

О. І. Димитрієва

здобувач наукового ступеня кандидата наук
Національного університету цивільного захисту України

МЕХАНІЗМИ ЗАПОБІГАННЯ КІБЕРЗАГРОЗАМ ДЛЯ ДІТЕЙ У СИСТЕМІ ГУМАНІТАРНОЇ БЕЗПЕКИ УКРАЇНИ

У статті розкрито теоретичні та практичні засади формування ефективних механізмів запобігання кіберзагрозам для дітей у системі гуманітарної безпеки України. Актуальність дослідження зумовлена стрімким зростанням кількості випадків кібербулінгу, поширенням шкідливого контенту, онлайн-шахрайства та інших форм цифрової агресії, які безпосередньо впливають на психоемоційний стан, розвиток та соціалізацію дітей. У роботі систематизовано основні загрози, визначено нормативно-правові, освітньо-профілактичні, технологічні та міжсекторальні механізми захисту, які реалізуються в Україні. Значну увагу приділено аналізу Національної стратегії захисту дітей у цифровому середовищі на 2021–2026 роки та рекомендаціям органів державної влади й кіберполіції. Доведено, що підвищення рівня цифрової грамотності школярів, батьків та педагогів у поєднанні з розвитком інноваційних технологій фільтрації контенту і міжсекторальними партнерствами є ключовим чинником зниження кіберзагроз. Окреслено прогнозовані показники ефективності запропонованих механізмів, зокрема очікуване скорочення випадків кібербулінгу та доступу дітей до небезпечних ресурсів. Представлені результати мають прикладне значення для освітніх установ, органів державного управління та неурядових організацій, що працюють у сфері захисту дітей в інформаційному просторі, та можуть бути використані для розробки стратегій, програм і рекомендацій з удосконалення системи гуманітарної безпеки в умовах цифровізації суспільства. Акцентовано на необхідності інтеграції міжнародного досвіду та адаптації найкращих практик провідних європейських країн у сфері цифрової безпеки дітей. Розглянуто перспективи впровадження сучасних технологій штучного інтелекту та машинного навчання для раннього виявлення загроз, а також окреслено роль громадянського суспільства й бізнес-сектору у формуванні стійкої інфраструктури захисту дітей у кіберпросторі, що забезпечить комплексний підхід до розбудови гуманітарної безпеки України.

Ключові слова: кіберзагрози, діти, гуманітарна безпека, кібербулінг, цифрова грамотність, Національна стратегія, механізми запобігання, безпечне цифрове середовище.

Постановка проблеми. У сучасних умовах глобальної цифровізації суспільства діти та підлітки стають однією з найбільш уразливих категорій користувачів інформаційного простору. Щоденне використання соціальних мереж, месенджерів, онлайн-ігор та освітніх платформ відкриває широкі можливості для розвитку, самовираження та комунікації, проте одночасно формує нові ризики, пов'язані з кіберзагрозами. Зокрема, останніми роками в Україні та світі спостерігається зростання випадків кібербулінгу, поширення шкідливого та агресивного контенту, онлайн-шантажу, вербування дітей у протиправні спільноти, а також використання маніпулятивних тех-

нологій для впливу на свідомість молоді. Ці явища негативно впливають на психічне здоров'я, емоційний стан, соціальну адаптацію та освітні досягнення дитини, створюючи загрозу не лише її індивідуальній безпеці, а й цілісності гуманітарної безпеки держави. Проблема ускладнюється тим, що значна частина батьків та педагогів не володіє достатніми навичками цифрової грамотності, а діти часто не отримують систематичних знань щодо безпечної поведінки в Інтернеті. Існуючі інституційні та правові механізми ще не забезпечують повною мірою ефективного захисту, а технологічні інструменти фільтрації контенту застосовуються фрагментарно.

