УДК 351:004.738.5-053.2(477)
DOI https://doi.org/10.32782/1813-3401.2023.1.28

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

ЗАСТОСУВАННЯ ТЕХНОЛОГІЧНИХ ІНСТРУМЕНТІВ У ДЕРЖАВНОМУ УПРАВЛІННІ КІБЕРБЕЗПЕКОЮ ДІТЕЙ

У сучасних умовах глобальної цифровізації питання забезпечення кібербезпеки дітей набуває особливого значення, адже саме неповнолітні користувачі найактивніше взаємодіють з інформаційними технологіями, водночас залишаючись найбільш вразливою категорією до кіберзагроз. У статті здійснено комплексний науковий аналіз застосування технологічних інструментів у державному управлінні кібербезпекою дітей, зокрема розглянуто сучасні методи моніторингу й аналітики даних, інтелектуальні системи фільтрації та попередження кіберінцидентів, а також механізми державно-приватного партнерства, які забезпечують підвищення ефективності реалізації державної політики у цій сфері. Автором підкреслено, що впровадження високотехнологічних рішень, таких як платформи штучного інтелекту, автоматизовані системи виявлення шкідливого контенту, національні реєстри кіберінцидентів та освітні онлайн-сервіси для дітей, сприяє формуванню безпечного цифрового середовища, зменшенню рівня кібербулінгу, онлайн-шахрайства та інших загроз, що негативно впливають на розвиток дитини. У роботі обґрунтовано необхідність інтеграції управлінських і технологічних рішень, підготовки фахівців з кібербезпеки для органів державної влади та впровадження інноваційних механізмів взаємодії з приватним сектором. Окрему увагу приділено аналізу нормативно-правового підґрунтя та практичним рекомендаціям щодо розбудови національної системи моніторингу кіберзагроз, орієнтованої на захист прав дітей. Підкреслюється важливість формування культури цифрової безпеки серед самих дітей та їхніх батьків, оскільки жодні технологічні засоби не будуть ефективними без належного рівня обізнаності й активної участі сімей та освітніх закладів у процесах захисту. Автор зазначає, що поєднання превентивних освітніх програм, сучасних аналітичних платформ та стратегічного державного планування створює комплексний підхід, здатний не лише знизити існуючі ризики, а й запобігати виникненню нових кіберзагроз для дітей у майбутньому. Зроблені висновки можуть бути корисними для науковців, фахівців державного управління, освітян та експертів з інформаційної безпеки, які працюють над удосконаленням практик забезпечення кібербезпеки у цифрову епоху.

Ключові слова: *кібербезпека дітей, державне управління, технологічні інструменти, штучний інтелект, моніторинг контенту, державно-приватне партнерство, інформаційна безпека, кіберзагрози, інтелектуальний аналіз даних, цифрове середовище.*

Постановка проблеми. Стрімкий розвиток інформаційно-комунікаційних технологій та активне впровадження цифрових сервісів у повсякденне життя дітей і підлітків зумовлюють як появу нових можливостей для навчання та розвитку, так і виникнення численних кіберзагроз, що негативно впливають на їхню безпеку та психоемоційний стан. Сучасні діти дедалі частіше стикаються з проявами кібербулінгу, онлайн-грумінгу, поширенням шкідливого контенту, фішинговими атаками та іншими формами протиправної діяльності в мережі, які є складними для своєчасного виявлення та попередження. У цій ситуації державні органи влади опиняються перед необхідністю розробки та впровадження ефективних механізмів управління кібербезпекою, що ґрунтуються на використанні сучасних технологічних інструментів і передових методів аналізу даних. Проте існує низка проблем, серед яких недостатня технічна оснащеність освітніх установ, відсутність єдиної державної платформи моніторингу кіберзагроз для дітей, слабка координація між органами влади та приватним сектором, а також низький рівень цифрової грамотності серед учасників освітнього процесу. Усе це знижує результативність державної політики у сфері захисту прав дітей у цифровому середовищі та вимагає наукового обґрунтування і розробки інноваційних підходів до впровадження техно-

логічних інструментів у систему державного управління кібербезпекою.

