторі, реалізуються на найближчому до громадян рівні, що забезпечує швидке реагування на загрози [3; 5].

Важливу роль відіграє і принцип адаптивності, який передбачає постійне оновлення функціональних механізмів моделі відповідно до нових видів кіберзагроз та швидкозмінного характеру цифрових технологій. Це відповідає підходам, описаним у роботах з основ кібербезпеки та кібероборони, де зазначається, що система захисту повинна бути динамічною, гнучкою та орієнтованою на майбутнє [5]. З огляду на світовий досвід, модель має включати принцип інтеграції публічно-приватного партнерства, коли держава та бізнес спільно формують політику кібербезпеки, обмінюються інформацією про інциденти, розробляють спеціалізовані програмні рішення та реалізують превентивні заходи [7].

Науково обґрунтоване поєднання зазначених принципів та механізмів дозволяє сформувати таку організаційно-функціональну модель, яка забезпечує цілісний, комплексний та проактивний підхід до захисту дітей у цифровому середовищі. Її теоретичні засади відображають потребу в нових інституційних формах, ефективних комунікаційних каналах між суб'єктами управління та безперервному вдосконаленні процедур моніторингу, реагування й аналітики, що підтверджено сучасними науковими дослідженнями у сфері кібербезпеки та державного управління.

Організаційно-функціональна модель державного управління кібербезпекою дітей передбачає наявність чітко структурованих функціональних блоків, які взаємодіють між собою та забезпечують комплексний підхід до захисту дітей у цифровому середовищі. Першим і фундаментальним є превентивний блок, що спрямований на формування в дітей навичок безпечної поведінки в Інтернеті, підвищення рівня цифрової грамотності та створення умов для зменшення ризиків ще до виникнення кіберінцидентів. У рамках цього блоку реалізуються освітні програми в школах, розробляються курси з кібергігієни для учнів і педагогів, проводяться всеукраїнські та регіональні інформаційні кампанії, створюються онлайн-платформи для самостійного навчання безпечному користуванню мережею. Як зазначає Даник Ю.Г. та Воробієнко П.П., саме рання профілактика є ключовою умовою забезпечення ефективного кіберзахисту [5]. Превентивні заходи охоплюють не лише дітей, але й батьків та вчителів, адже сімейне та шкільне середовище формує основу безпечної цифрової культури [3].

Другим важливим елементом є моніторинговий блок, який забезпечує систематичне спостереження за інформаційним простором, що використовується дітьми. Його функції включають створення та

роботу спеціалізованих центрів моніторингу, застосування технологій штучного інтелекту для аналізу контенту та виявлення потенційно шкідливих ресурсів, а також співпрацю з провайдерами для оперативного отримання даних про підозрілі сайти та акаунти. Як підкреслює Ланде Д.В. у своїх дослідженнях з інтелектуального аналізу даних, без потужної аналітичної складової неможливо своєчасно виявити нові загрози та адаптувати систему захисту [6]. Моніторинговий блок дозволяє не лише відстежувати небезпечні тенденції, а й формувати статистичні звіти, що стають підґрунтям для прийняття управлінських рішень [8].

Реагуючий блок є оперативною складовою моделі, завданням якої є негайне реагування на виявлені кіберінциденти та мінімізація їхніх наслідків. Він передбачає функціонування гарячих ліній і чат-ботів, куди діти, батьки або педагоги можуть звернутися по допомогу, а також координацію дій правоохоронних органів для швидкого блокування ресурсів або акаунтів, що розповсюджують заборонений чи шкідливий контент [2]. Окрему увагу в цьому блоці приділено правовому забезпеченню: чіткі процедури реагування, визначені нормативно-правовими актами, дозволяють уникнути бюрократичних затримок і гарантують захист прав постраждалих [1; 4]. Практика свідчить, що швидкість реагування є визначальним фактором у зменшенні шкоди від кіберзагроз, особливо коли йдеться про дітей [5].

Завершальним, але не менш значущим є аналітично-координаційний блок, який виконує функцію системного аналізу, прогнозування та узгодження дій між усіма учасниками процесу. Цей блок відповідає за збирання та узагальнення статистичних даних про кіберзагрози, проведення аналітичних досліджень для виявлення нових тенденцій, формування рекомендацій для органів державної влади та розробку національних стратегій і програм з кібербезпеки дітей [3; 4]. Завдяки роботі аналітичних підрозділів формується єдина база знань, що дозволяє визначати пріоритетні напрями фінансування, удосконалювати навчальні курси та вчасно оновлювати нормативно-правову базу [8]. Важливою функцією цього блоку є координація взаємодії між державними структурами, освітніми установами, IT-компаніями та громадськими організаціями, що забезпечує цілісність і послідовність усіх заходів у сфері кіберзахисту дітей [7].