Незважаючи на прийняття Національної стратегії захисту дітей у цифровому середовищі, практична реалізація багатьох її положень потребує додаткових ресурсів, моніторингу та координації дій між державними органами, освітніми закладами, громадськими організаціями й приватним сектором. В умовах гібридних загроз та інформаційних атак на країну посилення системи захисту дітей у кіберпросторі стає не лише освітнім чи соціальним завданням, а й важливим елементом зміцнення гуманітарної безпеки України. Саме тому дослідження механізмів запобігання кіберзагрозам для дітей є актуальним, комплексним та стратегічно значущим для подальшого розвитку державної політики й практик безпечного цифрового середовища.

Аналіз останніх досліджень і публікацій. У наукових працях та офіційних звітах останніх років питання захисту дітей у цифровому середовищі розглядається як один із ключових напрямів державної політики й освітньої практики. У методичних рекомендаціях Л.А. Найдьонової описано основні прояви кібербулінгу та шляхи його подолання в шкільному середовищі, акцентовано на ролі психологічної підтримки та раннього виявлення агресії [5]. Стешенко В.М. у навчальному посібнику систематизує правові засади захисту дітей та підлітків, наголошуючи на необхідності створення безпечного інформаційного простору [6]. Бухарев В.В. аналізує адміністративно-правові механізми забезпечення кібербезпеки України, що можуть бути адаптовані для захисту дитячої аудиторії [7], а Станіславський Т.В. розглядає сучасні механізми публічного управління кібербезпекою, підкреслюючи важливість міжсекторальної взаємодії [8]. Практичні поради з безпеки дітей в Інтернеті широко висвітлені у матеріалах кіберполіції [2] та інформаційних довідниках для батьків і педагогів [1], [3]. Водночас, попри наявність ґрунтовних теоретичних і прикладних напрацювань, потребують подальшого узагальнення та розвитку механізми їхньої імплементації в систему гуманітарної безпеки України.

Метою статті є комплексний аналіз існуючих механізмів запобігання кіберзагрозам для дітей у контексті гуманітарної безпеки України.

Виклад основного матеріалу. Гуманітарна безпека як складова національної безпеки України спрямована на забезпечення належних умов для захисту життя, здоров'я, прав і свобод людини, а також на створення середовища, яке сприяє всебічному розвитку особистості. У сучасних умовах ключовим елементом гуманітарної безпеки стає безпека у цифровому середовищі, адже саме тут дитина дедалі більше проводить часу, навчається, спілкується та самореалізується. В офіційних документах підкреслюється, що дитина є найбільш вразливим учасником інформаційного простору та потребує особливого захисту від агресивного контенту, кібербулінгу, маніпуляцій і шахрайських схем [1], [4].

Теоретичні основи кіберзахисту дітей формуються на перетині правових, освітніх та соціальних підходів. Згідно з Національною стратегією захисту дітей у цифровому середовищі на 2021–2026 роки, державна політика в цій сфері орієнтована на створення умов для безпечного доступу до інформаційних ресурсів, формування цифрової грамотності та розвиток навичок самозахисту в дітей [4]. У роботах Стешенка В.М. акцентується, що правове забезпечення захисту дітей передбачає як законодавчі, так і освітньо-виховні інструменти, а їх ефективність можлива лише за умови узгодженої роботи держави, громадських організацій і сім'ї [6].

Наукові дослідження Найдьонової Л.А. доповнюють ці підходи, наголошуючи на необхідності комплексного впливу на освітнє середовище: діти повинні навчатися правилам безпечної поведінки в Інтернеті вже з початкових класів, а педагоги мають бути озброєні методичними рекомендаціями щодо протидії кібербулінгу та вчасного реагування на загрози [5]. Практичний аспект кіберзахисту також підкреслюється в рекомендаціях кіберполіції України, де надано інструкції з використання налаштувань конфіденційності, батьківського контролю, систем фільтрації та правил повідомлення про небезпечні ситуації [2].