Аналіз останніх досліджень і публікацій. Проблематика кібербезпеки в контексті державного управління активно розглядається у працях сучасних українських науковців. Зокрема, у підручнику Ю.Г. Даника та П.П. Воробієнка висвітлено фундаментальні принципи кіберзахисту та окреслено загальні підходи до управління кіберзагрозами [1]. Д.В. Ланде, І.Ю. Субач та Ю.Є. Бояринова детально дослідили методи інтелектуального аналізу даних у сфері кібербезпеки, що може бути використано для моніторингу онлайн-активності дітей [2]. У роботі О.О. Вараксіна та співавторів розкрито особливості кібербезпеки мереж наступного покоління, які формують технічну основу захисту інформаційних ресурсів [3]. Є.В. Котух у монографії «Кібербезпека у публічному секторі» підкреслює необхідність розбудови сучасних інституційних механізмів у державному управлінні та впровадження технологічних інструментів контролю і реагування [4]. Аналітичні доповіді НІСД, підготовлені Д.В. Дубовим та колегами, розглядають перспективи державно-приватного партнерства у сфері кіберзахисту як ключового елемента забезпечення безпеки дітей в Інтернеті [6]. Разом ці дослідження створюють теоретичне та методичне підґрунтя для формування комплексного підходу до застосування сучасних технологій у державному управлінні кібербезпекою дітей.

Метою статті є обґрунтування та аналіз застосування сучасних технологічних інструментів у державному управлінні кібербезпекою дітей з метою підвищення ефективності захисту їхніх прав та створення безпечного цифрового середовища.

Виклад основного матеріалу. Теоретичні засади державного управління кібербезпекою дітей ґрунтуються на поєднанні принципів інформаційної безпеки, управлінських функцій держави та специфіки захисту прав неповнолітніх у цифровому середовищі. Сучасна наука розглядає державне управління у цій сфері як системний процес формування, реалізації та контролю за виконанням політики, що спрямована на запобігання кіберзагрозам, нейтралізацію ризиків і створення умов для безпечного використання інформаційно-комунікаційних технологій дітьми [1]. Такий підхід вимагає інтеграції стратегічних і тактичних рішень, розробки комплексних програм, нормативно-правового регулювання, а також залучення технічних і людських ресурсів.

В основі теорії управління кібербезпекою лежать принципи превентивності, безперервності та адаптивності. Превентивність означає, що заходи із захисту повинні бути спрямовані насамперед на запобігання загрозам, а не лише на реагування після інцидентів. Безперервність передбачає постійний моніторинг інформаційного простору, оновлення інструментів захисту й оперативне виявлення ризиків, що швидко змінюються. Адаптивність вимагає здатності державних структур підлаштовувати політику й технологічні рішення під нові виклики, зокрема під появу нових видів онлайн-контенту або схем шахрайства [2; 4].

У межах державного управління важливим є визначення суб'єктів та об'єктів управлінського впливу. Об'єктом у даному випадку виступає цифрове середовище, у якому перебувають діти: соціальні мережі, онлайн-ігри, освітні платформи та мобільні застосунки. Суб'єктами є органи державної влади, що формують політику та впроваджують технологічні інструменти захисту, зокрема Міністерство цифрової трансформації, Державна служба спеціального зв'язку та захисту інформації, профільні підрозділи МВС та Міністерства освіти і науки. Вони взаємодіють із приватним сектором і громадськими організаціями для реалізації комплексних програм кіберзахисту [6].

Теоретичні основи передбачають також формування нормативно-правової бази, яка забезпечує легітимність і чіткість управлінських дій. Це включає закони, підзаконні акти, методичні рекомендації та міжнародні стандарти, що регулюють обробку персональних даних дітей, обов'язки постачальників цифрових послуг і повноваження державних органів у сфері кіберзахисту. Як зазначає Є.В. Котух, у публічному секторі держава має діяти не лише як контролюючий орган, але й як партнер і модератор цифрових процесів, впроваджуючи технологічні інновації та підвищуючи цифрову грамотність населення [4].

Таким чином, теоретичні основи управління кібербезпекою дітей відображаються у системному підході, що поєднує правові, організаційні та технологічні механізми, спрямовані на забезпечення сталого та безпечного розвитку інформаційного простору для молодого покоління.

У сучасних умовах ефективне державне управління кібербезпекою дітей неможливе без

активного використання новітніх технологічних інструментів, які забезпечують постійний моніторинг цифрового середовища, оперативне виявлення загроз і швидке реагування на інциденти. Основою такої діяльності виступають спеціалізовані автоматизовані системи моніторингу контенту, що здатні аналізувати мільйони вебресурсів і комунікацій у соціальних мережах, онлайн-іграх та освітніх платформах з метою виявлення шкідливого чи небажаного матеріалу. Такі системи інтегрують фільтри за ключовими словами, алгоритми виявлення образливих чи насильницьких зображень, а також механізми блокування ресурсів, які порушують встановлені стандарти безпеки. Державні органи, зокрема CERT-UA, активно впроваджують ці рішення, щоб забезпечити захист молодших користувачів від доступу до небезпечних ресурсів [3].