Узагальнюючи, функціональні компоненти моделі утворюють взаємопов'язану систему, де кожен блок доповнює інший, створюючи багаторівневий захисний механізм. Такий підхід дозволяє не лише протидіяти вже існуючим загрозам, але й активно формувати безпечне цифрове середовище для дітей, адаптоване до динамічних викликів сучасного інформаційного простору.

Організаційний аспект формування державної системи кібербезпеки дітей визначає структурно-інституційне підґрунтя, на якому вибудовується вся організаційно-функціональна модель, і саме від нього залежить здатність держави ефективно реагувати на виклики цифрового середовища. В умовах сучасних глобалізаційних процесів та прискореного розвитку інформаційних технологій постає потреба у створенні багаторівневої, інтегрованої та гнучкої організаційної структури, здатної забезпечити координацію всіх суб'єктів, відповідальних за захист дітей у кіберпросторі [1; 3]. Центральною ланкою цієї структури доцільно визначити спеціалізований Національний координаційний центр з кібербезпеки дітей, який функціонує на базі існуючих органів державного управління, зокрема Ради національної безпеки і оборони України, Міністерства цифрової трансформації або окремої міжвідомчої платформи. Такий центр виконує роль головного координатора, який розробляє стратегічні плани, узгоджує діяльність профільних міністерств, контролює дотримання нормативно-правових актів та забезпечує комунікацію з міжнародними організаціями [4; 7].

На регіональному рівні організаційний аспект передбачає створення спеціалізованих підрозділів у складі обласних державних адміністрацій або центрів кібербезпеки при органах місцевого самоврядування. Ці підрозділи реалізують політику, розроблену на національному рівні, з урахуванням місцевих умов та

специфіки інформаційного середовища. Вони забезпечують проведення освітніх тренінгів, координацію з правоохоронними органами у випадку інцидентів, а також організовують моніторинг локальних інформаційних ресурсів [5]. Важливим елементом організаційної структури виступають консультативно-дорадчі ради, до складу яких входять представники громадських організацій, батьківських комітетів, ІТ-компаній, експерти з кіберправа та педагогічної спільноти. Такі ради не лише забезпечують зворотний зв'язок із суспільством, а й допомагають формувати рекомендації для державних органів, сприяючи розвитку політики, орієнтованої на реальні потреби дітей і батьків [3; 7].

Особливу увагу в організаційному аспекті слід приділяти вертикальним та горизонтальним комунікаційним зв'язкам між суб'єктами управління. Вертикальні зв'язки передбачають чітку підпорядкованість та ієрархічність у виконанні завдань, що забезпечує єдність рішень і контроль за їх реалізацією. Горизонтальні зв'язки спрямовані на налагодження партнерських стосунків між суб'єктами на одному рівні управління, що дає можливість оперативно обмінюватися інформацією, спільно реалізовувати освітні чи технічні проєкти, координувати дії під час масштабних кіберінцидентів [6; 8].

Не менш значущим є забезпечення чіткої нормативно-правової регламентації організаційної структури. Згідно з адміністративно-правовими засадами, кожен орган або підрозділ повинен мати визначені повноваження, завдання, функції та процедури взаємодії з іншими структурами, що виключає дублювання повноважень і підвищує ефективність використання ресурсів [2]. Доцільно також передбачити механізми внутрішнього контролю, аудиту та оцінювання ефективності діяльності підрозділів. Наприклад, щоквартальні звіти регіональних центрів перед Національним координаційним центром дозволять оперативно виявляти слабкі ланки в системі та своєчасно вживати коригувальних заходів [4].

Ключовим напрямом організаційного аспекту є інтеграція міжнародного досвіду та стандартів у діяльність національних структур. Дослідження, присвячені міжнародному публічно-приватному партнерству, доводять, що ефективність державної системи кібербезпеки дітей значно зростає, коли вона ґрунтується на найкращих практиках країн ЄС та НАТО, зокрема у сфері побудови міжвідомчих центрів реагування та інтегрованих інформаційно-аналітичних платформ [7]. Таким чином, організаційний аспект забезпечує інституційну основу моделі, без якої навіть найбільш досконалі функціональні механізми не зможуть ефективно реалізуватися, а кіберпростір залишатиметься загрозливим для найуразливіших учасників – дітей.