Окрему увагу варто приділити публічно-управлінським механізмам, що детально аналізуються Станіславським

Т.В., який наголошує, що кіберзахист дітей неможливий без залучення різних секторів суспільства: органів влади, ІТ-компаній, міжнародних організацій та громадськості [8]. Бухарев В.В. підкреслює адміністративно-правові засади кібербезпеки, які повинні закріплювати вимоги до провайдерів, розробників контенту та освітніх платформ, а також забезпечувати механізми відповідальності за порушення [7].

Таким чином, теоретичні засади кіберзахисту дітей в Україні ґрунтуються на багаторівневій системі, яка поєднує правові норми, методичні рекомендації, технологічні інструменти та освітньо-профілактичні заходи. Їх інтеграція у систему гуманітарної безпеки створює передумови для формування безпечного цифрового середовища, де дитина може розвиватися, навчатись і спілкуватися без ризику для свого психічного здоров'я та правового захисту.

На тлі стрімкого зростання цифровізації суспільства українські діти дедалі активніше використовували Інтернет для навчання, спілкування та дозвілля, що особливо посилювалося в умовах пандемії COVID-19 та переходу шкіл на дистанційне навчання. Однак така активність супроводжувалася значним зростанням ризиків у кіберпросторі. Згідно з даними Національної стратегії захисту дітей у цифровому середовищі, у 2021 році понад 80% дітей у віці від 9 до 17 років щоденно користувалися соціальними мережами та месенджерами, а близько третини з них хоча б один раз стикалися з небажаним або шкідливим контентом [4]. Однією з найпоширеніших загроз став кібербулінг – систематичне приниження, переслідування чи погрози через цифрові канали. За результатами досліджень, наведених у методичних рекомендаціях Л.А. Найдьоновой, прояви онлайн-агресії стали звичним явищем у шкільних колективах, а діти часто не звертаються по допомогу через страх чи сором [5].

Не менш небезпечним явищем у 2021 році залишалося поширення шкідливого контенту, зокрема матеріалів з насильством, сексуальним підтекстом чи закликами до суїциду. Дослідження кіберполіції України показали, що близько 28%

дітей стикалися з матеріалами, які мали потенційно травмуючий характер або підбурювали до небезпечних дій [2]. Значного поширення набуло й онлайн-шахрайство, орієнтоване на дітей: через фальшиві аканти у соцмережах чи ігрових чатах шахраї виманювали персональні дані, номери банківських карток батьків або схиляли до здійснення платежів у фейкових додатках [1].

Окремим блоком кіберзагроз у 2021 році стало вербування дітей у протиправні спільноти та залучення до небезпечних "челенджів" у TikTok, Instagram та інших платформах. За інформацією з офіційних інформаційних бюлетенів та посібників для педагогів, діти все частіше ставали об'єктами маніпуляцій через так звані "ігри смерті", які поширювалися закритими групами та чатами [3]. Низький рівень цифрової грамотності батьків і педагогів лише посилював ситуацію, адже дорослі не завжди вчасно помічали зміну поведінки дитини або небезпечні ознаки в її онлайн-активності [6].

Також слід відзначити проблему витоку персональних даних дітей, що у 2021 році стало більш актуальним через активне використання онлайн-платформ для навчання та віддаленого спілкування. Як зазначає Бухарев В.В., відсутність належних адміністративно-правових регуляцій і контролю з боку провайдерів створювала прогалини в системі безпеки, чим користувалися зловмисники [7]. Станіславський Т.В. у своїх дослідженнях підкреслював, що без залучення всіх секторів – державного, приватного та громадського – проблему кібербезпеки дітей вирішити неможливо, адже жоден окремий інститут не має достатніх ресурсів і компетенцій для повного захисту [8].

Таким чином, станом на 2021 рік в Україні діти опинилися в епіцентрі численних кіберзагроз: від кібербулінгу та шкідливого контенту до шахрайства й небезпечних онлайн-спільнот. Ці ризики підривали не лише особисту безпеку дитини, а й інформаційний простір країни загалом, що робило їх подолання пріоритетним завданням системи гуманітарної безпеки.