Значну роль відіграють інструменти штучного інтелекту, які дають змогу аналізувати поведінкові моделі користувачів і прогнозувати ймовірність кіберінцидентів. Наприклад, інтелектуальні алгоритми здатні визначати ознаки кібербулінгу в коментарях або чатах, попереджати про потенційні grooming-загрози чи ідентифікувати спроби фішингових атак. Такі технології використовуються у партнерстві з міжнародними IT-компаніями, що надають готові аналітичні модулі й API для інтеграції в державні системи [2].

Не менш важливим інструментом є створення та підтримка єдиних державних реєстрів інцидентів у сфері кібербезпеки дітей. Ці реєстри дозволяють акумулювати дані про загрози, класифікувати їх, формувати статистику та на основі аналізу визначати пріоритети для превентивних заходів. Такі бази даних можуть взаємодіяти з освітніми та правоохоронними структурами, забезпечуючи швидку передачу інформації про нові ризики та підвищуючи оперативність реагування [1; 4].

Окремої уваги заслуговують освітні платформи та цифрові сервіси, які спрямовані на формування культури безпечної поведінки в Інтернеті. Держава впроваджує онлайн-курси, інтерактивні тренінги та симулятори, які навчають дітей основам кібергігієни, розпізнаванню шахрайських схем і правилам безпечної комунікації. Такі ініціативи реалізуються у партнерстві з громадськими організаціями та приватними компаніями, що надають технологічну підтримку й методичні матеріали [6].

Крім того, для координації дій між різними суб'єктами державного управління впроваджуються інформаційно-аналітичні системи, які забезпечують обмін даними в режимі реального часу. Ці системи інтегрують інформацію з різних джерел, використовують аналітичні панелі та дашборди, що дає змогу керівникам оперативно приймати рішення, планувати профілактичні заходи та оцінювати ефективність уже реалізованих програм [7].

У підсумку технологічні інструменти, що використовуються у державному управлінні кібербезпекою дітей, утворюють цілісну екосистему, де поєднуються автоматизовані фільтраційні системи, аналітика великих даних, алгоритми штучного інтелекту, інформаційні платформи й освітні рішення. Така екосистема сприяє не лише зменшенню ризиків для дітей у цифровому середовищі, але й формуванню в суспільстві розуміння того, що безпека онлайн є спільною відповідальністю держави, бізнесу, освітян і самих користувачів.

Сучасні виклики у сфері кібербезпеки дітей вимагають від держави не лише впровадження власних механізмів захисту, а й активного залучення приватного сектору, який володіє технологіями, експертними знаннями та гнучкістю для швидкого реагування на нові загрози. Державне–приватне партнерство (ДПП) у цій сфері виступає ефективним інструментом, що дає змогу об'єднувати ресурси, компетенції та інноваційні рішення для досягнення спільної мети – створення безпечного цифрового середовища для дітей. В аналітичній доповіді НІСД підкреслюється, що саме завдяки ДПП можливо забезпечити масштабне впровадження фільтраційних систем у школах, реалізувати програми кіберосвіти та розбудувати національну інфраструктуру моніторингу загроз [6].

Приватні IT-компанії та телекомунікаційні оператори часто є розробниками сучасних антивірусних комплексів, систем фільтрації контенту та аналітичних платформ, які держава інтегрує у свої управлінські процеси. Прикладом такого підходу є створення спільних проєктів, де компанії надають державі ліцензії на використання програмного забезпечення або ж безкоштовно передають модулі для аналізу даних, а держава забезпечує нормативно-правову підтримку та організацію процесу впровадження. У межах таких проєктів розробляються мобільні застосунки для батьківського контролю, які, за підтримки держави, набувають широкого поши-

рення та стають елементом національної системи захисту дітей в Інтернеті.