У сучасних умовах розвитку цифрового середовища публічно-приватне партнерство (ППП) виступає одним із ключових механізмів, який дозволяє забезпечити ефективне функціонування організаційно-функціональної моделі державного управління кібербезпекою дітей. Його сутність полягає у спільній відповідальності держави й приватного сектору за створення безпечного інформаційного простору, де дитина може користуватися цифровими сервісами без ризику для свого розвитку та здоров'я. ППП дає змогу поєднати управлінський потенціал держави з технологічною експертизою бізнесу, що особливо актуально у сфері кіберзахисту, яка вимагає швидкого впровадження інновацій та гнучкої реакції на нові загрози [7].

У структурі ППП у сфері кібербезпеки дітей особливе місце займає співпраця з провайдерами інтернет-послуг, розробниками програмного забезпечення, платформами соціальних мереж та виробниками кіберзахисних технологій. Держава, виступаючи регулятором, створює нормативно-правове підґрунтя для впровадження механізмів захисту, наприклад, законодавчо зобов'язує провайдерів швидко блокувати сайти, які містять дитячу порнографію або заклики до суїциду, чи впроваджувати системи автоматичного фільтрування контенту [2; 3]. У свою чергу бізнес надає технічні рішення, впроваджує інноваційні технології штучного інтелекту для моніторингу та аналізу даних, а також проводить власні освітні програми для дітей та батьків.

Такий підхід відповідає міжнародним стандартам, які успішно використовуються у країнах ЄС, де приватні компанії співпрацюють з державними регуляторами в рамках спільних проектів захисту дитячого контенту [7].

Дослідження Котуха Є.В. підкреслюють, що саме завдяки публічно-приватному партнерству можливо швидко імплементувати сучасні стратегії кіберзахисту у публічному секторі, оскільки бізнес володіє гнучкістю, а держава – ресурсами та владними повноваженнями для масштабування рішень [3]. У рамках такої співпраці можуть створюватися спільні аналітичні платформи, які збирають дані про загрози, здійснюють прогнозування та інформують державні органи про нові ризики. Зокрема, міжнародний досвід свідчить про ефективність таких центрів, які фінансуються за рахунок державних і приватних коштів та діють як хаби інновацій у сфері кібербезпеки [7].

ППП у контексті кібербезпеки дітей також передбачає участь освітніх установ і громадських організацій, які, використовуючи підтримку ІТ-компаній, розробляють навчальні курси та інтерактивні платформи для підвищення рівня цифрової грамотності серед дітей. Таким чином, формується цілісна екосистема, де кожен учасник виконує свою роль: держава визначає правила гри й забезпечує контроль, бізнес пропонує технологічні рішення, громадськість здійснює просвітницьку роботу та зворотний зв'язок [1; 5].

Важливим елементом такого партнерства є також спільне фінансування програм і проєктів. Наприклад, держава може надати гранти для створення дитячих кібербезпекових платформ, а приватні компанії забезпечити технічне супроводження, хмарні сервіси чи консультаційні послуги. Крім того, ППП сприяє формуванню нової культури відповідального бізнесу, коли комерційні структури усвідомлюють свою соціальну роль у захисті дітей і готові вкладати ресурси в розробку безпечних цифрових продуктів [3; 7].

Отже, публічно-приватне партнерство у сфері кібербезпеки дітей є не лише допоміжним інструментом, а й одним із базових принципів сучасної організаційно-функціональної моделі державного управління. Його реалізація створює додану вартість для всієї системи кіберзахисту, забезпечує доступ до передових технологій, сприяє обміну досвідом і формує передумови для сталого розвитку безпечного цифрового середовища для підростаючого покоління.

Висновки. Розроблена та обґрунтована організаційно-функціональна модель державного управління кібербезпекою дітей у сучасних умовах цифрової трансформації є важливим кроком до формування цілісної та ефективної системи захисту найуразливішої категорії користувачів інформаційного середовища. Проведене дослідження показало, що побудова такої моделі повинна спиратися на комплекс теоретичних засад, які включають принципи системності, субсидіарності, інтеграції та адаптивності, а також на чітко окреслені функціональні компоненти, що взаємодіють між собою. Превентивний блок, орієнтований на освітні заходи та формування культури кібергігієни, забезпечує довгострокове зниження рівня кіберзагроз. Моніторинговий блок створює умови для своєчасного виявлення небезпек завдяки сучасним аналітичним інструментам і технологіям штучного інтелекту. Реагуючий блок гарантує швидку протидію інцидентам і надання допомоги постраждалим, а аналітично-координаційний блок забезпечує стратегічне планування, прогнозування та узгодження дій усіх суб'єктів у сфері кіберзахисту дітей.