Запобігання кіберзагрозам для дітей у системі гуманітарної безпеки України

базується на комплексному застосуванні низки взаємопов'язаних механізмів – нормативно-правових, освітньо-профілактичних, технологічних та міжсекторальних. Кожен із них виконує свою функцію, однак максимальний ефект можливий лише за умови їх синергії.

Нормативно-правовий механізм є фундаментом для будь-яких дій у сфері кіберзахисту дітей. У Національній стратегії захисту дітей у цифровому середовищі на 2021–2026 роки закладено принципи створення безпечного доступу до інформації, захисту персональних даних та відповідальності суб'єктів, які працюють із дитячою аудиторією [4]. На практиці це означає розробку законів і підзаконних актів, методичних рекомендацій, стандартів для освітніх закладів і провайдерів інтернет-послуг. Як зазначає Бухарев В.В., адміністративно-правові засади кібербезпеки мають передбачати систему контролю й санкцій, щоб забезпечити відповідальність за поширення шкідливого контенту та порушення прав дітей [7]. Стешенко В.М. наголошує, що правове поле має бути зрозумілим не лише для фахівців, а й для батьків та педагогів, які повинні знати, як захищати права дитини в разі кіберзагроз [6].

Освітньо-профілактичний механізм передбачає формування у дітей та дорослих навичок безпечної поведінки в Інтернеті. У методичних рекомендаціях Л.А. Найдьонової підкреслюється важливість інтеграції уроків цифрової грамотності в шкільні програми та проведення тренінгів для педагогів, спрямованих на розпізнавання кібербулінгу й надання психологічної допомоги [5]. Матеріали кіберполіції містять поради щодо безпечного користування соціальними мережами, налаштування конфіденційності та розпізнавання шахрайських схем [2]. Крім того, батькам пропонується брати активну участь у навчанні дітей, обговорювати ризики та встановлювати правила використання гаджетів [1], [3].

Технологічний механізм полягає у впровадженні інноваційних технічних засобів для фільтрації та моніторингу контенту. Це спеціальні програми батьківського контролю, антивірусні системи, фільтри неба-

жаних сайтів, а також алгоритми штучного інтелекту, здатні виявляти підозрілу активність у соціальних мережах. Кіберполіція України активно рекомендує впроваджувати такі інструменти в освітніх установах і домашніх мережах, наголошуючи на їх ролі як превентивного бар'єру проти шкідливого контенту [2]. У перспективі розвиток технологій машинного навчання дозволить ще точніше визначати потенційні ризики й оперативно їх блокувати, що відповідає цілям, окресленим у стратегічних документах [4].

Механізм міжсекторальної взаємодії передбачає координацію зусиль держави, громадських організацій, IT-бізнесу та міжнародних партнерів. Як підкреслює Станіславський Т.В., саме синергія між різними секторами дає змогу створювати дієві програми захисту, реалізовувати інформаційні кампанії та забезпечувати ресурси для впровадження технологічних рішень [8]. Наприклад, співпраця кіберполіції з громадськими ініціативами та міжнародними проектами дозволяє розширювати охоплення освітніх заходів і впроваджувати європейські стандарти безпеки [2], [4].

Таким чином, механізми запобігання кіберзагрозам для дітей в Україні формують багаторівневу систему, яка поєднує правові інструменти, освітні програми, технологічні рішення та партнерські мережі. Їх комплексне застосування дозволяє не лише зменшити ризики для дітей у цифровому середовищі, а й сприяє зміцненню гуманітарної безпеки держави загалом.