Інноваційні рішення у цій сфері ґрунтуються на використанні великих даних (Big Data) для виявлення тенденцій кіберзагроз, застосуванні машинного навчання для автоматичної класифікації небезпечного контенту та впровадженні технологій блокчейну для гарантування цілісності даних у процесі їх обробки. Наприклад, алгоритми машинного навчання можуть прогнозувати появу нових форм кібербулінгу на основі аналізу мільйонів коментарів у соціальних мережах, а системи блокчейну здатні забезпечити прозорий облік випадків порушень без можливості їх подальшої фальсифікації. Деякі країни вже реалізували на практиці пілотні проєкти, коли державні установи використовували блокчейн-рішення для збереження цифрових профілів школярів та їхнього прогресу в освітніх програмах із кібергігієни.

Додатково варто зазначити, що державно-приватне партнерство формує підґрунтя для створення інноваційних освітніх хабів, де діти та їхні батьки отримують доступ до інтерактивних курсів і симуляцій з кібербезпеки. Такі хаби працюють на базі державних шкіл, але наповнення контентом та технічну підтримку забезпечують приватні компанії. Завдяки цьому діти не лише навчаються безпечній поведінці в Інтернеті, а й знайомляться з передовими технологіями, що підвищує рівень їхньої цифрової грамотності та адаптованості до викликів сучасного інформаційного середовища.

У результаті, державне–приватне партнерство у сфері кібербезпеки дітей стає стратегічним напрямом розвитку інформаційної політики країни. Воно дозволяє не лише оперативно впроваджувати технологічні інновації, а й забезпечує сталість їхнього функціонування, оскільки об'єднує зусилля всіх зацікавлених сторін – державних органів, бізнесу, освітніх установ і громадянського суспільства – навколо спільної мети: створення безпечного, інноваційного та дружнього для дітей цифрового простору.

Попри значний прогрес у сфері державного управління кібербезпекою дітей, процес впровадження сучасних технологій супроводжується низкою суттєвих проблем, які гальмують ефективність уже розроблених рішень. Передусім це недостатня технічна оснащеність значної кількості освітніх закладів, особливо у віддалених і сільських регіонах. Лише близько половини шкіл мають стабільний доступ до високошвидкісного Інтернету та сучасних систем контент-фільтрації, що створює нерівні умови для впровадження єдиних стандартів кіберзахисту. Друга важлива проблема – брак кваліфікованих фахівців у державних органах і школах, які здатні не лише встановлювати й обслуговувати технологічні рішення, а й адаптувати їх до специфічних потреб дітей. Часто працівники освіти не володіють достатнім рівнем цифрової грамотності, що ускладнює використання навіть наявних інструментів кіберзахисту.

Ще однією проблемою є відсутність інтегрованої національної платформи для збору, систематизації та аналізу даних про кіберзагрози, які стосуються саме дітей. Наявні реєстри розпорошені між різними відомствами, що ускладнює обмін інформацією та оперативне реагування. Також слід зазначити недостатній рівень взаємодії між державними структурами й приватними компаніями. Хоча потенціал державно-приватного партнерства активно обговорюється, практичних механізмів для швидкої передачі технологій, спільних інвестицій і розвитку інноваційних сервісів поки що обмаль [6].

Разом із тим перспективи впровадження сучасних технологій у сфері кібербезпеки дітей є досить обнадійливими. З кожним роком збільшується кількість національних і регіональних проєктів, спрямованих на впровадження штучного інтелекту та машинного навчання в системи моніторингу шкідливого контенту. Уже сьогодні тестуються інтелектуальні алгоритми, здатні автоматично виявляти спроби кібербулінгу у шкільних чатах або попереджати дітей про небезпечні контакти. Також держава активно працює над створенням спеціалізованих центрів компетенцій, де готуватимуть фахівців з кіберзахисту, які надалі працюватимуть у школах та органах місцевого самоврядування.

Інноваційні перспективи включають і розбудову комплексної інформаційно-аналітичної платформи на державному рівні, яка інтегруватиме дані з різних джерел, надаватиме аналітичні звіти в режимі реального часу та автоматично формуватиме рекомендації для управлінців. Така платформа може стати основою для створення «цифрового щита» навколо дитячої аудиторії, забезпечуючи системне попередження кіберзагроз. Окрему роль у цьому процесі відіграє розвиток освітніх ініціатив: інтерактивні курси, симуляційні ігри та вебінари з кібергігієни дедалі частіше впроваджуються за підтримки Міністерства цифрової трансформації та приватних ІТ-компаній.