Організаційний аспект моделі чітко демонструє необхідність створення Національного координаційного центру з кібербезпеки дітей, розбудови регіональних підрозділів та впровадження вертикальних і горизонтальних зв'язків між ними, що підвищує керованість системи та швидкість обміну інформацією. Залучення консультативно-дорадчих рад, експертних груп і громадських організацій посилює практичну орієнтацію моделі та враховує реальні потреби дітей і батьків у цифровому середовищі.

Важливим висновком є також визначальна роль публічно-приватного партнерства, яке забезпечує синергію зусиль державних органів та бізнесу. Таке партнерство відкриває доступ до інноваційних рішень, сприяє швидкому впровадженню

технологій моніторингу й блокування небезпечного контенту, а також підтримує реалізацію освітніх і профілактичних проєктів у сфері кібербезпеки дітей.

Отже, запропонована модель не є статичною конструкцією, а виступає динамічною системою, здатною адаптуватися до нових викликів і технологічних змін. Її реалізація дозволяє сформувати багаторівневу систему захисту дітей, яка поєднує інституційні механізми, правові інструменти, технічні рішення та освітні ініціативи. Впровадження такої моделі сприятиме зміцненню національної безпеки в інформаційній сфері, формуванню безпечного цифрового середовища та розвитку соціально відповідальної цифрової культури серед підростаючого покоління, що відповідає сучасним міжнародним стандартам і перспективам розвитку українського суспільства.

Список використаної літератури:

1. 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.
2. 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.
3. Котух Є.В. Кібербезпека у публічному секторі: монографія. Харків: Колегіум, 2021. 272 с.
4. Котух Є.В. Національні стратегії кібербезпеки: порівняльний аналіз // Актуальні проблеми державного управління. 2021. № 1. С. 48–57.
5. Даник Ю.Г., Воробієнко П.П. Основи кібербезпеки та кібероборони: підручник. Одеса: ОНАЗ, 2019. 320 с.
6. Ланде Д.В., Субач І.Ю., Бояринова Ю.Є. Основи теорії і практики інтелектуального аналізу даних у сфері кібербезпеки: навч. посіб. Київ: ІСЗЗІ КПІ ім. Ігоря Сікорського, 2018. 300 с.
7. Державно-приватне партнерство у сфері кібербезпеки: міжнародний досвід та можливості для України: аналіт. доп. / [Д.В. Дубов та ін.]; за заг. ред. Д. Дубова. Київ: НІСД, 2018. 81 с.
8. 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.

Dymytrieva O. I. Organizational-functional model of state management of children's cybersafety

The article provides a thorough scientific understanding of the problem of forming and implementing an organizational-functional model of state management of children's cybersecurity in the context of global digitalization. The relevance of the study is due to the sharp increase in the share of children's audience on the Internet, which is exposed to constant risks of disinformation, cyberbullying, online fraud, sexualized content and other types of harmful effects of the digital environment. The work proves that effective management in this area requires a holistic model that ensures coordination of the activities of executive authorities, educational institutions, law enforcement agencies, private sector entities and public organizations. The conceptual foundations of the model are revealed, which is based on a combination of four functional blocks: preventive (development of children's digital literacy, implementation of educational programs and cyber hygiene courses), monitoring (creation of cyber surveillance centers and implementation of intelligent threat detection systems), reactive (organization of hotlines, operational blocking of dangerous resources, legal support for victims) and analytical and coordination (collection and analysis of statistical data, risk forecasting, development of national strategies and programs). The article emphasizes the need to form a national coordination center for children's cybersecurity, capable of ensuring interagency interaction and control over the implementation of tasks in this area. A special place is devoted to the analysis of international experience, in particular, examples of the implementation of public-private partnerships, which allow involving leading IT companies in projects on cyber protection of children, developing and implementing specialized software solutions, and creating information and analytical platforms. The paper emphasizes that the implementation of the proposed model will contribute to increasing the effectiveness of state policy on children's cybersecurity, creating a safe information

environment, forming a culture of responsible use of digital resources among young people, as well as adapting global standards of cyber protection to national conditions. The presented scientific provisions and practical recommendations have the potential to be used in the process of developing regulatory and legal acts, educational standards, as well as in the activities of state authorities and public institutions dealing with issues of child protection in the digital space.

Key words: *children's cybersecurity, public administration, organizational and functional model, cyber threats, monitoring of the digital environment, public-private partnership, digital transformation, national strategy, cyber hygiene, information security.*