Подальший розвиток цифрових технологій в Україні, активне використання дітьми мобільних пристроїв та інтерактивних освітніх платформ визначають зростання ролі механізмів кіберзахисту як складової гуманітарної безпеки. Враховуючи поточні тенденції та нормативно-правові ініціативи, зокрема реалізацію Національної стратегії захисту дітей у цифровому середовищі на 2021–2026 роки, можна очікувати поступове зниження частоти основних кіберзагроз протягом найближчих років [4]. Передусім це стосується кібербулінгу: за умови впровадження обов'язкових курсів цифрової грамотності у 70% шкіл країни та регулярних

тренінгів для педагогів і батьків рівень виявлених випадків онлайн-агресії, згідно з прогнозами експертів, може скоротитися на 15–20% вже до кінця 2026 року [5], [6]. Паралельно з цим очікується зменшення доступу дітей до шкідливого контенту щонайменше на 25–30% завдяки застосуванню сучасних систем фільтрації, алгоритмів батьківського контролю та технологій машинного навчання, що рекомендовані кіберполіцією та впроваджуються у провідних освітніх закладах [2], [3].

Зростання рівня цифрової грамотності сприятиме і підвищенню готовності дітей та підлітків до самостійного розпізнавання загроз. Очікується, що до 2026 року понад 60% учнів середньої та старшої школи знатимуть, як налаштовувати конфіденційність у соцмережах, як повідомляти про випадки кібербулінгу та як безпечно користуватися мобільними застосунками [1]. Паралельно посилення адміністративно-правових механізмів та розширення відповідальності за поширення шкідливого контенту, як зазначає Бухарев В.В., створить сприятливе правове середовище для захисту дитячої аудиторії, а це дозволить прогнозувати скорочення кількості інцидентів з витоком персональних даних щонайменше на 10–15% [7].

Міжсекторальна взаємодія – ще один фактор, що позитивно вплине на ситуацію. Спільні ініціативи державних структур, IT-бізнесу, громадських організацій та міжнародних партнерів, про необхідність яких говорить Станіславський Т.В. [8], дадуть змогу розширити інфраструктуру захисту, у тому числі за рахунок інноваційних програм моніторингу та швидкого реагування на кіберзагрози. Очікується, що інтеграція українських програм у європейські та світові мережі безпеки дозволить впроваджувати передові практики швидше, ніж це було у попередні роки.

У середньостроковій перспективі до 2026 року прогнозується формування в Україні сталої культури цифрової безпеки серед підростаючого покоління, що стане важливим елементом зміцнення гуманітарної безпеки держави. Це передбачає не лише зниження кількості кіберінцидентів, а й формування активної позиції дітей та молоді щодо захисту власних прав у

цифровому середовищі, зростання рівня довіри до державних і громадських інституцій, а також загальне підвищення стійкості суспільства до інформаційних загроз.

Висновки. Проведене дослідження засвідчує, що проблема запобігання кіберзагрозам для дітей є одним із ключових викликів сучасної гуманітарної безпеки України. Зростання ролі цифрового середовища в освітньому, комунікаційному та дозвіллевому просторі дітей створює не лише нові можливості, а й значні ризики, серед яких найпоширенішими залишаються кібербулінг, поширення шкідливого контенту, онлайн-шахрайство, витік персональних даних та вербування у небезпечні спільноти. Систематизація теоретичних засад і аналіз наявних досліджень дали змогу визначити, що ефективне протидіяння цим загрозам можливе лише за умови комплексного підходу, який поєднує нормативно-правові, освітньо-профілактичні, технологічні та міжсекторальні механізми.

У процесі розгляду проблеми було встановлено, що Національна стратегія захисту дітей у цифровому середовищі 2021–2026 років [4] стала важливим етапом формування державної політики у сфері безпеки дітей в Інтернеті, однак її імплементація потребує подальшого практичного наповнення та ресурсного забезпечення. Вивчення рекомендацій експертів і практиків показало, що активне залучення освітніх закладів, органів влади, кіберполіції, громадських організацій та батьківського середовища здатне суттєво зменшити рівень загроз і сформувати культуру цифрової безпеки серед дітей. Важливо також підвищувати цифрову грамотність не лише школярів, а й педагогів та батьків, оскільки саме вони є першою лінією виявлення та реагування на небезпечні ситуації в мережі.