Отже, попри наявні труднощі, впровадження технологій у державне управління кібербезпекою дітей має значні перспективи. Системний підхід, інвестиції в інфраструктуру, підготовка кадрів і активне партнерство з приватним сектором здатні створити ефективну, гнучку й інноваційну систему захисту, яка відповідатиме викликам сучасного цифрового світу та гарантуватиме безпечний простір для розвитку молодого покоління.

Висновки. Забезпечення кібербезпеки дітей у сучасному цифровому середовищі є одним із ключових завдань державного управління, що потребує комплексного підходу, поєднання правових, організаційних та технологічних механізмів. Аналіз теоретичних засад і практичного досвіду показав, що використання сучасних технологічних інструментів – від систем автоматизованого моніторингу контенту та інтелектуального аналізу даних до національних реєстрів кіберінцидентів і освітніх платформ – суттєво підвищує ефективність захисту прав неповнолітніх у мережі. Впровадження таких інструментів дає змогу не лише оперативно виявляти й нейтралізувати кіберзагрози, а й формувати культуру безпечної поведінки серед дітей, їхніх батьків і педагогів. Водночас дослідження засвідчило, що для подальшого розвитку цієї сфери необхідно посилювати технічну інфраструктуру освітніх установ, створювати інтегровані інформаційно-аналітичні платформи, підвищувати рівень цифрової грамотності всіх учасників процесу та розширювати механізми державно-приватного партнерства. Лише завдяки системній взаємодії держави, бізнесу, громадянського суспільства та наукової спільноти можливо вибудувати сучасну ефективну модель управління кібербезпекою дітей, яка відповідатиме викликам динамічного інформаційного простору та забезпечуватиме надійний захист молодого покоління.

Список використаної літератури:

1. Даник Ю.Г., Воробієнко П.П. Основи кібербезпеки та кібероборони: підручник. Одеса: ОНАЗ, 2019. 320 с.
2. 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.
3. Кібербезпека мереж наступного покоління: навч. посіб. у галузі знань 1701 “Інформаційна безпека” / О.О. Вараксін [та ін.]; за ред. В.Г. Кононовича. Одеса: ОНАЗ ім. О.С. Попова, 2013. 238 с.
4. Котух Є.В. Кібербезпека у публічному секторі: монографія. Харків: Колегіум, 2021. 272 с.
5. Гончар С.Ф. Оцінювання ризиків кібербезпеки інформаційних систем об’єктів критичної інфраструктури: монографія. Київ: Альфа Реклама, 2019. 175 с.
6. 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.
7. Котух Є.В. Основні виклики врядування у сфері кібербезпеки. Теорія та практика державного управління. 2020. № 4 (71). С. 38–46.
8. Оцінка електронної готовності України Державним агентством з питань електронного урядування URL: http://www.dknii.gov.ua/sites/default/files/dodatok_5.pdf

Dymytrieva O. I. Application of technological tools in state management of children's cybersafety

In today's conditions of global digitalization, the issue of ensuring children's cybersecurity is of particular importance, since it is underage users who interact most actively with information technologies, while remaining the most vulnerable category to cyberthreats. The article provides a comprehensive scientific analysis of the application of technological tools in state management of children's cybersecurity, in particular, modern methods of monitoring and data analytics, intelligent filtering systems and prevention of cyber incidents, as well as mechanisms of public-private partnership that ensure increased efficiency in the implementation of state policy in this area are considered. The author emphasizes that the implementation of high-tech solutions, such as artificial intelligence platforms, automated systems for detecting harmful content, national cyber incident registers and educational online services for children, contributes to the formation of a safe digital environment, reducing the level of cyberbullying, online fraud and other threats that negatively affect the development of the child. The work substantiates the need to integrate management and technological solutions, train cybersecurity specialists for state authorities and implement innovative mechanisms for interaction with the private sector. Special attention is paid to the analysis of the regulatory framework and practical recommendations for the development of a national system for monitoring cyber threats focused on protecting children's rights. The importance of forming a culture of digital security among children themselves and their parents is emphasized, since no technological means

will be effective without the proper level of awareness and active participation of families and educational institutions in the protection processes. The author notes that the combination of preventive educational programs, modern analytical platforms and strategic state planning creates a comprehensive approach that can not only reduce existing risks, but also prevent the emergence of new cyber threats for children in the future. The conclusions drawn may be useful for scientists, public administration specialists, educators and information security experts who are working to improve cybersecurity practices in the digital age.

Key words: *children's cybersecurity, public administration, technological tools, artificial intelligence, content monitoring, public-private partnership, information security, cyber threats, data mining, digital environment.*