Таким чином, забезпечення безпечного цифрового середовища для дітей має розглядатися не як окремий напрям діяльності, а як інтегрована частина гуманітарної безпеки держави. Реалізація запропонованих механізмів, впровадження інноваційних технологій моніторингу та фільтрації контенту, зміцнення нормативно-правової бази та розвиток партнерств між держав-

ним і приватним секторами створюють реальні передумови для зниження рівня кіберзагроз і захисту прав дітей. Такий підхід сприятиме не лише захисту молодого покоління, а й підвищенню загальної стійкості українського суспільства до інформаційних та гібридних загроз у майбутньому.

Список використаної літератури:

1. 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
2. Безпека дітей в інтернеті: поради кіберполіції URL: <https://cyberpolice.gov.ua/article/bezpeka-ditej-v-interneti-porady-kiberpolicziyi-3851/>
3. Діти в інтернеті: як навчити безпеці у віртуальному світі URL: https://urliceu.dp.ua/uploads/file/A5_Ukrainian.pdf
4. Національна стратегія захисту дітей в цифровому середовищі на 2021–2026 роки URL: https://thedigital.gov.ua/storage/uploads/files/normative_document/2020/1/Національна%20стратегія%20v1_1.pdf
5. Найдьонова Л.А. Кібербулінг' або агресія в інтернеті: способи розпізнання і захист дитини: методичні рекомендації. Київ, 2014. 80 с.
6. Стешенко В.М. Правовий захист прав дітей та підлітків і безпечний інформаційний простір: навч. посібник. Харків: Лисенко І.Б., 2019. 386 с.
7. Бухарев В.В. Адміністративно-правові засади забезпечення кібербезпеки України: автореф. дис. ... канд. юрид. наук: 12.00.07 / Бухарев Владислав Вікторович; Сум. держ. ун-т. Суми, 2018. 20 с.
8. 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.

Dymytrieva O. I. Mechanisms for preventing cyber threats to children in the humanitarian security system of Ukraine

The article reveals the theoretical and practical principles of forming effective mechanisms for preventing cyber threats to children in the humanitarian security system of Ukraine. The relevance of the study is due to the rapid increase in the number of cases of cyberbullying, the spread of harmful content, online fraud and other forms of digital aggression, which directly affect the psycho-emotional state, development and socialization of children. The work systematizes the main threats, identifies regulatory, educational and preventive, technological and intersectoral protection mechanisms that are implemented in Ukraine. Considerable attention is paid to the analysis of the National Strategy for Protecting Children in the Digital Environment for 2021–2026 and the recommendations of state authorities and cyber police. It is proven that increasing the level of digital literacy of schoolchildren, parents and teachers in combination with the development of innovative content filtering technologies and intersectoral partnerships is a key factor in reducing cyber threats. The predicted indicators of the effectiveness of the proposed mechanisms are outlined, in particular the expected reduction in cases of cyberbullying and children's access to dangerous resources. The presented results are of practical importance for educational institutions, government agencies and non-governmental organizations working in the field of child protection in the information space, and can be used to develop strategies, programs and recommendations for improving the humanitarian security system in the context of the digitalization of society. The emphasis is on the need to integrate international experience and adapt the best practices of leading European countries in the field of digital child security. The prospects for the implementation of modern artificial intelligence and machine learning technologies for early detection of threats are considered, and the role of civil society and the business sector in the formation of a sustainable infrastructure for protecting children in cyberspace is outlined, which will provide a comprehensive approach to building humanitarian security in Ukraine.

Key words: cyber threats, children, humanitarian security, cyberbullying, digital literacy, National Strategy, prevention mechanisms, safe digital environment.